PrivAI: Empowering Immigrants Through Privacy Preserving AI

Jamil Arbas, Toronto Metropolitan University

Abstract

PrivAI: Empowering Immigrants Through Privacy-Preserving AI tackles a critical issue at the intersection of artificial intelligence, privacy, and immigrant rights: how to protect sensitive attributes in high-resolution facial images without compromising realism or utility. As generative models become more powerful in synthesizing photorealistic images, they also raise serious privacy concerns. If such images leak or are misused, they can expose individuals to risks. Immigrants and asylum seekers—often required to submit legal documents, identification photos, and biometric data—are particularly vulnerable. Mishandling or exposure of this data may lead to profiling, discrimination, surveillance, or legal risks.

This project investigates the privatization of specific facial attributes such as gender and age through latent space manipulation in generative adversarial networks (GANs). Our approach applies differential privacy principles to ensure that privatized attributes cannot be reliably inferred or reversed, even by advanced adversarial models. The method selectively masks chosen features while preserving facial identity and visual realism, making it suitable for real-world deployment in migration and settlement contexts.

PrivAI introduces a novel framework that empowers individuals to control the personal characteristics embed- ded in their digital likenesses. By doing so, it addresses an urgent need for secure, privacy-conscious tools in the context of humanitarian technologies. The system ensures that biometric data shared during immigration processes cannot be exploited or weaponized. Ultimately, PrivAI aims to promote trust, autonomy, and dig- nity—providing immigrants with a safer pathway to engage with digital systems while safeguarding their most personal and sensitive traits.

Biography

Jamil Arbas is a PhD candidate in Computer Science at Toronto Metropolitan University. He began his PhD after completing a Master's at McMaster University, focusing on data privacy and machine learning. His research aims to enhance the fairness, security, and privacy of machine learning models. Recently, he has explored Local Differential Privacy, privacy-utility trade-offs, and private learning algorithms. Jamil co-authored the paper Polynomial Time and Private Learning of Unbounded Gaussian Mixture Models, which was accepted at the International Conference on Machine Learning (ICML) and presented in Hawaii in July 2023.