Data Synthesis with Differential Privacy

Chia-Mu Yu

National Yang Ming Chiao Tung University

Abstract

Despite an increased demand for valuable data, the privacy concerns associated with sensitive datasets present a barrier to data sharing. One may use generative models to generate synthetic data, but unfortunately the synthetic data in this way may still contain sensitive information. Currently, differential privacy is golden standard of data privacy. Thus, an alternative approach is to construct differentially private generative models that quantitatively ensure the disconnection between the sensitive data and synthetic data. In this talk, we will go through the idea of differential privacy and briefly describe the recent research progress on the development of differentially private generative models.