CamPI: Physical Adversarial Examples through Camera Power Signal Injection

Supplementary Material

A. Ablation Study

We investigate the performance of power injection attacks with different optimization methods in the white-box setting. We apply FGSM, BIM, and PGD as baseline methods. We adopt attack success rate as the evaluation metric, which can be calculated by the fraction of test images whose predicted label changes after the attack. The results are summarized in Tab. A1. Overall, our method consistently outperforms the baselines across most models, demonstrating the advantage of the CW-based optimization method. While iterative methods such as BIM and PGD achieve higher attack success than the single-step FGSM, the CW-based approach demonstrates consistent improvement across all tested models, further enhancing the attack effectiveness.

Table A1. Ablation study on optimization methods. The best results are highlighted with **bold**.

Model	Methods			
	FGSM	BIM	PGD	Ours
ResNet-101	30.10	85.77	88.65	**94.62**
Inception-v3	47.08	91.99	**96.42**	95.56
VGG-19	74.05	98.74	99.65	**99.81**
DenseNet-161	51.19	97.52	98.70	**98.73**
ResNeXt-101	23.47	72.90	78.19	**90.61**
SqueezeNet-1.1	76.86	99.54	**99.69**	99.24
ShuffleNet-V2	46.01	96.70	97.65	**99.04**
Average	49.82	91.88	94.14	**96.80**

B. Attack on Different Cameras

To validate the transferability of the power signal injection attack on different cameras, we apply the attack to six commercial-off-the-shelf cameras, including four CMOS cameras and two CCD cameras in Fig. B1. We successfully implement the power signal injection attack on all six cameras. as shown in Fig. B2, and record the injection frequencies and amplitudes in Tab. B1.

Table B1. Transferability of the attack on six commercial cameras.

No.	Model	Type	Freq.	Amp.
①	HIKVISION DS-2CE56C3T	CMOS	149.1M	59
②	HIKVISION DS-2CE16D1T	CMOS	143.7M	35
③	DH-HAC-HDW1120E-DIP	CMOS	150.9M	32
④	DH-HAC-HDW1120E-DIP	CMOS	148.2M	63
⑤	SHL-045	CCD	48.5M	42
⑥	Hayear-011	CCD	51.6M	48

Figure B1. The six commercial-off-the-shelf cameras used for power signal injection.

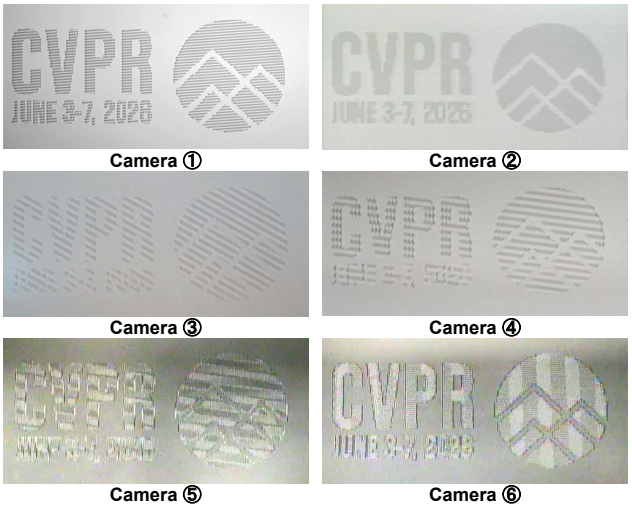

Figure B2. Feasibility of attack on various cameras.

C. More Visualization Results

C.1. Untargeted Attack

We present additional visualizations of untargeted attack in the white-box and black-box settings, as shown in Fig. D1. The attacks remain overall effective with different levels of perturbations, and larger perturbation budgets tend to induce misclassifications into a broader set of classes.

C.2. Affnity Targeted Attack

We provide the visualizations of the affinity target pairs listed in Tab. 2 in Fig. D2. We observe that certain object classes exhibit semantic proximity, giving rise to affinity targets that are susceptible to targeted adversarial attacks.

D. Ethical Considerations

Similar to other types of attack, the proposed attack may pose potential security risks to real-world vision systems. This work aims to highlight such vulnerabilities to raise awareness and motivate the development of more robust and secure vision systems. Possible mitigation strategies include incorporating power supply protection (eg, signal filtering) to reduce susceptibility to such attacks.

