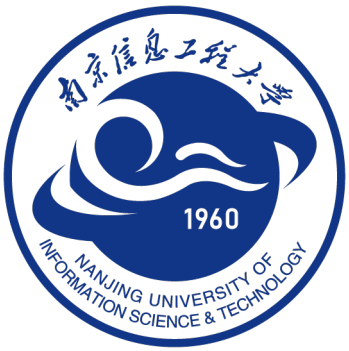
单位代码：10300

南京信息工程大学

本科毕业论文



题　目　DHCICFed：面向医学图像分类中数据异质性和类不平衡问题的加强联邦学习的设计与分析

学生姓名：沈禹豪

学　　号：202083290385

专　　业：计算机科学与技术

学　　院：计算机学院、网络空间安全学院

指导教师：瞿治国

二〇二四　年　五　月

郑　重　声　明

本人以“求实 创新”的科学精神从事科学研究工作，所呈交的论文是我个人在导师指导下进行的研究工作及取得的研究成果。本论文尽我所知，所有测试、数据和相关材料均为真实有效；文中除引文和致谢内容外，未抄袭其他人或其他机构已经发表或撰写过的研究成果。与我一同工作同志对本研究所做的贡献均已在论文中作了声明并表示谢意。

本人毕业论文及涉及相关资料若有不实，愿意承担一切相关的法律责任。

论文作者签名：沈禹豪　　签字日期：2024.5.3

论文使用授权说明

本人授权南京信息工程大学可以保留并向国家有关部门或机构送交论文的复印件和电子文档；允许论文被查阅和借阅；可以将学位论文的全部或部分内容编入有关数据库进行检索；可以采用影印、缩印或扫描等复制手段保存、汇编本学位论文。不可用于任何非法用途。本文电子文档的内容和纸质论文的内容相一致。论文的公布（包括刊登）授权南京信息工程大学教务处办理。

论文作者签名：沈禹豪　　签字日期：2024.5.3

指导教师签名：　　签字日期：

目　录

DHCICFed：面向医学图像分类中数据异质性和类不平衡问题的加强联邦学习的设计与分析

沈禹豪

南京信息工程大学计算机学院，江苏 南京 210044

摘要：联邦学习作为一种隐私保护框架，在医疗图像领域具有重要应用前景。本文中，较为详细地对联邦学习的发展历程、模型框架结构、研究的具体领域进行了介绍。同时，本文叙述了近年来联邦学习在医疗领域应用到若干种具体场景，并且对这些场景所遇到的具体问题进行了分析和阐述。当前，在联邦学习中普遍存在的数据异质性和类不平衡问题较为突出，它们严重影响了模型的性能和泛化能力。因此，针对这两个具体问题，本文提出了一种综合解决数据异质性和类不平衡问题的联邦学习框架。首先，针对数据异质性问题：在局部模型中，用幅度归一化将图像转换为频域信号，分解出代表低层次特征的幅度频谱，在保护核心结构语义不被破坏的同时，平衡各医疗机构所给出图像数据的低级特征；在全局模型中，对其聚合过程引入权重扰动这一随机性参数，不断优化梯度方向，从而避免局部陷阱。其次，针对不平衡问题：采用两级监督对比学习，对客户端内、客户端之间进行特征表示的优化，平衡特征之间的相似性，优化了先验概率分布，提升了分类模型的准确度。最后，在 ISIC 2019 皮肤病图像数据集上进行了模拟实验。结果表明，相较于主流的联邦学习方法如 FedAvg、FedFocal、PRR-Imb、CLIMB 等，本文的算法在所评测的性能指标上拥有更好的表现。

关键词：联邦学习；数据异质性；类不平衡；医疗图像分类

DHCICFed: Design and Analysis of Enhanced Federated Learning for Data Heterogeneity and Class Imbalance Problems in Medical Image Classification

Shen Yuhao
School of Computer Science，NUIST，Nanjing 210044，China

Abstract： Federated learning, as a privacy-preserving framework, has important application prospects in the field of medical images. In this paper, the development history, model framework structure, and specific areas of research of federated learning are introduced in more detail. At the same time, this paper describes the application of federated learning to several specific scenarios in the medical field in recent years and analyzes and elaborates on the specific problems encountered in these scenarios. Currently, the problems of data heterogeneity and class imbalance, which are prevalent in federated learning, are more prominent, and they seriously affect the performance and generalization ability of the model. Therefore, for these two specific problems, this paper proposes a federated learning framework that comprehensively solves the data heterogeneity and class imbalance problems. First, to address the data heterogeneity problem: in the local model, magnitude normalization is used to convert the image into a frequency domain signal and decompose the magnitude spectrum representing the low-level features, which balances the low-level features of the image data given by each healthcare organization while protecting the core structural semantics from being destroyed; in the global model, weight perturbation, a stochastic parameter, is introduced to its aggregation process to continuously optimize the gradient direction, thus avoiding the local traps. Second, for the imbalance problem: two-stage supervised comparison learning is used to optimize the feature representations within and between clients, balancing the similarity between features, optimizing the prior probability distribution, and improving the accuracy of the classification model. Finally, simulation experiments were conducted on the ISIC 2019

dermatology image dataset. The results show that compared to mainstream federated learning methods such as FedAvg, FedFocal, PRR-Imb, CLIMB, FedIIC, etc., the algorithm in this paper performs better on the medical image dataset for the performance metrics reviewed.

Key Words： Federal learning; Data heterogeneity; Class imbalance; Medical image classification

1 绪论

1.1 研究背景和意义

联邦学习（Federated Learning, FL）是一种允许分散的数据源在不共享数据的前提下，协作训练统一深度学习模型的隐私保护框架。由于其具有隐私保护的特性，医疗机构之间就能够通过在不泄漏医疗图像数据的情况下，共同训练一些疾病诊断模型。因此，联邦学习在医疗图像领域引起了广泛关注和应用。

对于联邦学习在该领域的应用，现存在许多突出的问题。其中，最为显著的问题之一是：不同来源的医疗图像之间存在数据异质性（data heterogeneity）[1][2][3]，即不同来源的医疗图像表现为“非独立同分布”的数据特征。这种数据异质性的原因是：数据由不同的扫描仪或协议来记录，从而产生一定的特征异构性，这种异构性会在本地和全局优化学习中，导致模型权重的偏移，这种偏移会损害模型收敛、降低全局模型性能。许多现有的工作都关注到了这个问题，并且尝试在全局或本地模型训练中解决数据偏移的问题，但是无论是试图在本地还是全局模型上解决数据偏移问题都不是彻底的，因为这两者归根到底是同源的：数据本身的异质性所导致，故需要同时解决。因此，从“非独立同分布”这个异质性核心点本身入手，且同时处理好全局和本地的数据偏移问题，才是解决此问题的主要抓手。

另外，除了数据异质性问题中，很多工作往往会忽略医疗场景中广泛存在的类不平衡（class imbalance）问题[4]。由于同一张医疗图像所呈现的身体部位往往可能会发生多种疾病，同时这些疾病的发病率存在差异，从而导致某几种疾病的样本会明显多于另外几种。继而，少数类的先验概率就相应地低于多数类，在医疗机构使用类不平衡数据进行联邦学习时，全局模型会出现明显的性能下降，这种下降通常表现为少数类（如罕见疾病）的识别准确率低于多数类（如常见疾病），模型往往会对多数类有倾向性。

针对以上两种问题，本文主要采用：（1）以标准化变换到频域的图像幅度来模拟统一的成像装置，来减轻本地模型的偏移，以在本地模型参与聚合前添加权重扰动，来缓解全局模型聚合后的偏移；（2）以客户端内部和客户端之间的两级监督对比学习方法，来平衡特征学习，减轻类别偏差带来的性能下降。

1.2 国内外研究现状

1.2.1 联邦学习在医疗领域应用的研究现状

随着相关法规的完善和公民意识的不断强化，越来越多的组织和个人开始重视起医疗数据在诸如大数据应用等方面的隐私问题。联邦学习是从医疗保健数据中数据挖掘和模型建立的一种具有良好潜力且切实可行的方法。医疗数据能够在联邦学习框架下，受到高度监管，无法随意与公众公开共享。因此，在确保隐私的前提下，利用人工智能和机器学习实现个性化医疗保健和计算机辅助诊断将大有裨益。下面概括一下当下在实际应用中的主要优势和局限性。

其在医疗应用中的一些优势包括：

1）保护隐私：医疗数据是高度敏感的，受到严格的隐私法规约束。联邦学习使医疗机构能够在不共享原始患者数据的情况下合作进行模型训练，从而保护隐私并遵守相关法规。

2）大规模数据利用：在不涉及隐私的情况下，医疗机构可以利用来自医院、诊所、可穿戴设备和电子健康记录等各种来源的大量数据，推进机器学习和计算机辅助诊断。

3）个性化医疗：通过利用患者的特定数据，个性化治疗计划将更为切实可行，从而实现更有效、更有针对性的医疗干预。

同时，联邦学习在医疗领域的具体应用场景中，也存在一些挑战和局限性，这些局限性有些是和联邦学习所具有的问题是相同的，还有一些是医疗领域应用所特有的：

1）异质性：医疗数据可能会来自不同的医院、诊所、个人健康监测设备，从而数据格式、质量、完整性和可用性的差异给整合数据并获得准确可靠的结果带来了挑战。

2）监管合规性：医疗保健行业受到严格监管，不同地区和国家都有自己的一套规则和标准。在实施联合学习的同时遵守监管规定，可能既复杂又耗时。

3）偏移和不平衡：联邦学习可能会继承参与机构数据中存在的偏差，从而可能导致模型结果存在偏差或不公平。

4）模型性能控制：确保不同机构的模型质量和一致性可能具有挑战性。模型监测、验证和质量控制机制对于保持高标准的医疗服务至关重要。联邦学习是医疗应用中一种具有良好前景的方法，有效应对这些挑战可对医疗机构运营形成有利影响。

