基于原型聚类机制的个性化联邦学习方法

刘海军，王浩龙，刘雅辉，马洪亮
（石河子大学信息科学与技术学院，新疆 石河子 832003）

摘　要：现有研究大多采用知识蒸馏或多任务训练来进行个性化联邦学习，但这些方法通常需要额外的蒸馏步骤或较高的通信开销，影响了模型的整体性能。为了解决这一挑战，提出了一种基于原型聚类的个性化联邦学习方法FedPC。该方法通过引入客户端聚类机制，以原型为依据将具有相似数据分布的客户端划分为一组，从而减轻数据分布差异对模型性能的影响；为了更好地适应参与方本地模型的个性化需求，将客户端模型解耦为特征提取器和个性化分类器两部分，同时采用自适应加权聚合策略和联合损失函数共同优化客户端与服务器的训练过程，以实现更优的模型性能。在3个常用数据集Cifar10、Cifar100和FMNIST上进行的实验结果表明，FedPC在模型准确率方面均优于传统的联邦学习方法，验证了其在处理数据异质性问题上的有效性。

关键词：个性化联邦学习；数据隐私；数据异质性；原型
中图分类号：TP301
文献标志码：A
DOI：10.11959/j.issn.1000–436x.2025235

Personalized federated learning method based on prototype clustering mechanism

LIU Haijun, WANG Haolong, LIU Yahui, MA Hongliang
School of Information Science and Technology, Shihezi University, Shihezi 832003, China

Abstract: Existing studies mostly adapt knowledge distillation or multi-task training for personalized federated learning, but these methods typically require additional distillation steps or high communication overhead, affecting overall model performance. To address this challenge, a personalized federated learning method FedPC based on prototype clustering was proposed. By introducing a client clustering mechanism, FedPC grouped clients with similar data distributions into clusters based on prototypes, thereby reducing the impact of data distribution differences on model performance. To better adapt the personalized needs of local models of participants, the client model was decoupled into a feature extractor and a personalized classifier. At the same time, an adaptive weighted aggregation strategy and a joint loss function were used to co-optimize the training processes of clients and the server, achieving better model performance. Experimental results on three commonly used datasets, Cifar10, Cifar100, and FMNIST, show that FedPC outperforms traditional federated learning methods in terms of model accuracy, verifying its effectiveness in handling data heterogeneity issues.

Keywords: personalized federated learning, data privacy, data heterogeneity, prototype

收稿日期：2025–08–14；**修回日期：**2025–09–15
通信作者：刘雅辉，lyh@shzu.edu.cn
基金项目：兵团重大科技基金资助项目（No.2023AA001）；八师石河子市财政科技计划基金资助项目（No.2024GY08）；兵团指导性科技计划基金资助项目（No.2023ZD045）；兵团重点领域科技攻关基金资助项目（No.2024AB080）；兵团科技创新人才计划基金资助项目（No.2023CB005, No.2023ZD066, No.2022CB002-08）
Foundation Items: Bingtuan Major Science and Technology Project (No.2023AA001), Shihezi Financial Science and Technology Project (No.2024GY08), Bingtuan Science and Technology Program (No.2023ZD045), Bingtuan Key Areas Science and Technology Research Project (No.2024AB080), Bingtuan Science and Technology Innovation Talent Program (No.2023CB005, No.2023ZD066, No.2022CB002-08)

0　引言

联邦学习作为隐私保护方法的一个分布式机器学习范式[1]，在训练过程中，每个客户端将自己收集到的数据保留在本地，并利用本地数据进行模型训练，随后将本地模型参数或梯度更新上传到中心服务器进行聚合来生成全局模型，最后将全局模型参数下发到各参与方进行下一轮训练。由于数据保留在本地而不进行直接的数据传输，从而减少了通信开销和隐私泄露问题。目前，联邦学习在许多场景中得到广泛应用。例如，在医疗领域，不同医疗机构可以共享病人的医疗数据进行疾病预测模型的训练，而不需要将敏感的病人数据进行集中存储；在金融领域，银行和金融机构利用联邦学习共同构建信用评估模型，同时保护客户的隐私。此外，联邦学习还被应用于物联网设备的数据分析、智慧城市管理等多个场景。

然而，联邦学习中客户端之间的差异会影响模型最终的性能。客户端之间的差异包括统计异质性、模型异质性和设备异构性[2]。客户端的统计异质性是指不同客户端所持有的本地数据分布存在显著差异的现象。这种差异体现在数据的特征、标签、数量或生成机制上，可能导致客户端的数据是非独立同分布（non-IID, non-independent identically distributed）的。Ng 等[3]的研究表明，数据 non-IID 问题对联邦学习的性能影响较大，是全局模型性能下降的主要原因。Liu 等[4]考虑到不同客户端的数据分布不同，将客户端数据的统计异质性作为衡量隐私预算分配的影响因素，实现了联邦学习中的个性化隐私保护。客户端的模型异质性是指不同客户端使用的本地模型结构、参数规模或训练方式存在一定差异。传统的联邦学习模型更加强调模型的泛化性能，但是实际中个性化模型能够更好地适应客户端数据的分布特点。然而，为每一个客户端定制一个个性化模型[5]，训练成本较高。在理想情况下，个性化模型应能对本地所有类进行良好预测，但实际情况并非如此，不同客户端可能有不同的主导类，某些类的样本数量极少甚至缺失，模型更倾向于拟合主导类，导致对少数类的预测效果不佳[6]。

