基于近端策略优化的联邦对比降维算法

叶进[1,2)]，杨治韬[1)]，胡慧琳[1)]

[1)] (广西大学计算机与电子信息学院　南宁　530004)
[2)] (广西多媒体通信与网络技术重点实验室　南宁　530004)
(yejin@gxu.edu.cn)

摘　要：对比降维算法因其卓越的视觉聚类分离性能以及准确的邻域结构保持能力，在视觉聚类分析领域具有重要的应用价值。然而在联邦学习场景下，各客户端持有的训练数据往往呈现非独立同分布特征，导致客户端在进行对比降维模型的更新时存在本地偏差。为了缓解这一问题，提出一种联邦对比降维算法。首先通过协同客户端的本地模型训练，提升全局模型在视觉聚类任务中的泛化性；然后通过将模型间的对比损失引入本地目标函数，校正因数据非独立同分布引起的视觉聚类偏差；最后设计了一种基于近端策略优化的自适应温度调节智能体，进一步增强模型对不同数据分布的适应能力。在 3 个公开数据集上的定量实验结果表明，在邻居命中率和 k 近邻分类准确率上，所提算法分别优于基线算法 16%和 9%。

关键词：联邦学习；对比学习；深度强化学习；视觉聚类分析
中图法分类号：TP391.41　　**DOI：**10.3724/SP.J.1089.2025-00252

Federated Contrastive Dimensionality Reduction Based on Proximal Policy Optimization

Ye Jin[1,2)], Yang Zhitao[1)], and Hu Huilin[1)]

[1)] (*School of Computer, Electronics and Information, Guangxi University, Nanning* 530004)
[2)] (*Guangxi Key Laboratory of Multimedia Communications and Network Technology, Nanning* 530004)

Abstract: Contrastive dimensionality reduction (CDR) has demonstrated significant value in visual cluster analysis due to its exceptional capabilities in cluster separation and neighborhood structure preservation. However, in the context of federated learning (FL), the training data held by each client often exhibits non-independent and identically distributed (non-IID) phenomenon, which will lead to local bias when clients update the CDR model. To alleviate this problem, we propose a federated contrastive dimensionality reduction algorithm (FedCDR). First, collaborative training across multiple client models is employed to improve the generalization capability of the model in visual clustering tasks. Second, a model contrastive loss is introduced into the local objective function to mitigate visual clustering bias caused by non-IID data. Finally, an adaptive temperature regulation agent based on proximal policy optimization is designed to further enhance the model's adaptability to different data distributions. Quantitative experiments on three public datasets demonstrate that FedCDR outperforms baselines by 16% in neighbor hit and 9% in *k*-NN classifier accuracy.

Key words: federated learning; contrast learning; deep reinforcement learning; visual cluster analysis

收稿日期：2025-07-04；修回日期：2025-09-06。**基金项目：**国家自然科学基金（U23A20313）。**叶进**（1970—），女，博士，教授，博士生导师，CCF 会员，主要研究方向为区块链、数据挖掘、联邦学习；**杨治韬**（1999—），男，硕士研究生，主要研究方向为联邦学习、可视化；**胡慧琳**（2001—），女，硕士研究生，主要研究方向为联邦学习、数据挖掘。

在大数据分析领域，视觉聚类技术为高维数据的模式识别和结构探索提供了直观、有效的手段，视觉聚类分析通常与降维技术相结合以支持聚类模式的可视化。现有的降维技术大多采用“距离”作为降维的依据，通过数据点对应的二维嵌入点之间的距离表达其相似性[1]，使具有相似特征的数据点能够直观地在二维嵌入空间中形成聚类分布。其中，*t*-SNE[2]和 UMAP[3]被认为是最先进的降维技术[4-5]，但其生成的可视化结果仍然难以清晰地区分所有结构；与之相比，对比降维（contrastive dimensionality reduction，CDR）技术[6]在视觉聚类分离性能和邻域结构保持能力方面显著优于传统算法。但 CDR 模型的聚类性能在类别非均衡的数据集上退化显著，此时单一用户的数据样本往往不足以训练出鲁棒的 CDR 模型，需要考虑多用户协同建模以缓解该现象。

在涉及多方数据协作的应用场景中，各数据持有方通常不愿意直接共享原始数据[7]。在此背景下，联邦学习（federated learning，FL）已经成为解决这一问题的关键技术框架[8-9]。然而，将 CDR 与 FL 框架相结合仍面临一些挑战，其中最关键的是在实际应用场景中，各客户端的训练数据往往呈现非独立同分布（non-independent and identically distributed，non-IID）特性。当 FL 系统面临 non-IID 数据问题时，其全局模型的性能会显著地退化[10]，这是由于客户端之间的数据分布差异，本地模型在训练过程中的更新方向偏离全局优化目标，并使得聚合后的全局模型难以收敛至全局最优解。例如，若某客户端的数据仅包含少数类别，则其本地模型极易过拟合于这些类别的特征，产生背离全局最优解的更新方向。

尽管已有大量研究致力于分布式聚类技术的探索[11-12]，但现有工作聚焦集中式聚类算法的并行或分布式实现，未能有效地缓解 non-IID 数据带来的技术挑战。为了缓解上述问题，本文提出一种基于近端策略优化（proximal policy optimization，PPO）[13]的联邦 CDR 算法（federated CDR，FedCDR），通过将 CDR 算法与 FL 框架相结合，缓解了传统 CDR 算法在非均衡数据集下的性能显著退化的问题；通过优化本地训练机制，缓解 non-IID 数据带来的客户端本地模型的视觉聚类偏差问题。首先在本地训练的目标函数中引入模型对比损失项，通过最小化本地模型与全局模型之间的数据表征差异校正视觉聚类偏差；然后设计一种基于 PPO 的自适应温度调节机制，在对比学习过程中实现温度的动态优化，进一步缓解视觉聚类偏差问题。在多个公开数据集上的实验结果表明，FedCDR 算法的多个聚类性能指标显著优于基线算法；消融实验进一步验证了各模块对算法整体性能提升的有效贡献。

1　相关工作

1.1　视觉聚类分析

视觉聚类分析作为高维数据可视化的重要手段，通常需要与降维技术相结合，通过将高维数据投影到二维空间实现聚类模式的可视化识别[1,14]。清晰的视觉聚类分离和正确的邻域结构保持是视觉聚类分析任务的 2 个重要目的。选择进行视觉聚类分析技术的关键是降维技术的属性，其中，线性与非线性属性最受关注[15]。

主成分分析（principal component analysis，PCA）[16]和因子分析（factor analysis，FA）[17]作为经典的线性降维技术，分别通过保留数据方差和提取潜在变量实现数据降维。这类线性降维技术在保留聚类密度方面具有优势[18]，其本质上是基于数据特征为全局线性的假设，通过线性变换将高维数据投影到低维空间。然而，这种假设在真实数据中往往不成立，线性降维算法构建的邻域关系出现显著失真。

t-SNE[2]和 UMAP[3]是在视觉聚类分析任务中广泛应用的非线性降维技术[19-20]。这类算法都显式或隐式地使用 *k* 最近邻（*k* nearest neighbors，*k*-NN）表示邻域结构，以便能识别高维数据中的非线性关系（如弯曲或嵌套结构），并在低维空间中保持这些关系的拓扑性质。然而，这类算法在低维空间生成的聚类结构往往存在视觉边界模糊的问题，不同类别之间的区分度不足，影响了视觉聚类分析的有效性[21]。

