计算机科学
COMPUTER SCIENCE

基于双重抗遗忘机制的轻量化联邦持续学习方法

王攀, 王吉, 钟正仪, 包卫东, 张耀鸿

引用本文

王攀, 王吉, 钟正仪, 包卫东, 张耀鸿. 基于双重抗遗忘机制的轻量化联邦持续学习方法[J]. 计算机科学, 2026, 53(4): 424-434.

WANG Pan, WANG Ji, ZHONG Zhengyi, BAO Weidong, ZHANG Yaohong. Lightweight Federated Continual Learning Method Based on Double Anti-forgetting Mechanism [J]. Computer Science, 2026, 53(4): 424-434.

计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.250500116

基于双重抗遗忘机制的轻量化联邦持续学习方法

王 攀 王 吉 钟正仪 包卫东 张耀鸿
国防科技大学大数据与决策国家级重点实验室 长沙 410000
(wangpan19@nudt.edu.cn)

摘 要 联邦学习在不共享数据的前提下,通过上传并聚合客户端模型实现不同客户端之间的知识共享。现有的联邦学习方法大多假设客户端数据是已知且固定的。然而,在现实场景中,客户端会不断地接收包含新类别数据的任务并更新模型,导致模型在旧任务上的表现持续下滑,即发生灾难性遗忘问题。为有效应对这一严峻挑战,研究者将持续学习方法引入联邦学习中,衍生出联邦持续学习这一研究方向。然而,随着客户端所接收的任务数量不断增加,现有联邦持续学习方法在缓解灾难性遗忘问题上的效果逐渐变差,尤其是在针对较为久远的任务时,准确率出现了大幅下降,且数据异构程度的提升也进一步削弱了模型的准确率表现。鉴于此,设计了本地-全局双重抗遗忘机制,以缓解模型在久远任务上的遗忘问题。具体而言,在客户端层面引入特定于任务的轻量化模块,有效克服了数据变化与模型更新引发的灾难性遗忘;在服务器端通过模型反演生成并筛选得到类别均衡的伪图像,缓解了数据分布差异导致的模型性能下降的问题。在 CIFAR10,CIFAR100 和 TinyImageNet 等数据集上开展了一系列实验,实验结果有力地证实了该机制的优越性,充分表明其相较于现有各类方法,在提升模型性能、缓解灾难性遗忘等方面具有显著优势。

关键词:联邦持续学习;灾难性遗忘;数据异构;轻量化模块;本地-全局抗遗忘
中图分类号 TP301

Lightweight Federated Continual Learning Method Based on Double Anti-forgetting Mechanism

WANG Pan,WANG Ji,ZHONG Zhengyi,BAO Weidong and ZHANG Yaohong
Laboratory for Big Data and Decision,National University of Defense Technology,Changsha 410000,China

Abstract Federated learning(FL) enables knowledge sharing among different clients by uploading and aggregating client models without sharing data. However,existing FL methods generally assume that client data is known and fixed. In reality,clients continuously receive tasks with new category data and update their models,which leads to a continuous decline in model performance on old tasks,known as catastrophic forgetting. To address this severe challenge,researchers have introduced continual learning (CL) into FL,giving rise to the research direction of federated continual learning(FCL). Nevertheless,as the number of tasks received by clients increases,existing FCL methods become less effective in alleviating catastrophic forgetting,especially for tasks that are relatively distant in time,where accuracy drops significantly. Moreover,the increasing degree of data heterogeneity further weakens model accuracy. To address this issue,this paper proposes a local-global anti-forgetting mechanism to mitigate the forgetting problem on distant tasks. Specifically,it introduces task-specific lightweight modules at the client level to effectively overcome catastrophic forgetting caused by data changes and model updates. At the server level,it generates and filters category-balanced pseudo-images through model inversion to alleviate the decline in model performance due to data distribution differences. Through a series of experiments conducted on CIFAR-10,CIFAR-100,and TinyImageNet datasets,the results strongly demonstrate the superiority of the proposed mechanism. Compared with existing methods,it shows significant advantages in improving model performance and alleviating catastrophic forgetting.

Keywords Federated continual learning,Catastrophic forgetting,Data heterogeneity,Lightweight modules,Local-global anti forgetting

到稿日期:2025-05-26 返修日期:2025-08-29
基金项目:国家自然科学基金(62002369)
This work was supported by the National Natural Science Foundation of China(62002369).
通信作者:王吉(wangji@nudt.edu.cn)

1　引言

在数字化时代，数据隐私保护[1]已成为全球关注的焦点。随着一系列严格隐私保护法律的实施，如中国的《中华人民共和国网络安全法》、美国《2018 年加州消费者隐私法案》[2]、欧盟的通用数据保护条例（GDPR）[3]等，社会各界对于数据在共享过程中的隐私保护要求愈发严格[4-7]。为了在隐私保护的前提下实现知识的共享，联邦学习（Federated Learning，FL）[8]作为一种高效的隐私保护机器学习框架应运而生。联邦学习允许多个参与方在不共享数据的前提下进行协同训练，实现了跨用户的知识共享。其核心理念是“数据不动模型动，数据可用不可见”[9]。尽管联邦学习在隐私保护方面表现出色，但其在实际应用中仍面临诸多挑战[10]，尤其是在数据动态变化的现实场景下。

传统的联邦学习通常假设数据是已知且静止不变的，然而现实世界中的数据呈现出高度动态变化的特性。客户端持续接收新的数据，这些数据可能包含新的类别或特征。将包含一组新类别的数据集合称为任务。在数据动态变化的环境中，传统的联邦学习方法训练得到的模型在处理新数据时往往表现不佳，原因在于它们未能充分考虑数据的动态变化特性。随着训练的进行，客户端不断接收包含新类别的任务，新任务的训练通常会覆盖原有模型的参数，导致模型在之前任务上的性能显著下降[11]。为了解决这一关键问题，研究者开始探索将联邦学习与持续学习[12-13]（Conitnual Learning，CL）相结合的新路径，从而催生了联邦持续学习[14-16]（Federated Conitnual Learning，FCL）这一创新研究方向。

联邦持续学习的目标是使模型在保留已有任务知识的基础上，能够不断学习新的任务，实现在时间和空间维度上的知识积累和模型更新。现有的联邦持续学习方法主要分为 3 类：基于数据的方法[17-18]、基于模型的方法[15,19]以及基于输出的方法[20-21]。基于数据的方法主要通过保留或生成旧任务的数据来缓解灾难性遗忘问题，通常在客户端上维护一个小型的数据缓冲区，用于存储旧任务的代表性样本，或者通过生成模型生成旧任务的数据，从而在模型学习新任务时回溯旧任务的知识。基于模型的方法通过调整模型的结构或参数来缓解灾难性遗忘。具体实现方式包括参数分解[15]、参数隔离[19]等，通过对模型进行特定的约束或设计，使其在学习新任务时尽量减少对旧任务知识的破坏。基于输出的方法利用模型的输出信息，如类别原型[20]或知识蒸馏[21]等，来实现知识融合，从而缓解灾难性遗忘现象。

然而，随着任务数量的不断增加，现有方法在应对久远的任务时，表现出明显的性能下降。受限于客户端有限的存储能力，模型往往只能在最新的任务上的进行迭代更新，导致在久远任务上的准确率急剧下降，尤其是当数据异构程度逐渐增加时，模型的下降程度更为显著。

本文选取了当前领域内的 3 种代表性方法作为实验基准，以全面评估其性能。具体而言，分别对 FedWeIT[15]，FedLWF[21]和 MFCL[22]这 3 种方法进行了详细的实验分析。这 3 种方法分别代表了基于模型、基于原型和基于数据的经典研究方向，涵盖了当前联邦学习领域中主流的技术路径。如图 1 所示，随着任务数量不断增加，现有方法训练得到的模型的平均准确率逐渐下降。如图 2 所示，模型在最近的任务上表现最好，随着时间推移，在以前的任务上的效果逐渐变差。表 1 展示了当任务数量为 20 时，不同的数据异构程度对现有联邦持续学习方法的影响。其中 α 表示数据异构程度，α 越小，数据异构程度越大。结果表明，现有的 SOTA 方法均不能实现较好的记忆效果，且随着数据异构程度的逐渐增加，现有方法表现出显著的性能下降。