对于这种数据不均衡问题，Li 等[7]提出通过对主导类的欠采样和少数类的过采样来达到样本数量均衡的目的，同时增加少数样本类的权重来提高模型性能的总体效果。Collins 等[8]将模型解耦为特征提取器和分类器两部分：特征提取器旨在训练得到本地数据样本的高效特征表示用于之后的分类，分类器旨在训练一个高分类精度的分类头，实现对不同类之间的平衡决策。对本地模型按顺序学习分类器和特征提取器部分，首先训练从服务器接收的具有固定主体的分类器，之后学习具有最新的个性化分类器固定的特征提取器。Liu 等[9]发现分类器是性能下降的主要原因，同时建议学习强代表性的表示来提高性能。Son 等[10]发现均衡数据集中不同类的表示在表示空间中均匀分布，当数据集不均衡时，少数类与多数类的表示重叠不均匀，通过引入分类器的维度概率分布的方差和编码器表示的超球面均匀性这两个正则化项用于局部训练，减弱了不均衡数据集对局部模型性能的影响。当客户端数量非常多时，这种做法的正则化项的计算可能会增加客户端的计算负担。

基于聚类的联邦学习（CFL, clustered federated learning）[11]考虑到客户端具有不同的数据分布，将具有相似分布的客户端进行分组聚类，之后进行模型的训练来提高模型性能。文献[12-13]在对客户端进行分组后，独立地去优化每个组的模型。这种做法没有利用其他组的模型知识，虽然这样能更好地适应组内客户端的个性化需求，但一定程度上忽略了组间客户端的泛化性能，无法实现组间的知识共享。Ma 等[14]在训练期间交替估计客户端的集群身份和集群模型的损失值，一定程度上实现了客户端之间的知识共享，但是消耗了大量的计算资源，增加了时间成本。

为了解决联邦学习中各客户端数据异质性造成的模型性能受限的问题，本文提出了基于原型聚类的个性化联邦学习方法 FedPC。原型[15]作为客户端本地数据特征的代表，有效封装了特定数据类的关键特征，能够很好地代表客户端数据分布情况。具有相似数据分布的客户端会生成相似的原型，具有不同数据分布的客户端生成的原型会有较大的差异，而本文提出的聚类联邦学习方法可以实现联邦学习中个性化和泛化的平衡。为了实现个性化，本文参考 Collins 等[8]的工作将客户端本地模型分为特征提取器和分类器两部分。在客户端正式训练之前，基于原型对客户端进行一次高效聚类，得到相似客户端的分组，减少训练任务的计算开销。由于

不同组间的知识差异对模型的贡献不一致，因此为了在模型聚合阶段利用其他组的模型知识，本文采用自适应加权聚合策略，为相似的组间分配较高的聚合权重，不相似的组间分配较低的权重，以此减轻non-IID数据带来的影响，提高模型的稳定性和收敛速度。

本文主要的研究工作如下。

1)设计了一种高效聚类的个性化联邦学习方法，解决客户端本地non-IID数据导致的模型性能低的问题。

2)根据原型对数据分布相似的客户端进行聚类，随后在训练过程中服务器对上传参数进行自适应加权聚合，实现跨集群知识共享。

3)在Cifar10、Cifar100和FMNIST这3个数据集上进行实验来评估本文提出的方法，实验结果表明，与传统的联邦学习方法相比，本文方法得到了更具有代表性的客户端分组，最终模型的平均准确率与最优的基线模型相比提升了5%以上。

1 相关理论

1.1 聚类联邦学习

联邦学习是谷歌公司提出的分布式机器学习框架，使原始数据在本地进行训练，并将参数上传到服务器进行聚合得到全局模型，保证数据可用不可见，达到数据隐私保护的目的。实际中客户端的数据通常是非独立同分布的，为了解决全局模型难以适应所有客户端本地数据分布的问题，CFL[16]应运而生。CFL通过将客户端划分为多个子群体，具有相似数据分布的客户端聚类到同一组中，之后在每个组内独立训练和优化本地模型，从而减少数据异质性对全局模型的影响。在聚类联邦学习中，通常包含客户端聚类、本地模型训练和模型聚合3个关键步骤。客户端可以根据自身的数据特点进行个性化模型训练，从而提高本地模型的准确性和稳定性[17]。

1.2 原型学习

基于原型学习，客户端从本地数据中学习潜在特征表示，进而捕获同类数据的共享特征，最终完成分类任务[18]。由于原型学习得到的每一个原型是该类样本特征平均表示的抽象知识，即使攻击者得到原型，也不能在有限时间内推出数据的原始特征，具有不可逆性，因此能够在提取数据抽象知识的同时保护数据样本的隐私。目前原型学习广泛地被用到各种机器学习任务中，例如少样本学习、监督学习和迁移学习等。

在联邦学习中，每个客户端可以独立地学习其本地数据的原型，并在不同客户端之间进行共享[19]。由于原型学习关注数据的代表性特征，因此在面对数据分布不一致的情况时，能够更好地捕捉到数据的本质特征，从而提高模型的性能和鲁棒性，可以有效地应对不同客户端数据non-IID问题。同时，与传统的参数更新相比，原型学习只需要上传少量的原型向量，就可以大大减少客户端与服务器之间的通信量[20]。

1.3 个性化联邦学习

现实场景中，每个客户端的数据可能来自不同的数据源，导致客户端本地数据的样本数量和类别有一定的差别，样本通常是类不均衡的，并且遵循长尾分布[21]。异质性数据在不同客户端之间的分布会显著削弱联邦学习的有效性，得到的模型会偏向于拟合头部数据而对尾部数据的学习经验较少。目前，解决类不均衡问题的常见方法主要有通过在数据重新分配或在训练过程中调整不同类的损失权重，设计类重新平衡范例减弱长尾分布的影响；为每个客户端定制训练适合本地数据样本的个性化模型，更好地拟合客户数据的不同分布。Arivazhagan等[22]设计了一种由主体和个性化头部组成的个性化本地模型，主体采用FedAvg方法进行学习。Li等[23]为每个客户端维持一个本地模型，通过将本地个性化模型与全局模型的距离作为正则项，保证全局模型和本地模型之间的一致性。