作为一种高效的自监督表示学习算法，对比学习在数据相似性判别方面表现出卓越的性能[22-23]。CDR[6]创新地将对比学习引入降维过程，通过重构损失函数的梯度计算弥补了传统 *k*-NN 的不足，在准确地保持邻域结构的同时，实现了更优秀的视觉聚类分离效果。然而，当前算法对数据分布不均衡表现出明显的敏感性，如何在用户个人数据集非均衡下有效地提升模型聚类性能，仍是亟待突破的关键问题。

1.2　FL

近年来，FL 凭借其去中心化的系统架构及其在隐私保护场景下的适用性，已经成为机器学习领域的重要研究方向[7,24]。联邦平均（federated av-

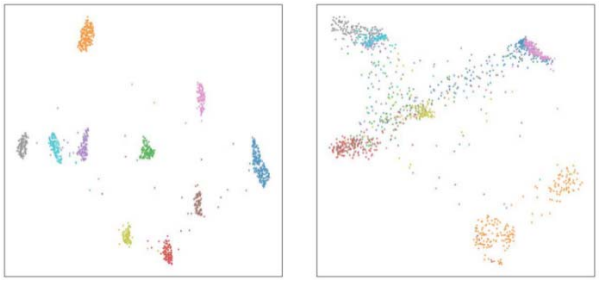
eraging，FedAvg）算法[25]为 FL 的实现提供了基础技术框架，其面临的核心挑战是如何有效地缓解 non-IID 数据导致的模型性能退化问题。针对这一挑战，现有的大量研究集中在优化客户端的本地训练过程。文献[26]从模型的角度出发，通过对每个本地模型进行额外的调整，以缓解 non-IID 数据的问题；文献[27-28]在损失函数中引入约束，平衡本地训练与全局模型泛化性之间的关系；文献[29-30]利用局部数据增强技术，通过生成额外的数据样本扩展本地数据集，构建近似独立同分布的训练环境。这些算法从不同的角度改进本地训练机制，有效地提升了 FL 在 non-IID 数据下的表现；然而，上述技术框架主要面向标记数据的监督学习任务而设计，在未标记数据的无监督学习场景中的适用性存在显著的局限性，甚至可能完全失效。

一些研究在 FL 框架下对未标记数据进行学习[31]。与简单地将 FL 与无监督学习相结合的研究不同，FedCA[32]通过字典模块和对齐模块的设计缓解未标记数据的 non-IID 问题，但其客户端数据的特征共享机制存在隐私泄露的隐患；FedU[33]在保护隐私的前提下，从优化模型聚合的角度抑制参数发散；FedX[34]则采用全局与局部知识蒸馏相结合的方式处理数据偏差问题。与上述算法不同，本文提出的 FedCDR 算法通过引入模型对比损失和设计自适应温度调整机制，从本地训练机制优化的角度缓解 non-IID 的未标记数据带来的挑战。

2 研究背景

为了验证数据分布对 CDR 模型的影响，本文在 USPS 数据集上展开实验。图 1 所示为采用 CDR 算法对 USPS 数据集进行可视化分析结果。实验结果表明，图 1a 中，当用户数据集呈现类别均衡分布特征时，CDR 算法能够实现清晰的视觉聚类分离效果；图 1b 中，在数据集是类别非均衡分布的情况下，其可视聚类的效果显著下降。这一现象说明，由于个体用户数据规模和分布的局限性，因此单独训练往往难以获得理想的模型性能。

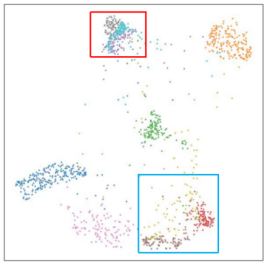
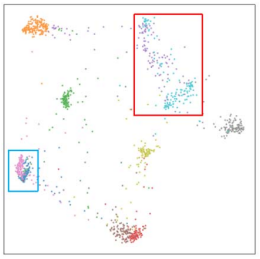
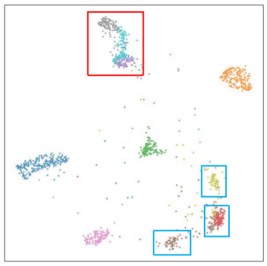
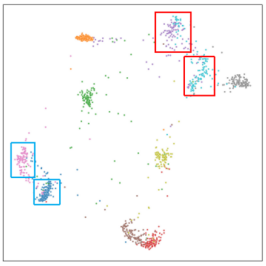
本文采用 Dirichlet 分布构建 non-IID 数据，其中，参数 β 用于控制数据的 non-IID 程度，其值越小，表示数据的 non-IID 程度越显著。实验中，参数配置分别为 $\beta=5.0$ 和 $\beta=1.0$，从训练数据集中抽样生成 5 个子集，并基于这些子集运行 FedAvg 算法；其中，所有客户端使用相同且固定不变的温度计算对比损失，可视化结果如表 1 所示。可以看出，与本地模型相比，全局模型的可视化结果呈现出更大的簇间距离，表明全局模型能够比本地模型学习到更好的特征表示；同时，由于客户端之间的数据分布差异，本地模型存在视觉聚类偏差，且随着数据 non-IID 程度的加剧，这一现象越来越显著。



a. 均衡的数据集　　b. 非均衡的数据集

图 1　使用均衡和非均衡数据集训练的可视化结果

表 1　采用 FedAvg 算法 2 种模型的可视化结果对比

模型	β = 5.0	β = 1.0
本地		
全局		

因此在 non-IID 数据场景下，需要引入模型之间的对比损失缩小本地模型和全局模型在表征学习方面的差异，以缓解客户端本地模型间的视觉聚类偏差，进而避免全局模型陷入局部最优。

3 FedCDR 算法

本文提出的 FedCDR 算法基于 FL 框架，通过 2 个核心模块缓解 non-IID 数据带来的视觉聚类偏差问题：（1）基于本地目标重定义的模型对比（model contrast CDR，MC-CDR）模块。该模块重构了客户端本地训练的目标函数，即通过 CDR 对比损失

实现优秀的聚类分离效果，在此基础上，引入模型对比损失实现本地模型表征学习的对齐。(2) 基于 PPO 的自适应温度调节（adaptive temperature CDR，AT-CDR）模块。通过构建智能体动态地优化对比学习过程中的温度，适配各客户端本地数据的分布特性。FedCDR 算法框架如图 2 所示。在 FL 的初始化阶段，各客户端完成本地模型的随机初始化，并部署专属的 PPO 智能体。