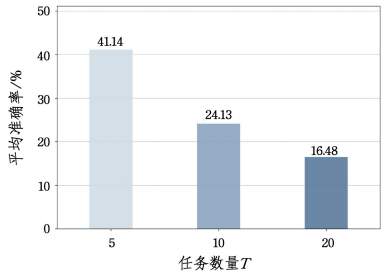


图 1　现有方法训练得到的模型准确率

Fig. 1　Accuracy of models trained by existing methods

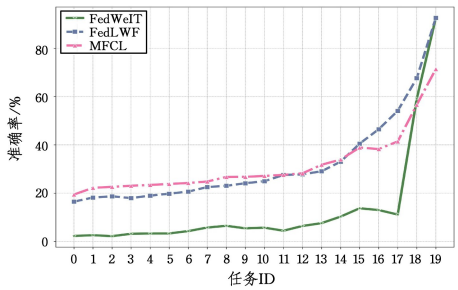


图 2　模型在每个任务上的表现

Fig. 2　Performance of the model on each task

表 1　在 CIFAR100 数据集上 $T=20$ 时各类方法的表现

Table 1　Performance of various methods when $T=20$ on the CIFAR-100 dataset

α	FedLWF[21]	MFCL[22]	FedWeIT[15]
$\alpha=1$	17.62	20.41	4.73
$\alpha=0.5$	16.48	19.41	2.26
$\alpha=0.3$	10.71	16.62	3.00
$\alpha=0.1$	9.51	12.84	3.19

对现有的联邦持续学习方法进行分析可知，FedLWF[21]方法必须将先前模型中的知识反复传递给当前任务模型。这种反复蒸馏导致知识逐渐弱化，最终无法保留长期记忆。MFCL[22]方法在新任务到来时重放以前任务的样本，导致样本质量逐渐下降，使得重新训练的模型无法有效保留长期记忆。FedWeIT[15]无法解决在扩展任务规模中的灾难性遗忘问题，这是因为任务规模的扩展使得参数共享变得越来越困难，导致参数更新产生冲突。为解决数据异构背景下的任务扩展带来的灾难性遗忘问题，本文提出了本地-全局的双重抗遗忘机制。具体而言，在客户端上保留每个任务的特定模型，从而实现对客户端上每个任务知识的完整保存，克服了任务增加导致抗遗忘效果衰退的困境。在服务器端，针对不同客户端上每个任务对应的模型进行模型反演操作，生成并筛选得到类别均衡且高质量的伪图像。使用生成的伪图像进一步对全局模型进行微调，

缓解了数据异构导致的全局模型性能下降的问题。

考虑客户端面临的存储、计算以及通信资源受限等问题，存储大量的任务模型会对客户端存储造成较大压力。受到大模型中微调技术的启发，将 LoRA 微调方法引入联邦持续学习。LoRA 方法适用于在资源受限的环境中对预训练模型进行微调，通过引入低秩矩阵来减少参数更新量，从而显著降低计算和存储成本，同时保持模型的性能。在客户端上使用 LoRA 方法针对每个任务进行微调，通过为每个任务保留特定的 LoRA 模块，以在客户端上实现低成本、高效率的本地抗遗忘。然而，仅在客户端本地实现抗遗忘仍存在较大的缺陷，数据异构导致不同客户端的数据可能在特征空间上存在显著差异，由此训练得到的客户端模型参数的更新方向不同。在聚合过程中，不同客户端更新的模型参数可能会产生冲突。这种参数冲突使得全局模型难以有效地整合所有客户端的知识，导致模型性能受损。对此，在不同阶段的任务中，以经过本地训练且尚未进行全局聚合的客户端模型为目标，开展基于模型反演方法的数据生成策略，筛选高质量且类别平衡的伪图像对全局模型进行微调，确保全局模型在训练时能够接触到所有任务的代表性样本，从而缓解数据分布差异导致的性能下降。在推理阶段，通过人工干预的方式提供任务的 ID 编号，在客户端加载相应的模型进行测试。

本文的主要贡献如下：

1)针对现有联邦持续学习方法在处理大规模任务时准确率剧烈下滑的问题，提出了本地-全局的双重抗遗忘机制。在客户端保留每个任务的特定模型，实现对客户端上每个任务知识的完整保存；在服务器端，通过数据反演的方法针对每个任务生成并筛选得到类别均衡且高质量的伪图像，通过对全局模型的微调，缓解了数据异构导致的全局模型性能下降问题。

2)将 LoRA 微调方法引入联邦持续学习，用于在客户端上针对每个任务进行微调。通过为每个任务保留特定的 LoRA 模块，在客户端上实现低成本、高效率的本地抗遗忘，有效缓解了客户端存储、计算以及通信资源受限的问题。

3)在 CIFAR10，CIFAR100 以及 TinyImageNet 数据集进行测试，在不同的数据异构程度下验证了本文方法的优越性，表明其相较于现有方法能显著提升性能。

2 相关工作

2.1 联邦学习

联邦学习[8]的概念最早由 Google 的研究人员在 2016 年提出。其核心思想是在多个设备或节点之间协作训练共享模型，而不必共享原始数据。这种模式有效解决了传统集中式机器学习在数据隐私保护方面的痛点，尤其是在移动设备场景下，既能够利用海量设备上的数据进行模型训练，又能避免用户数据的直接上传与泄露。自其诞生以来，随着全球隐私保护法规的日益严格，如欧盟的《通用数据保护条例》(GDPR)[3]等的出台，联邦学习逐渐成为学术界和工业界的研究热点。众多研究机构和企业纷纷投入到联邦学习的理论研究与实践应用中，推动了该领域的快速发展。联邦学习技术已经应用到政府事务[23]、推荐系统[24]等隐私敏感领域。

尽管联邦学习展现出巨大的潜力，但在实际应用中仍面临诸多挑战。一是通信开销问题，现有的工作试图通过数据压缩[25]或只允许将相关的输出发送回中央服务器来解决这个问题[26-27]。二是客户端上的数据异构导致全局模型的准确率下降，文献[28-29]等方法试图通过修改模型聚合方法来解决这个问题。三是投毒攻击[30]、后门攻击[31]等方法对联邦学习的隐私和安全造成了较大的威胁。

2.2 持续学习

持续学习[12-13](Continual Learning，CL)是一种机器学习方法，旨在模拟人类学习的特性，即模型能够在不断变化的环境中持续学习新任务，同时保留之前任务的知识。在传统的机器学习方法中，模型通常是在固定的、大规模的训练数据集上一次性训练完成的，在部署后不再更新。然而，这种方法在许多现实场景中是不适用的，因为数据分布可能会随时间变化，或者新任务可能会不断出现。持续学习的核心目标是解决灾难性遗忘[11](Catastrophic Forgetting)问题，即模型在学习新任务时可能会忘记之前任务的知识。现有的持续学习方法主要包括知识提取[32]、参数分离[33]、动态架构[34]、重放[35-37]等技术。正则化技术[38]旨在利用 Fisher 信息矩阵，确定对之前任务重要的参数，然后在学习新任务时，通过参数正则化的方法约束不断变化的重要参数，以防止灾难性遗忘。参数分离技术，如 PackNet[33]，只激活与特定任务相关的参数。动态架构方法[34]为新任务添加参数，同时保持旧参数不变。基于重放的方法[35-36]存储和重放以前的数据以减轻遗忘。知识蒸馏方法，如 LwF[37]，定期将知识从先前学习的模型转移到新模型，以减轻遗忘。这些方法的共同目标是通过不同的机制保留旧任务的知识，同时有效地学习新任务。

2.3 联邦持续学习

联邦类持续学习[39](Federated Class-Incremental Learning，FCIL)是一种特殊的联邦学习场景，旨在解决客户端在不断变化的类别集合中进行学习的问题。在这种设置中，每个客户端需要学习一个不断增长的类别集合，并在保护隐私的同时，将新类别知识与全局模型的知识融合。FCIL 的核心目标是确保全局模型能够准确识别所有客户端观察到的类别，同时避免灾难性遗忘。

