非独立同分布与长尾分布下的联邦学习优化方法*

冯文举[1]，杨焱青[1†]，贾振红[1]，张琳琳[2]

(1. 新疆大学 计算机科学与技术学院，新疆 乌鲁木齐 830017；2. 新疆大学 软件学院，新疆 乌鲁木齐 830091)

摘　要： 针对联邦学习中非独立同分布和长尾分布问题，结合对比学习和两阶段学习策略，提出了一种新型联邦学习方法. 利用对比学习对齐客户端模型与全局模型之间的特征，减少各客户端之间的特征差异，同时汇总并上传客户端的模型梯度，通过服务器端的虚拟特征重新训练分类器，提升全局模型对少数类数据的学习能力. 结果表明：所提方法在Fashion-MNIST数据集上准确率最高提升0.36%，在CIFAR-10数据集上准确率最高提升1.64%.

关键词： 联邦学习；非独立同分布；长尾分布；对比学习；两阶段学习

DOI： 10.13568/j.cnki.651094.651316. 2024.12.30.0001

中图分类号： TP183　**文献标识码：** A　**文章编号：** 2096-7675(2025)04-0425-09

引文格式： 冯文举，杨焱青，贾振红，张琳琳. 非独立同分布与长尾分布下的联邦学习优化方法[J]. 新疆大学学报(自然科学版中英文)，2025，42(4)：425-433.

英文引文格式： FENG Wenju，YANG Yanqing，JIA Zhenhong，ZHANG Linlin. Federated learning optimization method in non-IID and long-tail distributions[J]. Journal of Xinjiang University(Natural Science Edition in Chinese and English)，2025，42(4)：425-433.

Federated Learning Optimization Method in Non-IID and Long-Tail Distributions

FENG Wenju[1], YANG Yanqing[1], JIA Zhenhong[1], ZHANG Linlin[2]

(*1. School of Computer Science and Technology, Xinjiang University, Urumqi Xinjiang 830017, China;*
2. School of Software, Xinjiang University, Urumqi Xinjiang 830091, China)

Abstract： To address the challenges of non-independent and identically distributed data and long-tail distributions in federated learning, a novel federated learning method is proposed by integrating contrastive learning with a two-stage learning strategy. The approach employs contrastive learning to align feature representations between client models and the global model, thereby reducing feature discrepancies across clients. Simultaneously, it aggregates and uploads client model gradients, enabling retraining of the classifier through virtual features on the server side to enhance the global model's learning capability for minority class data. Experimental results demonstrate that the proposed method achieves maximum accuracy improvements of 0.36% on the Fashion-MNIST dataset and 1.64% on the CIFAR-10 dataset.

Key words： federated learning; non-independent and identically distributed; long-tail distribution; contrastive learning; two-stage learning

∗ **收稿日期：** 2024-12-30

基金项目： 新疆维吾尔自治区天山英才科技创新团队“面向公共安全的信号检测与处理技术研究”（2023TSYCTD0012）；新疆维吾尔自治区教育厅高校科研计划“基于深度生成模型的工控网络攻击检测技术研究”（XJEDU2021Y003）；新疆维吾尔自治区重大科技专项“能源数据标准化体系研究”（2022A01007-4）.

作者简介： 冯文举（1998—），男，硕士生，从事联邦学习的研究，E-mail：107552203994@stu.xju.edu.cn.

† **通讯作者：** 杨焱青（1981—），男，博士，副教授，主要从事网络空间安全和隐私计算的研究，E-mail：qing010@xju.edu.cn.

0 引 言

近年来，以深度学习为代表的人工智能已广泛应用于人们的生活，并且在图像识别[1]和自然语言处理[2]等领域逐渐改变大家的生活方式. 然而，深度学习也面临一些挑战，如“数据孤岛”和数据隐私保护问题[3]. 各国政府为此制定了相关的隐私保护法规，如欧盟2018年发布的《通用数据保护条例》[4]和我国2021年正式施行的《中华人民共和国数据安全法》. 为克服“数据孤岛”和隐私保护的挑战，联邦学习应运而生[5−6]. 联邦学习由谷歌提出[7]，通过对参与训练的客户端模型参数进行平均聚合以构建全局模型，并将该全局模型分发回客户端，循环执行这一过程以不断优化模型，从而保护参与方的隐私[8].

