GANs Across Diverse Domains: A Review on Utility and Privacy

Boudaoud Arbia
Ahmed Draia University, Algeria

Kabou Salheddine
Higher Normal School - Bechar, Algeria

Abstract:

As privacy concerns intensify with the increasing collection and sharing of sensitive data, privacy-preserving techniques have become crucial in protecting personal information. In recent years, deep learning has emerged as a key player in privacy protection, offering advanced methods to generate synthetic data while maintaining privacy. Among these techniques, Generative Adversarial Networks (GANs) have gained significant attention due to their unique ability to create realistic data that mimics original datasets without compromising sensitive information. Various approaches utilizing GANs for privacy have been developed, addressing issues such as data anonymization, differential privacy, and adversarial robustness, while balancing data utility across diverse domains such as healthcare, finance, and Urban Mobility. This review paper systematically categorizes the existing studies on privacy preservation using deep learning, particularly focusing on GAN-based methods. It highlights the differences, strengths, and limitations across diverse privacy-preserving scenarios. Additionally, this paper discusses key challenges aiming to advance the application of GANs for privacy in real-world contexts.

Keywords:

Generative adversarial networks, privacy-preserving, Synthetic data.