PrivImage: Differentially Private Synthetic Image Generation using Diffusion Models with Semantic-Aware Pretraining

Kecen Li, *Institute of Automation, Chinese Academy of Sciences and University of Chinese Academy of Sciences;* Chen Gong, *University of Virginia;* Zhixiang Li, *University of Bristol;* Yuzhong Zhao, *University of Chinese Academy of Sciences;* Xinwen Hou, *Institute of Automation, Chinese Academy of Sciences;* Tianhao Wang, *University of Virginia*

https://www.usenix.org/conference/usenixsecurity24/presentation/li-kecen

This artifact appendix is included in the Artifact Appendices to the Proceedings of the 33rd USENIX Security Symposium and appends to the paper of the same name that appears in the Proceedings of the 33rd USENIX Security Symposium.

August 14–16, 2024 • Philadelphia, PA, USA

978-1-939133-44-1

USENIX Security '24 Artifact Appendix: PrivImage: Differentially Private Synthetic Image Generation using Diffusion Models with Semantic-Aware Pretraining

Kecen Li, Gong Chen, Zhixiang Li, Yuzhong Zhao, Xinwen Hou, Tianhao Wang

A Artifact Appendix

A.1 Abstract

We propose a novel Differential Privacy (DP) image synthesis method, termed PrivImage, which meticulously selects pre-training data, promoting the efficient creation of DP datasets with high fidelity and utility. PrivImage first establishes a semantic query function using a public dataset. Then, this function assists in querying the semantic distribution of the sensitive dataset, facilitating the selection of data from the public dataset with analogous semantics for pre-training. Finally, we pre-train an image generative model using the selected data and then fine-tune this model on the sensitive dataset using DP Stochastic Gradient Descent. On average, PrivImage achieves 6.8% lower FID and 13.2% higher Classification Accuracy than the state-of-the-art method. This artifact appendix mainly include instructions on how to reproduce FID and Classification Accuracy of PrivImage+D on `CIFAR-10` reported in our paper.

A.2 Description & Requirements

This section lists all the information necessary to recreate the same experimental setup we have used to run our artifact.

A.2.1 Security, privacy, and ethical concerns

All experiments are conducted on public image datasets and there is not any risk for evaluators while executing this artifact to the machine security, data privacy or others ethical concerns.

A.2.2 How to access

Our artifact can be accessed at GitHub[1]. You can download the entire project onto your Linux server.

A.2.3 Hardware dependencies

All experiments are conducted with Python 3.8 on a LINUX server with 4 NVIDIA GeForce 80G A100s, 512GB memory and stable internet connectivity for installing required packages. There is not specific need for the number of processors/cores.

A.2.4 Software dependencies

All the required packages and their installation can be found in the "requirements.txt" in the repository of our GitHub.

A.2.5 Benchmarks

We utilize `ImageNet`, a widely used dataset for pre-training in computer vision, along with `CelebA` and `CIFAR-10` for DP image synthesis research.

A.3 Set-up

This section includes all the installation and configuration steps required to prepare the environment to be used for the evaluation of our artifact.

A.3.1 Installation

First, you need to download Anaconda on the your server and use Anaconda to create your own Python environment like “conda create -n PrivImage python=3.8”. After activating this environment using “conda activate PrivImage”, you can install the required packages following the Section 3.1 of our GitHub.

A.3.2 Basic Test

The "README.md" in the repository provides an example for how to successfully reproduce the results on `CIFAR-10` in our paper.

[1] https://github.com/SunnierLee/DP-ImaGen/releases/tag/v1.0

A.4 Version

Based on the LaTeX template for Artifact Evaluation V20231005. Submission, reviewing and badging methodology followed for the evaluation of this artifact can be found at https://secartifacts.github.io/usenixsec2024/.