Fang 等[17]提出了面向不平衡数据的联邦类别增量学习，该方法提出了一种基于条件生成对抗网络的无数据存储重放再训练方法，可有效应对多种 Non-IID 场景，并且具备抵御恶意客户端发起的中毒攻击的能力。FedWeIT 框架[15]通过分解网络权重并采用加权组合方式，使客户端能在学习过程中有效获取其他客户端的有用知识，减少任务干扰并促进知识转移。此外，该方法在降低通信成本方面表现出色。Zhang 等[19]提出了一种新型联邦连续学习方法 CFedSI，通过引入其他局部模型的知识来提高 Non-IID 设定下模型的性能，并通过双向压缩和误差补偿算法来实现通信高效的联邦持续学习方法。Usmanova 等[21]提出了一种基于蒸馏的方法来解决联邦学习中的灾难性遗忘问题，以人类活动识别任务为例进行测试和验证。上述方法推动了联邦学习与持续学习的融合，为解决联邦学习框架下的灾难性遗忘问题做出了较大贡献。然而当任务数量不断扩展时，上述方法在较为久远

的任务上均表现出严重的性能下滑。

3　本文方法

为解决现有联邦持续学习方法在久远任务上准确率急速下降的问题，本文设计了本地-全局的双重抗遗忘机制。在客户端存储每个任务特定的模型参数，以实现本地抗遗忘；在服务器端对不同客户端上的每个任务进行模型反演操作生成伪图像，在全局模型层面克服数据异构带来的参数冲突。下面对联邦持续学习方法进行定义，并对本文方法进行详细介绍。

3.1　问题定义

客户端集合$C=\{C_1,C_2,\cdots,C_N\}$包含N个分布式客户端，数据集表示为$\mathcal{D}=\{\mathcal{D}_n\}_{n=1}^{N}$，$\mathcal{D}_n=\{\mathcal{D}_n^t\}_{t=0}^{T-1}$表示每个客户端上的数据集，$\mathcal{D}_n^t$为对应任务的数据集，$|\mathcal{D}_n^t|$表示客户端上数据集的大小。一系列任务$\mathcal{T}=\{\mathcal{T}^t\}_{t=0}^{T-1}$按顺序到达客户端，由此训练得到对应的模型表示为$M_n^t$，服务器端使用生成图像训练得到任务对应的全局模型表示为M_G^t。全局轮次设置为R，本地轮次设置为e，本地学习率为l_c，全局学习率为l_G。

客户端模型M_n^t由基础模型M_B以及特定于任务的模块$M_{\Delta,n}^t$组成，即：

$$M_n^t=(M_B,M_{\Delta,n}^t) \tag{1}$$

保持基础模型冻结，$M_B=M_B^*$，仅对特定于任务的模块进行调整。则客户端上的训练目标为：

$$M_{\Delta,n}^t=\arg\min_{\mathcal{M}_{\Delta,n}^t}\mathcal{L}_n^t(M_B^*,M_{\Delta,n}^t;D_n^t) \tag{2}$$

即使用本地数据D_n^t对$M_{\Delta,n}^t$进行训练。损失函数$\mathcal{L}_n^t$被定义为：

$$\mathcal{L}_n^t(M_B^*,M_{\Delta,n}^t;D_n^t)=\mathbb{E}_{(x,y)\sim\mathcal{D}_n^t}[\ell(y,M_n^t(x))] \tag{3}$$

其中，ℓ是损失函数，x是输入样本，y是相应的标签。

3.2　方法框架

本文方法的框架如图3所示，客户端$C=\{C_1,C_2,\cdots,C_N\}$接收一系列任务$\mathcal{T}=\{\mathcal{T}^t\}_{t=0}^{T-1}$，训练特定于任务的轻量化模块，将其上传至服务器端并复制保留在客户端，由此克服模型更新带来的灾难性遗忘。将上传至服务器端的轻量化模块$M_{\Delta,n}^t$与基础模型M_B组合，结合激活最大化方法进行模型反演。针对生成的伪图像$Z_n^{t,Cat}$进行筛选，得到类别均衡的伪图像集$Z_s^t=\bigcup_{cat=1}^{Cat^t}Z_s^{t,Cat}$，然后对全局轻量化模块$M_{\Delta,g}^t$进行微调，缓解数据异构带来的模型损耗问题。

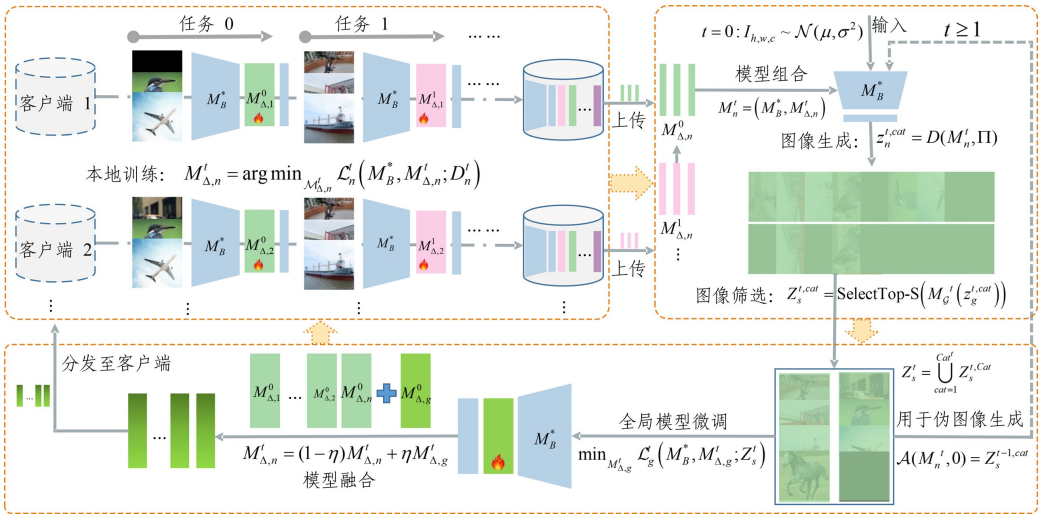


图3　基于双重抗遗忘机制的轻量化联邦持续学习

Fig. 3　Lightweight federated continual learning based on a dual anti-forgetting mechanism

3.3　本地抗遗忘机制

传统的联邦持续学习方法希望在新任务的学习与旧任务的记忆中寻得平衡，但这会不可避免地导致可塑性和记忆性冲突，并在实现过程中导致性能下降。在新任务的学习上，本文设定学习目标为在新任务上表现最好；在旧任务的记忆方面，本文方法通过存储旧任务的轻量化模块实现知识累积，达到克服遗忘的目的。该方法确保轻量化模块在每个对应的任务上表现最佳，避免了可塑性和记忆性冲突导致的性能下降问题，通过存储少量模块克服灾难性遗忘。实施步骤如下。

客户端C_n持续接收一系列类增量持续学习任务$\mathcal{T}=\{\mathcal{T}^t\}_{t=0}^{T-1}$。受限于存储空间，客户端不存储与当前任务无关的其他数据。当第t个任务到达时，客户端存储第$t-1$个轻量化模块并初始化第t个轻量化模块，在第t个任务上进行训练。本地训练过程可表示为：

$$\theta_{\mathcal{M}_{\Delta,n}^t}^{r,e}=\theta_{\mathcal{M}_{\Delta,n}^t}^{r}-l\cdot\nabla_\theta\mathcal{L}(M_B^*,M_{\Delta,n}^t,\mathcal{D}_n^t) \tag{4}$$

其中，θ表示模型对应的参数。当第t个任务训练完成后，保存第t个任务对应的轻量化模块，即：

$$\mathcal{M}_{\Delta,n}^{t-1}=\bigcup_{t=0}^{t-1}M_{\Delta,n}^0 \tag{5}$$

$$\mathcal{M}_{\Delta,n}^t=\{\mathcal{M}_{\Delta,n}^{t-1}\cup M_{\Delta,n}^t\}_{t=0}^{T-1} \tag{6}$$