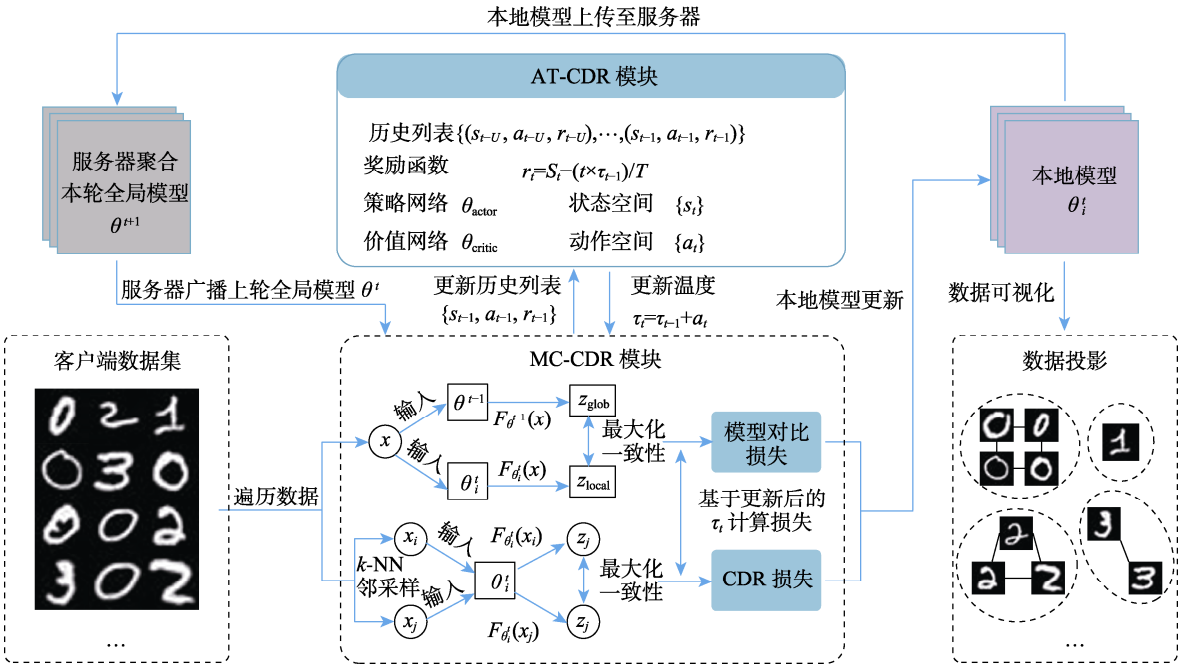


图 2　FedCDR 算法框架

设 P_i 表示参与 FL 的客户端，FedCDR 的第 t 轮本地更新包含 2 个步骤：

Step1：客户端通过 AT-CDR 模块输出动作，实现本轮温度 τ_t 的更新。

Step2：客户端基于调节后的温度 τ_t，通过 MC-CDR 模块训练并更新本地模型。

在客户端 P_i 接收到服务器广播的全局模型 θ^t 后，其 AT-CDR 模块通过与 FL 环境交互地更新历史列表；然后基于历史列表中存储的历史状态、动作和奖励进行策略网络和价值网络的离线自我训练，并根据更新后的策略网络输出动作，实现本轮温度的自适应调节；最后由 MC-CDR 模块结合调节后的温度 τ_t 计算 CDR 损失和模型对比损失，其中，对于从 k-NN 中采样得到的正对数据点，CDR 损失最大化它们通过本地模型得到的表示之间的一致性，而模型对比损失则最大化同一数据点分别通过本地模型和上一轮全局模型得到的表示之间的一致性。这 2 个损失函数共同构成本地训练的目标函数，客户端基于此目标函数完成本地模型的更新。

待所有客户端完成本地更新后，服务器端对本地模型执行联邦平均聚合得到本轮全局模型；不断循环 FL 过程，直至达到预设 FL 总轮次，获得最终全局模型。

3.1　MC-CDR 模块

MC-CDR 模块重新定义了客户端本地训练的目标函数：(1) 通过学习数据特征间的相似性实现聚类分析；(2) 通过对本地模型学习到的表示添加约束，实现对视觉聚类偏差的校正。客户端使用重新定义的本地目标在全局模型的基础上继续训练，得到本轮的本地模型。

下面分别从模型的网络结构和本地目标的重定义 2 个方面介绍 MC-CDR 模块。

3.1.1　网络结构

与 SimCLR[22]类似，该网络由 1 个编码器和 1 个投影头 2 部分组成，其中，编码器从输入中提取表示向量，投影头将表示向量映射到具有固定维度的空间。为了方便起见，设 θ 表示模型参数，$F(\cdot)$ 表示整个网络，$F(x)$ 指由网络产生的输入数据 x 的特征表示。

3.1.2　本地目标的重定义

如图 3 所示，MC-CDR 损失由数据间的对比损失和模型间的对比损失 2 部分组成。其中，数据间的对比损失记为 L_{NT}，本文引入的模型间的对比损失记为 L_{con} [28]。

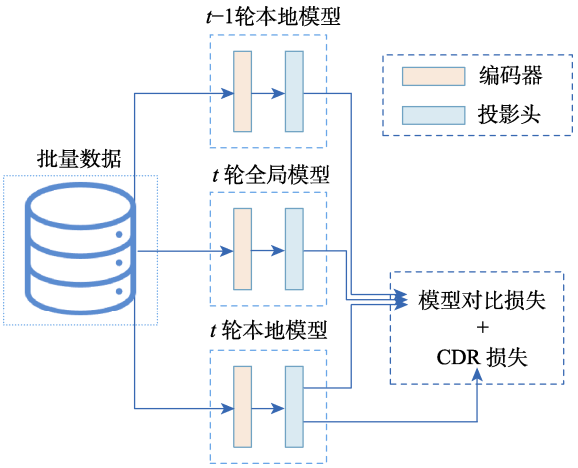


图 3 本地目标重定义

（1）数据间的对比损失 L_{NT}

CDR 基于对比学习，使用正对和负对的概念将高维数据投影到二维嵌入空间中。为了使对比学习能学习到聚类级别的判别而非实例级别的判别，CDR 将属于同一聚类结构中的数据点对指定为正对，而不是将同一个数据点的不同视图指定为正对；其中，点 x_i 同一聚类结构中的数据点抽样于其 k-NN。CDR 还通过指定负对实现不相似数据点的远离。在实际的训练过程中，每批量数据包含 B 个数据点及其对应的正对点，因此每批量数据最终由 $2B$ 个点组成。对于批量数据中的每个点，除去其自身及其对应正对点之外的 $2(B-1)$ 个点都被指定为负对的对应点。

CDR 采用 NT-Xent[35]作为对比损失函数，在一个训练批量中，点 x_i 的 NT-Xent 损失定义为

$$L_{\mathrm{NT}}(x_i)=-\ln\frac{\exp(q_{ij}/\tau)}{\sum_{k=1}^{2B}l_{[k\neq i]}\exp(q_{ij}/\tau)}。$$

其中，$l_{[k\neq i]}\in\{0,1\}$ 为指示函数，当 $k\neq i$ 时取值为 1；τ 表示温度，用于调节模型对数据之间相似性的敏感程度；

$$q_{ij}=\frac{1}{1+a\left(\left\|z_i-z_j\right\|_2^2\right)^b}$$

表示点 z_i 和点 z_j 之间的相似度；z_i 和 z_j 分别表示原始高维空间中的点 x_i 和点 x_j 在低维空间的映射表示。

由于高维空间中一个点的 k-NN 可能包含不同类别的点，因此简单地在低维空间保留所有 k-NN 将保留这些误差。与交叉熵损失相比，L_{NT} 损失增加了温度 τ，有助于加强模型对此类误差的辨别能力。

