A. Artifact Appendix[1]

In the *LiVSec* project, to defend against the face spoofing attacks that face authentication systems can be effectively compromised by the 3D face models presented in the 3D surveillance video, we propose to proactively and benignly inject adversarial perturbations to the surveillance video in real time, which prevents the face models from being exploited to bypass deep learning-based face authentications while maintaining the required quality and functionality of the 3D video surveillance. The details of this project can be found in our MMSys'23 paper:

Zhongze Tang, Huy Phan, Xianglong Feng, Bo Yuan, Yao Liu, and Sheng Wei. 2023. Security-Preserving Live 3D Video Surveillance. In Proceedings of the 14th ACM Multimedia Systems Conference (MMSys '23), June 7–10, 2023, Vancouver, BC, Canada.

The GitHub repository of this project is at

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

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

- Reproduce the experimental results reported in the paper.
- Train your own 3D face authentication model and the real-time perturbation generator to prevent the face models in the surveillance video from being exploited to spoof the face authentication.
- Set up the end-to-end security-preserving live 3D video surveillance system integrating the perturbation generator.

We recommend that interested readers 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'23 and not intended for publication with the camera-ready paper.