基于上述优势与挑战的论述，现如今的联邦学习在医疗领域的应用也开始出现一些尝试性的、有潜力的解决方案[5]，描述如下。由于人口统计、生活方式等方面的差异，实现个性化医疗保健系统一直是人们的长期目标。FedAP 基于批量归一化层的统计来学习客户端之间的相似性，同时通过不同的本地批量归一化保留客户端的个性，为每个客户端开发个性化模型。 MetaFed 是一种基于循环知识蒸馏（KD）的新型医疗联邦学习框架，它可以在不损害隐私和安全的情况下积累来自不同联邦的公共信息，并通过自适应 KD 为每个联邦实现个性化模型。在 2DFL 网络中，跨多个个人设备和多个用户的异构数据共享有助于开发更精确的个性化 HAR 模型。另外，在联邦学习框架中，并非所有节点都对提高模型性能做出同等贡献。更有研究提出了一种贡献感知的联邦学习方法，该方法提供了一种新颖的联邦学习聚合方法来选择性能最佳的子模型分发给联邦学习参与者以进行下一轮本地训练。与传统的分布式优化相比，联邦学习面临着统计异质性，即整个网络中分布不同的数据。于是，FedProx 添加了一个近端项来概括和重新参数化 FedAvg，以提高方法的稳定性并考虑数据异质性，在平均模型之前使用局部批量归一化来减轻特征偏移，以解决非独立同分布训练数据。

总体而言，这些解决有关医疗数据的几个问题的方法，已经显现出联邦学习在医疗领域的研究前景，具有很大潜力和拓展空间。

1.2.2 联邦学习中数据异质性和类不平衡问题的研究现状

由于本文主要针对解决联邦学习中的具体问题是数据异质性和类不平衡，因此本章节有必要对这两个方面的问题研究进展作出充分论述。

对于数据异质性问题的相关研究：在若干论文中，已从经验和理论上证明，客户端之间的这种数据异构性会在本地（客户端）和全局（服务器）优化中产生权重偏移，使得收敛缓慢且不稳定[6][7][8]。Jiang 等人在 2022 年的论文中提出，特别是在本地更新中，每个客户端模型将针对其自己的本地最优值（即拟合其单独的特征分布）进行优化，而不是解决全局目标，这会在客户端的本地模型之间产生偏移。同时，在聚合这些分散的局部模型的全局更新过程中，服务器模型进一步受到一组不匹配的局部最优的干扰，这就进而导致服务器模型的全局偏移[9]。

此外，现有的工作主要可以分为两组，分别对应于解决局部或全局权重偏移。对于局部，其强调如何更好地规范这些多样化的数据：Sheller 等人[10]进行了一项开创性研究，并提出使用数据预处理来减少数据异质性。最近，Li 等人[11]提出的 FedBN 在本地保留批量归一化层以归一化本地数据分布。对于全局服务器端，调整聚合权重是一种典型的

策略，例如 Yeganeh 等人使用反距离来自适应地重新加权聚合，Reddi 等人[12]提出了 FedAdam 框架，用于引入自适应优化来稳定异构数据中的服务器更新。然而，这些方法部分地通过客户端或服务器更新来解决异构性。局部偏移和全局偏移本质上是耦合的，但如何从整体上共同解决它们仍不清楚。因此，数据异质性问题在当下仍然十分严峻，相关研究一直致力于能够找到更为优秀的普遍性方法。

对于类不平衡问题的相关研究：在医疗机构使用全局类不平衡数据进行联邦学习时，对于全局模型可能会出现的性能下降，通常表现为罕见疾病的识别准确率低于常见疾病[13]。部署这样一个全局或联邦模型可能会产生致命后果，尤其是在误诊罕见疾病时[14][15]。因此，解决联合学习中的类不平衡问题具有重要价值。已有多个联邦学习框架被提出来处理不平衡数据[16][17]。继重新加权[18]之后，Wang 等人[19]提出了一种名为比值损失的交叉熵损失加权形式，它依赖于服务器的平衡辅助数据集来计算权重。Sarkar 等人[20]引入了焦点损失[21]来提高硬样本的权重。CLIMB[22]通过元算法为更有可能拥有少数类别的客户分配更大权重。受解耦[23]的启发，CR- eFF[24]在服务器中使用平衡的合成特征重新训练了一个新的分类器。但是，所有这些方法的目的都是从分类器的角度平衡类别，而不是利用类别不平衡的数据探索更好的表示方法以提高性能，因此这一问题的解决方案当下仍然具有很大提升空间。

1.3 本文研究内容

本文针对提出的两个问题给出了两个较为合理的解决策略，并且将这两种策略有机集成在同一个联邦学习的框架中，以期能够实现一种框架同时较为有效地解决两种问题。

一方面，对于数据异质性问题：首先通过标准化变换图像在频域中的幅度[25]来模拟成像装置的统一化，缓解图像的特征异构性，减轻本地模型更新权重时的偏移，从而协调本地客户端之间的特征。其次，基于协调的特征，在本地模型反向传播更新本地模型的权重时，设置一个客户端权重扰动[25]，引导全局模型聚合每个客户端局部模型时，实现平衡化的模型更新，而不是偏移后的最优更新。这种权重扰动在标准联邦学习过程之外，不增加任何额外通信成本。

另一方面，对于类不平衡问题：通过客户端内和客户端间分别进行两级监督对比学习[26][27]来处理属性偏差，将对比学习的结果转换为相应系数附加到损失函数中，从而实现间接校准提取到的特征矩阵，缓解对类不平衡的所带来的全局模型先验偏差。由于类别偏差是指不同类别的先验概率不同，导致预测结果偏向多数类别，这种对比学习的思想是为了通过比较数据样本之间的相似性和差异性，来学习特征表示，进而使得：最大

化同一类别样本之间的相似性、最小化不同类别样本之间的相似性。使得模型学习到的的特征表示，具有更好的鲁棒性和可区分性的特点。

1.4 本文章节结构

全文共分为五章，章节具体安排如下：

第一章，绪论。本章主要通过对联邦学习在医疗图像分类领域的相关研究背景的引入，阐明了两个遇到的基本问题：数据异质性和类不平衡。通过结合对这两个问题的研究现状的分析，指出了相关研究如今仍然存在的不足之处与可提升空间，继而论述本文的研究方向和思想。

第二章，基础知识。主要解释了联邦学习框架的组成部分，汇总了联邦学习在医疗领域的应用场景、优势与挑战，以及一些解决方案和方法，总结了当前联邦学习在医疗领域的潜力和前景，以及面临的挑战和解决方案。同时，阐述了数据异质性和类不平衡问题的定义和相关研究所涉及的解决方案。

第三章，增强化联邦学习算法过程。为了减少数据异质性带来的局部偏移和全局偏移，分别进行频域幅度归一化和权重扰动。为了缓解类不平衡带来的先验偏差和预测结果偏向性，对类不平衡数据的所提取到的特征，进行两级监督对比学习。继而，在公开的 ISIC 2019 皮肤病图像数据集上，进行定向（模拟数据异质性和类不平衡）数据划分和模拟实验。通过实验模拟，对本文所提出的方法进行性能评估，并与现有相似研究中的联邦学习方法进行性能等方面开展进一步的对比实验，分析本文提出方法模型的优势。

第四章，总结。对本文所提出的联邦学习中两个问题的改进方法进行归纳，对实验结果进行分析合理性分析，且指出仍然有待改进的地方，最后提出对该领域的相关研究的展望。

2 基础知识

2.1 联邦学习概述

2.1.1 联邦学习的发展历程

联邦学习（Federated Learning）一词是根据谷歌 2016 年开展的移动设备文本输入预测研究项目成果发表的论文中提出的。该论文中为一组被称为客户端的设备设计了一个协作环境，由一个中央服务器进行协调。此文还在图像分类和语言处理应用的基准数据集上使用不同的模型结构对该模型进行了实证研究。

随着时代的步伐向前迈进，人们对于数据安全与用户隐私的顾虑日益加深，已成为举世瞩目的焦点。媒体报道和政府行动纷至沓来，针对公共数据泄露问题，社会掀起了一股浓厚的关注浪潮。为了应对这一挑战，各国紧锣密鼓地加强对数据安全与隐私的法律保障。举例而言，欧盟于 2018 年 5 月 25 日正式实施了《通用数据保护条例》（GDPR），旨在护航用户的个人隐私和数据安全。此法规要求企业在用户协议中使用通俗易懂的措辞，并赋予用户“被遗忘权”，即用户可随时要求删除或撤回其个人数据。与此同时，美国和中国也相继制定了类似的隐私与安全法案，如中国 2017 年颁布的《网络安全法》和《民法总则》。这些法令的实施无疑有助于塑造更文明的社会风貌，但也给当下人工智能领域普遍采用的数据交易流程带来了全新的挑战。

联邦学习这种新方法，是应对这些挑战的一种十分具有潜力的解决方案。其主要想法是基于分布在多个设备上的数据集建立机器学习模型，同时防止数据泄露。最近的改进主要集中在以下问题上：提高安全性、更个性化的联邦学习、通信成本、不均衡的数据、设备可靠性等。本文的研究方向主要针对于数据异质性和类不平衡两个问题，在数据预处理、客户端本地训练模型和全局模型聚合过程中，使用统计方法和数学原理搭建算法模型，对其进行技术性的性能优化。

2.1.2 联邦学习的相关研究方向

下面将分别详细解释联邦学习框架的组成部分：存储、隐私、通信、联邦聚合和隐私保护机器学习，并且详细介绍用于训练去中心化数据的不同机器学习模型、它们的用例和应用程序，以及一些对实施有用的技术细节[28]。

（1）存储

联邦学习是一个能够连接不同组织的框架。因此，不同数据中心的特征和观察结果可能会有所不同。根据数据中心的结构、数据的划分方式，讨论了水平划分、垂直划分和迁移学习三种场景。

I. 水平分区：水平联邦学习也称为基于样本的联邦学习，是指数据中心具有相同特征但样本空间不同，需要修改训练模型的场景。例如，银行的网络分别从其客户那里收集特定的信息列表。在此示例中，客户端是不同的。因此，银行之间的样本空间有所不同。横向联邦学习允许实体基于更大的数据池构建通用的全局模型，而不会损害隐私。

II. 垂直分区：垂直联邦学习也称为基于特征的联邦学习，是指局部数据集具有相同的样本空间但特征不同的情况。许多研究人员探索了针对垂直分区数据指定的训练模型。例如，一家当地银行和一家保险公司共享相同的客户，但收集不同类型的信息。如果两个实体要协作构建本地模型，则两个数据集将具有共同的样本空间，但特征却截然不同。常见的聚合方法对于垂直分区的数据并不有效。因此，特征空间之间的差异带来了不同的挑战，并为进一步研究解决故障诊断问题创造了机会。