非独立同分布数据[9−10]和长尾数据[11]是联邦学习中常见且具有挑战性的问题，为解决数据异质性和长尾效应引发的模型性能下降问题，研究人员进行了多方面的探索与研究. Li等[12]提出了一种名为FedProx的方法，通过在本地训练过程中引入近端项，对服务器和客户端参数之间的差距施加二次惩罚，然而近端项也进一步限制了模型的本地更新. Karimireddy等[13]提出了SCAFFOLD算法，通过引入控制变量校正客户端的局部梯度差异，显著提高了联邦学习在非独立同分布数据下的收敛速度和全局模型的泛化能力，但由于每个客户端均需要保存自己的控制变量，该方法在实际系统中有一定实现难度. Li等[14]提出了FedDANE算法，通过使用控制变量的方法来处理客户端的局部更新，进一步提高收敛性能，但该方法会增加计算负担. 汤凌韬等[15]提出了一种面向非独立同分布数据的联邦学习数据增强框架，通过在每个客户端本地生成虚拟样本并在节点间共享，缓解了数据分布差异导致的模型偏移问题，但虚拟样本的生成对于硬件较差的客户端不够友好. Li等[16]通过在模型层面引入对比学习机制，缓解了因客户端本地数据分布差异导致的模型更新偏移问题，然而该方法在一定程度上限制了模型的个性化能力. Shang等[17]通过在服务器端重新训练全局分类器并结合联邦特征来克服分类器偏差问题，该方法有较大的计算负担，不适用计算资源受限的场景. Shi等[18]通过知识蒸馏向客户端模型传输视觉-语言先验知识，从而增强客户端模型的特征表示能力，由于对训练过程的依赖较强，该方法需要较长的训练时间才能达到最佳效果.

尽管以上方法在解决数据异质性和长尾问题方面取得了显著进展，但仍存在一定的局限性. 大多数方法在提升模型性能的同时增加了计算和通信开销，且在极端数据异质性情况下依旧面临收敛速度慢或泛化能力不足的问题. 针对这些问题，本文提出了FedCoAlign算法，利用对比学习和两阶段学习减少不同客户端之间的特征差异，提升全局模型在处理尾部类别数据时的学习能力.

1 相关知识

1.1 联邦学习

在联邦学习中，主要通过对各客户端的模型进行加权平均来更新全局模型，以最具代表的算法FedAvg[7]为例，具体过程通常包括以下四个阶段.

1）初始化模型. 服务器初始化一个全局模型w^0并将其发送给每个客户端.

2）客户端本地训练. 假设有K个客户端，每个客户端k拥有本地数据集D_k，并使用该数据集训练模型. 对于每一轮t，客户端使用本地数据集更新模型参数w_k^t，计算方式为

$$w_k^{t+1} = w_k^t - \eta \nabla L_k(w^t; D_k), \tag{1}$$

式中：η是学习率；$L_k(w^t; D_k)$是本地损失函数.

3）模型聚合. 对于K个客户端，每个客户端k拥有的本地数据集大小为n_k，总数量为$n = \sum_{k=1}^{K} n_k$. 服务器接收所有客户端更新后的模型参数w_k^{t+1}，并根据客户端数据量进行加权汇聚，即

$$w^{t+1} = \sum_{k=1}^{K} \frac{n_k}{n} w_k^{t+1}. \tag{2}$$

4）全局模型更新. 服务器将汇聚后的全局模型参数w^{t+1}发送给所有客户端，客户端再以此为基础进行下一轮训练.

通过不断迭代这个过程，最终训练出一个全局优化的模型，而各客户端的数据始终保留在本地，保护了数据隐私.

1.2　对比学习

对比学习[19]是一种自监督学习技术，通过比较样本间的相似性与差异性来学习数据的有效表征. 对比学习的核心思想是将相似的样本，即正样本对拉近，使其在表征空间中更加接近，而将不相似的样本，即负样本对推远.

给定一个样本x_i，会生成一个与其相似的正样本x_i^+和若干不相似的负样本x_j^-，训练模型使得x_i同x_i^+在特征空间中距离更近，而x_i同x_j^-的距离更远. 对比学习的核心在于损失函数，最常见的是InfoNCE Loss，即

$$L=-\log\frac{\exp(s_{i+}/\tau)}{\exp(s_{i+}/\tau)+\sum_{j=1}^{N}\exp(s_{i-}^{j}/\tau)}, \tag{3}$$

式中：$s_{i+}=sim(z_i,z_i^+)$，表示输入样本z_i和正样本z_i^+之间的相似度；$s_{i-}^{j}=sim(z_i,z_j^-)$，表示输入样本$z_i$和负样本$z_j^-$之间的相似度；$\tau$是温度参数；$N$是负样本数量.

该损失函数通过最大化正样本对的相似性、最小化负样本对的相似性，以学习一个表征空间，从而获得高质量的特征表示.

1.3　两阶段学习

两阶段学习[20]是一种常用于分类任务的学习策略，特别是在不平衡数据集中，可以提升模型性能. 其将训练过程分为两个阶段：第一阶段，主要关注提取特征，学习具有普遍性且通用的特征；第二阶段，更加关注分类器训练，尤其是针对类别不平衡的优化.

1）阶段一：特征提取. 目标是训练模型从数据中提取有用的特征，主要关注学习到高质量且可区分的特征表示，而不是直接优化分类精度. 损失函数可表示为

$$L_1=-\sum_{i=1}^{N}y_i\log(f(x_i;\theta)), \tag{4}$$

式中：N是样本数量；y_i是样本i的标签；$f(x_i;\theta)$是模型对样本x_i的输出概率；θ表示模型的参数.