2 FedPC模型

2.1 问题阐述

考虑一个拥有n个客户端的联邦学习场景，每个客户端拥有K个类。$\boldsymbol{X}$代表样本的特征空间，$\boldsymbol{y}$代表对应的标签空间，每个客户端的本地模型解耦为特征提取器f_e和分类器f_c。所有客户的样本共享同一个特征空间，分类器将dx维度特征作为输入，得到dy维度的标签预测向量。个性化联邦学习的目标是为每个客户端建立一个本地个性化模型，目标函数为最小化每个客户端的损失，损失权重代表模型本地拥有的数据量占比，客户端的数据量越大，损失权重占比越大。对于参与联邦学习过程的

n个客户，全局优化目标表示为

$$\min \sum_{i=1}^{n} \frac{N_i}{N} L_i(\omega_i; D_i) \tag{1}$$

其中，L_i、ω_i、D_i、N_i分别代表客户端i的损失函数、模型参数、本地数据集、本地数据集的样本数量，N代表所有客户端的样本总数量。

2.2　模型框架

本文提出的FedPC模型框架如图1所示，主要角色包括参与联邦学习的n个客户端和负责聚合任务的中心服务器。FedPC主要包含模型参数初始化、基于原型的客户端聚类、本地模型个性化训练以及服务器参数聚合4个模块。下面将详细介绍FedPC的4个模块。

1) 模型参数初始化

联邦学习开始之前，服务器首先选定参与本次任务的所有客户端$U=\{u_1,u_2,\cdots,u_n\}$。客户端选择完成之后，服务器初始化客户端模型参数，并发送到参与本轮训练的客户端，客户端接收到初始化模型参数之后就开始基于本地数据进行聚类过程和模型训练。

2) 客户端聚类

为了得到更符合每个客户端本地数据分布的个性化模型，本文将客户端本地模型分为两部分：特征提取器和分类器。其中，特征提取器作为原型学习网络来学习每个数据样本的抽象表示，分类器作为本地模型的个性化部分保留在客户端本地。全局参数聚合阶段只需将特征提取部分的参数与本地得到的类原型一起上传到服务器。本文规定客户端i的特征提取器参数为θ_i，特征提取器为$f_e(\theta_i)$，特征提取器得到的输出结果$\boldsymbol{z}$作为输入数据样本x的对应特征表示，即$\boldsymbol{z}=f_e(\theta_i,x)$。将$\boldsymbol{z}$作为分类器$f_c$的输入，得到样本$x$的预测$f_c(\varphi_i,\boldsymbol{z})$，其中$\varphi_i$为客户端$i$的分类器参数。为了更好地捕捉客户端的数据分布特征，本文将客户端数据中属于同一类样本的特征平均表示作为该类样本的抽象表示，即原型。

本文定义$\boldsymbol{P}_i^k$为客户端i属于第k类的数据得到的原型，即

$$\boldsymbol{P}_i^k = \frac{1}{N_i^k} \sum_{x \in D_i^k} f_e(\theta_i,x) \tag{2}$$

其中，D_i^k代表客户端i中属于类k的样本子集，N_i^k代表客户端i中属于类k的样本数量。

为了解决各个客户端数据分布不一致带来的模型性能下降问题，本文采用基于原型的客户端聚类机制将相似数据分布的客户端划分到一个组中，通过层级聚合来解决数据异质性问题，得到个性化联邦学习模型。在本文方法中，第一轮迭代开始之前，参与训练的所有客户端首先将从服务器下载的全局模型解耦为特征提取器和分类器两部分。客户端基于自己的本地数据，使用特征提取器得到每类数据样本的原型，并以此代表该客户端的数据分布，用于之后的聚类过程。将数据分布相似的客户端分为一组，能够有效地捕捉客户端的数据分布特征。在聚类之前，考虑到聚类的计算和时间开销，