III. 迁移学习：迁移学习是一种学习结构，其中局部数据集在样本空间和特征空间上都不同。因此，知识来自各种来源以实现全球模型。尽管还存在很多挑战，迁移学习已应用于不同领域的各种问题，并且具有进一步改进的巨大潜力。

（2）隐私

在很多敏感数据中学习时，保护隐私是一个重要的约束，需要防止数据泄露和对抗性攻击。对于这个组成部分，有以下两种解决方向。

I. 添加扰动方法：这是一种基于向数据添加噪声的隐私保护方法。例如，差分隐私就是一种扰动机制，涉及向数据添加噪声以掩盖敏感数据并确保联邦学习框架的安全性。扰动方法可以有效保护数据，但会降低学习准确性。差异隐私基于语义安全的概念，这意味着加密系统可以防止在学习过程中包含任何数量的信息。

II. 密码学方法：这种方法使用密码原语保护数据隐私，包括同态加密、乱码电路、安全处理器和保序加密。同态加密的组成部分是密钥生成、加密、解密和评估算法。同态加密是一种密码系统，涉及使用公钥或私钥对数据进行加密，并在

对等方之间共享密钥以解密密文。通过使用加法和乘法运算符对数据进行数学转换来对数据进行加密。

（3）本地 - 服务器交互

本地数据中心和中央服务器之间的通信需要足够的连接和带宽，以确保本地数据中心和中央服务器之间的安全和私密通信。虽然通信效率高度依赖于现有基础设施，但减少数据中心和中央服务器之间的交互次数可以提高联邦学习模型的效率。此外，联邦学习框架还带来了数据中心和中央服务器之间的公平性问题。通信效率和安全性带来的限制是大规模实施联邦学习的持续挑战。

（4）联邦模型聚合

聚合是从本地数据中心接收模型参数并输出聚合后的模型参数以更新训练模型的功能。将加密后的模型参数上传到中央服务器，利用局部模型的平均更新来更新和改进全局模型。客户端提供的模型参数使用方程 $\delta_{t+1} \leftarrow \sum_{k=1}^{K} \frac{n_k}{n} \delta_{t+1}^{k}$ 聚合在中央服务器上。然后，新模型被发送回客户。这个迭代过程一直持续到模型参数收敛到特定的性能水平或任务完成。例如，FedAvg 是一种最常用的方法之一，它不需要数据中心披露其数据。然而，沟通成本的问题可能在聚合算法的运行中造成性能下降。为了解决这个问题，便由此提出了 FedAvg 的变体：加权 FedAvg 方法、合作聚合（CO-OP）等方法在近些年被提出。

（5）其他研究

在联邦学习中，学习模型是在中央服务器和数据中心之间协作构建和调整的。从分布式数据中学习，存在着不同的问题。因此，人们探索了不同的机器学习模型来比较学习模型的性能和效率。例如，有研究为了提高设备的安全性，使用 K 最近邻、逻辑回归、随机森林和支持向量机作为机器学习模型，构建了联邦学习恶意软件分类模型。

对于构建不同模型学习的策略选择，近年来通常聚焦于下列方法：回归模型、支持向量机、树模型、朴素贝叶斯算法、深度学习、无监督机器学习、集成学习、元启发式方法、区块链技术、强化学习。这些方法常常用于与联邦学习策略相结合，以多来源数据的隐私保护划分方式，进行传统意义上的机器学习构建分类、识别、分割等计算机视觉模型，以适应更多且更复杂的现实世界中的问题背景。

2.1.3 联邦学习的通用结构模型

分布式机器学习算法创建了一个在分布式机器组上，进行数据存储和训练的环境。然而，分布式学习和联邦学习之间的主要区别在于隐私概念，过去十年数据分析能力的进步使我们能够大规模开发和部署隐私保护算法。联邦学习是在本地训练数据并改进全局模型的过程。在联邦学习框架中，数据存储在本地数据中心，学习任务所需的有限信息与中央服务器私下通信。这种架构称为客户端 - 服务器设计。

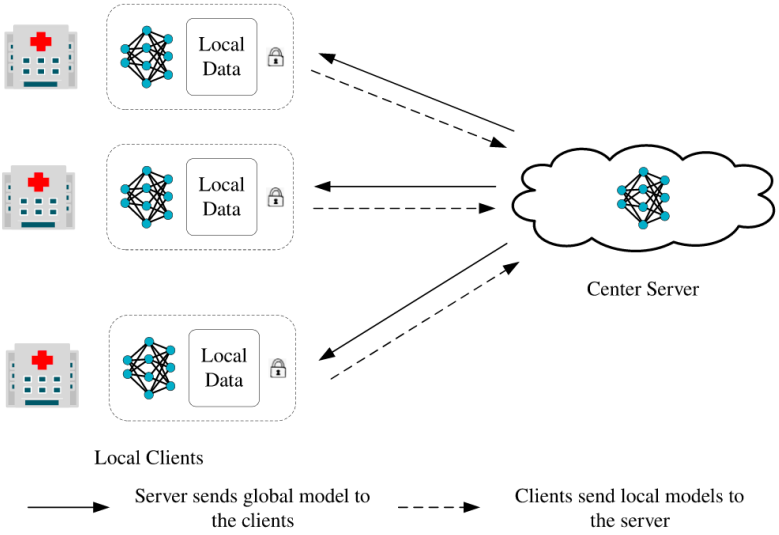


图 1　联邦学习通用框架

联邦学习的流程包括三个阶段：（1）模型初始化：初始 ML 模型通过 FL 服务器传送到每个客户端的设备。（2）本地模型训练：每个客户端设备使用特定于客户端的训练数据来训练自己的模型。（3）本地模型的聚合：FL 服务器收集更新的模型权重并将其组合到全局模型中，然后使用全局模型替换每个客户端的本地模型。

联邦学习的理论算法流程如下：假设 n 是样本点的总数。在这种情况下，K 是客户端总数，n_k 是客户端 k 的样本点总数，η 是学习率。联邦学习的目标是最小化目标函数 f ，也称为损失函数，其中 $f_k(\delta)$ 是损失函数， δ 是第 k 个客户端的评估值，评估值公式为 $f(\delta):=\sum_{k=1}^{K}\frac{n_k}{n}f_k(\delta)$ 。在这个方程中，δ 在每次迭代后更新，直到达到最优解或满足设置为停止标准的迭代次数。联邦学习从数据中心的本地数据存储开始，与中央服务器通信，迭代聚合模型参数并更新全局模型，以实现数据中心所需的学习准确性。

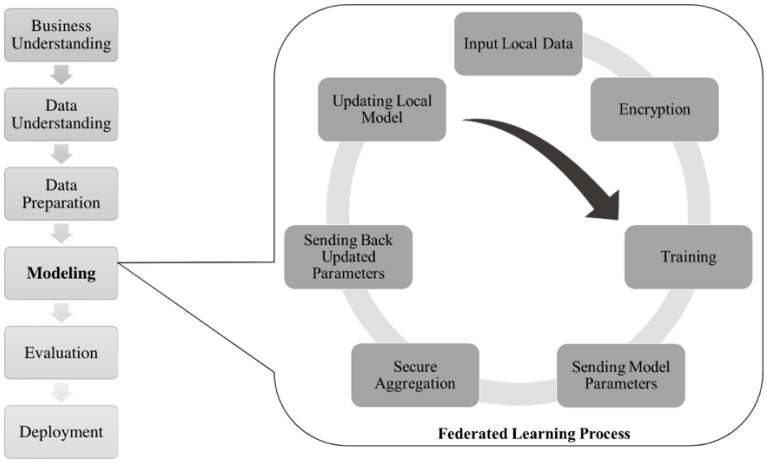


图 2　联邦学习数据挖掘流程

2.1.4 联邦学习在医疗场景的具体应用场景

联邦学习保证了持有数据的实体在保护隐私的同时，为聚合大模型做出贡献，这就有助于促进医疗领域的进步。联邦学习已应用于广泛的医疗保健数据和应用，其包括：（1）使用胸部 X 射线进行疾病进展分析；（2）脑肿瘤分割；（3）药物发现；（4）心肌梗死预测；（5）反射率共焦显微镜；（6）阿尔茨海默氏病分析；（7）全玻片图像分析等具体医疗场景。

具体来说，利用如 MRI、CT 等图像进行训练的联邦学习模型逐渐成为热门趋势，只因其具备隐私保护的特性在当今拥有广泛的社会接受度。诸如图像分类、图像分割、目标检测等 CV 任务也逐渐成为联邦学习在医疗图像领域受到广泛关注的核心任务。

2.1.5 联邦学习在医疗场景中的研究前景[29]

I. 缓解数据异质性：数据异质性是从不同来源收集的数据多样性的结果，例如不同的数据格式、特征分布或噪声水平。这是联邦学习中最紧迫的问题之一，因为它会显着影响训练时间并降低联邦学习的准确性。数据异质性可以进一步分为数据空间异质性和统计异质性。

II. 缓解资源异构性：数据并不是联邦系统中异构性的唯一来源。由于每个客户端都是完全自主的，因此除了前面讨论的数据收集机制之外，它们每个都拥有不同级别的资源。不同规模和不同城市的医院可能具有不同的计算能力或通信带宽。物联网设备可能会受到更大的影响，因为应考虑不同的设备型号、个人通信资源可能明显少于医院可用的资源，并且必须就数据隐私等做出个人决定。

III. 解决模型偏见：广泛的研究表明，人工智能系统可以在各种情况下系统地、不公平地表现出针对某些人群的偏见，导致由年龄、种族/民族、性别、社会经济地位等受保护属性定义的不同亚群体表现出不同的表现。解决医疗保健领域的这一普遍问题并确保公平的机器学习模型的开发对于联邦学习同样重要。然而，由于数据模态和模型的变化，这些挑战在多模态的背景下变得更加复杂。

IV. 增强隐私与数据安全：联邦学习中的主要安全问题涉及机密性、完整性和可用性，而主要隐私问题包括可追溯性、可识别性、分析和本地化。有多种安全和隐私攻击可能会危害联邦学习，包括中毒攻击、推理攻击和水印攻击，防御这些攻击对于联邦学习至关重要。多模态联邦学习中的中毒攻击是指恶意行为者故意操纵数据或模型参数以破坏全局模型的准确性的攻击类型。数据中毒和模型中毒是联邦学习中毒的两种主要方法。当攻击者为单一模态或多种模态注入恶意数据，从而操纵训练数据集的数据分布时，就会发生数据中毒。这种操作会带来良好的整体性能，但会降低模型针对特定受害者的性能。模型中毒攻击涉及操纵模型更新的训练参数或插入后门。有时，模型和数据攻击可以一起应用。