服务器端接收并保存所有客户端C_n上的不同任务对应的轻量化模块集合$M_{\Delta,n}^t$，然后开始全局抗遗忘操作。

3.4　全局抗遗忘机制

将客户端上的任务特定模块集合$\mathcal{M}_{\Delta,n}^t$上传至服务器上，使用式(1)进行组合得到完整模型，服务器通过模型反演生成每个类别的合成图像。

$$z_n^{t,cat}=D(M_n^t,\Pi) \tag{7}$$

其中，$z_n^{t,cat}$是经过Π轮优化得到的生成图像；$D(M_n^t,\Pi)$表示对模型M_n^t进行Π轮反演。传统的模型反演方法通常假设特

征统计量在 BN 层遵循高斯分布，使用均值和方差对该分布进行定义，通过减少生成图像和原始图像在不同层次特征的差异来提高生成图像的质量。

本文上传的 LoRA 模块中不包含 BN 层，使用激活最大化方法进一步增强图像质量。

设模型 M_n^t 对输入图像 z 的预测输出为 $f(z)$，目标类别为 cat，损失函数定义为 $A(z)=-f_{cat}(z)$，其中 $f_{cat}(z)$ 表示模型对类别 cat 的预测得分。通过梯度上升，优化输入图像 z，即：

$$z_{r+1}=z_r+\alpha\cdot\nabla_z A(z) \tag{8}$$

损失函数表示为：

$$L(z)=\alpha_{tv}R_{TV}(z)+\alpha_{l_2}R_{l_2}(z)-A(z) \tag{9}$$

$R_{TV}(z)$ 为总变差正则化，是用于保持信号或图像平滑的正则化方法。其通过惩罚相邻像素 (i,j) 和 $(i+1,j)$ 之间的剧烈变化，达到去噪、保持边缘或防止过拟合的目的。

$$TV(z)=\sum_{i,j}\sqrt{(z_{i+1,j}-z_{i,j})^2+(z_{i,j+1}-z_{i,j})^2} \tag{10}$$

l_2 正则化的作用是防止模型过拟合，通过约束权重参数的幅度，提升泛化能力。在损失函数中添加权重参数的平方和作为惩罚项，迫使模型选择较小的权重值，降低对噪声的敏感度。

$A(z)$ 为激活最大化损失，其目的是初始化并不断更新输入图像，使得神经网络中特定的神经元或神经元组的激活值达到最大。

$$A(z)=-f_{cat}(z) \tag{11}$$

综合考虑上述损失函数，最终得到优化目标为：

$$\min_z \alpha_{tv}R_{TV}(z)+\alpha_{l_2}R_{l_2}(z)-\alpha_{cat}f_{cat}(z) \tag{12}$$

其中，α_{tv}，α_{l_2}，α_{cat} 为对应损失函数的系数。

模型反演可表示为：

$$\mathcal{A}(M_n^t,\Pi):z\leftarrow z-\eta_1\nabla_z L(z) \tag{13}$$

当 $t=0$ 时，用高斯噪声初始化图像，创建一个随机的起始点来生成图像。通过优化过程，调整图像的像素值，使模型对生成图像的预测尽可能接近模型对真实图像的预测分布，不断迭代优化，直到生成的图像在模型上达到与真实图像相似的预测分布，并且具有较好的视觉质量，即：

$$\begin{aligned}\mathcal{A}(M_n^0,\gamma=0)&=z_n^{0,cat}\\&=I_{h,w,c}\sim\mathcal{N}(\mu,\sigma^2),I\in\mathbb{R}^{H\times W\times C}\end{aligned} \tag{14}$$

当 $t\geqslant 1$ 时，使用第 $t-1$ 个任务的生成图像作为输入，能够更快地优化出与当前任务相关的特征。

$$\mathcal{A}(M_n^t,0)=z_n^{t-1,cat},t>0 \tag{15}$$

初始化后，使用 $z_n^{t,cat}=\mathcal{A}(M_n{}^t,\Pi)$ 进行多轮优化，最终得到每个任务中不同类别的伪图像 $Z_n^{t,cat}=\{z_n^{t,cat}\}_{cat=1}^{cat}$。随后服务器将合成图像聚合，形成全局集合。

$$Z_g^{t,cat}=\bigcup_{n=1}^{N}Z_n^{t,cat} \tag{16}$$

为了确保类别平衡以及数量相同的表示，对每个类别 cat，按 logit 值从高到低排序后，使用 SelectTop-S 函数选择前 S 张图像作为最终的伪图像集：

$$Z_s^{t,cat}=SelectTop\text{-}S(M_G^t(z_g^{t,cat})),\forall\, cat\in\{1,\cdots,cat\} \tag{17}$$

其中，$Z_s^{t,cat}$ 是为类 cat 选择的伪图像集。任务 t 的最终伪图像池为：

$$Z_s^t=\bigcup_{cat=1}^{cat^t}Z_s^{t,cat} \tag{18}$$

使用伪图像池 Z_s^t 训练全局任务特定模块 $M_{\Delta,g}^t$。

$$M_{\Delta,g}^t=\arg\min_{M_{\Delta,g}^t}\mathcal{L}_g^t(M_B^*,M_{\Delta,g}^t;Z_s^t) \tag{19}$$

其中，全局损失函数为：

$$\mathcal{L}_g^t(M_B^*,M_{\Delta,g}^t;Z_s^t)=\mathbb{E}_{(x,y)\sim Z_s^t}[\mathcal{L}(y,M_g^t(x))] \tag{20}$$

其中，$M_g^t=(M_B^*,M_{\Delta,g}^t)$ 是任务 t 的全局模型。

为了推动本地-全局双重抗遗忘机制的融合，每个客户端将其任务特定模块与全局任务特定模块结合。客户端可以通过集成全局模块来更新其任务特定模块。

$$M_{\Delta,n}^t=(1-\eta)M_{\Delta,n}^t+\eta M_{\Delta,g}^t \tag{21}$$

其中，η 是一个混合系数，决定了全局模块的影响程度，这里取 η 为 0.5，即为全局模块与客户端模块的平均加权。

3.5 算法流程

算法的伪代码如算法 1 所示，算法流程如下。

算法 1 基于双重抗遗忘机制的联邦轻量化持续学习方法

输入：数据集 $\mathcal{D}_n^t$，基础模型 M_B，全局轮次 R，本地轮次 e，本地学习率 l_c，全局学习率

输出：客户端任务特定模块 $M_{\Delta,n}^t$

客户端本地抗遗忘

```
for r=1 to R:
    for C={C_1,C_2,…,C_N}do:
        M_B=M_B^*,Initialize D_n^t,M_{Δ,n}^t
        for e=1 to E:
            M_n^t=(M_B,M_{Δ,n}^t)
            loss=CrossEntropy((batch.x),batch.y)
            M_{Δ,n}^t←SGD(loss,l_c)
        end for
        {M_{Δ,n}^t}←{M_{Δ,n}^t}∪M_{Δ,n}^t
    end for
end for
```

服务器端样本生成

```
for t in {1,…,T}:
    for cat in {1,…,cat}:
        if t=0:
            A(M_n^t,γ=0)=z_n^{0,cat}=I_{h,w,c}~N(μ,σ^2),I∈R^{H×W×C}
        else:
            A(M_n^t,0)=z_n^{t-1,cat}(t>0).
    end for
end for
```

类样本筛选

```
Z_s^t=∅
for cat in {1,…,cat}:
    Z_g^{t,cat}=∪_{n=1}^{N} Z_n^{t,cat}
    Z_s^{t,cat}=SelectTop-S(M_G^t(z_g^{t,cat}))
    Z_s^t ∪_{cat=1}^{cat^t} Z_n^{t,cat}
end for
```

全局模型微调

```
Initialize M_{Δ,g}^t
```

27. for e=1 to E do：

28.　$M_g^t=(M_B^*, M_{\Delta,g}^t)$

29.　$\mathcal{L}_g^t(M_B^*, M_{\Delta,g}^t; Z_s^t=\mathbb{E}_{(x,y)\sim Z_s^t}[\ell(yk, M_g^t(x))]$

30.　$M_{\Delta,g}^t \leftarrow SGD(loss, lr=l_G)$

31. end for

模型集成

32. for $C=\{C_1, C_2, \cdots, C_N\}$ do：

33.　$M_{\Delta,n}^t=(1-\eta)M_{\Delta,n}^t+\eta M_{\Delta,g}^t$

34. end for

1）初始化模型和参数。在客户端和服务器端初始化基础模型 M_B，用于后续的知识共享和模型更新。设置联邦学习的超参数，包括全局轮次 R、本地轮次 e、本地学习率 l_c 和全局学习率 l_g 等。