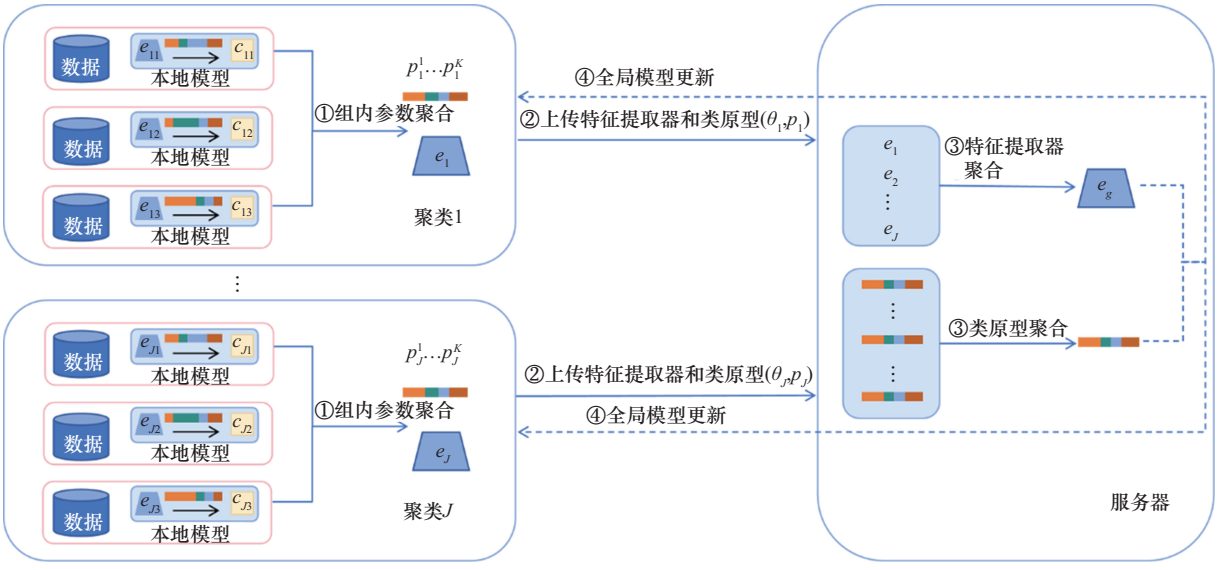

图1　本文提出的FedPC模型框架

FedPC通过对原型采用主成分分析（PCA）降维实现高效聚合，聚类过程采用K-means算法。通过聚类，相似数据分布的客户端被划分到同一组中。之后每个组向服务器上传代表本组客户端的特征提取器参数和类原型向量，用于全局聚合。这样可以实现组间的知识共享，有利于客户端学习到其他组的数据分布。

3) 本地模型个性化训练

在客户端分组后的每一轮训练中，客户端通过下载全局特征提取器和全局原型到本地，进行本轮的特征提取器和分类器训练。由于全局特征提取器中包含其他组的客户端知识，可以使客户端更好地共享组间知识。在本地训练时，对于客户端的原型损失，FedPC尽可能使属于同一类的数据样本表示接近该类的全局原型，而远离其他类的全局原型。客户端i的本地原型与全局原型对比损失定义为

$$L_p = \sum_{k=1}^{K} \text{Distance}\ (P_i^k, P^k) \tag{3}$$

其中，Distance为欧氏距离，K代表客户端数据样本类别数量。

客户端i的损失函数L_i由L_{ce}和L_p构成，系数分别为α和γ，L_{ce}是每个客户端分类任务的交叉熵损失，最终联合优化损失函数定义为

$$L_i = \alpha L_{\text{ce}} + \gamma L_p \tag{4}$$

本文采用L_{ce}和L_p具有相同权重，即α=γ=0.5作为最终联合优化损失函数的系数。

4) 服务器参数聚合

为了减少计算量和通信开销，采用分层聚合算法，组内客户端本地训练完成之后先进行组内特征提取器参数和原型聚合。在得到代表各组内所有客户端特征提取器参数和原型之后，每个组向服务器上传代表本组客户端的特征提取器参数和原型用于之后的全局聚合。分层聚合策略可以实现组间的全局知识共享，有利于客户端学习到其他组数据分布的知识。考虑到每个组对全局模型的贡献度有一定差异，FedPC设计了一种基于原型相似度的组间自适应加权聚合算法，服务器根据每个组上传的原型进行组间相似度计算，然后根据得到的相似度向量计算其他组相对于本组的贡献权重，最终对每组的特征提取器和原型采用自适应加权聚合，得到全局原型和特征提取器。第j组与其他组之间的$1\times J$维相似度向量定义为

$$\boldsymbol{M}_j = \cos\left(P_j, \left[P_1, P_2, \cdots, P_J\right]\right) \tag{5}$$

其中，J为客户端分组总数。基于相似度向量计算第k组相对于本组的聚合权重

$$\rho_j^k = \frac{M_j^k}{\sum_{k=1}^{J} M_j^k} \tag{6}$$

之后服务器端进行自适应加权聚合，第j组的全局原型表示为

$$\boldsymbol{P}_j = \rho_j^1 \boldsymbol{P}_1 + \rho_j^2 \boldsymbol{P}_2 + \cdots + \rho_j^J \boldsymbol{P}_J \tag{7}$$

同理可得第j组的特征提取器参数表示为

$$\theta_j = \rho_j^1 \theta_1 + \rho_j^2 \theta_2 + \cdots + \rho_j^J \theta_J \tag{8}$$

5) 本地模型更新

服务器对原型和特征提取器聚合完成之后，每个客户端下载全局原型和特征提取器参数进行本地更新，开始下一轮的迭代训练，直到模型达到预设的精度阈值或固定迭代次数。

2.3 算法总览

本文提出的FedPC个性化联邦学习算法如算法1所示。

算法1 基于原型聚类的个性化联邦学习算法

输入 客户端集合$U=\{u_1, u_2, \cdots, u_n\}$，全局迭代次数$R$

输出 各客户端本地个性化模型

服务器初始化参数w_g, P_g
for each client i in U do
    $(\theta_i, \varphi_i) \leftarrow w_g$
    P_i= LocalProto (θ_i, D_i) //客户端进行原型表示
end for
$[C_1, C_2, \cdots, C_J]$ = Cluster(P_1, P_2, $\cdots$, P_n) //客户端聚类
for round=0,1, $\cdots$, R−1 do
    for cluster j in $[C_1, C_2, \cdots, C_J]$ do
        for each client i do
            $w_i \leftarrow$ LocalTrain(w_g, P_g)//本地个性化训练
        end for
        组内聚合

13)　　θ_j= IntraAgg(θ_j^1, θ_j^2,⋯, θ_j^i)

14)　　P_j= IntraAgg(P_j^1,P_j^2,⋯, P_j^i)