V. 增强透明度和可解释性：解释联邦学习具有挑战性，主要是由于数据隐私问题导致本地数据不可见。联邦学习可能容易受到诸如梯度泄漏攻击之类的攻击，其中可以重建训练数据，以减轻使用差异隐私（在模型参数中注入噪声）的情况，但是，这样做会阻碍基于梯度的解释。此外，多模态学习继承了其可解释性问题。尽管透明度和可解释性在医疗保健领域至关重要，但医疗保健领域对联邦学习可解释性的探索是有限的，此类问题使得在联邦学习中向非专业利益相关者解决人工智能解释更具挑战性。

2.2 数据异质性和类不平衡概述

2.2.1 数据异质性问题的介绍

数据异质性指的是由于数据的来源不同，例如成像设备、医疗机构、采集时的光影环境等。这些因素都使得图像在最基本的特征层面上产生根本性区别，从而在模型学习的过程中，如果不对这些最为直接的图像差异进行缓解甚至消除，模型的训练精度将会大打折扣。

假使用较为精准的术语来描述这个问题，就是所谓的非独立同分布（Non-IID）问题，即图像数据的概率分布显然不属于同一个统计分布，因此很多基于统计原理的方法

并不能直接在该图像数据上面使用，必须先人为消除非独立同分布问题。同时，运用联邦学习对图像数据集进行模型训练时，由于该问题的存在，会导致本地训练的模型受到图像基本特征的影响，从而使得当前本地模型与其余客户端的模型产生较大的权重偏差，研究工作中常常将这种偏差称为模型的偏移（Drift）。

针对这种问题，现今业界常用的手段包括但不限于：在数据预处理阶段向图像中添加相同性质的噪声或者进行滤波以使得回到独立同分布的情况下、在全局模型聚合时引入专家系统聚合出多个全局专家，在对于不同特征的数据集输入使用一定决策规则进行专家模型的选取以对该图像进行分类等等。

2.2.2 类不平衡问题的介绍

现有的联邦学习研究常常仅关注客户端之间的数据异质性，而忽略了医疗场景中广泛存在的类别不平衡问题。在临床实践中，由于人群的发病率不同，不同疾病的样本数量可能会有很大差异。当对具有全局类别不平衡数据的合作医疗机构进行联邦学习时，全局模型可能会出现明显的性能下降，表现为：少数类别（例如罕见病）的识别准确率比大多数类别（例如常见病）更低。同时，部署这种有偏见的全局模型是可能会致命的，特别是对于可能出现的误诊罕见疾病，但医生和联邦学习模型都没有识别出来，这样也会使得病人得不到有效的积极治疗，该医疗机构的声誉也会严重受损。因此，解决联邦学习中的类别不平衡问题在实际应用场景中，占有十分重要的价值地位。

针对上述问题，现今业界常用的手段包括但不限于：在损失函数引入相关惩罚项重新加权、梯度更新优化时引入扰动系数、在加权聚合全局模型动态调整权重等等。

3 增强化联邦学习算法过程

针对在 2.2.2 节中所提出的联邦学习在医疗领域面临的挑战，本章针对“数据异质性”和“类不平衡”两个问题，提出一种结构化的、全面的解决策略。

下面给出本节算法的整体结构图，如下：

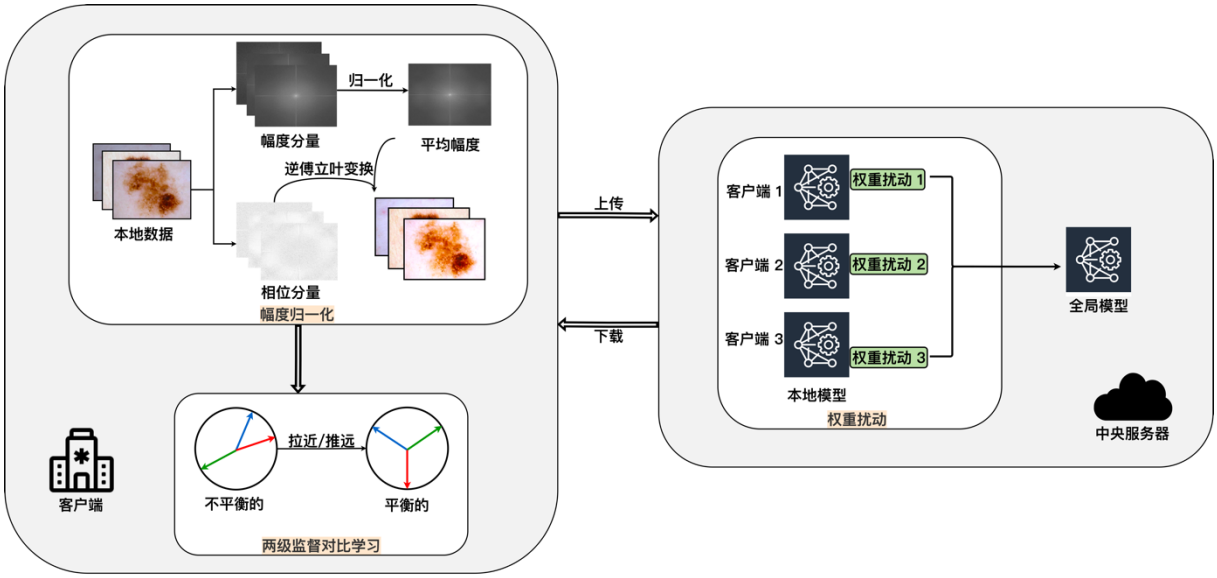


图 3　算法结构总览

3.1 数据异质性的优化策略

3.1.1 解决局部偏移的局部幅度归一化算法

（1）整体思路

一般来讲，结构层次的语义（如医疗图像的特定属性特征、疾病要素等）是医学影像分析过程中的核心要素。而低层次统计数据语义（如颜色、对比度等）通常与区分图像的结构特点和识别设备特点有关。简单来说，结构语义是图像参与分类器识别的核心特征，是区分这张图是哪一种疾病的最关键要素；低层次语义相当于一种协变量，这种协变量既能够用以区分图像的来源，又能够影响结构语义被模型学习到的准确度。

利用快速傅立叶变换（FFT），将图像转换为频域信号，就可以分解出代表图像低层次特征的幅度频谱[30]。使用这个方法的重要意义在于：通过对幅度频谱图的操作，能够在保护核心结构语义不被破坏的同时，协调并平衡各医疗机构所给出图像数据的低级特征，又一定程度上实现了数据降维的效果。

（2）图像频域转换

频域信号中，包含了图像中不同频率的变化信息，不同的频率代表着图像结构和纹理的信息，这种转换可以更细致地分析图像的特征。

而图像的幅度频谱代表了不同频率成分的强度，可以通过分析幅度频谱，来了解图像中哪些频率的成分对图像的整体特征贡献较大，从而更好地理解图像的低层次特征。

具体来说，对于第 i 个客户端输入的图像 x，我们将图像 $x \in \mathbb{R}^{H\times W\times C}$ 的每个通道转换为频率空间信号 $\mathcal{F}_i(x)(u,v)=\sum_{h=0}^{H-1}\sum_{w=0}^{W-1} x(h,w)e^{-j2\pi\left(\frac{h}{H}u+\frac{w}{W}v\right)}$ 。然后，我们可以从频率信号 $\mathcal{F}_i(x)$ 中分离出实部 $\mathcal{R}_i(x)$ 和虚部 $\mathcal{I}_i(x)$ 。振幅和相位分量可表示为：

$$\mathcal{A}_i(x)=[\mathcal{R}_i^2(x)+\mathcal{I}_i^2(x)]^{1/2} \tag{1}$$

$$\mathcal{P}_i(x)=\arctan[\mathcal{I}_i(x)/\mathcal{R}_i(x)] \tag{2}$$

（3）围绕平均振幅的幅度归一化算法

对于幅度归一化，采用移动平均项的方式，即每幅图像的振幅分量是基于分批归一化的思想实现的：对于第 k 批的第 M 幅采样图像，首先分解该批 $(batch)$ 内每幅图像 x_m 的振幅 $\mathcal{A}_{i,x_m}$ 和相位 $\mathcal{P}_{i,x_m}$。我们计算批内平均振幅，并添加衰减系数 v 更新平均振幅（衰减系数是为了使得平均振幅更加稳定，准确地反映图像数据的长期统计特性，提高模型的稳定性和泛化能力）：

$$\overline{\mathcal{A}}_{i,k}=(1-v)\overline{\mathcal{A}}_{i,k-1}+v\frac{1}{M}\sum_{m=1}^{M}\mathcal{A}_{i,x_m} \tag{3}$$

其中，$\overline{\mathcal{A}}_{i,k-1}$ 是根据前一批图像计算得出的平均振幅，第一批图像的这一项设为零。$\overline{\mathcal{A}}_{i,k}$ 表示协调之后的客户端内部的低层特征，并且通过加权计算，一定程度上包含了整个客户端图像振幅的共同特点，使得该批图像幅度归一化后能够实现全局范围内的图像都能够具有相似的低层特征，从而就解决了“非独立同分布”的核心问题。

有了更新后的归一化幅度分量，第 k 批的每幅原始图像则会使用“批内平均振幅” $\overline{\mathcal{A}}_{i,k}$ 与“原始相位分量” $\mathcal{P}_{i,x_m}$ 进行归一化处理：

$$\Psi(x_m)=\mathcal{F}^{-1}(\overline{\mathcal{A}}_{i,k},\mathcal{P}_{i,x_m}) \tag{4}$$

其中， $\mathcal{F}^{-1}$ 为反傅立叶变换。

当本轮中所有客户端训练完成后，仅包含“平均振幅”的振幅归一化信息，将被发送到中央服务器，从而生成“全局振幅”。这个全局振幅折中了不同客户端的各种低级

视觉特征，当它传递到下一轮处理图像的过程中，就能有助于减少下一轮每批图像计算中的局部偏移。在实验中发现，仅在第一轮进行本地与全局通信，生成并固定的第一个全局振幅，就能很好地协调非独立同分布特征，并不用每轮都生成一个新的全局振幅，这样更是节省了通信成本。

