Applying Local Differential Privacy in Handwriting Recognition-based Systems*

Faculty Poster Abstract

Sajedul Talukder[1] *and Abdur R. Shahid*[2]
[1]*Southern Illinois University*
Carbondale, IL 62901
sajedul.talukder@siu.edu
[2]*Robert Morris University*
Moon Township, PA 15108
shahid@rmu.edu

Abstract

The sharing of handwritten text via applications, widely used in various consumer electronic devices and the Internet of Things (IoT) for handwriting recognition purposes, does not provide adequate privacy assurances. Privacy leakage can happen at any point of the recognition system, which includes 1) data collection, 2) model training, 3) output generation, and 4) model usage by the user. Breaching of a handwriting recognition-enabled application might result in the release of sensitive personal information on its writer, which can have significant ramifications. In this work, we present a method to distort a user's original handwriting before sharing it with a specific application by adding configurable statistical noise to achieve local differential privacy (LDP). We construct a shape-deformed test set by applying the method to the MNIST dataset and implement a visualization tool to illustrate the impact of the proposed approach on recognition to analyze and quantify its impact. Then, using the MNIST dataset, we train, assess, and compare convolutional neural networks (CNN), Naive Bayes, random forest, support vector machine, and decision tree classifiers. Our work shows that in local differential privacy settings, without adjusting the CNN for private pictures, it is possible to obtain approximately 80% accuracy, paving the way for more study in this area.