15)　　end for

16)　　组间聚合

17)　　θ_g= InterAgg(θ_1, θ_2,⋯, θ_j)

18)　　P_g= InterAgg(P_1, P_2,⋯, P_j)

19)　end for

20)　Return w_1, w_2,⋯, w_n

算法1中，IntraAgg( )为客户端组内聚合函数，对组内客户端的原型和特征提取器参数进行平均聚合，θ_j^1, θ_j^2, ⋯, θ_j^i代表第j组所有客户端的特征提取器参数，P_j^1, P_j^2,⋯, P_j^i代表第j组所有客户端的原型。InterAgg( )为组间聚合函数，采用基于式(5)~式(8)的自适应加权策略，θ_1, θ_2, ⋯, θ_j代表第j组本组的特征提取器参数，P_1, P_2, ⋯, P_j代表第j组本组的原型。

3　实验

为了验证FedPC方法的有效性，本节在不同分类任务的图片数据集上进行实验，并与其他基线方法进行比较及分析。

3.1　实验数据

本文在3个广泛研究并采用的基准图片分类数据集Cifar10、Cifar100和FMNIST上进行FedPC方法有效性的验证，数据集的统计结果如表1所示，下面详细介绍每个数据集。

1) Cifar10数据集

Cifar10数据集包含60 000张32×32大小的彩色图像，分为10个类别，每个类别有6 000张图像，图像类别涵盖飞机、汽车、鸟类、猫、鹿、狗、青蛙、马、船和卡车。数据集被分为50 000张训练图像和10 000张测试图像。

2) Cifar100数据集

Cifar100数据集是Cifar10的扩展版本，包含60 000张32×32大小的彩色图像，数据集分为100个类别，其中每个类别有600张图像。与Cifar10相比，Cifar100的类别更加细分，每个类别的图像数量较少。数据集被分为50 000张训练图像和10 000张测试图像。

3) FMNIST数据集

FMNIST数据集包含70 000张28×28大小的灰度图像，分为10个类别，每个类别有7 000张图像，图像类别涵盖T恤、裤子、连衣裙、外套、凉鞋、衬衫、运动鞋、包、踝靴和连体衣。数据集被分为60 000张训练图像和10 000张测试图像。

表1　数据集统计结果

数据集名称	训练集/张	测试集/张	类别数/个
Cifar10	50 000	10 000	10
Cifar100	50 000	10 000	100
FMNIST	60 000	10 000	10

3.2　实验设置

1) 实现细节

在本文的实验设置中，使用卷积神经网络（CNN）来进行本地模型训练，其中包含两层卷积层和三层线性层。本文将前四层作为本地客户端的特征提取器部分，将最后一层线性层作为本地的分类器保留在本地而不上传到服务器，只上传客户端的特征提取器参数进行聚合。为了验证客户端对数据异质性的性能，本文使用迪利克雷分布模拟客户端数据不均衡的场景，其中参数β代表不同的数据分布异质性，β的大小和异质程度成反比，采用β=0.3和β=1.0来进行实验，使客户具有不同的类分布和样本数量。实验中设置100个客户端，每个客户的数据不重叠，数量也各不相同。对于每个客户本地的数据集划分，75%的数据用于训练，25%的数据用于测试，批量大小设置为10，本地训练epoch=5，进行200轮迭代，具体实验环境配置和模型参数配置分别如表2和表3所示。

表2　实验环境配置

实验环境	具体配置
操作系统	Windows11
CPU	Intel(R)Core(TM)i9-13900H 2.60 GHz
内存	16 GB
硬盘	950 GB
开发框架	PyTorch 1.11.0

2) 基线模型

本文将FedPC与6个联邦学习基线模型进行比较，包括FedAvg[4]、FedProto[20]、FedNH[19]、FedRep[8]、FedPer[22]和Ditto[23]。

表3 模型参数配置

参数	取值
优化算法	Adam
学习率	0.001
编码器层数	5
分布β	0.3、1.0
客户端数量	100
批次大小	10
全局轮数	200
原型维度	192
本地epoch	5

基于参数优化的联邦学习策略。FedAvg将本地模型的参数或梯度更新发送给服务器，服务器收到所有客户端的更新后，进行平均聚合来更新全局模型，并返回给客户端。Ditto在客户端本地同时更新全局模型和本地模型，通过引入一个正则化项来限制个性化模型与全局模型的偏离。FedPer允许每个客户端在全局模型的基础上，进一步针对客户端的本地数据进行微调，优化本地的个性化模型。

基于参数解耦的联邦学习策略。FedRep通过学习一个跨客户端共享的特征提取器，同时为每个客户端学习一个独特的本地头部。FedNH通过参数解耦和为分类器平滑地融入类别语义信息来提高模型在本地任务上的性能。

基于原型学习的联邦学习策略。FedProto向服务器上传客户端原型来指导本地模型训练，使本地原型靠近全局原型。

3) 评价指标

本文通过GM、PM(V)、PM(L)3个指标来比较模型的综合性能，其中，GM为全局模型的准确率，PM(V)通过为所有出现的类分配相等的权重来报告个性化模型性能，PM(L)通过假设训练和测试数据集具有相同的分布来报告个性化模型性能。最终结果采用平均准确率进行比较，通过对相同的随机因子进行3次实验得到平均值，并将其作为最终本地模型准确率来评价模型的平均性能。