（4）核心算法实现

对于上文所描述算法中的数学思想，下面将在伪代码 Algorithm 1 中予以呈现该算法的思路。

算法 1：幅度归一化

输入：图像 $x \in R^{H\times W\times C}$，衰减因子 v
输出：归一化图像 $\Psi(x)$
函数 幅度归一化 (x, v)
    初始化平均幅度 $\bar{A}_{k-1} = 0$
    for 每个批次 k **do**：
        初始化批次幅度 $\bar{A}_k = 0$
        for 每个批次中的图像 x_m **do**：
            计算幅度谱 $\mathcal{A}_{i,x_m}$ 和相位 $\mathcal{P}_{i,x_m}$
            更新批次幅度 $\bar{A}_k \leftarrow (1-v)\cdot \bar{A}_{k-1} + v\cdot \frac{1}{M}\sum_{m=1}^{M} \mathcal{A}_{i,x_m}$
            归一化图像 $\Psi(x_m) \leftarrow \mathcal{F}^{-1}(\bar{A}_k, \mathcal{P}_{i,x_m})$
        end for
        更新平均幅度 $\bar{A}_{k-1} \leftarrow \bar{A}_k$
    end for
    return 归一化图像
end 函数

总体分析：整个算法的作用在于对图像进行频域处理，通过提取幅度频谱并进行归一化操作，实现了对图像低级特征的协调和平衡，同时保护了核心结构语义不被破坏，达到了一定程度的数据降维效果。

3.1.2 解决全局偏移的权重扰动算法

（1）整体思路

由于全局模型的聚合通常是加权平均（如 FedAvg 算法）这一类策略，在加权平均的过程中通过整合各个客户端的局部最优解，来计算出全局模型的最优权重。那么，这

个时候如果局部最优解越接近全局最优解，整体的模型偏移就越小。从而，问题就被简化为“如何使用一种策略使得局部最优解最接近全局解”。

这里所添加的权重扰动，本质上是一种启发式优化算法中引入随机性的思想，并且该权重扰动与模拟退火算法的策略是有异曲同工之妙的。

权重扰动是通过以下几个方面的作用，从而实现局部、全局最优解的最小共同损失统一的。

1）梯度方向调整：在模型训练过程中，通常会根据损失函数的梯度来更新模型参数。权重扰动通过微调梯度方向，使得参数更新的路径更加平缓。这样做可以防止模型参数在局部最优解附近出现剧烈波动，从而使得参数空间更加平滑。

2）参数空间探索：权重扰动还可以帮助模型更全面地探索参数空间。通过引入微小的随机性，可以使得模型在参数空间中更加灵活地移动，从而更有可能找到全局最优解。

3）降低损失波动：在局部最优解附近，损失函数通常会出现波动。权重扰动可以帮助降低损失函数的波动性，使得模型训练过程更加稳定。这样做有助于模型更快地收敛到全局最优解附近。

4）避免局部陷阱：局部最优解往往会导致模型陷入局部最小值附近，难以跳出。通过引入微小的扰动，可以帮助模型跳出局部陷阱，继续向全局最优解的方向前进。

（2）全局优化目标

如果求解局部最优解的求解空间较为尖锐（不平滑），那么求解过程中常常容易陷入较差的局部最优解而无法从当前的“山谷”中及时跳出来。

因此，如果求解空间更为平滑化，那么上述问题就能够得到适当地解决，继而客户端之间能很好地相互协调[31]。而对于在不平滑的求解空间所求得的局部极小值，即使各类模型参数变化不大，聚合后的全局模型预测误差也会大幅增加。受对抗训练的启发，我们提出了每个客户端的局部优化目标如下：

$$\min_{\theta} \sum_{(x,y)\sim\mathcal{D}_i} \max_{\|x'-x\|_p\leq\delta} \ell(x', y; \theta) \tag{5}$$

其中，x' 是在以原始图像 x' 为中心的 L_p 范式有界区域内的对抗图像，对抗图像的生成与 x 的标签相同，但特征偏移不同。然而，对抗图像的生成过程，会带来额外的通信负担，因为这需要在客户端之间传输特征分布信息。为了尽量避免增加额外的通

信负担，这里考虑在 2.1 章所得到协调特征的基础上，设计一种特殊的权重扰动，以有效解决公式 (5) 。

这种新的扰动方法，能够直接应用于模型权重。扰动的生成是利用了协调特征的梯度，因此没有额外的通信成本。具体来说，对于第 k 个批次，首先计算客户模型 $\theta_{i,k-1}$ 在振幅归一化特征 $\Psi(x)$ 上的梯度，该梯度由公式 (4) 计算得出。然后，使用欧氏距离 $\|\cdot\|_2$ 对梯度进行归一化处理，并得到当前梯度下降更新时的扰动项：

$$\delta_k = \alpha \frac{\nabla \ell_i(\Psi(x), y; \theta_{i,k-1})}{\|\ell_i(\Psi(x), y; \theta_{i,k-1})\|_2} \tag{6}$$

其中是一个 α 超参数，通过人为设置用以控制扰动程度。

客户端局部最优解周围的平滑区域越大，就要使用更大的 α 来扩展该区域。得到扰动项 δ_k 后，我们按如下方法最小化参数扰动模型的损失：

$$\theta_{i,k} \leftarrow \theta_{i,k-1} - \eta_l \nabla \ell_i(\Psi(x), y; \theta_{i,k-1} + \delta_k) \tag{7}$$

（3）核心算法实现

对于上文所描述算法中的数学思想，下面将在算法伪代码 Algorithm 2 中予以呈现。

算法 2：权重扰动

输入：本地模型参数 $\theta_{i,k-1}$, 振幅归一化特征 $\Psi(x)$, 梯度步长 η_l , 扰动系数 α

输出：更新后的模型参数$\theta_{i,k}$

函数 生成扰动

    计算 $\theta_{i,k-1}$ 在 $\Psi(x)$ 上的梯度范数 $grad\_norm$

    for 每个参数 p 在 $\theta_{i,k-1}$ 中 **do:**

        计算尺度 $scale = \frac{\alpha}{grad\_norm+1e-12}$

        计算扰动 $\delta = \alpha \times \frac{\nabla \ell_i(\Psi(x),y;\theta_{i,k-1})}{\|\nabla \ell_i(\Psi(x),y;\theta_{i,k-1})\|_2}$

        更新参数 $p \leftarrow p + \delta$

    end for

end 函数

具体实现时，可以在优化器中设置两个特定迭代处理函数，使得全局模型在更新时，实现权重扰动的思想，并利用权重扰动更新模型参数。

总体分析：这个优化器类通过在梯度更新过程中引入微小的随机性，使得参数更新的路径更加平缓和稳定，从而使得求解空间更为平滑化。这样做有助于避免模型陷入局部最优解附近而产生剧烈波动，提高模型训练的鲁棒性和收敛速度。

3.2 类不平衡的优化策略

3.2.1 解决属性偏差的两级监督对比学习算法

（1）整体思路

对比学习的思想是：通过比较数据样本之间的相似性和差异性，来学习特征表示。它的具体方法是，最大化“同一类别”样本之间的相似性，最小化“不同类别”样本之间的相似性，从而使得模型学习到的的特征表示，具有更好的可区分性的特点，从而提升分类模型的鲁棒性。

在这一小节，主要的逻辑思路是：在客户端内部、客户端之间，在提取图像的特征矩阵的函数处理过程中，使用对比学习的思想，在损失函数里面添加两个惩罚项 $\mathcal{L}_{Inter}$ 和 $\mathcal{L}_{Intra}$ ，在反向传播后，让余弦相似度越高的特征越远，反之则越近。最后使得客户端提取到的特征矩阵中，任何一对不同属性的特征都能拥有相同的余弦相似度，从而真正意义上实现类别平衡化。

（2）客户端内部对比学习

一般来说，有限数量的本地数据会影响数据的多样性，从而尤其是对于少数类别的结构特征（即用以分类图像所代表疾病的特定特征，如第 2.1.1 节所述）的可区分性降低。为了更加重视结构特征的学习，在局部训练中引入了监督对比学习，该方法已被证明是有效的[32][33][34][35]。SCL 的基本损失函数可以表述为：

$$\mathcal{L}_{SCL}=\sum_{i\in I}\frac{-1}{|P(i)|}\sum_{j\in P(i)}\log\frac{\exp\left(z_i\cdot z_j/\tau\right)}{\sum_{a\in A(i)}\exp\left(z_i\cdot z_a/\tau\right)} \tag{8}$$

其中，I 表示由不同扩增方法生成的多批次的索引集，$|\cdot|$ 表示集合中元素的数量，$A(i)=I\backslash\{i\}, P(i)=\{s\in A(i)\mid y_s=y_i\}, \tau$ 表示温度，z 表示 l_2 正则化样本 x 的嵌入。

这里使用 2 层感知机 $h(\cdot)$ 来获得 z，再将其归一化[36]，即 $z=\frac{h(g(x))}{\|h(g(x))\|_2}$ 。在多视图批处理中，$\mathcal{L}_{SCL}$ 使得相同的嵌入类会保持更近，同时将不同类的嵌入推得更远，这利于模型根据更多样化的低层特征更好地学习每个类的结构特征。然而，SCL 无法完美解决类别不平衡问题，因为大多数类别会从公式 (8) 中受益更多。公式 (8) 遵循传统训练损失（例如交叉熵损失）。为了克服这个问题，受[37][38]启发，在公式 (8) 中采用

动态温度 $\tau' := P\tau = (p^i p^j)^t \tau$ 。其中 p^i 是本地数据集中第 i 类的先验概率，t 是默认设置为 0.5 的参数。因此，损失函数被重写为：

$$\mathcal{L}_{Intra} = \sum_{i \in I} \frac{-1}{|P(i)|} \sum_{j \in P(i)} \log \frac{\exp(z_i \cdot z_j / \tau')}{\sum_{a \in A(i)} \exp(z_i \cdot z_a / \tau')} \tag{9}$$