2）客户端本地抗遗忘过程。当新任务 t 到达客户端时，客户端为该任务初始化一个轻量化模块 $M_{\Delta,n}^t$，该模块只在当前任务 t 上进行训练，用于捕捉当前任务的特征。利用当前任务的数据 $\mathcal{D}_n^t$ 对基础模型 M_B 和轻量化模块 $M_{\Delta,n}^t$ 进行联合训练。完成本地训练后，客户端将更新后的轻量化模块发送给服务器，同时保留本地的轻量化模块副本，以便在客户端层面实现知识的积累，克服灾难性遗忘。

3）服务器端全局抗遗忘过程。服务器收集所有客户端发送的轻量化模块 $\{\mathcal{M}_{\Delta,n}^t\}_{t=0}^{T-1}$。对于客户端集合 $C=\{C_1, C_2, \cdots, C_N\}$ 中每个客户端的第 t 个任务对应的轻量化模块 $M_{\Delta,n}^t$，服务器利用模型反演技术，生成不同客户端上每个任务对应的伪图像 $Z_n^{t,cat}$。

4）伪图像筛选。服务器使用 SelectTop-S($M_G^t(z_g^{t,cat})$) 函数对生成的伪图像进行筛选和处理，形成一个类别均衡且高质量的伪图像集合 $Z_s^t=\bigcup_{cat^t} Z_n^{t,cat}$，该集合具有每个客户端上不同任务的代表性特征和模式。

5）全局模型微调。使用筛选后的伪图像集合 Z_s^t 对全局轻量化模块 $M_{\Delta,g}^t$ 进行微调，通过优化全局损失函数来更新全局模型的参数，从而缓解数据分布差异导致的模型性能下降问题。

6）模型集成与更新。客户端将服务器端更新后的全局模型 $M_{\Delta,g}^t$ 与本地的轻量化模块 $M_{\Delta,n}^t$ 进行结合，随后将其下发至客户端，用于后续任务的推理。通过本地-全局的双重抗遗忘机制，客户端模型既能够利用全局模型来缓解不同客户端由于数据分布带来的模型性能损耗问题，又能通过本地轻量化模块的存储实现对旧任务的良好性能，从而有效缓解灾难性遗忘问题。

4　实验及结果分析

实验部分主要介绍实验设置以及在 CIFAR10，CIFAR100 以及 TinyImageNet 数据集上的实验结果。

4.1　实验设置

4.1.1　数据集

CIFAR10 数据集[40]包含 60000 张 32×32 像素的彩色图像，分为 10 个类别，如飞机、汽车、鸟类、猫、鹿、狗、青蛙、马、船和卡车，每类有 6 000 张图。其中 50 000 张用于训练，10000张用于测试。CIFAR100 数据集[40]包含 100 个不同的类别共 60000 张图片，每个类别有 600 张彩色图像，图像尺寸为 32×32 像素。其中 50 000 张用于训练，10 000 张用于测试。TinyImageNet 数据集[41]是基于 ImageNet 数据集构建的一个子集，旨在为在资源受限环境下的深度学习研究提供一个相对较小但又能保持一定复杂度的数据集。它包含 200 个类别，每个类别有 500 张训练图像、50 张验证图像和 50 张测试图像，图像尺寸为 64×64 像素。这些图像从 ImageNet 的 1 000 个类别中选取。为了模拟客户端不断接收包含新类别数据的任务，将数据集按照类别划分为多个任务，每个任务包含一组新的类别。训练过程中，客户端依次接收这些任务，逐步学习新类别的数据。为了模拟数据的异构性，采用了非独立同分布(Non-IID)的数据划分策略。具体而言，首先根据狄利克雷分布为每个客户端分配不同类别的数据，从而控制客户端之间数据分布的差异程度。通过调整狄利克雷分布的参数 α，能够灵活地模拟不同程度的数据异构性。

4.1.2　基准

本文使用的基准算法主要包括联邦学习领域的经典方法 FedAvg[8]和 FedProx[42]，以及联邦持续学习领域的 SOTA 方法 FedLWF[21]，MFCL[22]，FedWeIT[15]，FedTA[43]。具体介绍如下。

FedAvg[8]由 Google 提出，是联邦学习中的经典算法。客户端在本地数据上独立训练模型多个轮次后，将模型参数上传至服务器，服务器对各客户端模型参数取平均得到全局模型，再传输回客户端进行下一轮训练。

FedProx[42]在 FedAvg 基础上引入近端项，对客户端模型更新进行约束，防止客户端更新过度偏离全局模型，适用于客户端系统异构或存在恶意客户端的情况。

FedLWF[21]通过零样本蒸馏进行联邦类持续学习，在不涉及用户真实数据的情况下，利用全局信息生成合成数据，提取旧任务知识。

MFCL[22]利用生成模型来合成过去分布的样本。这些数据可以稍后与训练数据一起使用，以减轻灾难性遗忘。

FedWeIT[15]将网络权重分解为全局参数和特定任务参数，每个客户端可以通过对其特定任务参数进行加权组合，从其他客户端那里获得选择性知识。FedWeIT 最大限度地减少了不兼容任务之间的干扰，并且在学习过程中允许客户端之间的积极知识转移。

FedTA[43]方法通过将可训练的尾锚(Tail Anchor)与冻结的输出特征混合，调整它们在特征空间中的位置，克服了参数遗忘和输出遗忘的问题。

4.1.3　模型与超参数

使用预训练好的 ResNet18 模型作为基础模型，客户端数量为 50，每轮有 10% 的客户端参与训练。本地轮次设置为 100，本地学习率设置为 0.05，全局学习率设置为 0.001。每个任务生成的伪图像数量设置为 256，筛选每个客户端模型中不同任务的质量最好的 64 张伪图片进行聚类，随后对全局模型进行微调。在推理阶段，任务的 ID 序号由手工标注的方式给出，随后根据任务 ID 调用相应的任务模型。

4.2 评估指标

为了验证本地-全局双重抗遗忘机制的有效性，采用了标准的持续学习指标，包括所有任务的平均准确率$\bar{\mathcal{A}}$和平均遗忘率$\bar{\mathcal{F}}$。此外，考虑到联邦学习中的资源限制，引入了运行时间$\mathcal{T}$、存储、计算、通信资源作为评估指标，以直观地评估资源消耗情况，验证 LoRA 方法的引入降低了资源的消耗。

1)平均准确率$\bar{\mathcal{A}}$。对于所有已观察到的类别，模型在每个任务 t 上的准确率表示为$\mathcal{A}_t$。$\bar{\mathcal{A}}$表示在所有 T 个可用任务上$\mathcal{A}_t$的平均值：

$$\bar{\mathcal{A}}=\frac{1}{T-1}\sum_{t=0}^{T-1}\mathcal{A}_t \tag{22}$$

2)平均遗忘率$\bar{\mathcal{F}}$。任务 t 的遗忘率定义为模型在训练任务 t 时达到的最高准确率 $a_{r,t}$ 与其在后续推理中的表现之间的差值。因此，可以通过在任务$\mathcal{T}_t$结束时，对从任务 0 到 $T-1$ 的所有$\mathcal{T}_t$进行平均来评估平均遗忘率。

$$\bar{\mathcal{F}}=\frac{1}{T-1}\sum_{t=0}^{T-1}\max_{r\in\{1,\cdots,R\}}(a_{r,t}-\mathcal{A}_t) \tag{23}$$

3)最低准确率。对于所有已观察到的类别，模型在 t 个任务上的准确率中的最小值表示为$\mathcal{A}_{\min}$。

4)运行时间$\mathcal{T}$。测量服务器或客户端在每轮联邦学习中所花费的时间，单位为秒。该时间在本地 NVIDIA 4090 GPU 上记录，并在不同客户端之间进行平均。

