University at Buffalo The State University of New York

April 25, 2022

Dear Editor/Reviewer,

We would like to submit a research article entitled “Federated Learning with Privacy- Preserving Ensemble Attention Distillation” for consideration in the Special Issue on Federated Learning for Medical Imaging of IEEE Transactions on Medical Imaging (TMI).

Our article focuses on “Privacy-preserving federated learning” and its applications. It is an extended version of our previous work accepted by the International Conference on Computer Vision 2021:

> Xuan Gong, Abhishek Sharma, Srikrishna Karanam, Ziyan Wu, Terrence Chen, David Doermann, Arun Innanje, “Ensemble Attention Distillation for Privacy-Preserving Federated Learning,” The International Conference on Computer Vision (ICCV), 2021.

This extended version presents a comprehensive study of privacy-preserving federated distillation applied to three different tasks, chest-x-ray image classification, brain tumor segmentation, and brain MRI reconstruction, which we believe will be of interest to the readers of the journal.

The significant differences between this article and the conference submission includes extended and improved methods including the extension of Ensemble Attention Distillation to self-attention and image reconstruction task, more extensive evaluation and discussions including cross-domain theoretical analysis.

1. We extended the Related Work section with more details on federated learning methods, and also included the relevant works on structure knowledge distillation.
2. We extended our bound constraint from classification-specific top-down attention to also supporting self-attention, which is general in neural networks and can be applied to a broader range of tasks.
3. In addition to classification and segmentation-related tasks, we extended our framework to more general medical tasks, i.e., brain magnetic resonance image reconstruction. We conducted extensive empirical evaluations on FastMRI, BraTS2020, and IXI dataset on both T1 and T2-weighted modalities.
4. We theoretically analyze the performance bound of the central model learned through cross-domain knowledge distillation, where the local/teacher models are trained with private data from different domains.
5. We provide more comprehensive empirical studies on chest-x-ray image classification (Table I) and brain tumor image reconstruction (Table VI) in cross-domain scenarios, where local data are across different datasets, and public data are in other domains with local data.
6. We do more ablation studies on the number of local nodes, local heterogeneity (Table II), and public data size (Table III).
7. For generalization evaluation, we added experiment settings including public data with modalities different from local ones (Table V), and test data with different domain with public and all local training data (Table VII).

Part of theoretical analysis in the manuscript is related to our previous work accepted by the AAAI Conference on Artificial Intelligence 2022:

> Xuan Gong, Abhishek Sharma, Srikrishna Karanam, Ziyan Wu, Terrence Chen, David Doermann, Arun Innanje, "Preserving Privacy in Federated Learning with Ensemble Cross-Domain Knowledge Distillation," The AAAI Conference on Artificial Intelligence (AAAI), 2022.

This conference paper studies one-shot federated distillation applied in classification and segmentation tasks on natural images, medical images and text. The main differences between this journal submission and the conference paper can be summarized as:

1. The FL frameworks are different. In this manuscript we focus on attention ensemble distillation mechanism that can better leverage structure knowledge to explore local expertise consensus and diversity whereas the AAAI conference paper distills only logits from local nodes in federated learning.
2. In addition to classification-related tasks, we extended our framework to more general medical tasks, i.e., brain magnetic resonance image reconstruction. We conducted extensive empirical evaluations on FastMRI, BraTS2020, and IXI dataset on both T1 and T2-weighted modalities.
3. This manuscript includes additional discussions.
4. Our proposed attention ensemble distillation in this submission is more generally applicable to other tasks (e.g. image reconstruction), while the conference article only employ logits distillation specific to classification/segmentation tasks.
5. We set experiment protocol in typical medical image applications, while the conference article focuses more on image/language classification.
6. For generalization evaluation in this manuscript, we added experiment settings including public data with modalities different from local ones (Table V), and test data with different domain with public and all local training data (Table VII).

We have no conflicts of interest to disclose. Please address all correspondence concerning this manuscript to me at xuangong@buffalo.edu.

Thank you for your consideration of this manuscript.

Sincerely,

Xuan Gong

University of Buffalo