3.3 结果和分析

本节将对不同non-IID场景下基于原型聚类机制的FedPC算法与基线模型的性能进行比较。

Cifar10、Cifar100和FMNIST数据集的不同数据异质性程度下各模型的GM、PM(V)、PM(L)值如表4所示。从表4可以看到，FedPC在3个指标上都达到最高的准确率。实验中，不同数据non-IID分布场景值下FedPC的准确率相较于其他模型提升5%~8%，获得了较高的准确率。FedPC的准确率在FMNIST数据集和Cifar10数据集β=0.3数据异质性场景下相对最优模型准确率提升较大，分别提升了4.1%和7.2%。在β=1.0数据分布场景下，由于各客户端数据异质性差异较小，FedPC在Cifar10、Cifar100和FMNIST数据集相对最优模型分别提升了0.6%、1.7%和2.8%。

在客户端数据异质性较高（β=0.3）情况下，FedAvg、FedRep和Ditto策略对全局参数根据样本数量进行加权平均，可能无法充分捕捉每个客户端数据的分布特征差异。FedProto仅通过原型知识来指导本地训练，没有考虑其他客户端的数据异质性对全局原型的不同贡献，导致全局原型有一定的倾向性，在客户端数量较多时与FedPC相比模型准确率较低。FedNH虽然也引入了原型进行模型训练，但是对特征提取器进行平均聚合，没有考虑到其他客户端的贡献度。FedPer将模型解耦为全局模型和局部模型，由于客户端数据分布差异较大，仅依赖本地数据训练的局部模型缺乏跨客户端的知识经验，因此模型性能较低。

由于Cifar100数据集的分类难度较大，且在β=0.3的数据异质性场景下，数据分布的复杂性进一步增加，这使模型的训练和优化面临更大的挑战。尽管如此，FedPC模型的准确率仍高于当前最优的FedNH模型2%。这一结果表明，FedPC在处理多分类问题时采用的客户端聚类机制和自适应加权聚合机制，能够充分学习组间、组内客户端的知识经验和数据分布，一定程度上降低数据异质性带来的影响，提升客户端个性化模型的性能。

在客户端数据异质性较低（β=1.0）的情况下，可以看到，不同数据集中FedAvg、FedPer、Ditto和FedNH对全局模型采用平均聚合得到的全局模型相对于原型中所含知识较多，准确率比单一根据原型优化的FedProto和本地顺序个性化训练的FedRep要高。

图2~图7分别表示不同模型随着训练迭代轮数的准确率变化。由图2和图3、图6和图7可以看

表 4　不同数据集下各模型准确率

数据集	方法	β=0.3			β=1.0		
		GM	PM(V)	PM(L)	GM	PM(V)	PM(L)
Cifar10	FedAvg	66.4%	63.1%	84.0%	73.0%	68.0%	79.1%
	FedProto	—	41.4%	68.3%	—	39.6%	53.2%
	FedNH	69.0%	65.0%	84.6%	75.4%	69.6%	79.5%
	FedRep	40.1%	56.4%	80.2%	47.9%	55.0%	68.9%
	FedPer	61.5%	59.6%	82.4%	63.3%	60.6%	73.4%
	Ditto	66.4%	53.6%	80.8%	73.0%	61.2%	74.7%
	FedPC	**77.3**%	**72.2**%	**85.6**%	**77.6**%	**73.1**%	**80.1**%
Cifar100	FedAvg	35.1%	31.8%	50.7%	36.0%	28.8%	38.3%
	FedProto	—	10.6%	19.1%	—	9.2%	12.6%
	FedNH	41.3%	38.2%	55.2%	43.1%	36.8%	45.4%
	FedRep	5.4%	13.5%	29.45%	6.3%	9.4%	16.0%
	FedPer	15.0%	16.1%	33.1%	14.6%	11.6%	19.0%
	Ditto	35.1%	26.1%	45.9%	36.0%	22.9%	32.8%
	FedPC	**43.3**%	**40.1**%	**57.0**%	**45.1**%	**41.3**%	**47.1**%
FMNIST	FedAvg	76.3%	75.6%	81.3%	85.4%	84.3%	87.2%
	FedProto	—	76.3%	84.5%	—	85.3%	87.9%
	FedNH	83.7%	78.1%	85.3%	88.4%	84.1%	87.0%
	FedRep	80.7%	81.5%	84.7%	87.0%	84.5%	87.3%
	FedPer	84.5%	84.5%	87.1%	88.1%	86.7%	87.2%
	Ditto	85.4%	82.2%	87.6%	87.5%	85.0%	86.4%
	FedPC	**89.5**%	**88.6**%	**92.9**%	**90.8**%	**88.4**%	**90.7**%

出，对于分类难度较低的数据集 FMNIST 和 Cifar10，各个模型的准确率较高。由图 4 和图 5 可以看出，在分类难度较高的 Cifar100 数据集中，模型 FedProto、FedPer 和 FedRep 在两种不同数据异质性场景下的模型准确率较低。对于 Ditto 和 FedAvg，在训练过程中，由于得到的是完整的模型参数或者梯度更新，包含的知识经验相对于模型解耦的 FedPer 和 FedRep 以及单一原型指导本地训练的 FedProto 所含的知识经验较多，模型准确率较高。FedNH 通过原型知识和全局特征提取器能够较好地捕获客户端知识经验，但缺乏捕获相似客户端数据分布的潜在知识，模型性能相对 FedPC 较低。