（2）模型间的对比损失 L_{con}

在第 t 轮 FL 中，客户端 P_i 从服务器接收全局模型 θ^t，并使用本地训练数据将其更新为 θ_i^t。对每个输入数据 x_j，提取 3 种不同的表示形式：a. 全局模型 θ^t 学习到的表示 $z_{\mathrm{glob}}=F_{\theta^t}(x_j)$；b. 上一轮的本地模型 θ_i^{t-1} 学习到的表示 $z_{\mathrm{prev}}=F_{\theta_i^{t-1}}(x_j)$；c. 当前的本地模型 θ_i^t 学习到的表示 $z=F_{\theta_i^t}(x_j)$。由于全局模型能学习到更准确的表示，因此 L_{con} 的目标是最小化 z 和 z_{glob} 之间的距离，同时最大化 z 和 z_{prev} 之间的距离。L_{con} 定义为

$$L_{\mathrm{con}}=-\ln\frac{\exp\left(S\left(z,z_{\mathrm{glob}}\right)/\tau\right)}{\exp\left(S\left(z,z_{\mathrm{glob}}\right)/\tau\right)+\exp\left(S\left(z,z_{\mathrm{prev}}\right)/\tau\right)}。$$

其中，τ 表示温度，用于调节 z 向 z_{glob} 靠近的速度；$S(\cdot,\cdot)$ 表示 2 个模型学习到的表示之间的相似度。因此，对于输入数据 x_j 的 MC-CDR 损失计算公式为

$$L=L_{\mathrm{NT}}(\theta_i^t,x_j)+\mu L_{\mathrm{con}}(\theta_i^t,\theta_i^{t-1},\theta^t,x_j)。$$

其中，μ 表示控制模型对比损失权重的超参数。本地目标是最小化

$$E_{x_j}\left[L_{\mathrm{NT}}(\theta_i^t,x_j)+\mu L_{\mathrm{con}}(\theta_i^t,\theta_i^{t-1},\theta^t,x_j)\right]。$$

3.2 AT-CDR 模块

在 FedCDR 算法中，L_{NT} 和 L_{con} 都受到温度 τ 的影响，温度越低，本地训练时对数据相似性的敏感性越高，并且本地模型学习到的表示靠近全局模型的速度越快。然而，集中式 CDR 算法中的温度通常设置为全局固定值，难以适配 FL 场景下客户端间具有显著差异的数据分布，甚至进一步加剧客户端的本地模型的视觉聚类偏差[36]。深度强化学习结合强化学习与深度学习各自的优势，能够有效地完成复杂策略的探索任务。其中，PPO 算法因其强大的稳定性和高计算效率，成为实现自适应温度调节机制的理想选择。本文基于 PPO 算法构建智能体，使得各个客户端能够根据其所处的状态动态地优化本地训练的温度，以缓解本地模型的视觉聚类偏差，并提高全局模型的性能。

下面分别从智能体的设计和智能体的部署 2 个方面介绍 AT-CDR 模块。

3.2.1 智能体的设计

本文中，各客户端动态地调节其温度的策略由

一个智能体控制。

（1）状态空间

状态 s_t 是智能体对其所在的 FL 环境的描述，定义为 $s_t=\{t,S_t,\tau_t,L_t\}$。其中 t 表示 FL 的通信轮次；S_t 表示第 t 轮本地模型参数与全局模型参数之间的相似度，在 FL 场景中，由于模型参数的方向一致性比绝对值差异更重要，因此本文使用余弦相似度度量模型参数间的相似度；τ_t 表示第 t 轮本客户端所使用的温度；L_t 表示第 t 轮本地模型的损失。

（2）动作空间

动作 a_t 由智能体根据状态产生，负责控制如何调节温度 τ。本文中，智能体的动作空间由一组离散值组成，控制温度的调节方向，定义为

$$a_t\in\{-0.1,0,0.1\}。$$

智能体每次与环境进行交互时，都根据状态选择一个动作，新的温度由动作决定。本文将温度的范围限制在 $[0.2,1.0]$，防止温度失控。

（3）奖励函数

奖励 r_t 为智能体的行动提供明确的反馈，其引导智能体的学习向优化目标靠近。本文的优化目标是尽可能地减小本地模型与全局模型之间的偏差，因此模型相似度是奖励函数的重要组成部分之一。

在训练初期若使用过小的温度可能导致模型过拟合；同时，FL 初期的全局模型可能表现不佳，过早地使本地模型很快地靠近全局模型可能陷入局部最优。因此，本文在 FL 初期使用较高的温度，并随着通信轮次的增加使温度逐渐变低，在提高模型对数据相似性的敏感性的同时，逐步加快本地模型靠近全局模型的速度。奖励函数定义为

$$r_t=S_t-\frac{t\times\tau_{t-1}}{T}。$$

其中，T 表示 FL 的总轮数。

（4）历史列表

每个智能体独立地维护一个历史列表 h_t，其中保存了若干轮智能体的历史信息用于更新智能体的神经网络。历史列表定义为

$$h_t=\left[\left\langle s_{t-U+1},a_{t-U+1},r_{t-U+1}\right\rangle,\cdots,\left\langle s_t,a_t,r_t\right\rangle\right]。$$

其中，U 表示历史列表的长度。

3.2.2　智能体的部署

（1）智能体的初始化

在 FL 的初始化阶段，客户端在本地初始化各自的智能体。智能体之间各自维护相互独立的神经网络与历史列表，并独立地完成更新。所有客户端使用的温度初始化为一个较大值 τ_0。

（2）神经网络的更新

本文中，智能体基于 PPO 算法实现自我训练获得最优策略 Π。PPO 定义了策略网络和价值网络 2 种类型的神经网络，其中，策略网络参数设为 θ_{actor}，价值网络参数设为 θ_{critic}。

在第 t 轮 FL 中，智能体通过与 FL 环境交互更新历史列表，并开始更新神经网络。策略网络的损失函数定义为

$$L_{\text{actor}}=E_{s,a}\left[\min\left(\frac{\Pi_k(a|\mathrm{s})}{\Pi_{k-1}(a|\mathrm{s})}A_{s,a},C\left(\frac{\Pi_k(a|\mathrm{s})}{\Pi_{k-1}(a|\mathrm{s})},1-\delta,1+\delta\right)A_{s,a}\right)\right]。$$

其中，Π_{k-1} 和 Π_k 分别表示原策略和新策略；C 表示裁剪函数，δ 表示裁剪参数；A 表示优势函数。价值网络的损失函数定义为

$$L_{\text{critic}}=E_{s,a}\left[\left(\gamma V(s_{t+1})+r_t-V(s_t)\right)^2\right]。$$

策略网络和价值网络的更新公式为

$$\theta_{t,i}^{\text{actor}}=\theta_{t,i}^{\text{actor}}-\eta_{\text{a}}\nabla L_{\text{actor}}，$$

$$\theta_{t,i}^{\text{critic}}=\theta_{t,i}^{\text{critic}}-\eta_{\text{c}}\nabla L_{\text{critic}}。$$

其中，η_{a} 和 η_{c} 分别表示 2 个网络的学习率。

（3）温度的调节

完成策略网络和价值网络的更新后，各客户端的智能体根据策略网络以及当前状态选择本轮动作 a_t，并基于 a_t 得到本轮温度 τ_t，即 $\tau_t=\tau_{t-1}+a_t$；然后，客户端使用调节后的温度 τ_t 完成本轮本地训练。

4　收敛性分析

本节对 FedCDR 算法进行收敛性分析，探讨 PPO 与联邦聚合的交互作用对全局模型收敛的影响，并在标准光滑性假设下推导算法的理论边界。

4.1　模型定义

FL 的通信轮次 $t\in[0,T-1]$ 共 T 轮。第 t 轮开始时，服务器广播的全局模型为 θ^t（由第 $t-1$ 轮本地模型聚合得到）。第 t 轮客户端 P_i 训练得到的本地模型为 θ_i^t（由客户端 P_i 基于 θ^t 训练后得到）。其本地更新公式为 $\theta_i^t=\theta^t-\eta\nabla f^i\left(\theta^t\right)$。其中，$\eta$ 表示学习率。第 t 轮全局模型聚合公式为 $\theta^{t+1}=\frac{1}{N}\sum_{i=1}^{N}\theta_i^t$。其中，$N$ 表示客户端总数。