2）阶段二：分类器重训练. 重点是在固定特征提取器的基础上，重新训练分类器部分. 由于在不平衡数据集上某些类的样本较少，直接使用原始的特征分布进行分类将导致效果不理想，故可以针对数据的分布特点进行优化. 损失函数可表示为

$$L_2=-\sum_{i=1}^{N}w_iy_i\log(g(z_i;\phi)), \tag{5}$$

式中：w_i是样本i的权重；z_i是由第一阶段训练好的特征提取器输出的特征；$g(z_i;\phi)$是第二阶段重新训练的分类器输出；ϕ表示分类器的参数.

2　问题定义

2.1　非独立同分布数据问题

非独立同分布数据意味着不同客户端的本地数据分布不同，在联邦学习中，全局模型的目标是最小化所有客户端加权后的总损失函数，即

$$L(w^t)=\sum_{k=1}^{K}\frac{n_k}{n}L_k(w^t), \tag{6}$$

式中：$L_k(w^t)$是客户端k在t轮的本地损失.

假设客户端k的数据分布为$P_k(x,y)$，而全局数据分布为$P(x,y)$，由于$P_k(x,y)\neq P(x,y)$，客户端本地损失函数$L_k(w)$优化的方向会偏向其本地数据分布，导致客户端的局部更新方向不同，进而使得全局模型聚合时难以找到一个全局最优解.

2.2　长尾分布数据问题

长尾分布问题是指客户端或全局数据集中某些类别的数据量远远大于其他类别的数据量，在长尾数据集中，类别c的样本量呈现不均衡现象. 假设类别c的数据量为N_c，则长尾数据的分布可以表示为$N_c=N_1/IF$，其

中：N_1是头部类别的样本量，IF是长尾数据的不均衡因子. 当IF取值为m时，表示数据集中头部类别的数量是尾部类别数量的m倍，故模型的总梯度会偏向头部类别，导致尾部类别学习不足. 模型参数更新方式为

$$w^{t+1}=w^t-\eta\sum_{k=1}^{K}\frac{n_k}{n}\sum_{c=1}^{L}p_c^k\nabla L_k(w^t;D_k), \tag{7}$$

式中：p_c^k是客户端k中类别c的数量；L是类别数量；n_k是客户端k的数据集大小；$L_k(w^t;D_k)$是客户端k的本地损失函数. 由于p_c^k在长尾分布中差异巨大，头部类别p_{c1}^k的值远大于尾部类别p_{cL}^k，导致模型的梯度更新偏向头部类别，尾部类别的梯度更新贡献微弱.

3 基于对比学习与两阶段学习策略的联邦学习方法

在本地端，引入对比学习，以确保当前训练的模型特征与服务器重训练后的全局特征对齐，同时防止模型在本地训练过程中过度依赖某一轮的更新，从而提高模型的泛化能力. 在服务器端，通过生成的虚拟平衡特征和从预训练模型提取的文本特征，以重训练全局模型分类器，从而改善模型对少数类别的识别能力. FedCoAlign整体架构如图1所示.

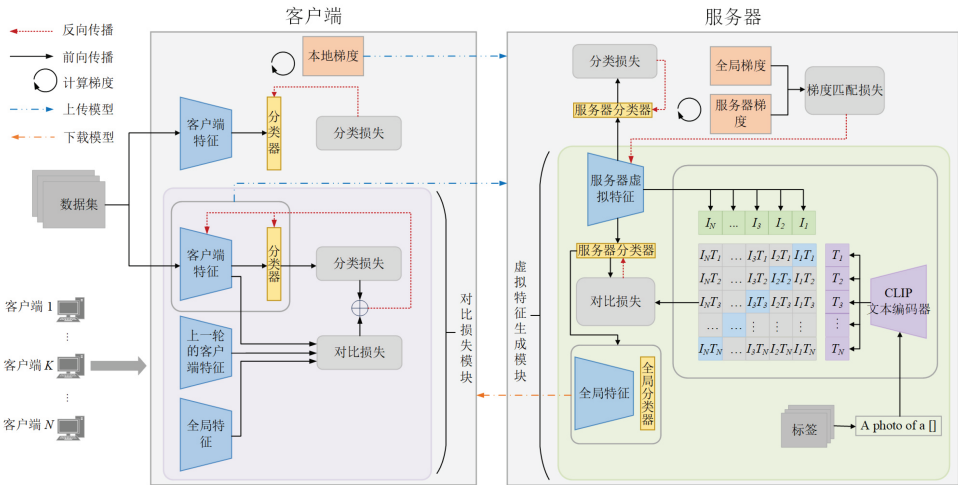


图 1 FedCoAlign整体架构

3.1 客户端模型训练

在本地训练中，损失函数由分类损失和对比损失两部分构成，分类损失用于衡量模型在本地数据上的分类性能，而对比损失负责约束当前模型生成的特征与服务器重训练后的特征保持一致.

