

Supplementary Material for ProjAttacker: A Configurable Physical Adversarial Attack for Face Recognition via Projector

Yuanwei Liu^{1,2*} Hui Wei^{1,2*} Chengyu Jia^{1,2} Ruqi Xiao^{1,2}
Weijian Ruan^{3,4} Xingxing Wei⁵ Joey Tianyi Zhou⁶ Zheng Wang^{1,2†}

¹National Engineering Research Center for Multimedia Software, Institute of Artificial Intelligence, School of Computer Science, Wuhan University, Wuhan, China ²Hubei Key Laboratory of Multimedia and Network Communication Engineering, Wuhan, China
³Hangzhou Research Institute of Xidian University, Hangzhou, China ⁴Smart City Research Institute of China Electronics Technology Group Corporation, Shenzhen, China ⁵Institute of Artificial Intelligence, Beihang University, Beijing, China
⁶Centre for Frontier AI Research (CFAR), Agency for Science, Technology and Research (A*STAR), Singapore

A. Practicality Analysis

For physical adversarial attacks, constructing perturbation patterns in the real world is crucial for effective attacks. Our ProjAttacker employs a projector to cast perturbation patterns onto human faces. This process involves an alignment issue—determining the precise projection location on the face. To enhance robustness against alignment deviations, we introduce random projection and rotation perturbations during optimization. Additionally, the mask pattern of ProjAttacker closely aligns with the structural features of a real human face, enabling projection calibration based on facial landmarks (Fig. A). Experimental results from 50 physical tests confirm that calibration issues are negligible.

For real-world deployment, our attack requires only a compact, portable projector, making it highly mobile and adaptable to diverse scenarios. In contrast, existing physical attack methods, such as 3D-printed masks [5], depend on specialized 3D printing equipment, involve lengthy fabrication processes, and lack flexibility in switching attack targets. In comparison, our method incurs minimal time and cost while enabling real-time adaptation to diverse attack targets. These practical advantages make ProjAttacker well-suited for deployment in access control, mobile unlocking, and facial recognition attendance systems.

B. Details of using hiPAA Evaluation

As described in Sec. 4.3 of the main paper, we evaluated various attack methods, including TAP [4], AT3D [5], and our proposed ProjAttacker, using the hiPAA metric [3]. The hiPAA evaluation considers six dimensions: Effectiveness, Stealthiness, Robustness, Practicability, Aesthetics,

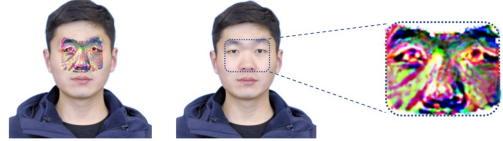


Figure A. The adversarial pattern contains features such as eyes, nose, and eyebrows. During projection, align the pattern with the eyebrows, the outer corner of the right eye, and the bottom of the nose to complete the calibration.

and Economics. Among these, Stealthiness, Practicability, and Aesthetics were assessed through a user study. We recruited 30 participants, providing them with prerequisite knowledge about physical adversarial attacks. Each participant then compared the three attack methods in terms of Stealthiness, Practicability, and Aesthetics using a form (as shown in Fig. B) and selected the method they deemed superior in each aspect. In total, we collected 90 responses from 30 participants, enabling a quantitative evaluation of our method against alternative approaches.

C. Light Reflection Function

To enhance the attack success rate of the generated adversarial pattern in real-world scenarios, our ProjAttacker incorporates a Light Reflection Function to simulate the imaging characteristics of projected light on human skin. As illustrated in Fig. C, the Light Reflection Function aims to capture specific spectral data to compute the resulting RGB values after projection. $S_{Projector}$ represents the power spectral distribution of the projector, where each pixel corresponds to a distinct spectral curve. The detailed parameters can be found in the projector's official documentation. S_{Nature} denotes the spectral power distribution of sunlight. $\rho(\lambda)$ represents the spectral reflectance curve of Asian skin, while $\sigma(\lambda)$ follows the XYZ color matching functions as




*Equal contribution †Corresponding author

User Study

Evaluation using HIPAA Metrics.

[Sign in to Google](#) to save your work. [Learn more](#)

Which result is better for attack stealthiness?