以上公式即为客户端内部的对比学习算法策略。通过 P 函数，少数类别的样本对相对于多数类别的样本对的权重增加，从而实现更好的平衡。

（3） 客户端之间对比学习

鉴于联邦学习下的本地数据数量有限，因此客户端内部对比学习的有效性相应地也是有限的。为了从全局角度出发，更好地利用跨客户端数据，对于进一步提升性能至关重要。受到原型学习的启发[39][40][41]，提出了客户端间对比学习。假设一组跨客户端共享的类原型 $V = \{v^1, v^2, \ldots, v^L\}$ ，本地模型可以通过以下方式进行训练：

$$\mathcal{L}_{Inter} = \sum_{i \in I} \frac{-1}{|P(i)|} \log \frac{\exp(z_i \cdot v^{y_i} / \tau)}{\sum_{j=1}^{L} \exp(z_i \cdot v^j / \tau)} \tag{10}$$

其中， y_i 是样本 i 的标签。当最小化 $\mathcal{L}_{Inter}$ 时，每个样本将更接近同一类的原型（prototype），同时远离不同类的原型，从而鼓励局部模型学习具有相同类的样本的共同属性（即类特定属性）。

通过添加 $\mathcal{L}_{Inter}$ 惩罚项，实现客户端之间的对比学习，从而使得特征之间的相似度达到平衡，进而解决类不平衡问题。

（4）定义损失函数

使用交叉熵损失函数作为基础损失系数，增加两个层次的对比学习的损失系数，作为惩罚项，并且引入两个权衡超参数 k_1 和 k_2 。

$$\mathcal{L}_{new} = \mathcal{L} + k_1 \mathcal{L}_{Intra} + k_2 \mathcal{L}_{Inter} \tag{11}$$

在每个客户端的本地训练阶段最小化 $\mathcal{L}_{new}$ 后，使用 FedAvg 方法并结合如 2.2 节所述的权重扰动策略，聚合全局模型。

（5）核心算法实现

对于上文所描述算法中的数学思想，下面将在算法伪代码 Algorithm 3 中予以呈现。

总体分析：这两个函数通过计算特征之间的余弦相似度，并使用损失函数对相似度进行优化，以实现类别平衡化的目标。在客户端内部和客户端之间，都采用了类似的方式来处理特征，从而使得不同客户端提取到的特征具有相似的余弦相似度。

算法 3：两级监督对比学习

输入：特征 z , 目标 y , 温度 τ , 类原型 v , 类别计数 $temp$, 损失系数 k_1, k_2
输出：总损失 L_{new}
函数 1 客户端内部对比学习 $(z, y, \tau$,temp):
    基于特征 z 计算相似度矩阵 $logits$
    使用类别计数 $temp$ 对相似度矩阵进行归一化
    计算对数似然矩阵 log_prob
    计算正样本上的平均对数似然
    基于平均对数似然计算损失 L_{Intra}
return L_{Intra}
end 函数 1
函数 2 客户端之间对比学习 (z, y, τ, v):
    基于特征 z 和类原型 v 计算相似度矩阵 $logits$
    使用温度 τ 对相似度矩阵进行归一化
    计算对数似然矩阵 log_prob
    计算正样本上的平均对数似然
    基于平均对数似然计算损失 L_{Inter}
    return L_{Inter}
end 函数 2
定义新损失函数 $L_{new} = L + k_1 \cdot L_{Intra} + k_2 \cdot L_{Inter}$

3.3 实验

3.3.1 实验环境配置

1）CPU：16 vCPU Intel(R) Xeon(R) Gold 6430

2）GPU：RTX 4090 (24GB) * 1

3）内存：120 GB

4）硬盘：80 GB

5）解释器参数：PyTorch 1.11.0，Python 3.8(ubuntu20.04)，Cuda 11.3

3.3.2 数据集准备和预处理

使用具有类不平衡特征的数据集，面向联邦学习进行特定场景划分（即模拟来源于不同的客户端），描述如下：

皮肤病分类数据集（记为 ISIC 2019[42][43]），其中一共包含 8 个类别的疾病，即类别数量为 8 ，将数据集按 7:1:2 分割，分别用于训练、验证和测试。同时，基于狄利克雷分布（即 $Dir(\alpha = 1.0)$）用于生成 10 个客户端的高度异构、不平衡的数据分区。

对面向数据异质性和类不平衡的目标，对数据集进行分割后，将划分好的数据集中各个客户端所分到的疾病图像类别进行统计，其可视化结果如下：

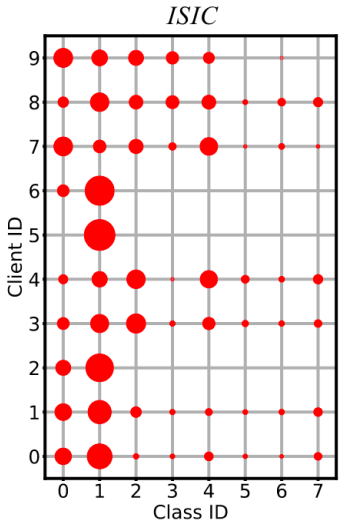


图 4　数据集划分后，各个客户端的疾病类别分布状况

3.3.3 模型参数

（1）神经网络框架：EfficientNet[44] ，示意图如图 5 所示，由 ImageNet[45] 预训练。

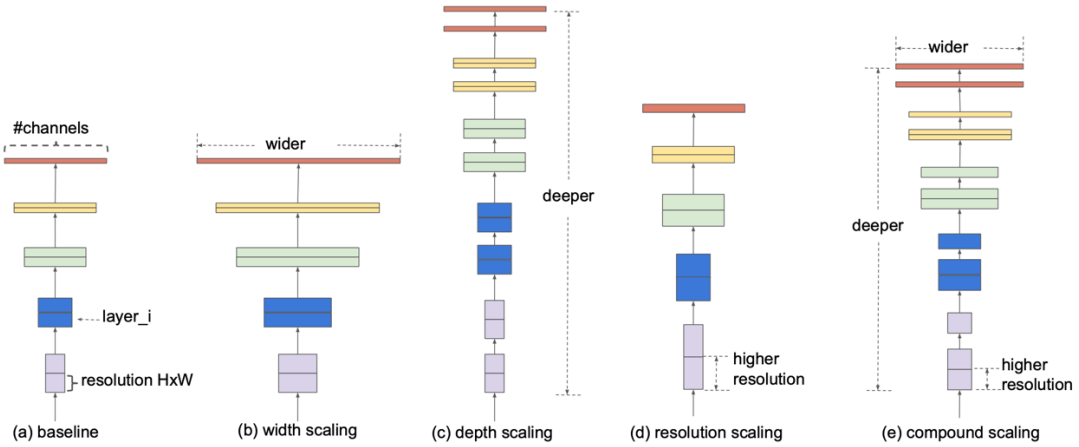


图 5　EfficientNet 模型尺度变换策略

（2）优化器：采用 Adam 优化器模型，其系数 β 为 0.9 和 0.999 ，权重衰减 $weight\_dacay$ 为 $5e-4$，恒定学习率 lr 为 $3e-4$ ，批量大小 $batch\_size$ 为 64（其对应实际意义是每个 epoch 一次性处理 64 张图片）。

（3）数据增广方法：由 RandAug[46] 和 SimAugment[47] 进行处理。

（4）联邦学习一般参数：本地训练轮次设置为 1 ，全局训练轮次设置为 100 ，客户端数量设置为 10 。在每一轮中，所有客户端都会被聚合在全局模型中。

（5）与本文所介绍算法相关的超参数：对于权重扰动算法，公式 (3) 中的超参数设置为衰减因子 v 设置为 0.1 ，并通过网格搜索将扰动项的程度设置为 $5e-2$ 。对于两级监督对比学习算法，公式 (11) 中的超参数 k_1 和 k_2 设置为 2.0 。

3.3.4 性能评价指标

（1）BACC：在 ISIC 2019 竞赛之后，平衡准确性（BACC）被用作类别不平衡测试集的主要指标。

$$\mathrm{BACC}=\frac{1}{2}\left(\frac{TP}{TP+FN}+\frac{TN}{TN+FP}\right) \tag{12}$$

（2）F1 分数：统计学中用来衡量分类模型精确度的一种指标。

$$F_1=2\cdot\frac{precision\cdot recall}{precision+recall} \tag{13}$$

（3）ACC：未平衡化的准确率，即计算 BACC 之前的初始值。

$$\mathrm{ACC}=\frac{TP+TN}{TP+TN+FP+FN} \tag{14}$$

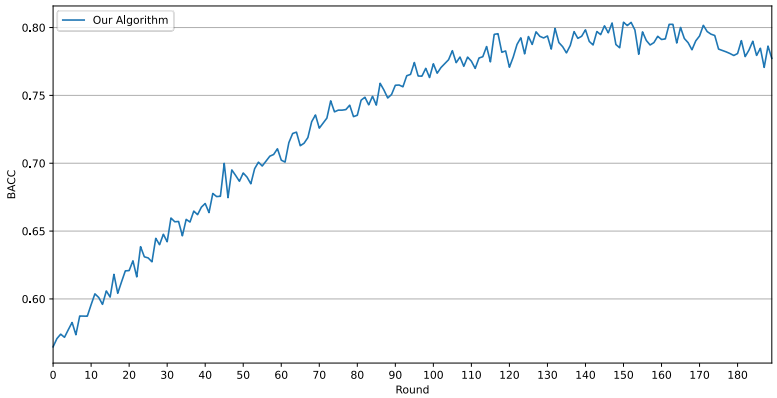
3.3.5 模型测试结果

使用上述算法对两个方面的问题进行处理后，在上述环境参数条件下，在验证集（Value）上求得：最优 BACC 为 55.85% ，最优 F1 分数为 56.73% ，ACC 达到 79.62% 。

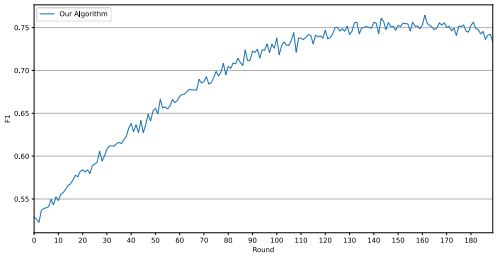
在本地客户端与全局模型交互 190 轮（round）情况下，三种评价指标的迭代变化折线图如下图 6 所示。

此外，选取某一个客户端（Client 1），可视化其在训练过程中的 $loss$ 、$loss\_intra$、$loss\_inter$ 这三个变量的变化情况，如下图 7 所示。

