MLDL project report - Federated Learning and Distributed Training

Mohamed Mostafa Kotb Hatem
s346906

Emin Oral
s343124

Sergio Petrone
s346070

Alican Akkiprik
s349610

Abstract

In an era where Machine Learning models demand increasingly larger datasets and concerns regarding data privacy are growing, Federated Learning (FL) emerges as a crucial paradigm for distributed training. By enabling multiple clients to collaboratively learn a global model without sensitive local data leaving their devices, FL offers an innovative solution to challenges related to privacy, security, and data decentralization. This approach represents a key frontier in Distributed Training, facilitating the development of intelligent systems that operate at scale with efficiency and data protection.

This work presents a detailed framework for applying Federated Learning to image classification on complex datasets such as CIFAR-100. The methodology employs Vision Transformer (ViT) models, specifically the vit_small_patch16_224 architecture, pre-trained via DINO (Self-distillation with NO labels) to ensure robust feature extraction. Our pipeline supports fine-tuning of the model's linear head directly on decentralized data, simulating scenarios of statistical heterogeneity (IID and non-IID) among clients. To address computational efficiency and scalability challenges in distributed environments, advanced pruning strategies (based on Fisher sensitivity, magnitude, and a hybrid approach) are integrated and evaluated to introduce sparsity into local models. Local training on each client is further optimized by the use of SparseSGDM, a specialized variant designed to efficiently manage gradients of sparse models. Model aggregation among clients is handled by the Federated Averaging (FedAvg) algorithm.

Our work includes a comparative analysis between the proposed FL approach and an equivalent centralized training setup. The effectiveness of ViT fine-tuning is attested by an accuracy of 45.6% on CIFAR-100 in the centralized setting. In summary, our framework provides concrete contributions to the optimization of federated training for computer vision, demonstrating how sparsity techniques can significantly improve the efficiency and robustness of models in decentralized data scenarios.

The code is available at `https://github.com/Mohamed-Hatem346906/FL-Project`