1）分类损失. 设输入数据为$X_k=\{x_k^1,x_k^2,\cdots,x_k^n\}$，真实标签为$Y_k=\{y_k^1,y_k^2,\cdots,y_k^n\}$，则分类损失定义为

$$L_{CE}=-\frac{1}{n}\sum_{i=1}^{n}y_k^i\log(f(x_k^i;\theta)), \tag{8}$$

式中：k表示客户端编号；n表示数据样本的数量；$f(x_k^i;\theta)$是模型对样本x_k^i的输出概率；θ表示模型的参数.

2）对比损失. 对比学习通过正样本和负样本的对比以优化特征表示，本文将当前轮次模型生成的特征z_c和服务器端聚合后的全局特征z_s作为正样本对，将z_c和上一轮模型的特征z_o作为负样本对，对比损失函数为

$$L_{CON}=-\log\frac{\exp(sim(z_c,z_s)/\tau)}{\exp(sim(z_c,z_s)/\tau)+\exp(sim(z_c,z_o)/\tau)}. \tag{9}$$

通过最小化这个对比损失，当前模型的特征z_c将被优化，使其更加接近服务器全局特征z_s，从而缓解由于本地数据偏差造成的特征不一致问题. 在本地训练中，如果仅仅依赖本轮的数据更新模型，会导致模型忽视之前学习到的知识，这种现象特别容易出现在数据异质性较大的情况下. 故本地更新中使用上一轮模型的特征z_o，还可以有效缓解灾难性遗忘问题. 本地训练的总损失函数L是分类损失和对比损失的加权和，即

$$L=L_{CE}+\mu L_{CON}, \tag{10}$$

式中：μ是一个超参数，可以平衡模型的分类性能和特征对齐的效果.

最后，通过总损失函数对本地模型进行更新，即

$$w_k^{t+1} = w_k^t - \eta \nabla L_k(w^t). \tag{11}$$

在本地训练中，客户端还需要计算各类别的真实特征梯度并将其上传到服务器，以便服务器进行虚拟平衡特征的优化. 客户端类别梯度计算方法为

$$g_k^c = \frac{1}{n_k^c} \sum_{i=1}^{n_k^c} \nabla L_{CE}(z_k^{i,c}; y_k^i), \tag{12}$$

式中：g_k^c是客户端k中类别c的特征梯度；n_k^c是客户端k中类别c的样本数量；$z_k^{i,c}$是客户端k中类别c第i个样本的特征；y_k^i是样本i的真实标签.

该梯度反映了模型在本地训练过程中对于类别c的特征变化. 客户端将这些特征梯度与本地模型参数一同上传至服务器，用于全局模型的优化.

3.2　服务器端模型聚合

服务器端会初始化一组虚拟特征z_s和服务器分类器v_s，并通过梯度匹配损失更新虚拟特征. 首先对客户端上传的各类梯度信息进行汇聚，计算方式为

$$g_{avg}^c = \frac{1}{K} \sum_{k=1}^{K} g_k^c, \tag{13}$$

式中：K是客户端数量；g_{avg}^c是类别c汇总后的特征梯度.

尽管各个客户端上传的梯度是不平衡的，但通过服务器端的梯度汇总和平均过程，服务器实际上获得了一种全局平均的特征梯度. 这相当于从多个客户端的数据中提取一个全局平均的特征更新方向. 然后服务器端会使用服务器分类器v_s获取服务器梯度，即

$$g_s^c = \frac{1}{m} \sum_{i=1}^{m} \nabla L_{CE}(z_s^{i,c}; y_s^i), \tag{14}$$

式中：$z_s^{i,c}$是虚拟特征中类别c的第i个样本；y_s^i是样本i的标签；g_s^c是类别c的服务器梯度.

在每次迭代中，服务器通过梯度下降法最小化梯度匹配损失L_M，不断更新虚拟特征z_s，使其生成的特征梯度g_s^c更加接近汇总后的平均特征梯度g_{avg}^c，多个迭代后，虚拟特征会逐渐优化，生成的特征梯度更具全局代表性，反映了不同类别之间的平衡. z_s的更新方式为

$$z_s \leftarrow z_s - \eta \nabla L_M, \tag{15}$$

式中：L_M为梯度匹配损失[21].

$$L_M = \frac{1}{C} \sum_{j=1}^{C} \left(1 - \frac{g_s^c[j] \cdot g_{avg}^c[j]}{\|g_s^c[j]\| \times \left\|g_{avg}^c[j]\right\|} \right). \tag{16}$$

在服务器端训练中，虚拟特征z_s表示服务器端在全局范围内通过多个客户端的本地梯度生成的视觉特征，而通过CLIP[22]预训练模型提取的文本特征z_t，则是与这些视觉特征语义对齐的文本表示. 通过将两者在表征空间进行对齐，可以得到每个类别标签的语义信息与全局模型的相似度. 将虚拟平衡特征生成的预测分布与基于预训练模型提取的文本特征生成的分布进行特征对齐，从而实现知识蒸馏，增强全局模型分类器的学习效果. 对齐过程为

$$L_{KD} = KL(z_s || (z_s \cdot z_t)), \tag{17}$$

式中：KL是Kullback-Leibler散度[23].