客户端 P_i 的本地目标函数为

$$f^i(\theta)=L^i_{\mathrm{NT}}(\theta)+\mu L^i_{\mathrm{con}}(\theta,\theta^t)。$$

其中，μ 表示权重参数，$\mu>0$。

FedCDR 的全局优化目标为

$$f(\theta^{t+1})=\frac{1}{N}\sum_{i=1}^{N}f^i(\theta_i^t)。$$

4.2 核心假设

假设 1：连续性和光滑性。$f^i(\cdot)$ 满足 R-Smooth 和 G-Lipschitz 条件，即对任意 θ_1 与 θ_2 满足

$$\left\|\nabla f^i(\theta_1)-\nabla f^i(\theta_2)\right\|\leqslant R\|\theta_1-\theta_2\|,$$

$$\left|f^i(\theta_1)-f^i(\theta_2)\right|\leqslant G\|\theta_1-\theta_2\|。$$

其中，G 表示函数值变化率的最大上界；R 表示光滑常数；客户端学习率 η 满足 $0<\eta\leqslant 1/R$。

假设 2：梯度有界性。模型对比损失 $L^i_{\mathrm{con}}(\theta,\theta^t)$ 的梯度有界，即存在常数 M 使得 $\left\|\nabla L^i_{\mathrm{con}}(\theta,\theta^t)\right\|\leqslant M$。

假设 3：温度调节约束。PPO 动态调节的温度参数 τ 满足有界性 $\tau_{\min}\leqslant\tau\leqslant\tau_{\max}$；相邻通信轮次间温度变化步长 $|\tau_t-\tau_{t-1}|\leqslant\Delta\tau$，其中，$\Delta\tau$ 是一个小常数量。温度调节带来的目标函数值变化率上界为一个常数，即存在常数，$C>0$ 使得 $\left\|\nabla f^i_\tau(\theta)\right\|\leqslant C\Delta\tau$。

4.3 收敛性定理与证明

定理 1：在假设成立的条件下，若总通信轮次 T 满足

$$T\geqslant O\left(\frac{f(\theta^0)-f(\theta^*)-\varepsilon}{\eta\left(1-\frac{R\eta}{2}\right)(G+\mu M+C\Delta\tau)^2}\right),$$

则 FedCDR 收敛到模型的 ε-近似最优解 θ^*，即 $E\left[f(\theta^T)\right]\leqslant f(\theta^*)+\varepsilon$。

证明：由假设 1 的 R-Smooth 条件可得

$$f^i(\theta_1)\leqslant f^i(\theta_2)+\left\langle\nabla f^i(\theta_2),\theta_1-\theta_2\right\rangle+\frac{R}{2}\|\theta_1-\theta_2\|。$$

取 $\theta_1=\theta^t$，$\theta_2=\theta_i^t$，结合本地更新公式可得

$$f^i(\theta_i^t)\leqslant f^i(\theta^t)-\eta\left(1-\frac{R\eta}{2}\right)\left\|\nabla f^i(\theta^t)\right\|^2 \quad (1)$$

将全局优化目标结合式（1）可得

$$f(\theta^{t+1})\leqslant \frac{1}{N}\sum_{i=1}^{N}f^i(\theta^t)-\eta\left(1-\frac{R\eta}{2}\right)\frac{1}{N}\sum_{i=1}^{N}\left\|\nabla f^i(\theta^t)\right\|^2 \quad (2)$$

由 $\frac{1}{N}\sum_{i=1}^{N}f^i(\theta^t)\leqslant\frac{1}{N}\sum_{i=1}^{N}f^i(\theta_i^{t-1})=f(\theta^t)$，结合式（2）可得

$$f(\theta^{t+1})\leqslant f(\theta^t)-\eta\left(1-\frac{R\eta}{2}\right)\frac{1}{N}\sum_{i=1}^{N}\left\|\nabla f^i(\theta^t)\right\|^2 \quad (3)$$

结合假设 1 和假设 2 并考虑假设 3 中温度调节的影响，结合式（3）可得

$$f(\theta^{t+1})\leqslant f(\theta^t)-\eta\left(1-\frac{R\eta}{2}\right)(G+\mu M+C\Delta\tau)^2 \quad (4)$$

对式（4）两边从 $t=0$ 到 $T-1$ 累加并化简，可得

$$f(\theta^T)\leqslant f(\theta^0)-T\eta\left(1-\frac{R\eta}{2}\right)(G+\mu M+C\Delta\tau)^2 \quad (5)$$

对式（5）取期望并令 $f(\theta^*)$ 为最优值，可得

$$E\left[f(\theta^T)\right]\leqslant f(\theta^*)+f(\theta^0)-f(\theta^*)-T\eta\left(1-\frac{R\eta}{2}\right)(G+\mu M+C\Delta\tau)^2。$$

令

$$f(\theta^0)-f(\theta^*)-T\eta\left(1-\frac{R\eta}{2}\right)(G+\mu M+C\Delta\tau)^2\leqslant\varepsilon,$$

则达到误差阈值 ε 需要 T 的量级为

$$T\geqslant O\left(\frac{f(\theta^0)-f(\theta^*)-\varepsilon}{\eta\left(1-\frac{R\eta}{2}\right)(G+\mu M+C\Delta\tau)^2}\right)。$$

证毕。

5 实验及结果分析

5.1 实验设置

5.1.1 数据集和分布差异

本文基于 3 个公开数据集进行实验，包括图像数据集 USPS、文本数据集 Texture 和表格数据集 WiFi。与文献[37]一样，本文采用 Dirichlet 分布生成 non-IID 数据，并使用参数 β 控制数据的 non-IID 程度（默认 $\beta=0.5$）。

5.1.2 实验细节和评估指标

本文基于 PyTorch 实现了 FedCDR 和其他基线算法。在同一个实验中，所有算法都使用相同的超参数，以确保它们得到公平的比较。

为了准确地评估全局模型的性能，本文使用可信度、连续性[38]、邻居命中率[39]和 k-NN 分类准确率[40]评估各算法的全局模型性能。

（1）可信度衡量嵌入空间的局部结构在原始高维空间中的保留程度；

（2）连续性衡量原始高维空间的局部结构在嵌入空间中的保留程度；

（3）邻居命中率衡量嵌入空间中数据点的局部结构与其在原始高维空间中的局部结构的相似程度；

（4）k-NN 分类准确率衡量在嵌入空间中基于 k-NN 分类器的精度。

这 4 个指标归一化为 $[0,1]$，便于后续的处理和比较，数值越高表示性能越好。

5.2　对比实验

将 FedCDR 与 2 种经典算法进行对比实验，包括 FedAvg[25]和 FedProx[27]。此外，还比较了一种名为 SOLO 的基线算法，其中，每个客户端都使用本地数据训练模型而不参与 FL，最终的性能取所有客户端本地模型性能的平均值。