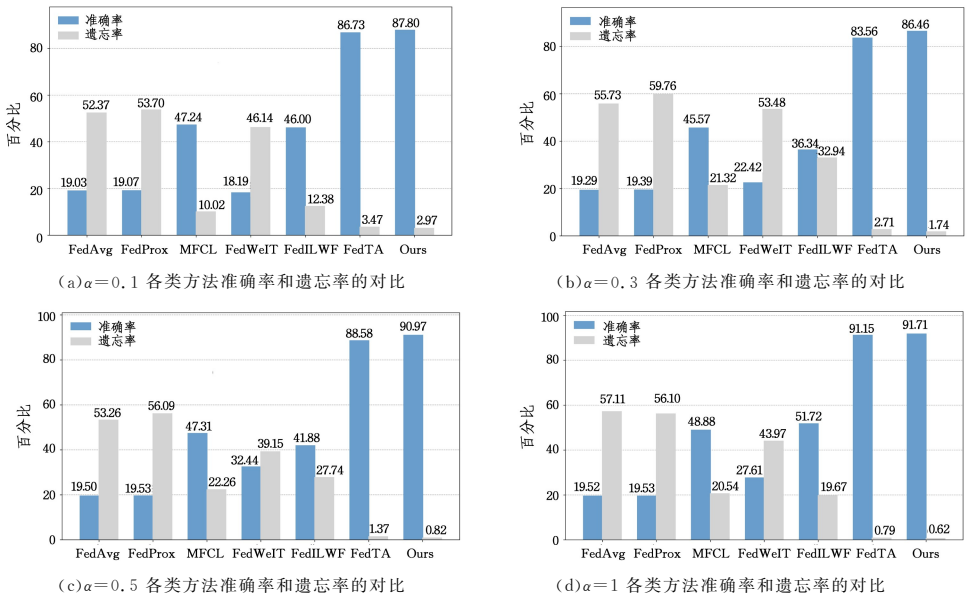
5)计算资源。在模型训练和推理过程中所使用的计算设备的资源总量，包括计算设备的使用时间、计算频率、内存占用以及浮点运算次数等。本文主要以运行时间和模型的收敛速度来衡量计算资源消耗。

6)存储资源。在联邦学习过程中，客户端用于存储模型参数、历史数据以及其他相关辅助信息所占用的存储空间大小。在资源受限的设备上，如移动设备或边缘设备，存储空间通常是有限的。因此，存储消耗是一个重要的评估指标，它直接影响到联邦学习系统的可扩展性和实用性。

7)通信压力。在联邦学习过程中，客户端与服务器之间传输更新的模型参数所需的通信资源。

4.3 主要实验结果

首先针对较小规模的任务数量开展实验。在 CIFAR10 数据集上，将设置任务数量为 $T=5$，$\alpha=\{0.1,0.3,0.5,1\}$4 种不同的异构场景。全局轮次设置为 20。如图 4 所示，在不同的异构场景中，本文方法相较于其他方法，在准确率和遗忘率两个指标上有优异的表现。



(a)$\alpha=0.1$ 各类方法准确率和遗忘率的对比　(b)$\alpha=0.3$ 各类方法准确率和遗忘率的对比

(c)$\alpha=0.5$ 各类方法准确率和遗忘率的对比　(d)$\alpha=1$ 各类方法准确率和遗忘率的对比

图 4　在 CIFAR10 数据集上 $T=5$ 时不同异构场景下各类方法的表现

Fig. 4　Performance of various methods under different heterogeneous scenarios on the CIFAR10 dataset with $T=5$

为进一步验证本文方法在大规模任务数量场景下的有效性在 CIFAR100 数据集[40]上开展实验，设置任务数量为 $T=20$，$\alpha=\{0.1,0.3,0.5,1\}$4 种不同的异构场景，α 越小，表示数据异构程度越强烈。全局轮次为 50。结果如表 2 所列，本文方法在 4 个不同的数据异构实验场景中，平均准确率均远超其他方法，分别达到 63.96%，78.84%，80.21% 和 85.08%，相较于次优方法有 26.42%～68.14%的提升。本文方法在最小准确率这一指标上均高于其他方法，充分表明了本文方法的可靠性。经典的联邦学习方法以及联邦持续学习方法表现均较差。本文方法的平均遗忘率极低，这表明本文方法在更新模型以适应新数据时，能够有效保留对旧数据的学习成果，确保模型性能的连贯性和稳定性，避免了模型更新导致的灾难性遗忘问题。当数据异构程度逐渐增加时，本文方法相比次优方法的准确率提升更为明显。当 $\alpha=1$ 时，本文方法的准确率是次优方法的 1.26 倍，当 $\alpha=0.1$ 时，本文方法的准确率是次优方法的 1.68 倍，进一步验证了本文方法在缓解数据异构方面的有效性。原因在于本文方法设计的全局抗遗忘机制针对数据异构设计，当数据异构程度增加时，模型聚合过程中参数冲突导致的模型遗忘问题越明显。全局抗遗忘机制通过生成具有代表性的高质量伪图像，并训练全局模型以缓解模型的参数冲突导致的遗忘问题。在时间维度上，本文方法仅次于 FedLWF 方法，远超其他的联邦持续学习方法。

表 2　CIFAR100 数据集上 $T=20$ 时各方法在不同数据异构程度下的表现

Table 2　Performance of various methods under different degrees of data heterogeneity when $T=20$ on the CIFAR-100 dataset

数据异构程度	方法	$\bar{\mathcal{A}}$(%)	$\mathcal{A}_{\min}$/%	$\bar{\mathcal{F}}$/%	$\mathcal{T}$/s
$\alpha=0.1$	FedAvg	3.79	0.00	67.96	163.75
	FedProx	4.14	0.00	65.34	218.93
	MFCL	3.19	4.40	54.39	441.24
	FedWeIT	9.51	0.00	37.18	513.31
	FedLWF	16.16	0.00	23.43	**96.72**
	FedTA	38.04	31.20	10.64	163.77
	Ours	**63.96**	**41.80**	**0.12**	104.98
$\alpha=0.3$	FedAvg	4.59	0.00	77.16	142.47
	FedProx	4.42	0.00	77.05	200.76
	MFCL	21.80	2.60	24.39	432.04
	FedWeIT	5.04	0.00	28.10	123.03
	FedLWF	17.17	0.00	74.26	111.36
	FedTA	52.24	40.60	9.82	163.67
	Ours	**78.84**	**72.20**	**0.34**	**97.57**
$\alpha=0.5$	FedAvg	4.79	0.00	79.43	172.80
	FedProx	4.57	0.00	78.92	232.42
	MFCL	21.51	5.80	29.98	502.79
	FedWeIT	2.26	0.00	82.35	410.59
	FedLWF	12.48	0.00	36.22	**94.06**
	FedTA	65.53	53.00	0.47	163.73
	Ours	**80.21**	**73.00**	**0.31**	119.42
$\alpha=1$	FedAvg	4.76	0.00	81.61	145.08
	FedProx	4.77	0.00	81.20	212.27
	MFCL	23.92	9.60	29.16	415.29
	FedWeIT	4.73	0.00	79.25	417.01
	FedLWF	17.62	0.40	38.14	**92.63**
	FedTA	67.53	58.40	0.93	163.72
	Ours	**85.08**	**77.00**	**0.08**	99.96

4.4　在超大任务规模上的进一步验证

在数据异构场景 $\alpha=0.1$ 的设置下，TinyImageNet 数据集[41]划分任务数量为 $T=40$，全局轮次为 50，以此验证本文方法在数据异构场景下对大规模任务的有效性。如表 3 所列，现有的联邦学习以及联邦持续学习方法在面对高度数据异构和大规模任务的场景时，准确率严重下滑，遗忘率极高，模型不能实现对任务的有效记忆；而本文方法的平均准确率和最低准确率均优于传统的联邦学习方法和联邦持续学习方法。这一差距表明，在面对超大任务规模和极端数据异构性时，本文方法展现出了卓越的学习能力和泛化性能。其能够有效整合来自不同任务、不同数据分布的样本信息，构建出一个具备较高准确率的全局模型，而其他方法则难以在这种复杂的环境下准确捕捉数据特征，导致模型性能大幅下降。