☐ (a)
☐ (b)
☐ (c)

Figure B. **Screenshot from the user study.** Each of the images labeled (a), (b), and (c) represents results obtained from different methods. The participants’ task was to choose the image they believed exhibited better attack stealthiness.

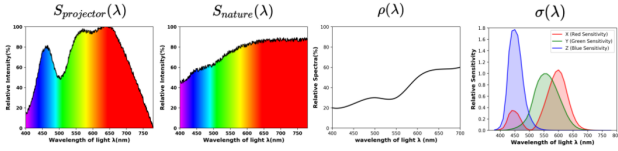


Figure C. By combining the projector spectrum, natural light, skin reflectance, and observer functions, the RGB values of the projected pattern can be precisely calculated.

defined by the official CIE standard.

D. Camera ISP Proxy Network

As outlined in Sec. 3.5 of the main paper, to address the physical-to-digital gap introduced by camera capture when deploying the ProjAttacker in real-world scenarios (see Fig. 2), we incorporate a camera capture simulation module. Specifically, this module employs a camera ISP proxy network that models the image processing pipeline. In this section, we provide a detailed explanation of the camera ISP proxy network and its role in bridging the domain gap.

Network Architecture: We employ a variant of the U-Net CNN architecture [2], utilizing 3×3 convolutions and 2×2 max pooling operations. The encoder consists of feature channels with sizes $\{32, 64, 128, 256, 512\}$, mirrored in reverse order for the decoder.

Input: The input consists of an RGB image and a 6-dimensional conditional input of hyperparameters. The val-

ues and meanings of these hyperparameters are listed in Tab. A.

Output: The output is an RGB image corresponding to the given conditional input hyperparameters.

Parameter	Sign	Value interval	Max
Brightness Contrast Control	a	(64, 256)	2^8
Hue Saturation Control	b	(64, 256)	2^8
Gamma Adjustment	γ	(0.4, 2.0)	2^1
Color Correction Matrix	c	(512, 1024)	2^{10}
Spatial Filtering	d	(0.1, 2.0)	2^1
Non-Local Means	e	(1.0, 32.0)	2^5

Table A. **Hyperparameters we select from the software camera ISP for building a differentiable camera ISP proxy network.** We focus on six parameters related to Color & Tone Correction and Denoising functions.

Training: We leverage an open-source, non-differentiable camera ISP simulator* and the COCO dataset [1] to generate 2,270 data pairs for training our camera ISP proxy network. The model is trained for 500 epochs, which is sufficient for loss convergence. We select the weights that yield the best performance.

References

- [1] Tsung-Yi Lin, Michael Maire, Serge Belongie, James Hays, Pietro Perona, Deva Ramanan, Piotr Dollár, and C Lawrence Zitnick. Microsoft coco: Common objects in context. In *European conference on computer vision*, 2014. 2
- [2] Olaf Ronneberger, Philipp Fischer, and Thomas Brox. U-net: Convolutional networks for biomedical image segmentation. In *Medical Image Computing and Computer-Assisted Intervention—MICCAI 2015: 18th International Conference, Munich, Germany, October 5–9, 2015, Proceedings, Part III* 18, pages 234–241. Springer, 2015. 2
- [3] Hui Wei, Hao Tang, Xuemei Jia, Zhixiang Wang, Hanxun Yu, Zhubo Li, Shin’ichi Satoh, Luc Van Gool, and Zheng Wang. Physical adversarial attack meets computer vision: A decade survey. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 2024. 1
- [4] Zihao Xiao, Xianfeng Gao, Chilin Fu, Yinpeng Dong, Wei Gao, Xiaolu Zhang, Jun Zhou, and Jun Zhu. Improving transferability of adversarial patches on face recognition with generative models. In *Proceedings of the IEEE/CVF conference on computer vision and pattern recognition*, pages 11845–11854, 2021. 1
- [5] Xiao Yang, Chang Liu, Longlong Xu, Yikai Wang, Yinpeng Dong, Ning Chen, Hang Su, and Jun Zhu. Towards effective adversarial textured 3d meshes on physical face recognition. In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*, pages 4119–4128, 2023. 1

*<https://github.com/QiuJueqin/fast-openISP>