5.2.1　降维技术指标对比

在 non-IID 数据背景下，将 FedCDR 与其他基线算法进行对比。使用 $\beta = 0.5$ 的 Dirichlet 分布从公共数据集中抽样，为 5 个客户端构建本地训练数据集。实验中，每个客户端执行 100 个通信轮次，每轮通信中客户端执行 10 个本地训练轮次。

在 3 个数据集上，将 6 种算法训练得到的全局模型进行比较，结果如表 2 所示。可以看出，其中，SOLO 的结果最差，说明了 FL 的优势；在所有 FL 算法中，FedAvg[25]的性能相对较低，这是由于 FedAvg[25]没有针对 non-IID 设置进行任何优化；在所有数据集上，FedCDR 算法的可信度、邻居命中率和 k-NN 分类准确率都优于对比算法，说明该算法提高了邻域精度和纠正错误邻域的能力。

表 2　3 个数据集上 6 种算法的评估指标对比

算法	可信度			连续性			邻居命中率			k-NN 分类准确率		
	USPS	WiFi	Texture	USPS	WiFi	Texture	USPS	WiFi	Texture	USPS	WiFi	Texture
SOLO	0.845 85	0.886 80	0.944 59	0.901 49	0.889 41	0.947 44	0.624 52	0.838 50	0.693 62	0.738 30	0.892 21	0.789 59
FedAvg[25]	0.869 12	0.929 90	0.967 75	0.908 06	0.923 93	0.954 03	0.641 70	0.915 76	0.698 00	0.760 50	0.938 00	0.796 83
FedProx[27]	0.875 89	0.932 81	0.964 55	0.912 42	0.934 39	0.953 59	0.691 17	0.932 33	0.701 01	0.789 25	0.945 79	0.795 47
MC-CDR	0.874 28	0.934 50	0.967 57	0.908 35	0.930 92	0.960 11	0.673 81	0.927 44	0.718 07	0.783 53	0.945 79	0.803 84
AT-CDR	0.896 25	0.943 72	0.975 91	**0.937 78**	0.941 01	0.966 01	0.723 07	0.931 71	0.740 93	0.823 86	0.946 73	0.828 73
FedCDR	**0.903 28**	**0.945 98**	**0.981 45**	0.931 22	**0.944 27**	**0.968 91**	**0.744 52**	**0.940 62**	**0.754 84**	**0.831 12**	**0.955 14**	**0.842 53**

注：粗体表示最优值。

5.2.2　T 的影响

5 种算法在 USPS 数据集上进行训练的过程中，全局模型性能随 T 变化的对比如图 4 所示。可以看出，与其他算法相比，FedCDR 和 AT-CDR 在模型达到收敛时表现更好，说明本文提出的自适应温度调节机制有利于提高全局模型性能，防止其陷入局部最优；与其他算法相比，FedCDR 的收敛速度更快，这是由于加入模型对比损失后，FedCDR 更早地开始纠正 non-IID 数据带来的视觉聚类偏差。

5.2.3　β 的影响

在 USPS 数据集上，使用不同 β 的 Dirichlet 分布构造数据集进行实验，评估数据分布差异对各种算法的影响，结果如表 3 所示。从中可以得出结论，随着 non-IID 的程度逐渐加深，3 种算法的性能都有不同程度的下降，但本文算法相较于其他算法依然保持了最优秀的性能。

5.2.4　N 的影响

在 USPS 数据集上，对 FedCDR 在客户端数量 N 变化时是否仍能保持有效性进行实验，结果如表 4 所示。可以看出，随着参与 FL 的客户端数量增加，所有算法的全局模型性能均有所提升，这主要得益于客户端数量增加所带来的训练数据规模扩大；与基线算法相比，FedCDR 训练出的全局模型仍然保持了最佳性能，表明该算法在面对客户端数量变化时具有较强的稳健性。

5.3　模块有效性验证

5.3.1　PPO 与其他温度策略的比较

通过实验，探究不同的温度策略对 FedCDR 的影响，验证 AT-CDR 模块的有效性，结果如表 5 所示。其中，涉及的温度策略包括 3 个使用静态温度的策略（0.2，0.6 和 1.0），以及一个名为线性衰减的策略。在线性衰减策略中，温度的初始值被设置为 1.0，并以每 10 个通信轮次下降 0.1 的速度衰减。可以看出，线性衰减策略的表现一般，静态温度时 $\tau = 0.2$ 能实现不错的性能；PPO 策略优于所有的静态温度策略，这可能是由于这些策略都是客户端共用一个静态或者线性衰减的温度，而非如同 PPO 一样客户端独立调节温度，表明了 PPO 在面对 non-IID 数据时的优势。

5.3.2　模型对比损失的有效性分析

在 USPS 数据集上，经过相同 T 的训练后，对 FedAvg 和 MC-CDR 的全局模型的视觉聚类效果进行比较，验证 MC-CDR 模块中模型对比损失的有效性。T 为 10、50 和 100 时，2 种算法的可视聚