表 3　TinyImageNet 数据集上 $T=40$，$\alpha=0.1$ 时各类方法的对比结果

Table 3　Comparative results of various methods when $T=40$, $\alpha=0.1$ on the TinyImageNet dataset

数据异构程度	方法	$\bar{\mathcal{A}}$(%)	$\mathcal{A}_{\min}$/%	$\bar{\mathcal{F}}$/%	$\mathcal{T}$/s
$\alpha=0.1$	FedAvg	1.46	0.00	49.87	64.97
	FedProx	0.60	0.00	48.02	71.71
	MFCL	4.05	0.00	42.58	231.33
	FedWeIT	0.50	0.00	48.16	440.83
	FedLWF	2.35	0.00	45.74	114.80
	FedTA	35.62	24.39	14.67	178.34
	Ours	**41.64**	**26.24**	**5.91**	**58.39**

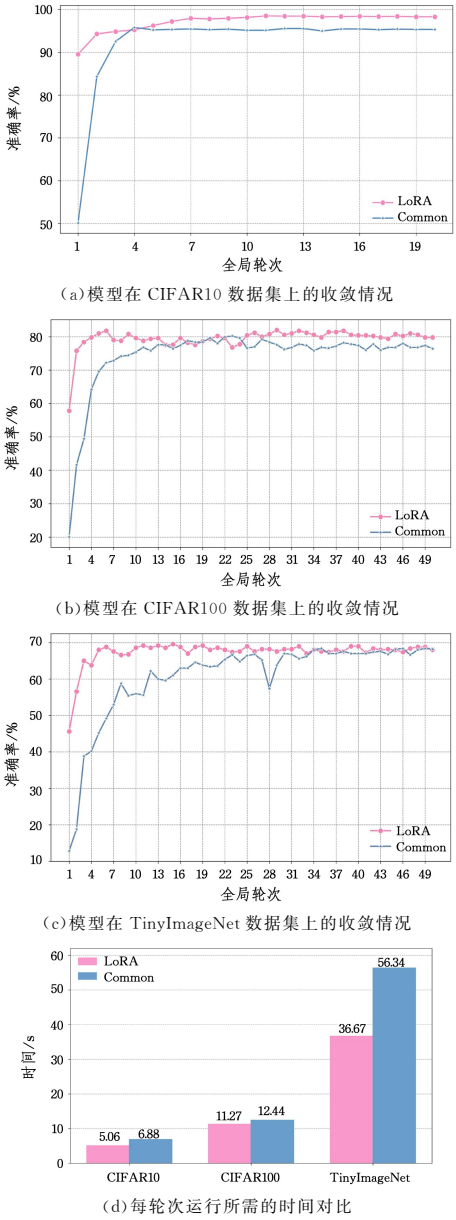
在平均遗忘率方面，本文方法为 5.91%，相较于其他方法同样具有明显优势。较低的遗忘率意味着，本文方法在不断学习新任务知识的同时，能够更好地保留对先前任务的学习成果，有效缓解了灾难性遗忘问题。其他方法在处理大量异构任务时，往往容易出现对旧任务知识的遗忘，从而影响模型的综合性能。本文方法的运行时间为 58.39 s，相较于 MFCL，FedWeIT，FedLWF，FedTA 等联邦持续学习方法，具有明显的时间效率优势；与经典的联邦学习算法 FedAvg 和 FedProx 的运行时间较为接近，但准确率远超经典的联邦学习算法。

4.5　消融实验

4.5.1　LoRA 组件的消融实验

将使用 LoRA 组件进行训练时的资源消耗状态与未使用 LoRA 组件时的资源消耗进行对比，从计算、存储、通信资源等方面进行全面评估。

1）计算资源分析。通过对客户端模型的收敛情况进行分析，展示计算资源的消耗情况，如图 5 所示。



(a)模型在 CIFAR10 数据集上的收敛情况

(b)模型在 CIFAR100 数据集上的收敛情况

(c)模型在 TinyImageNet 数据集上的收敛情况

(d)每轮次运行所需的时间对比

图 5　LoRA 方法和常规训练方法的收敛轮次和时间对比

Fig. 5　Comparison of convergence rounds and time between the LoRA method and the conventional training method

如图 5(a)—图 5(c)所示，在各类数据集上进行的测试结果表明，在客户端模型训练过程中使用 LoRA 方法可以使模型收敛得更快，且准确率更高。图 5(d)对每轮次运行所需时间进行了可视化，可以看出，本文方法在相同条件下，花费更少的时间实现了每轮次的训练。综上，本文方法可以在较早的轮次实现收敛，并且每轮次所需训练时长较短，表明了本文方法相较于传统方法可以节约计算资源。

2)存储和通信资源分析。如表 4 所列，在客户端使用 LoRA 方法对模型进行微调，仅需要调整并传输少量的模型参数，每轮传输的模型参数量仅占原有模型大小的 1%～2%。在通信资源受限的场景(如带宽有限的移动或边缘设备)中，LoRA 方法具有明显优势，其降低了通信开销，使模型微调更可行和高效。在存储特定于任务的轻量化模块时，客户端仅需存储被修改部分的特定于任务的模型参数，因此存储资源的占用与任务数量相关。相较于客户端计算资源以及准确率的大幅提升，客户端的存储资源略有提高是可以接受的。必要时，客户端可以仅保存常用任务的轻量化模块。

表 4 通信及存储资源分析

Table 4 Analysis of communication and storage resources

数据集	方法	修改/上传参数	参数总和	百分比/%	存储资源/MB
CIFAR10	LoRA	122 880	11 304 522	1.09	$0.49*T+44.59$
	NO_LoRA	11 172 164	11 172 164	100	44.59
CIFAR100	LoRA	122 880	11 350 692	1.08	$0.48*T+44.59$
	NO_LoRA	11 181 642	11 181 642	100	44.59
TinyImageNet	LoRA	209 653	11 181 642	1.83	$0.82*T+44.59$
	NO_LoRA	11 429 928	11 429 928	100	44.59

4.5.2 全局抗遗忘组件的消融实验

如表 5 所列，综合 3 个数据集的实验结果来看，去除全局微调操作后，模型的准确率在各个数据集上均出现了不同程度的下降，准确率的平均下降幅度约为 11.78%。这充分证明了全局抗遗忘组件在联邦持续学习中对于克服数据异构性具有显著的贡献。它通过在全局模型层面进行进一步的优化调整，有效缓解了数据异构带来的模型性能下降问题，从而取得了更高的准确率。

表 5 全局微调方法的消融实验结果

Table 5 Ablation experimental results for the global fine-tuning method

数据集	方法	修改/上传参数	参数总和	百分比/%
CIFAR10	LoRA	122 880	11 304 522	1.09
	NO_LoRA	11 172 164	11 172 164	100
CIFAR100	LoRA	122 880	11 350 692	1.08
	NO_LoRA	11 181 642	11 181 642	100
TinyImageNet	LoRA	209 653	11 181 642	1.83
	NO_LoRA	11 429 928	11 429 928	100

结束语 本文提出了一种基于双重抗遗忘机制的轻量化联邦持续学习方法，旨在解决联邦持续学习中任务数量增加以及数据异构程度提高导致的灾难性遗忘问题。该方法在客户端设计特定于任务的轻量化模块，克服数据变化及模型更新导致的灾难性遗忘；在服务器端通过无数据知识蒸馏生成类别均衡的伪图像，缓解数据分布差异导致的遗忘。

实验结果表明，该方法在 CIFAR10，CIFAR100 和 TinyImageNet 数据集上均取得了较高的性能提升，在不同数据异构程度下均展现出良好的效果。与其他方法相比，本文方法在平均准确率和平均遗忘率等指标上均具有显著优势，同时在计算资源和通信资源方面也表现出较高的效率。在超大任务规模和极端数据异构场景下，本文方法依然能够有效地整合不同任务、不同数据分布的样本信息，构建出具备较高准确率的全局模型，并有效缓解灾难性遗忘问题。然而，当任务数量不断增多时，大量的轻量化模块会对客户端造成存储压力，此时可综合考虑客户端的计算资源，决定是否开启一轮联邦学习的训练。在未来的研究中，可探索差分隐私机制在图像生成过程中的应用，以进一步保护数据隐私。

参 考 文 献

[1] DE CAPITANI DI VIMERCATI S, FORESTI S, LIVRAGA G, et al. Data privacy: Definitions and techniques[J]. International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, 2012, 20(6): 793-817.

