A. Artifact Appendix[1]

In this project, we develop a protective perturbation generator at the user end, which adds perturbations to the input images to prevent privacy leakage. In the meantime, the image recognition model still runs at the service provider end to recognize the protected image without the need of being re-trained. The detail of this project is described in our recently accepted MMSys'22 paper:

Mengmei Ye, Zhongze Tang, Huy Phan, Yi Xie, Bo Yuan, Sheng Wei. Visual Privacy Protection in Mobile Image Recognition Using Protective Perturbation. ACM Multimedia Systems Conference (MMSys), June 2022.

The GitHub repository of this project is at

`https://github.com/hwsel/ProtectivePerturbation`

which contains both the code and the instructions for the following three components:

- Set up the end-to-end image recognition system (both client and server) with the protective perturbation generator deployed at the client using our pre-trained model.
- Train our protective perturbation generator, with different target models and auxiliary models.
- Reproduce the experimental results reported in the paper.

We recommend the interested readers to follow the code and instructions in the GitHub repository to reproduce our system and results.

[1] This appendix is only for the reproducibility review at MMSys'22 and not intended for publication with the camera ready paper.