通过服务器虚拟特征z_s计算服务器分类损失L_{CE}，再将其与对齐损失L_{KD}进行加权求和，可以得到服务器重训练阶段的总损失，即

$$L_s = L_{CE} + \lambda L_{KD}. \tag{18}$$

最终，利用服务器虚拟特征z_s重新训练聚合后的全局模型分类器v_g^t如下：

$$v_g^t \leftarrow v_g^t - \eta \nabla L_s(z_s; y_s). \tag{19}$$

4 实验结果及分析

本文在Fashion-MNIST和CIFAR-10数据集上进行验证，实验环境配置如表1所示.

表 1 实验环境配置

配置项	配置信息
CPU	12 vCPU Intel(R) Xeon(R) Platinum 8336C CPU @ 2.30 GHz
GPU	NVIDIA GeForce RTX 2080 Ti ×2
RAM（CPU）	32 GB
RAM（GPU）	22 GB

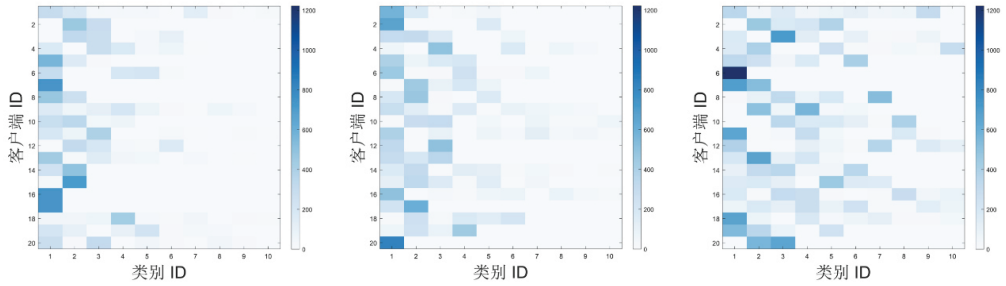
4.1 实验设置

Fashion-MNIST数据集包含10个类别的灰度图片，每张大小为28×28像素，共70 000张，其中60 000张用于训练、10 000张用于测试. 每张图片展示了一件不同类型的服装，如T恤、裤子、鞋子等.

CIFAR-10数据集包含10个类别的彩色图片，每张大小为32×32像素，共60 000张，其中50 000张用于训练、10 000张用于测试.

本文通过Dirichlet分布[24]参数α来调控数据的异质性程度，并使用长尾因子IF来控制数据的长尾分布特性. 为聚焦IF的主效应，实验中α固定为0.5；IF取值为100、50和10，表示数据集中头部类别数量是尾部类别的100倍、50倍和10倍. 所有对比算法均采用ResNet-8[25]作为训练网络，并使用相同的超参数配置，即：共设置20个本地客户端，每轮随机选择其中8个参与训练，整体训练过程共执行200轮，客户端本地训练轮数为10，学习率为0.01. FedCoAlign算法中，超参数τ在0.01~0.5中进行粗粒度搜索，并最终取为0.1.

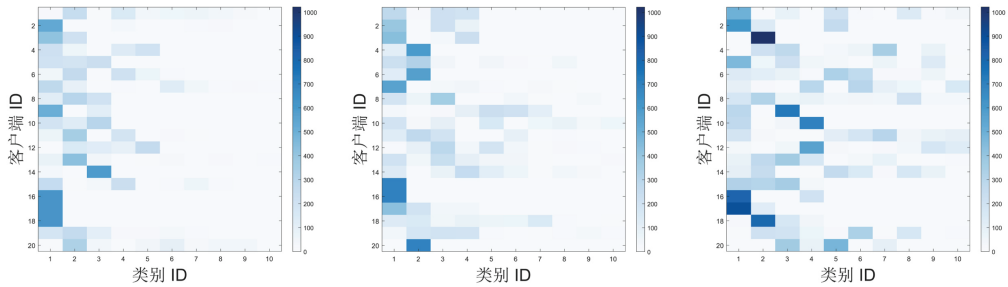
各客户端在Fashion-MNIST数据集上的数据分布情况如图2所示，其中图2（a）、图2（b）、图2（c）分别表示IF取值为100、50、10时的数据分布.