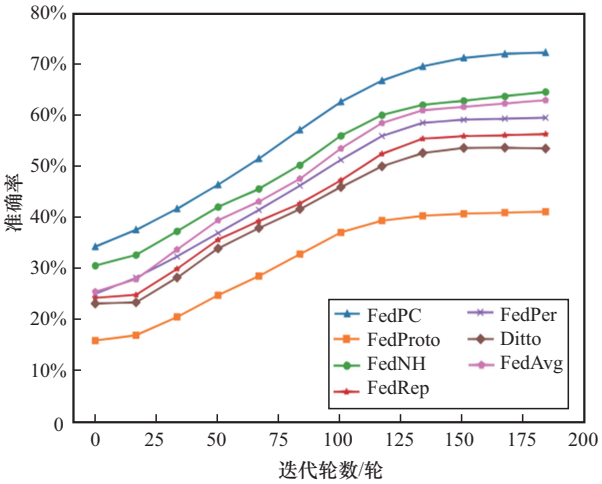

图 2　Cifar10 数据集 β=0.3 模型准确率

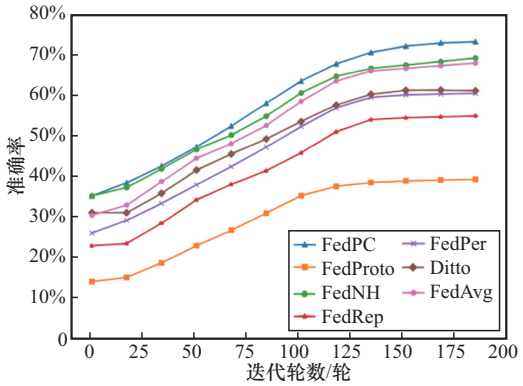

图3　Cifar10 数据集β=1.0 模型准确率

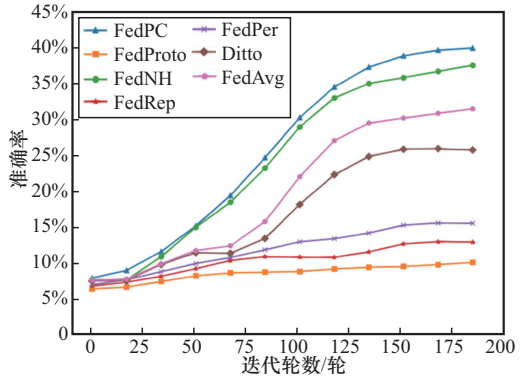

图4　Cifar100 数据集β=0.3 模型准确率

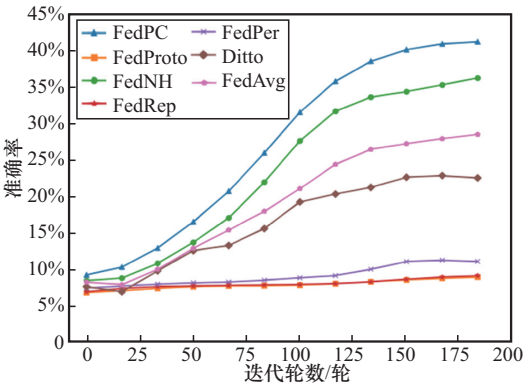

图5　Cifar100 数据集β=1.0 模型准确率

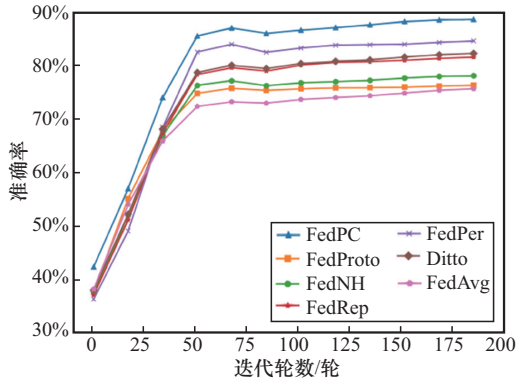

图6　FMNIST 数据集β=0.3 模型准确率

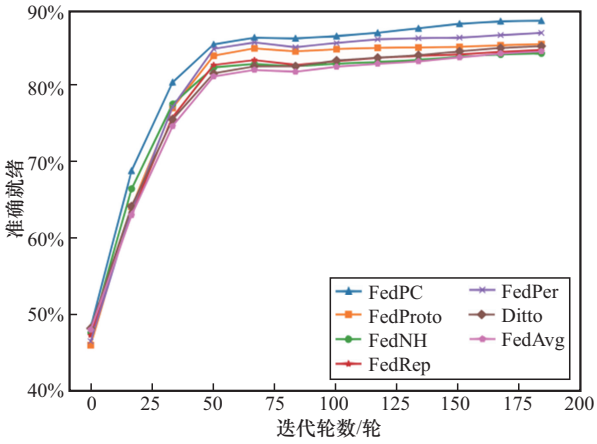

图7　FMNIST 数据集β=1.0 模型准确率

4　结束语

针对个性化联邦学习中的数据异质性问题，本文提出了一种基于原型聚类机制的个性化联邦学习方法FedPC，首先通过客户端原型将具有相似数据分布的客户端聚类为一组，之后对每组聚合后的特征提取器参数和原型进行组间自适应加权聚合得到全局特征提取器和全局原型，提升了本地个性化模型的性能，减轻了客户端数据非独立同分布问题对个性化联邦学习过程的影响。

FedPC 通过原型聚类机制减轻了客户端数据非独立同分布问题对个性化联邦学习过程的影响，在多个数据集上表现出色，然而存在一定的局限性。FedPC 对动态客户端场景的适应性需要进一步研究。在通信参数的安全性方面，原型传输过程中也存在一定的隐私风险。在未来的工作中，本文将进一步探索应用同态加密或安全多方计算等密码学技术来进一步提升通信参数在个性化联邦学习过程中的安全性，实现高效的加密原型传输方案。同时将探索跨模态原型表示学习，实现对非结构化数据（如文本）的适应性。

参考文献：

[1] MCMAHAN B, MOORE E, RAMAGE D, et al. Communication-efficient learning of deep networks from decentralized data[C]//Proceedings of the 20th International Conference on Artificial Intelligence and Statistics (AISTATS). Massachusetts: MIT Press, 2017: 54.