[2] PARDAU S L. The california consumer privacy act: Towards a European-style privacy regime in the united states[J]. Journal of Technology Law & Policy, 2018, 23: 68.

[3] VOIGT P, VON DEM BUSSCHE A. The EU general data protection regulation(GDPR)[M]. Cham: Springer, 2017.

[4] CHI J L, FENG D G, ZHANG M., et al. Research Progress on Privacy-Preserving Ciphertext Retrieval Technology[J]. Journal of Electronics and Information, 2024, 46(5): 1-24.

[5] FIENBERG S E, SLAVKOVIĆ A B. Data privacy and confidentiality[M]// International Encyclopedia of Statistical Science. Berlin: Springer, 2025: 615-619.

[6] OMID P, SOREN F. The Digital Double: Data Privacy, Security, and Consent in AI Implants West[J]. Journal of Dental Sciences, 2025, 2(1): 108.

[7] BALOGUN A Y. Strengthening compliance with data privacy regulations in US healthcare cybersecurity[J]. Asian Journal of Research in Computer Science, 2025, 18(1): 154-173.

[8] 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.

[9] YANG Q. AI and Data Privacy Protection:Solution of Federated Learning[J]. Information Security Research,2019,5(11):961.

[10] DEMBANI R,KARVELAS I,AKBAR N A,et al. Agricultural data privacy and federated learning:A review of challenges and opportunities[J]. Computers and Electronics in Agriculture,2025,232:110048.

[11] KEMKER R,MCCLURE M,ABITINO A,et al. Measuring catastrophic forgetting in neural networks[C]// Proceedings of the AAAI Conference on Artificial Intelligence. 2018.

[12] LI Y C,WANG H Z,XU W C,et al. Unleashing the power of continual learning on non-centralized devices: A survey[J]. IEEE Communications Surveys & Tutorials, 2025, 28: 1059-1098.

[13] QU H,RAHMANI H,XU L,et al. Recent advances of continual learning in computer vision:An overview[J]. IET Computer Vision,2025,19(1):e70013.

[14] YANG X,YU H,GAO X,et al. Federated continual learning via knowledge fusion:A survey[J]. IEEE Transactions on Knowledge and Data Engineering,2024,36(8):3832-3850.

[15] YOON J,JEONG W,LEE G,et al. Federated continual learning with weighted inter-client transfer[C]// International Conference on Machine Learning. PMLR,2021:12073-12086.

[16] ZHANG J,CHEN C,ZHUANG W,et al. Target:Federated class-continual learning via exemplar-free distillation[C]// Proceedings of the IEEE/CVF International Conference on Computer Vision. 2023:4782-4793.

[17] FANG Z X,FU X D,DING J M,et al. Federated Class-incremental Learning for Unbalanced Data[J]. Journal of Chinese Computer Systems,2025,46(9):2121-2129.

[18] TONG G,LI G,WU J,et al. GradMFL:Gradient memory-based federated learning for hierarchical knowledge transferring over non-iid data[C]// International Conference on Algorithms and Architectures for Parallel Processing. Cham: Springer, 2021: 612-626.

[19] ZHANG Z,ZHANG Y,GUO D,et al. Communication-efficient federated continual learning for distributed learning system with Non-IID data[J]. Science China Information Sciences, 2023, 66(2):122102.

[20] CICIRELLO V,HU K,LU M,et al. A Federated Incremental Learning Algorithm Based on Dual Attention Mechanism[J]. Applied Sciences,2022,12(19),10025.

[21] USMANOVA A,PORTET F,LALANDA P,et al. A distillation-based approach integrating continual learning and federated learning for pervasive services[J]. arXiv:2109.04197,2021.

[22] BABAKNIYA S,FABIAN Z,HE C,et al. A data-free approach to mitigate catastrophic forgetting in federated class incremental learning for vision tasks[J]. Advances in Neural Information Processing Systems,2023,36:66408-66425.

[23] GUBEROVIĆ E,ALEXOPOULOS C,BOSNIĆ I,et al. Framework for federated learning open models in e-government applications[J]. Interdisciplinary Description of Complex Systems: INDECS,2022,20(2):162-178.

[24] FATHIMAA S,BASHA S M,AHMED S T,et al. Empowering consumer healthcare through sensor-rich devices using federated learning for secure resource recommendation[J]. IEEE Transactions on Consumer Electronics,2025,71(1):1563-1570.

[25] KONEČNÝ J,MCMAHAN H B,YU F X,et al. Federated learning:Strategies for improving communication efficiency[J]. arXiv:1610.05492,2016.

[26] HSIEH K,HARLAP A,VIJAYKUMAR N,et al. Gaia:{Geo-Distributed} machine learning approaching {LAN} speeds[C]// 14th USENIX Symposium on Networked Systems Design and Implementation(NSDI 17). 2017:629-647.

[27] LUPI NG W,WEI W,BO L I. CMFL:Mitigating communication overhead for federated learning[C]// 2019 IEEE 39th International Conference on Distributed Computing Systems(ICDCS). IEEE,2019:954-964.

[28] BONAWITZ K,EICHNER H,GRIESKAMP W,et al. Towards federated learning at scale:System design[J]. Proceedings of Machine Learning and Systems,2019,1:374-388.

[29] LIU Y,JAMES J Q,KANG J,et al. Privacy-preserving traffic flow prediction:A federated learning approach[J]. IEEE Internet of Things Journal,2020,7(8):7751-7763.

[30] TANG L T,WANG D,ZHANG L F,et al. A Federated Learning Scheme Based on Secure Multi-Party Computation and Differential Privacy[J]. Computer Science,2022,49(9):297-305.

[31] SHEN W,HUANG W,WAN G,et al. Label-free backdoor attacks in vertical federated learning[C]// Proceedings of the AAAI Conference on Artificial Intelligence. 2025:20389-20397.

[32] MAI Z,LI R,JEONG J,et al. Online continual learning in image classification:An empirical survey[J]. Neurocomputing, 2022, 469:28-51.

[33] MALLYA A,LAZEBNIK S. Packnet:Adding multiple tasks to a single network by iterative pruning[C]// Proceedings of the IEEE Conference on Computer Visionand Pattern Recognition. 2018:7765-7773.

[34] ALJUNDI R,CHAKRAVARTY P,TUYTELAARS T. Expert gate:Lifelong learning with a network of experts[C]// Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition. 2017:3366-3375.

[35] ROLNICK D,AHUJA A,SCHWARZ J,et al. Experience replay for continual learning[C]// Proceedings of the 33rd International Conference on Neural Information Processing Systems. 2019:350-360.

[36] SHIN H,LEE J K,KIM J,et al. Continual learning with deep generative replay[J]. arXiv:1705.08690,2017.

[37] LI Z,HOIEM D. Learning without forgetting[J]. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2017, 40(12):2935-2947.

[38] KIRKPATRICK J,PASCANU R,RABINOWITZ N,et al. Overcoming catastrophic forgetting in neural networks[J]. Proceedings of the National Academy of Sciences,2017,114(13): 3521-3526.

[39] DONG J,WANG L,FANG Z,et al. Federated class-incremental

learning[C]// Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition. 2022:10164-10173.
[40] ALEX KRIZHEVSKY. Cifar-10 and cifar-100 datasets[EB/OL]. http://www.cs.toronto.edu/ kriz/cifar.html.
[41] LE Y, YANG X. Tiny imagenet visual recognition challenge [EB/OL]. http://vision.stanford.edu/teaching/cs231n/reports/2015/pdfs/yle_project.pdf.
[42] 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.
[43] YU H, YANG X, ZHANG L, et al. Handling spatial-temporal data heterogeneity for federated continual learning via tail anchor[C]// Proceedings of the Computer Vision and Pattern Recognition Conference. 2025: 4874-4883.

WANG Pan, born in 2002, postgraduate. His main research interests include federated learning and continual learning.

WANG Ji, born in 1990, Ph.D, associate professor, master's supervisor. His main research interests include deep learning and edge intelligence.

(责任编辑:何杨)