(a) IF=100 (b) IF=50 (c) IF=10

图 2 客户端在Fashion-MNIST数据集上的数据分布

图3展示了各客户端在CIFAR-10数据集上的数据分布情况，其中图3（a）、图3（b）、图3（c）分别表示IF取值为100、50、10时的数据分布. 可知，随着IF的减小，尾类数据样本量逐渐增多.



(a) IF=100 (b) IF=50 (c) IF=10

图 3 客户端在CIFAR-10数据集上的数据分布

4.2　实验结果

为体现FedCoAlign在数据异质性且长尾分布下的优异性能，将其与联邦学习算法FedAvg、FedProx、CReFF和CLIP2FL进行比较，实验结果如表2所示.

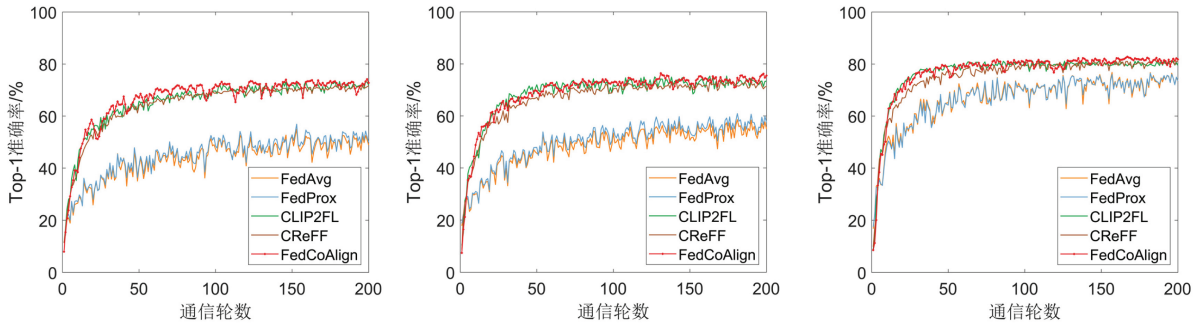
表 2　不同IF下的准确率比较

算法	Fashion-MNIST			CIFAR-10		
	IF=100	IF=50	IF=10	IF=100	IF=50	IF=10
FedAvg[7]	87.85%	89.80%	91.11%	56.17%	59.36%	77.45%
FedProx[12]	87.90%	90.11%	91.08%	56.92%	60.89%	76.53%
CReFF[17]	88.79%	90.15%	90.97%	70.55%	73.08%	80.87%
CLIP2FL[18]	88.99%	90.26%	91.18%	73.34%	75.35%	81.18%
FedCoAlign（本文）	**89.35%**	**90.34%**	**91.45%**	**74.36%**	**76.42%**	**82.82%**

注：加粗数值为最优结果

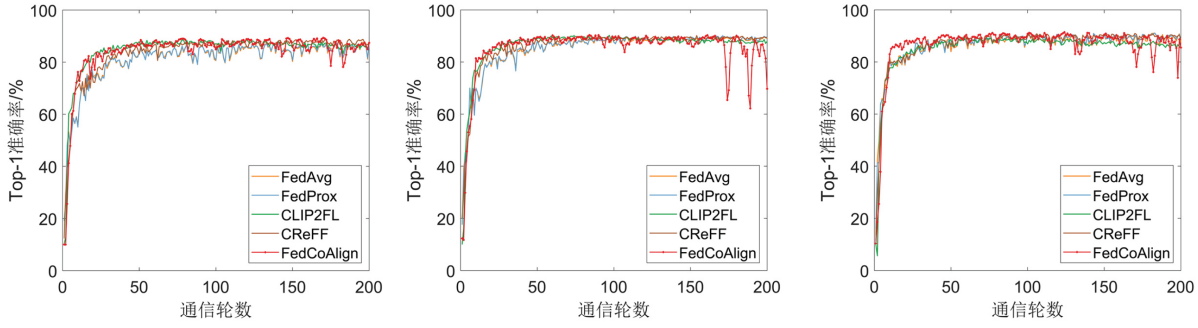
由表2可知，在Fashion-MNIST数据集上，FedCoAlign表现最佳，IF=100时的准确率为89.35%，随着IF减小，准确率提升至91.45%. FedCoAlign通过对比学习机制有效减少了客户端之间的数据差异，特征对齐提高了全局模型的稳定性和一致性，使其在异质性数据上表现出色. 在CIFAR-10数据集上，FedCoAlign同样领先，IF=100时的准确率为74.36%，随着IF减小，准确率提升至82.82%. 通过对本地和全局特征的一致性约束，FedCoAlign能更好应对复杂和不平衡的数据集. 同时，服务器端的虚拟特征优化和梯度匹配机制，确保了全局模型在长尾数据上保持较好的平衡.