[2] ABDELMONIEM A M, HO C Y, PAPAGEORGIOU P, et al. A comprehensive empirical study of heterogeneity in federated learning[J]. IEEE Internet of Things Journal, 2023, 10(16): 14071-14083.

[3] NG D, LAN X, YAO M M, et al. Federated learning: a collaborative effort to achieve better medical imaging models for individual sites that

have small labelled datasets[J]. Quantitative Imaging in Medicine and Surgery, 2021, 11(2): 852-857.

[4] LIU J X, LOU J, XIONG L, et al. Cross-silo federated learning with record-level personalized differential privacy[C]//Proceedings of the 2024 on ACM SIGSAC Conference on Computer and Communications Security. New York: ACM Press, 2024: 303-317.

[5] TANG Z W, XU S W, JIN H Z, et al. Personalized federated learning via decoupling self-knowledge distillation and global adaptive aggregation[J]. Multimedia Systems, 2025, 31(2): 131.

[6] JIANG Y L, WANG D, SONG B, et al. A prototype-assisted clustered federated learning for big data security and privacy preservation[J]. Future Generation Computer Systems, 2024, 161: 376-389.

[7] LI A R, WANG G J, HU M, et al. Joint client-and-sample selection for federated learning via bi-level optimization[J]. IEEE Transactions on Mobile Computing, 2024, 23(12): 15196-15209.

[8] COLLINS L, HASSANI H, MOKHTARI A, et al. Exploiting shared representations for personalized federated learning[C]//Proceedings of the International Conference on Machine Learning. New York: ACM Press, 2021: 2089-2099.

[9] LI X J, SUN S, LIU M, et al. FedCRAC: improving federated classification performance on non-IID data via classifier re-calibration[J]. IEEE Transactions on Mobile Computing, 2025, 24(1): 482-299.

[10] SON H M, KIM M H, CHUNG T M, et al. FedUV: uniformity and variance for heterogeneous federated learning[C]//Proceedings of the 2024 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR). Piscataway: IEEE Press, 2024: 5863-5872.

[11] MORAFAH M. Clustered federated learning: a review[J]. Artificial Intelligence, 2025, 1(23): 331-342.

[12] WANG Z Y, XU H L, LIU J C, et al. Resource-efficient federated learning with hierarchical aggregation in edge computing[C]//Proceedings of the IEEE INFOCOM 2021-IEEE Conference on Computer Communications. Piscataway: IEEE Press, 2021: 1-10.

[13] LIU B Y, GUO Y, CHEN X Q. PFA: privacy-preserving federated adaptation for effective model personalization[J]. arXiv Preprint, arXiv: 2103.01548, 2021.

[14] MA Q P, XU Y, XU H L, et al. FedUC: a unified clustering approach for hierarchical federated learning[J]. IEEE Transactions on Mobile Computing, 2024, 23(10): 9737-9756.

[15] YANG H M, ZHANG X Y, YIN F, et al. Robust classification with convolutional prototype learning[C]//Proceedings of the 2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition. Piscataway: IEEE Press, 2018: 3474-3482.

[16] CHENG Y J, ZHANG W T, ZHANG Z W, et al. SnapCFL: a preclustering-based clustered federated learning framework for data and system heterogeneities[J]. IEEE Transactions on Mobile Computing, 2025, 24(6): 5214-5228.

[17] RUAN Y C, JOE-WONG C. FedSoft: soft clustered federated learning with proximal local updating[J]. Proceedings of the AAAI Conference on Artificial Intelligence, 2022, 36(7): 8124-8131.

[18] LAI Y Y, FU L L, LIAO T C, et al. FedSeProto: learning semantic prototype in federated learning[C]//European Conference on Artificial Intelligence. Berlin: Springer, 2024: 2122-2129.

[19] DAI Y T, CHEN Z Y, LI J N, et al. Tackling data heterogeneity in federated learning with class prototypes[J]. Proceedings of the AAAI Conference on Artificial Intelligence, 2023, 37(6): 7314-7322.

[20] TAN Y, LONG G D, LIU L, et al. FedProto: federated prototype learning across heterogeneous clients[J]. Proceedings of the AAAI Conference on Artificial Intelligence, 2022, 36(8): 8432-8440.

[21] LI Y, LIU X, LI K. A federated learning method based on class prototype guided classifier for long-tailed data[J]. Signal, Image and Video Processing, 2024, 18(12): 8999-9007.

[22] ARIVAZHAGAN M G, AGGARWAL V, SINGH A K, et al. Federated learning with personalization layers[J]. arXiv Preprint, arXiv: 1912.00818, 2019.

[23] LI T, HU S Y, BEIRAMI A, et al. Ditto: Fair and robust federated learning through personalization[C]//Proceedings of the International Conference on Machine Learning. New York: ACM Press, 2021: 6357-6368.

[作者简介]

刘海军（2000– ），男，河北张家口人，石河子大学硕士生，主要研究方向为联邦学习、隐私保护。

王浩龙（2000– ），男，河南商丘人，石河子大学硕士生，主要研究方向为分布式系统、区块链共识算法。

刘雅辉（1979– ），女，新疆石河子人，博士，石河子大学副教授，主要研究方向为数据挖掘、数据库、社会计算和信息安全。

马洪亮（1977– ），男，新疆石河子人，博士，石河子大学副教授，主要研究方向为网络安全、数据安全、人工智能安全和异常检测。