EE599 Deep Learning – Initial Project Proposal

©K.M. Chugg

April 14, 2020

Project Title: Obfuscating Web User Search Queries via Generative Adversarial Privacy

Project Team: **Jiang Zhang, Zhongxuan Ruan, Mengwei Yang.**

Project Summary: In this project, we propose to obfuscate web user search queries via Generative Adversarial Privacy (GAP) architecture. Specially, we will train a pair of Deep Neural Networks (DNNs): one is the generator to mutate work tokens in web user search queries, and the other acts as an adversary to distinguish obfuscated queries from origin queries. By maximizing the prediction loss of adversary and minimizing the Euclidean distance between obfuscated queries and origin queries, the privacy of web user search queries will be enhanced and the utility loss can be traded. This project will involve implement two RNNs and leverage adversarial learning techniques to train them. And we will utilize AOL dataset releaseb in 2006. A successful outcome would be some demos of obfuscated search queries generated by GAP.

Data Needs and Acquisition Plan: We have downloaded AOL dataset, which contains real web search queries of more than 650,000 anonymous users over 3 months period in 2006. We will firstly preprocess the whole dataset and select 10,000 users who have more then 100 queries. Then, we will employ the existing *Word2vec* model proposed by Google to covert work tokens in queries into feature vectors (with dimension of 300). Finally, we will store the extracted features into h5 file.

Primary References and Codebase: We propose to build on the approach used in

1 Huang Chong, et al., "Generative adversarial privacy. arXiv preprint arXiv:1807.05306, 2018."

2 Masood Rahat, et al. "Incognito: A method for obfuscating web data. Proceedings of the 2018 World Wide Web Conference, 2018."

3 Dataset download link: AOL dataset.

4 *Word2vec* blog link: Google's trained Word2Vec model in Python.

Architecture Investigation Plan: We plan to first utilize the architecture used in [1] and replace the task with search query obfuscation in [2]. Then, we will explore replacing the MLPs with RNNs.

Estimated Compute Needs: Considering that we only select part of the whole AOL dataset and our GAP architecture will not contains CNNs, we estimate that we mainly utilize CPU server to run our training task (e.g. t2.2xlarge, $0.4 per hour). However, due to the complexity on data processing and potential usage of RNN, the total usage estimation would be $200.

Team Roles: The following is the rough breakdown of roles and responsibilities we plan for our team:

- Jiang Zhang: Implement the basic GAP architecture, including one generator and one adversary.
- Zhongxuan Ruan: Prepossess AOL dataset and convert word tokens in queries into feature vectors.
- Mengwei Yang: Investigate DNN models in GAP architecture.

All team members will work on the final presentation, slides, and report. And they will contribute equally to this project.

Requested Mentor with Rationale: We request Prof. Konstatinos Psounis to be our team mentor because he has expertise in GAP architecture. Jiali is our second choice because of his expertise in GANs. We have a good idea of what we want to do and have a good starting point from the references, so we are flexible regarding our mentor assignment.