图4展示了在CIFAR-10数据集上5种不同联邦学习算法的Top-1准确率随通信轮数的变化情况. CLIP2FL和CReFF在中度不平衡时表现相对较好；FedAvg和FedProx在所有条件下表现较差，特别是在高度不平衡时，其对尾部类别的学习能力明显不足，导致整体准确率较低. FedCoAlign在所有不平衡因子条件下表现最优，值得注意的是，IF=100时FedCoAlign相对其他算法优势最明显，这是因为IF=100表示数据高度不平衡，稀有类别样本非常少，头部类别占据主导. FedCoAlign机制能有效应对这种不平衡，而传统算法在尾部类别上表现较差.



(a) IF=100　(b) IF=50　(c) IF=10

图 4　在CIFAR-10数据集上Top-1准确率随通信轮数的变化

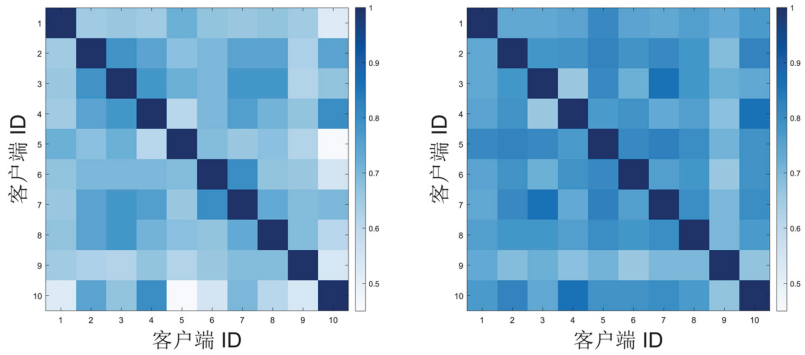


(a) IF=100　(b) IF=50　(c) IF=10

图 5　在Fashion-MNIST数据集上Top-1准确率随通信轮数的变化

图5展示了在Fashion-MNIST数据集上5种不同联邦学习算法的Top-1准确率随通信轮数的变化情况. 该数据集由灰度图片组成，特征较少，故算法更容易从这些简单的特征中提取有用信息，不同算法之间的准确率差距不会太大. 尽管IF取值为50和10时，FedCoAlign的准确率在170轮附近有所下降，但整体而言，FedCoAlign的效果均优于其他算法.

图6展示了FedAvg和FedCoAlign在不同客户端间的CKA（Centered Kernel Alignment）相似性. 使用CKA可以衡量不同客户端模型特征表示之间的相似性，数值越大，说明特征表示越相似；数值越小，说明特征表示差异越大. 由图6（a）可知，FedAvg的CKA相似性图中颜色差异较大，尤其是多个客户端之间的相似性较低. 这是由于FedAvg在处理数据异质性时无法很好对齐不同客户端的特征，导致全局模型难以捕捉各客户端间的一致特征. 由图6（b）可知，FedCoAlign的CKA相似性明显更高，大部分客户端之间的相似性更为接近，颜色分布较为均匀，整体相似性较高，表示客户端间的特征表示更加一致. 表明FedCoAlign在不同客户端之间能够有效对齐特征表示，即使在数据异质性较大的情况下，也能保证不同客户端生成的特征具有较高的相似性.



（a）FedAvg （b）FedCoAlign

图 6 不同联邦算法的客户端CKA相似性

5 结束语

本文所提FedCoAlign算法，通过引入对比学习机制和虚拟特征优化，实现了客户端本地特征与全局特征的有效对齐，提升了全局模型在异质性数据上的性能. 结果表明：FedCoAlign在不同数据集和不平衡因子条件下均表现出色，尤其在数据高度不平衡的情况下，其性能优于传统的联邦学习算法. 考虑到FedCoAlign额外上传了本地训练的梯度信息，而现有方法可以通过梯度反演攻击重建原始训练样本[26]，故后续将考虑在通信过程中采用差分隐私技术进一步提升安全性.

参考文献：

[1] XIAO J S，GUO H W，ZHOU J，et al. Tiny object detection with context enhancement and feature purification[J]. Expert Systems with Applications，2023，211：118665.

[2] 杨晓奇，刘伍颖. 文本特征和图结点混合增强的图卷积网络文本分类[J]. 新疆大学学报(自然科学版)(中英文)，2024，41(1)：69-77+109.
YANG X Q，LIU W Y. Hybrid augmentation of text feature and graph node for graph convolutional networks text classification[J]. Journal of Xinjiang University(Natural Science Edition in Chinese and English)，2024，41(1)：69-77+109. (in Chinese)

[3] LI Z P，SHARMA V，MOHANTY S P. Preserving data privacy via federated learning：Challenges and solutions[J]. IEEE Consumer Electronics Magazine，2020，9(3)：8-16.

[4] European Union. General data protection regulation[EB/OL]. (2018-05-25)[2024-11-30]. https://gdpr-info.eu/.

[5] WEN J，ZHANG Z X，LAN Y，et al. A survey on federated learning：Challenges and applications[J]. International Journal of Machine Learning and Cybernetics，2023，14(2)：513-535.