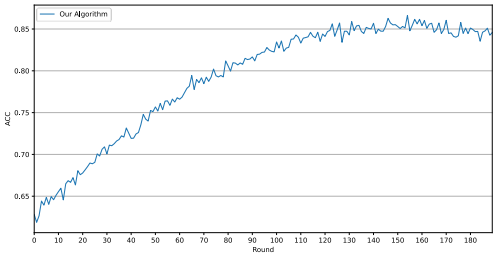
从下图的损失系数变化趋势来看，模型所采用的训练策略具有良好的鲁棒性，收敛情况保持在达到 190 round 之后，模型逐渐趋于稳定。



(a) BACC 迭代变化趋势

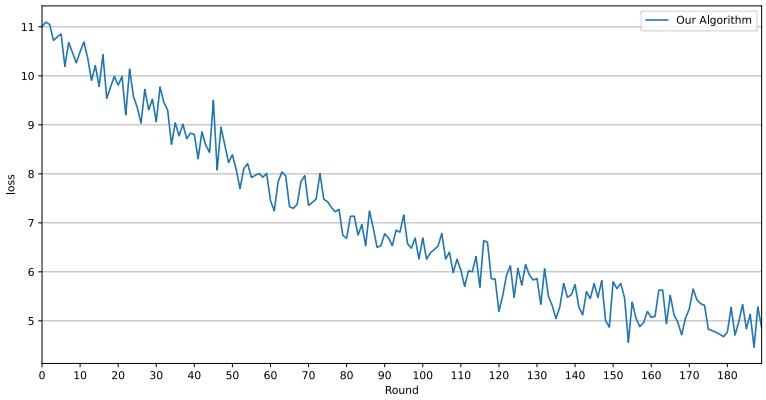


(b) F1 迭代变化趋势

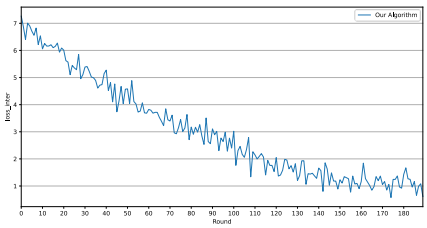


(c) ACC 迭代变化趋势

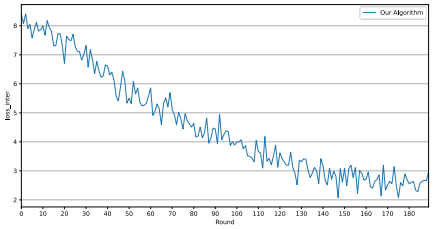
图 6 评价指标迭代变化趋势



(a) loss 迭代变化趋势（Client 1）



(b) loss_inter 迭代变化趋势（Client 1）



(c) loss_intra 迭代变化趋势（Client 1）

图 7 客户端 Client 1 的三个损失项的迭代变化趋势

3.3.6 对比实验

将本文实验结果与约 10 种相关方法进行全面比较，包括 FedAvg[48]、FedProx[49]解决数据异质性、MOON[50] 和 FedProc[51] 利用联邦学习中的对比学习、FedFocal[52] 利用焦点损失[53]进行平衡，FedRS[54] 解决类缺失问题，FedLC[55] 在联邦学习中应用频率相关的 logits 调整，PRR-Imb[56] 使用异质性数据和不平衡数据训练个性化模型，以及 CLIMB[57] 和 CReFF[58] 解决联邦学习中的类不平衡全局数据。所有方法都采用与本文中相同的实验细节参数，以便进行公平比较。

对比的结果如表 1 所示。其中，最后一行黑色加粗是本文实验结果，黑色常规大小数值为劣于本文实验结果的模型，红色数值为较优于本文实验结果的模型。

表 1 使用 ISIC 2019 数据集在不同联邦学习模型上的定量比较结果

FL 方法	BACC	F1	ACC
FedAvg	49.41	54.31	72.50
FedProx	69.00	69.46	80.50
MOON	66.31	71.27	81.38
FedProc	31.16	35.45	66.88
FedRS	24.93	26.01	61.39
FedLC	45.84	41.89	70.33
FedFocal	47.68	38.29	56.99
PRR-Imb	49.97	46.52	68.18
CLIMB	49.70	52.32	71.65
CReFF	71.52	57.83	72.92
FedIIC	78.84	78.05	85.71
Ours	**80.85**	**77.13**	**86.62**

从上表可以看出，本文的模型在 BACC 指标上优于上述所有模型，在 F1 指标上仅稍逊于 FedIIC，在 ACC 指标上优于上述所有模型。

因此，可以根据表 1 的数据总结出：本文的模型能够实现优于很大一部分的当下在该领域较为新颖的主流模型。

4 总结

本文中，在联邦学习的假设背景下（允许分散的数据源在不共享数据的前提下，协作训练统一深度学习模型的隐私保护框架），对于该领域目前频繁面对的两个问题：数据异质性和类不平衡，基于统计原理、优化策略、模型框架改良等思路基础，分别给出了两个方面的合理解决策略：频域幅度归一化和客户端权重扰动、两级监督对比学习。通过在大型的 ISIC 2019 皮肤病图像数据集上进行了数据集划分和模拟实验。所得结果表明，本文对相关问题所提出的方法，相较于很大一部分的主流联邦学习方法具有更好的性能。

对于数据异质性问题：局部模型中使用幅度归一化方法，将图像转换为频域信号分解出代表图像低层次特征的幅度频谱。在保护核心结构语义不被破坏的同时，协调并平衡各医疗机构所给出图像数据的低级特征，一定程度上实现了数据降维。全局模型中使用添加权重扰动方法，在全局模型的聚合中，通过引入权重扰动这一随机性参数，调整梯度方向、探索参数空间、降低损失波动，从而避免局部陷阱。

对于不平衡问题：采用对比学习的思想，最大化同一类别样本之间的相似性，最小化不同类别样本之间的相似性，从而使得模型学习更平衡的特征表示，优化先验概率分布，提升分类模型的准确度和鲁棒性。

本文中所采用的数据集是来源于 ISIC 2019 年竞赛的大型数据集，其数据特征较为丰富完善，作为联邦学习的原始数据集是完全符合该情境中的理论假设的。而对于本文模型的性能对比，在该平台上也具有很多的比赛模型可供对比实验，故有助于提高了本文实验的便利性和可靠性。

至此，基于本文的解决策略和模型改进方法，实现了一定程度上的模型优化任务，但是仍然存在未来可提升或改进的空间，以下是一些展望[59][60][61]：

1）深入探索数据异质性处理方法：尽管本文提出了频域幅度归一化的方法来处理数据异质性，但仍有许多其他方法可以尝试，如特征选择、特征融合等。未来的研究可以进一步探索这些方法的有效性，并比较它们与现有方法的性能。

2）改进类不平衡处理策略：本文采用了对比学习方法来处理类不平衡问题，但这只是众多可行方法之一。未来的工作可以尝试其他方法，如过采样、欠采样、集成学习等，以改善模型在少数类别上的性能。

3）优化联邦学习框架：联邦学习在医疗图像分类中具有广阔的应用前景，但仍存在许多挑战，如通信开销、隐私保护、模型融合等。未来的研究可以致力于优化联邦学习框架，提高其效率和性能。

4）实验验证与临床应用：本文的实验主要基于 ISIC 2019 皮肤病图像数据集进行模拟，未来的研究可以进一步验证所提方法在真实临床环境中的有效性和可行性。此外，可以将这些方法应用于其他医学图像数据集，并与传统的集中式学习方法进行比较，以评估其在实际临床应用中的优势。

5）跨学科合作与应用拓展：未来的研究可以与医学领域的专家、临床医生等进行密切合作，共同探索联邦学习在医疗图像领域的更广泛应用。此外，可以将联邦学习框架扩展到其他医学任务，如医学影像分割、病理诊断等，以实现更全面的医疗数据分析和应用。

参考文献

[1] Li Q, He B, Song D. Model-contrastive federated learning[C]//Proceedings of the IEEE/CVF conference on computer vision and pattern recognition. 2021: 10713-10722.

[2] Li T, Sahu A K, Zaheer M, et al. Federated optimization in heterogeneous networks[J]. Proceedings of Machine learning and systems, 2020, 2: 429-450.

[3] Mu X, Shen Y, Cheng K, et al. Fedproc: Prototypical contrastive federated learning on non-iid data[J]. Future Generation Computer Systems, 2023, 143: 93-104.

[4] Wu N, Yu L, Yang X, et al. Federated learning with imbalanced and agglomerated data distribution for medical image classification[J]. arXiv preprint arXiv:2206.13803, 2022.

[5] Zhao, Y.; Li, M.; Lai, L.; Suda, N.; Civin, D.; and Chandra, V. 2018. Federated learning with non-iid data. arXiv preprint arXiv:1806.00582.

[6] Li X, Huang K, Yang W, et al. On the convergence of fedavg on non-iid data[J]. arXiv preprint arXiv:1907.02189, 2019.

[7] Karimireddy S P, Kale S, Mohri M, et al. Scaffold: Stochastic controlled averaging for federated learning[C]//International conference on machine learning. PMLR, 2020: 5132-5143.

[8] Jafarigol E, Trafalis T, Razzaghi T, et al. Exploring Machine Learning Models for Federated Learning: A Review of Approaches, Performance, and Limitations[J]. arXiv preprint arXiv:2311.10832, 2023.

[9] Jiang M, Wang Z, Dou Q. Harmofl: Harmonizing local and global drifts in federated learning on heterogeneous medical images[C]//Proceedings of the AAAI Conference on Artificial Intelligence. 2022, 36(1): 1087-1095.

[10] Sheller M J, Reina G A, Edwards B, et al. Multi-institutional deep learning modeling without sharing patient data: A feasibility study on brain tumor segmentation[C]//Brainlesion: Glioma, Multiple Sclerosis, Stroke and Traumatic Brain Injuries: 4th International Workshop, BrainLes 2018, Held in Conjunction with MICCAI 2018, Granada, Spain, September 16, 2018, Revised Selected Papers, Part I 4. Springer International Publishing, 2019: 92-104.

[11] Li X, Jiang M, Zhang X, et al. Fedbn: Federated learning on non-iid features via local batch normalization[J]. arXiv preprint arXiv:2102.07623, 2021.

[12] Reddi S, Charles Z, Zaheer M, et al. Adaptive federated optimization[J]. arXiv preprint arXiv:2003.00295, 2020.

[13] Shang X, Lu Y, Huang G, et al. Federated learning on heterogeneous and long-tailed data via classifier re-training with federated features[J]. arXiv preprint arXiv:2204.13399, 2022.