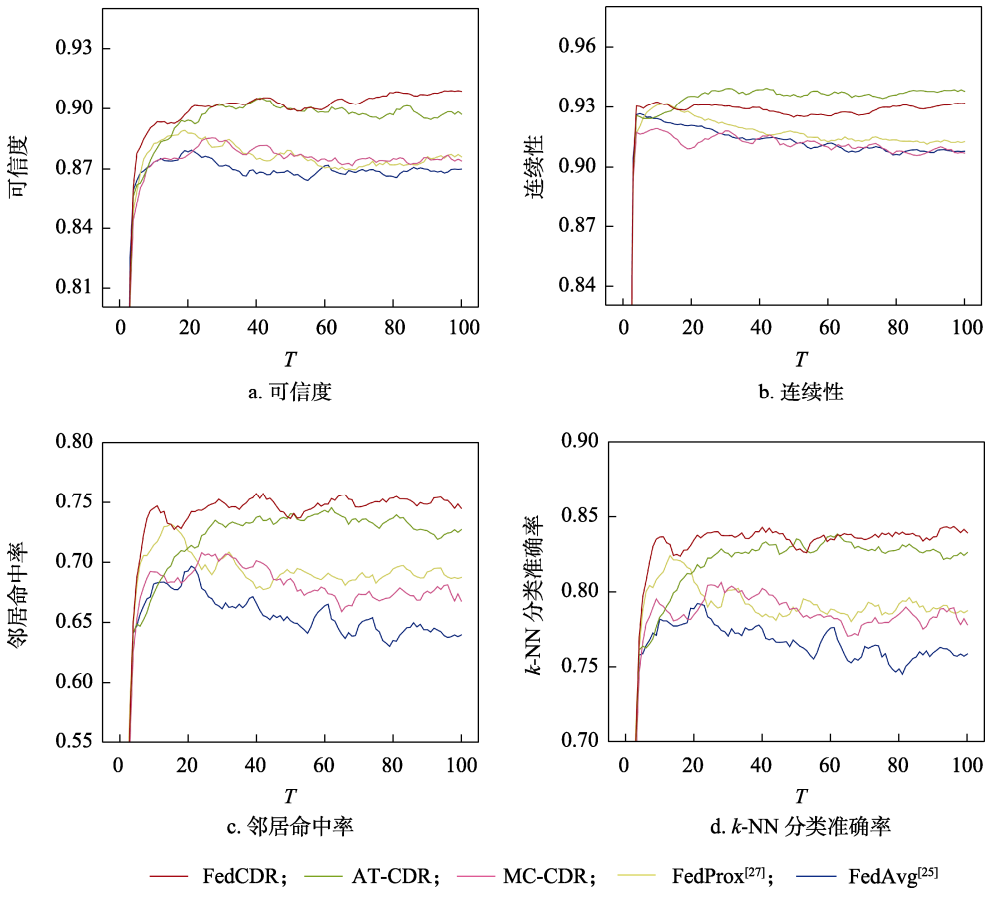


图 4 在 USPS 数据集上全局模型性能随 T 变化的对比

表 3 在 USPS 数据集上 β 不同时的性能对比

β	算法	可信度	连续性	邻居命中率	k-NN 分类准确率
5.0	FedAvg[25]	0.89583	0.94106	0.84061	0.89099
	FedProx[27]	0.90095	0.94124	0.85027	0.89553
	FedCDR	**0.91809**	**0.94543**	**0.85435**	**0.90076**
1.0	FedAvg[25]	0.88746	0.93033	0.71592	0.78860
	FedProx[27]	0.89314	0.93492	0.74998	0.82707
	FedCDR	**0.91342**	**0.94419**	**0.79219**	**0.85785**
0.5	FedAvg[25]	0.86912	0.90806	0.64170	0.76050
	FedProx[27]	0.87589	0.91242	0.69117	0.78925
	FedCDR	**0.90328**	**0.93122**	**0.74452**	**0.83112**
0.1	FedAvg[25]	0.79051	0.86461	0.46124	0.61200
	FedProx[27]	0.81792	0.87228	0.52235	0.66964
	FedCDR	**0.83240**	**0.87712**	**0.53717**	**0.68269**

注：粗体表示最优值。

类结果如表 6 所示。可以看出，在相同T下，MC-CDR 的全局模型始终展现出更优的聚类分离性能，即簇间距离更大、簇内距离更小。实验结果表明，模型对比损失的引入不仅能显著地提升全局模型的视觉聚类能力，还能有效地加速全局模型的收

表 4 在 USPS 数据集上 N 不同时的性能对比

N	算法	可信度	连续性	邻居命中率	k-NN 分类准确率
3	FedAvg[25]	0.85338	0.89110	0.62722	0.74948
	FedProx[27]	0.85400	0.90507	0.66910	0.76762
	FedCDR	**0.87239**	**0.91075**	**0.67841**	**0.78108**
5	FedAvg[25]	0.86912	0.90806	0.64170	0.76050
	FedProx[27]	0.87589	0.91242	0.69117	0.78925
	FedCDR	**0.90328**	**0.93122**	**0.74452**	**0.83112**
10	FedAvg[25]	0.87494	0.92818	0.67846	0.79577
	FedProx[27]	0.88964	0.93497	0.71645	0.80949
	FedCDR	**0.91810**	**0.95017**	**0.75960**	**0.84578**

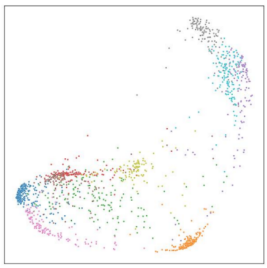
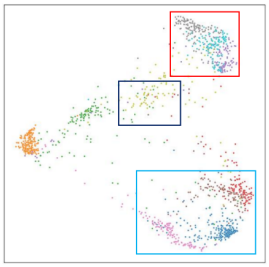
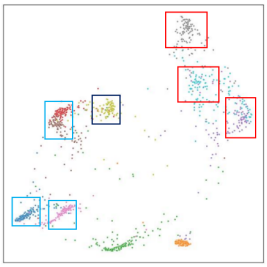
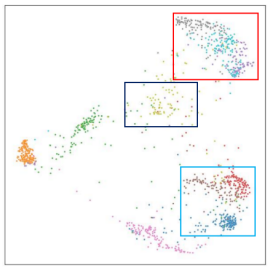
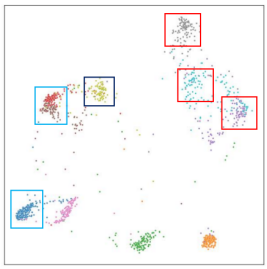
注：粗体表示最优值。

表 5 不同温度策略的性能对比

评价指标	PPO	线性衰减	τ		
			0.2	0.6	1.0
可信度	**0.90328**	0.89527	0.89763	0.88584	0.87428
连续性	**0.93122**	0.92197	0.92647	0.91538	0.90835
邻居命中率	**0.74452**	0.70974	0.70533	0.69739	0.67381
k-NN 分类准确率	**0.83112**	0.80760	0.81732	0.79958	0.78353

注：粗体表示最优值。

表 6　*T* 不同时 2 种算法的可视化结果对比

T	FedAvg[25]	MC-CDR
10		
50		
100		

敛过程。

5.4　FedCDR 算法的泛化性和局限性

本文设计的基于 PPO 的自适应温度调节智能体，展现出对不同数据分布差异的良好适应性。得益于去中心化的理念，独立智能体的设计在面对参与学习任务的客户端数量变化时具备稳健性；同时，状态空间、动作空间和奖励函数的设计相对独立于具体学习任务，使其具备迁移至其他联邦对比学习任务场景的潜力，提升了算法的通用性。

此外，FedCDR 算法基于本地训练机制进行优化，严格遵循 FL 场景的隐私保护约束。由于该算法邻域结构的设计主要面向空间特征进行优化，因此在空间关系特征显著的数据集上展现出良好性能，但在保留时序数据中的动态关系特征方面存在一定局限性。未来，将探索针对时序特征的邻域采样策略，进一步提升 FedCDR 算法的适用性。

6　结　语

本文提出了一种基于 PPO 的 FedCDR 算法，在客户端数据 non-IID 的条件下，通过 MC-CDR 和 AT-CDR 这 2 个模块优化客户端的本地训练机制，缓解本地模型的偏差。MC-CDR 模块在使用 CDR 损失实现更优秀的聚类分离效果的基础上，引入模型对比损失校正本地模型与全局模型之间的表征差异；AT-CDR 模块构建基于 PPO 的智能体以实现温度的自适应调节，有效地提高了全局模型的性能。在 3 个数据集上进行实验，证明了 FedCDR 算法在 non-IID 数据场景下的优势。

参考文献（References）：

[1] Wenskovitch J, Crandell I, Ramakrishnan N, *et al*. Towards a systematic combination of dimension reduction and clustering in visual analytics[J]. IEEE Transactions on Visualization and Computer Graphics, 2018, 24(1): 131-141

[2] van der Maaten L, Hinton G. Visualizing data using *t*-SNE[J]. Journal of Machine Learning Research, 2008, 9(86): 2579-2605

[3] McInnes L, Healy J, Melville J. UMAP: uniform manifold approximation and projection for dimension reduction[OL]. [2025-07-04]. https://arxiv.org/abs/1802.03426

[4] Damrich S, Hamprecht F A. On UMAP's true loss function[C] //Proceedings of the 35th International Conference on Neural Information Processing Systems. Red Hook: Curran Associates Inc, 2021: Article No.443

[5] Pezzotti N, Lelieveldt B P F, van der Maaten L, *et al*. Approximated and user steerable *t*-SNE for progressive visual analytics[J]. IEEE Transactions on Visualization and Computer Graphics, 2017, 23(7): 1739-1752

[6] Xia J Z, Huang L Q, Lin W X, *et al*. Interactive visual cluster analysis by contrastive dimensionality reduction[J]. IEEE Transactions on Visualization and Computer Graphics, 2023, 29(1): 734-744