[6] ZHANG C，XIE Y，BAI H，et al. A survey on federated learning[J]. Knowledge-Based Systems，2021，216：106775.

[7] MCMAHAN H B，MOORE E，RAMAGE D，et al. Communication-efficient learning of deep networks from decentralized data[EB/OL]. 2016：1602.05629. https://arxiv.org/abs/1602.05629v4.

[8] BRAUNECK A，SCHMALHORST L，MAJDABADI M M K，et al. Federated machine learning，privacy-enhancing technologies，and data protection laws in medical research：Scoping review[J]. Journal of Medical Internet Research，2023，25：e41588.

[9] ZHU J C，CAO J N，SAXENA D，et al. Blockchain-empowered federated learning：Challenges，solutions，and future directions[J]. ACM Computing Surveys，2023，55(11)：240.

[10] CHEN H M，WANG H D，LONG Q Y，et al. Advancements in federated learning：Models，methods，and privacy[J]. ACM Computing Surveys，2024，57(2)：46.

[11] SHUAI X，SHEN Y L，JIANG S Y，et al. BalanceFL：Addressing class imbalance in long-tail federated learning[C]//2022 21st ACM/IEEE International Conference on Information Processing in Sensor Networks (IPSN). May 4-6，2022. Milano，Italy. IEEE，2022：271-284.

[12] LI T，SAHU A K，ZAHEER M，et al. Federated optimization in heterogeneous networks[EB/OL]. 2018：1812.06127. https://arxiv.org/abs/1812.06127.

[13] KARIMIREDDY S P，KALE S，MOHRI M，et al. SCAFFOLD：Stochastic controlled averaging for federated learning[EB/OL]. 2019：1910.06378. https://arxiv.org/abs/1910.06378.

[14] LI T，SAHU A K，ZAHEER M，et al. FedDANE：A federated Newton-type method[C]//2019 53rd Asilomar Conference on Signals，Systems，and Computers. November 3-6，2019. Pacific Grove，CA，USA. IEEE，2019：1227-1231.

[15] 汤凌韬，王迪，刘盛云. 面向非独立同分布数据的联邦学习数据增强方案[J]. 通信学报，2023，44(1)：164-176.
TANG L T，WANG D，LIU S Y. Data augmentation scheme for federated learning with non-IID data[J]. Journal on Communications，2023，44(1)：164-176. (in Chinese).

[16] LI Q B，HE B S，SONG D. Model-contrastive federated learning[C]//2021 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR). June 20-25，2021. Nashville，TN，USA. IEEE，2021：10708-10717.

[17] SHANG X Y，LU Y，HUANG G，et al. Federated learning on heterogeneous and long-tailed data via classifier re-training with federated features[EB/OL]. 2022：2204.13399. https://arxiv.org/abs/2204.13399v1.

[18] SHI J M，ZHENG S S，YIN X B，et al. CLIP-guided federated learning on heterogeneous and long-tailed data[EB/OL]. 2023：2312.08648. https://arxiv.org/abs/2312.08648v1.

[19] HE K M，FAN H Q，WU Y X，et al. Momentum contrast for unsupervised visual representation learning[C]//2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR). June 13-19，2020. Seattle，WA，USA. IEEE，2020：9726-9735.

[20] REN S Q，HE K M，GIRSHICK R，et al. Faster R-CNN：Towards real-time object detection with region proposal networks[J]. IEEE Transactions on Pattern Analysis and Machine Intelligence，2017，39(6)：1137-1149.

[21] LUO M，CHEN F，HU D P，et al. No fear of heterogeneity：Classifier calibration for federated learning with non-IID data[EB/OL]. 2021：2106.05001. https://arxiv.org/abs/2106.05001v1.

[22] RADFORD A，KIM J W，HALLACY C，et al. Learning transferable visual models from natural language supervision[EB/OL]. 2021：2103.00020. https://arxiv.org/abs/2103.00020.

[23] JI S Y，ZHANG Z Z，YING S H，et al. Kullback-Leibler divergence metric learning[J]. IEEE Transactions on Cybernetics，2022，52(4)：2047-2058.

[24] WANG Y S，TONG Y X，SHI D Y. Federated latent Dirichlet allocation：A local differential privacy based framework[J]. Proceedings of the AAAI Conference on Artificial Intelligence，2020，34(4)：6283-6290.

[25] HE K M，ZHANG X Y，REN S Q，et al. Deep residual learning for image recognition[C]//2016 IEEE Conference on Computer Vision and Pattern Recognition (CVPR). June 27-30，2016. Las Vegas，NV，USA. IEEE，2016：770-778.

[26] ZHU L G，LIU Z J，HAN S. Deep leakage from gradients[EB/OL]. (2019-12-12)[2024-11-30]. https://proceedings.neurips.cc/paper_files/paper/2019/file/60a6c4002cc7b29142def8871531281a-Paper.pdf.

责任编辑：张自强