[14] Ju L, Wu Y, Wang L, et al. Flexible sampling for long-tailed skin lesion classification[C]//International Conference on Medical Image Computing and Computer-Assisted Intervention. Cham: Springer Nature Switzerland, 2022: 462-471.

[15] Yang Z, Pan J, Yang Y, et al. Proco: Prototype-aware contrastive learning for long-tailed medical image classification[C]//International Conference on Medical Image Computing and Computer-Assisted Intervention. Cham: Springer Nature Switzerland, 2022: 173-182.

[16] Yang M, Wang X, Zhu H, et al. Federated learning with class imbalance reduction[C]//2021 29th European Signal Processing Conference (EUSIPCO). IEEE, 2021: 2174-2178.

[17] Duan M, Liu D, Chen X, et al. Self-balancing federated learning with global imbalanced data in mobile systems[J]. IEEE Transactions on Parallel and Distributed Systems, 2020, 32(1): 59-71.

[18] Cui Y, Jia M, Lin T Y, et al. Class-balanced loss based on effective number of samples[C]//Proceedings of the IEEE/CVF conference on computer vision and pattern recognition. 2019: 9268-9277.

[19] Wang, L., Xu, S., Wang, X., Zhu, Q.: Addressing class imbalance in federated learning. In: AAAI. pp. 10165–10173 (2021)

[20] Sarkar D, Narang A, Rai S. Fed-focal loss for imbalanced data classification in federated learning[J]. arXiv preprint arXiv:2011.06283, 2020.

[21] Lin T Y, Goyal P, Girshick R, et al. Focal loss for dense object detection[C]//Proceedings of the IEEE international conference on computer vision. 2017: 2980-2988.

[22] Shen Z, Cervino J, Hassani H, et al. An agnostic approach to federated learning with class imbalance[C]//International Conference on Learning Representations. 2021.

[23] Kang B, Xie S, Rohrbach M, et al. Decoupling representation and classifier for long-tailed recognition[J]. arXiv preprint arXiv:1910.09217, 2019.

[24] Shang X, Lu Y, Huang G, et al. Federated learning on heterogeneous and long-tailed data via classifier re-training with federated features[J]. arXiv preprint arXiv:2204.13399, 2022.

[25] Jiang M, Wang Z, Dou Q. Harmofl: Harmonizing local and global drifts in federated learning on heterogeneous medical images[C]//Proceedings of the AAAI Conference on Artificial Intelligence. 2022, 36(1): 1087-1095.

[26] Wu N, Yu L, Yang X, et al. Federated learning with imbalanced and agglomerated data distribution for medical image classification[J]. arXiv preprint arXiv:2206.13803, 2022.

[27] Khosla P, Teterwak P, Wang C, et al. Supervised contrastive learning[J]. Advances in neural information processing systems, 2020, 33: 18661-18673.

[28] Shang X, Lu Y, Huang G, et al. Federated learning on heterogeneous and long-tailed data via classifier re-training with federated features[J]. arXiv preprint arXiv:2204.13399, 2022.

[29] Thrasher J, Devkota A, Siwakotai P, et al. Multimodal Federated Learning in Healthcare: a review[J]. arXiv preprint arXiv:2310.09650, 2023.

[30] Nussbaumer H J, Nussbaumer H J. The fast Fourier transform[M]. Springer Berlin Heidelberg, 1982.

[31] Keskar N S, Mudigere D, Nocedal J, et al. On large-batch training for deep learning: Generalization gap and sharp minima[J].

[32] Marrakchi Y, Makansi O, Brox T. Fighting class imbalance with contrastive learning[C]//International Conference on Medical Image Computing and Computer-Assisted Intervention. Cham: Springer International Publishing, 2021: 466-476.

[33] Kang B, Li Y, Xie S, et al. Exploring balanced feature spaces for representation learning[C]//International Conference on Learning Representations. 2020.

[34] Li T, Cao P, Yuan Y, et al. Targeted supervised contrastive learning for long-tailed recognition[C]//Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition. 2022: 6918-6928.

[35] Zhu J, Wang Z, Chen J, et al. Balanced contrastive learning for long-tailed visual recognition[C]//Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition. 2022: 6908-6917.

[36] Chen T, Kornblith S, Norouzi M, et al. A simple framework for contrastive learning of visual representations[C]//International conference on machine learning. PMLR, 2020: 1597-1607.

[37] Zhu J, Wang Z, Chen J, et al. Balanced contrastive learning for long-tailed visual recognition[C]//Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition. 2022: 6908-6917.

[38] Kang B, Li Y, Xie S, et al. Exploring balanced feature spaces for representation learning[C]//International Conference on Learning Representations. 2020.

[39] Mu X, Shen Y, Cheng K, et al. Fedproc: Prototypical contrastive federated learning on non-iid data[J]. Future Generation Computer Systems, 2023, 143: 93-104.

[40] Chen Z, Yang C, Zhu M, et al. Personalized retrogress-resilient federated learning toward imbalanced medical data[J]. IEEE Transactions on Medical Imaging, 2022, 41(12): 3663-3674.

[41] Guo Q, Qi Y, Qi S, et al. Dual class-aware contrastive federated semi-supervised learning[J]. arXiv preprint arXiv:2211.08914, 2022.

[42] Tschandl P, Rosendahl C, Kittler H. The HAM10000 dataset, a large collection of multi-source dermatoscopic images of common pigmented skin lesions[J]. Scientific data, 2018, 5(1): 1-9.

[43] Combalia M, Codella N C F, Rotemberg V, et al. Bcn20000: Dermoscopic lesions in the wild[J]. arXiv preprint arXiv:1908.02288, 2019.

[44] Tan M, Le Q. Efficientnet: Rethinking model scaling for convolutional neural networks[C]//International conference on machine learning. PMLR, 2019: 6105-6114.

[45] Deng J. A large-scale hierarchical image database[J]. Proc. of IEEE Computer Vision and Pattern Recognition, 2009, 2009.

[46] Cubuk E D, Zoph B, Shlens J, et al. Randaugment: Practical automated data augmentation with a reduced search space[C]//Proceedings of the IEEE/CVF conference on computer vision and pattern recognition workshops. 2020: 702-703.

[47] Chen T, Kornblith S, Norouzi M, et al. A simple framework for contrastive learning of visual representations[C]//International conference on machine learning. PMLR, 2020: 1597-1607.

[48] McMahan B, Moore E, Ramage D, et al. Communication-efficient learning of deep networks from decentralized data[C]//Artificial intelligence and statistics. PMLR, 2017: 1273-1282.

[49] Li T, Sahu A K, Zaheer M, et al. Federated optimization in heterogeneous networks[J]. Proceedings of Machine learning and systems, 2020, 2: 429-450.

[50] Li Q, He B, Song D. Model-contrastive federated learning[C]//Proceedings of the IEEE/CVF conference on computer vision and pattern recognition. 2021: 10713-10722.

[51] Mu X, Shen Y, Cheng K, et al. Fedproc: Prototypical contrastive federated learning on non-iid data[J]. Future Generation Computer Systems, 2023, 143: 93-104.

[52] Sarkar D, Narang A, Rai S. Fed-focal loss for imbalanced data classification in federated learning[J]. arXiv preprint arXiv:2011.06283, 2020.

[53] Lin T Y, Goyal P, Girshick R, et al. Focal loss for dense object detection[C]//Proceedings of the IEEE international conference on computer vision. 2017: 2980-2988.

[54] Li X C, Zhan D C. Fedrs: Federated learning with restricted softmax for label distribution non-iid data[C]//Proceedings of the 27th ACM SIGKDD Conference on Knowledge Discovery & Data Mining. 2021: 995-1005.

[55] Zhang J, Li Z, Li B, et al. Federated learning with label distribution skew via logits calibration[C]//International Conference on Machine Learning. PMLR, 2022: 26311-26329.

[56] Chen Z, Yang C, Zhu M, et al. Personalized retrogress-resilient federated learning toward imbalanced medical data[J]. IEEE Transactions on Medical Imaging, 2022, 41(12): 3663-3674.

[57] Shen Z, Cervino J, Hassani H, et al. An agnostic approach to federated learning with class imbalance[C]//International Conference on Learning Representations. 2021.

[58] Shang X, Lu Y, Huang G, et al. Federated learning on heterogeneous and long-tailed data via classifier re-training with federated features[J]. arXiv preprint arXiv:2204.13399, 2022.

[59] 王慨.基于联邦学习的糖尿病并发症预测研究[D].大连理工大学,2021.DOI:10.26991/d.cnki.gdllu.2021.002631.

[60] 叶健东.基于深度神经网络的乳腺癌全切片病灶区域识别[D].北京邮电大学,2020.DOI:10.26969/d.cnki.gbydu.2020.001364.

[61] 沈亦凡.基于可解释深度学习的医疗图像诊断技术研究[D].北京邮电大学,2022.DOI:10.26969/d.cnki.gbydu.2022.000781.

致　谢

在本文完成之际，我想对许多人表达我的真诚感谢。首先，我要感谢导师瞿治国教授，您不仅在学术上给予了我无私的指导和支持，还教会了我如何独立思考、勇于探索。没有您的悉心指导，我无法完成这篇论文。

其次，我要感谢三位舍友。在大学四年的时光里，我们互相扶持、相互鼓励，共同度过了许多难忘的时刻。谢谢你们在我最困难的时候给予我支持和理解。

我还要感谢家人，是你们一直以来的支持和鼓励，让我能够坚持走到今天。你们的无私奉献和爱是我不断努力的动力源泉。

此外，我还要感谢朋友们，是你们在我人生的每个阶段都陪伴着我，给我带来了无尽的快乐和启发。感谢你们的陪伴和支持，让我感受到了友情的温暖和力量。

回首本科生活，我深深感受到了成长的喜悦和挑战的艰辛。在这四年里，我学到了许多知识，结识了许多朋友，也遇到了许多困难和挑战。但正是这些经历塑造了我成为今天的自己，让我更加坚强、自信和成熟。

对于未来，我充满了期待和憧憬。我希望能够继续努力学习，不断提升自己的能力和素质。我相信，在未来的道路上，我会遇到更多的挑战和机遇，我会继续坚持不懈，勇往直前，实现自己的人生目标和梦想。

最后，再次感谢所有关心和支持我的人，你们的爱和帮助永远铭记在心。愿我们共同携手，共同成长，共同追求美好的未来！