[7] Yang Q, Liu Y, Chen T J, *et al*. Federated machine learning: concept and applications[J]. ACM Transactions on Intelligent Systems and Technology, 2019, 10(2): Article No.12

[8] Bonawitz K, Ivanov V, Kreuter B, *et al*. Practical secure aggregation for privacy-preserving machine learning[C] //Proceedings of the ACM SIGSAC Conference on Computer and Communications Security. New York: ACM Press, 2017: 1175-1191

[9] Bonawitz K A, Eichner H, Grieskamp W, *et al*. Towards federated learning at scale: system design[C] //Proceedings of the 2nd Conference on Machine Learning and Systems. Stanford: mlsys.org, 2019: 374-388

[10] Wu Wentai, Wu Yingliang, Lin Weiwei, *et al*. Horizontal federated learning: research status, system applications and open challenges[J]. Chinese Journal of Computers, 2025, 48(1): 35-67(in Chinese)
(吴文泰, 吴应良, 林伟伟, 等. 横向联邦学习: 研究现状、系统应用与挑战[J]. 计算机学报, 2025, 48(1): 35-67)

[11] Cuomo S, de Angelis V, Farina G, *et al*. A GPU-accelerated parallel K-means algorithm[J]. Computers & Electrical Engineering, 2019, 75: 262-274

[12] Januzaj E, Kriegel H P, Pfeifle M. Scalable density-based distributed clustering[C] //Proceedings of the 8th European Con-

ference on Principles and Practice of Knowledge Discovery in Databases. Heidelberg: Springer, 2004: 231-244

[13] Schulman J, Wolski F, Dhariwal P, *et al*. Proximal policy optimization algorithms[OL]. [2025-07-04]. https://arxiv.org/abs/1707.06347

[14] Yuan J, Xiang S X, Xia J Z, *et al*. Evaluation of sampling methods for scatterplots[J]. IEEE Transactions on Visualization and Computer Graphics, 2021, 27(2): 1720-1730

[15] Espadoto M, Martins R M, Kerren A, *et al*. Toward a quantitative survey of dimension reduction techniques[J]. IEEE Transactions on Visualization and Computer Graphics, 2021, 27(3): 2153-2173

[16] Abdi H, Williams L J. Principal component analysis[J]. WIREs Computational Statistics, 2010, 2(4): 433-459

[17] Mair P. Modern psychometrics with R[M]. Cham: Springer, 2018

[18] Chatzimparmpas A, Martins R M, Kerren A. *t*-viSNE: interactive assessment and interpretation of *t*-SNE projections[J]. IEEE Transactions on Visualization and Computer Graphics, 2020, 26(8): 2696-2714

[19] Arora S, Hu W, Kothari P K. An analysis of the *t*-SNE algorithm for data visualization[C] //Proceedings of the 31st Conference on Learning Theory. Stockholm: PMLR, 2018: 1455-1462

[20] Linderman G C, Steinerberger S. Clustering with *t*-SNE, provably[J]. SIAM Journal on Mathematics of Data Science, 2019, 1(2): 313-332

[21] Xia J Z, Zhang Y C, Song J, *et al*. Revisiting dimensionality reduction techniques for visual cluster analysis: an empirical study[J]. IEEE Transactions on Visualization and Computer Graphics, 2022, 28(1): 529-539

[22] Chen T, Kornblith S, Norouzi M, *et al*. A simple framework for contrastive learning of visual representations[C] //Proceedings of the 37th International Conference on Machine Learning. New York: PMLR, 2020: 1597-1607

[23] He K M, Fan H Q, Wu Y X, *et al*. Momentum contrast for unsupervised visual representation learning[C] //Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition. Los Alamitos: IEEE Computer Society Press, 2020: 9726-9735

[24] Kairouz P, McMahan H B, Avent B, *et al*. Advances and open problems in federated learning[J]. Foundations and Trends® in Machine Learning, 2021, 14(1-2): 1-210

[25] 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. Brookline: Microtome Publishing, 2017: 1273-1282

[26] Chen H K, Zhang Y, Krompass D, *et al*. FedDAT: an approach for foundation model finetuning in multi-modal heterogeneous federated learning[C] //Proceedings of the 38th AAAI Conference on Artificial Intelligence. Palo Alto: AAAI Press, 2024: 11285-11293

[27] Li T, Sahu A K, Zaheer M, *et al*. Federated optimization in heterogeneous networks[C] //Proceedings of the 3rd Conference on Machine Learning and Systems. Austin: mlsys.org, 2020: 429-450

[28] Li Q B, He B S, Song D. Model-contrastive federated learning[C] //Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition. Los Alamitos: IEEE Computer Society Press, 2021: 10708-10717

[29] Li Zhipeng, Guo Yong, Chen Yaofo, *et al*. Class-balanced federated learning based on data generation[J]. Chinese Journal of Computers, 2023, 46(3): 609-625(in Chinese)
(李志鹏, 国雍, 陈耀佛, 等. 基于数据生成的类别均衡联邦学习[J]. 计算机学报, 2023, 46(3): 609-625)

[30] Xiao Y P, Li X F, Li T, *et al*. A distributed generative adversarial network for data augmentation under vertical federated learning[J]. IEEE Transactions on Big Data, 2025, 11(1): 74-85

[31] van Berlo B, Saeed A, Ozcelebi T. Towards federated unsupervised representation learning[C] //Proceedings of the 3rd ACM International Workshop on Edge Systems, Analytics and Networking. New York: ACM Press, 2020: 31-36

[32] Zhang F D, Kuang K, Chen L, *et al*. Federated unsupervised representation learning[J]. Frontiers of Information Technology & Electronic Engineering, 2023, 24(8): 1181-1193

[33] Zhuang W M, Gan X, Wen Y G, *et al*. Collaborative unsupervised visual representation learning from decentralized data[C] //Proceedings of the IEEE/CVF International Conference on Computer Vision. Los Alamitos: IEEE Computer Society Press, 2021: 4892-4901

[34] Han S, Park S, Wu F Z, *et al*. FedX: unsupervised federated learning with cross knowledge distillation[C] //Proceedings of the 17th European Conference on Computer Vision. Heidelberg: Springer, 2022: 691-707

[35] Sohn K. Improved deep metric learning with multi-class *N*-pair loss objective[C] //Proceedings of the 30th International Conference on Neural Information Processing Systems. Red Hook: Curran Associates Inc, 2016: 1857-1865

[36] Qian Y, Ma T, Zhang C, *et al*. Dual-level hypergraph contrastive learning with adaptive temperature enhancement[C]// Proceedings of the ACM Web Conference 2024. New York: ACM Press, 2024: 859-862

[37] Yurochkin M, Agarwal M, Ghosh S, *et al*. Bayesian nonparametric federated learning of neural networks[C] //Proceedings of the 36th International Conference on Machine Learning. Long Bach: PMLR, 2019: 7252-7261

[38] Kaski S, Nikkilä J, Oja M, *et al*. Trustworthiness and metrics in visualizing similarity of gene expression[J]. BMC Bioinformatics, 2003, 4: Article No.48

[39] Paulovich F V, Nonato L G, Minghim R, *et al*. Least square projection: a fast high-precision multidimensional projection technique and its application to document mapping[J]. IEEE Transactions on Visualization and Computer Graphics, 2008, 14(3): 564-575

[40] Cunningham P, Delany S J. *K*-nearest neighbour classifiers-a tutorial[J]. ACM Computing Surveys, 2022, 54(6): Article No.128