University of Utah
UNDERGRADUATE RESEARCH JOURNAL

LEARNING EFFICIENCY OF FEATURES EXCHANGE IN FEDERATED LEARNING

Xintong Liu (Mingyue Ji)
Department of Electrical and Computer Engineering

Abstract

In communication systems, a wealth of datasets can significantly improve the learning ability of models also the user experience on the device. However, due to the high amount of data that is hard to centralize into one location for training, and also many users expected the personal datasets can be maintained privacy constraints, the conventional training approach appears many restrictions. Our program uses an alternative training approach which is implementing features exchange in federated learning to train the model by aggregating locally computed updates without sharing datasets between workers. The purpose of the research is to investigate and conclude the feasibility of features exchange approaches in federated learning under the private condition. We show features exchange approach can reach a higher training accuracy value as compared to the training approach that without aggregation between workers.

Introduction

Federated learning is a learning technique that enables many workers to learn shared models collaboratively from rich data while keeping all the training data on the local device [1]. There are communications between each worker after specific amounts of local updates to share training features with others to improve learning efficiency. The communication between workers is called aggregation. Each worker has a local training dataset that is biased and non-IID. In the aggregation process, each worker can share any features of images with others but not the local image itself to maintain the users' privacy. So, each worker can obtain the training parameters of other workers but cannot access their input image datasets. In this condition, the communication between workers can increase their learning efficiency while protecting the privacy of each local device.

In the communication between workers, after receiving some exchanged features from others, each worker can somehow obtain more information about the image datasets and equivalently see more data. Thus, the trained model can achieve better accuracy ideally. For example, if the worker wants to train a model to classify a cat, but only have a few images of cats. Then this worker may want to ask other features of cats from other workers. With those features, the local model could be more accurately trained. Hence, the learning efficiency of the model could be improved by exchanging features in aggregation.

Methods

The simulation is designed to create a federated learning model by using the TensorFlow library in the *Python* software with Keras package. The designed code is used to build a training model for classifying the MNIST datasets image. There are four workers to train models, each worker is randomly distributed ¼ of images from the MNIST dataset for training. The training models are constructed by two dense layers in each has 64 neurons and 10 neurons respectively.

To investigate the feasibility of the features exchange approach, the model which is trained with this approach will be compared with the baseline model which is trained without features exchange. In the baseline model, each worker trains 500 iterations locally to update the training parameters and there is no communication between workers. The loss and accuracy outcomes will be stored and compared with the other case.

The case of features exchange is also trained with four workers. The exchanged features are weight parameters in each layer of the model. In the aggregation process, the central cloud waits for all workers to send their features, aggregate them, and send the updated parameters back to all workers afterward. Overall, each worker obtains more features from other workers through aggregations and ideally can improve the learning efficiency in comparison to the baseline model. The program is implemented in Google Colab to collect the testing loss and accuracy outcomes. By comparing the results of testing accuracy, we can conclude the feasibility of features exchange approach in federated learning.

Results

To evaluate the learning efficiency of the features exchange approach, the software program computes the testing loss and accuracy of the features exchange model and the baseline model. The testing accuracy outcome of the features exchange model is around 92.5% for each worker. However, the baseline model which does not contain any aggregation between workers reaches the testing accuracy around 88%. Thus, as we expected, the features exchange model has realized a similar learning performance as compare with the conventional training model while this model deals with the rich datasets challenge. Overall, the features exchange approach can improve the learning efficiency of the model while protecting the privacy of the user's datasets.

Conclusions

Based on the comparison of testing accuracy outcomes, the cases of features exchange model can reach higher accuracy outcomes as compared to the baseline model which does not train with features exchange approach. While the features exchange approach successfully achieves the learning performance of the conventional training, this approach overcomes the limitation of a wealth amount of datasets and also offers many privacy benefits for the user's device since the dataset does not require to be centralized into the cloud. Overall, the features exchange approach in federated learning can improve the learning efficiency of the model, and this approach is feasible to perform a high quality of training performance while solving the rich datasets challenge and guaranteeing the privacy of each user's device.

References

[1] H. B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. y Arcas, "[PDF] Communication-Efficient Learning of Deep Networks from Decentralized Data: Semantic Scholar," *undefined*, 01-Jan-1970.