Evaluation of Differential Privacy Variants in Deep Learning

Ivoline Ngong, Protiva Sen, Olivia Wilson

Deep learning models require large volumes of data to produce reasonable results after training. This data may contain sensitive information which can be exposed through the models. In this project, we intend to implement differential privacy in a deep learning model. Specifically, we will perform experiments with the DP-SGD, Renyi differential privacy and zero-concentrated differential privacy using a Convolutional Neural Network (CNN). All experiments will be implemented on the MNIST dataset and their performances evaluated. With this approach, we get to see how these approaches work in a deep learning setting.