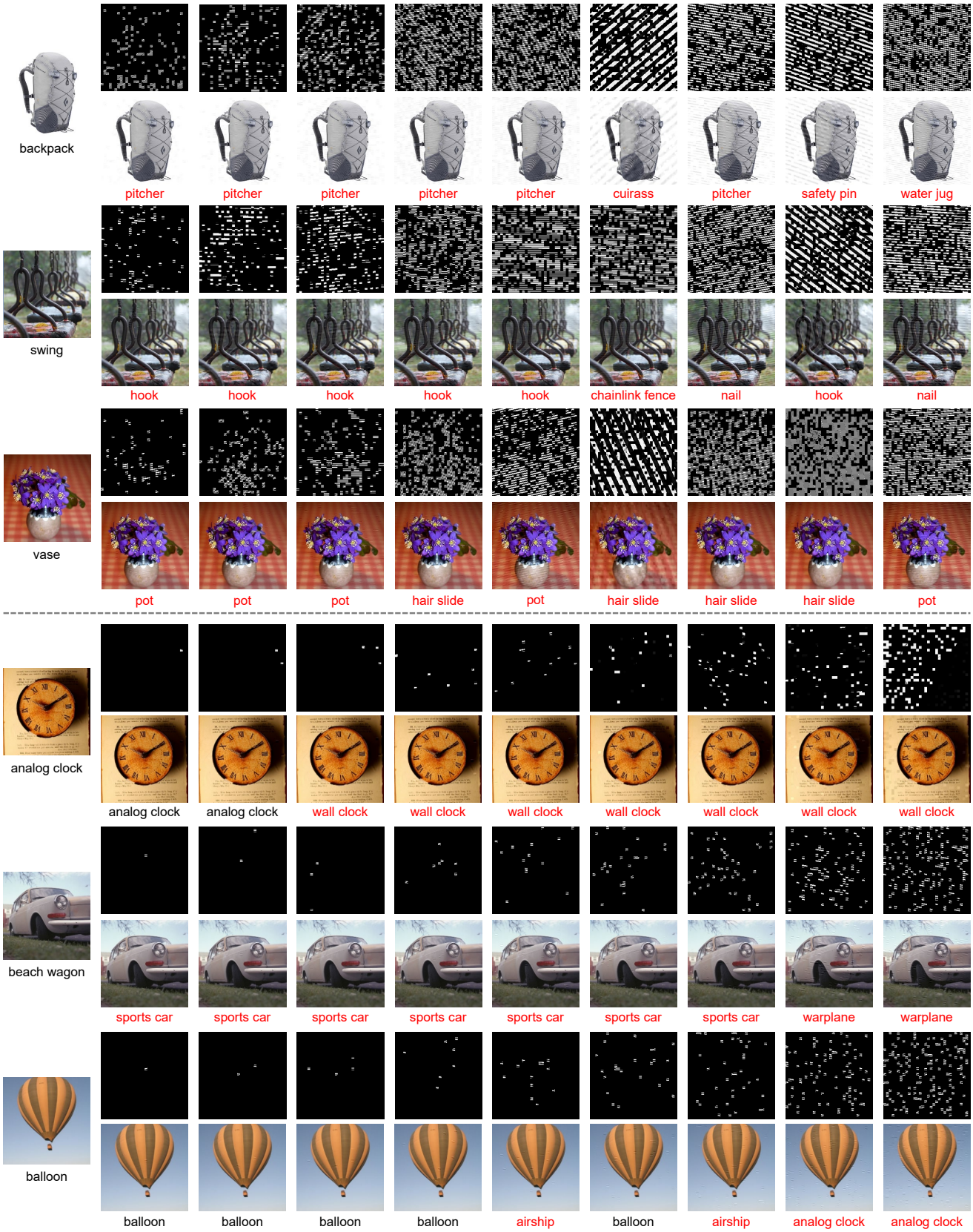

Figure D1. Visualization results of untargeted attack under different levels of perturbation in the white-box (top three rows) and black-box setting (bottom three rows).

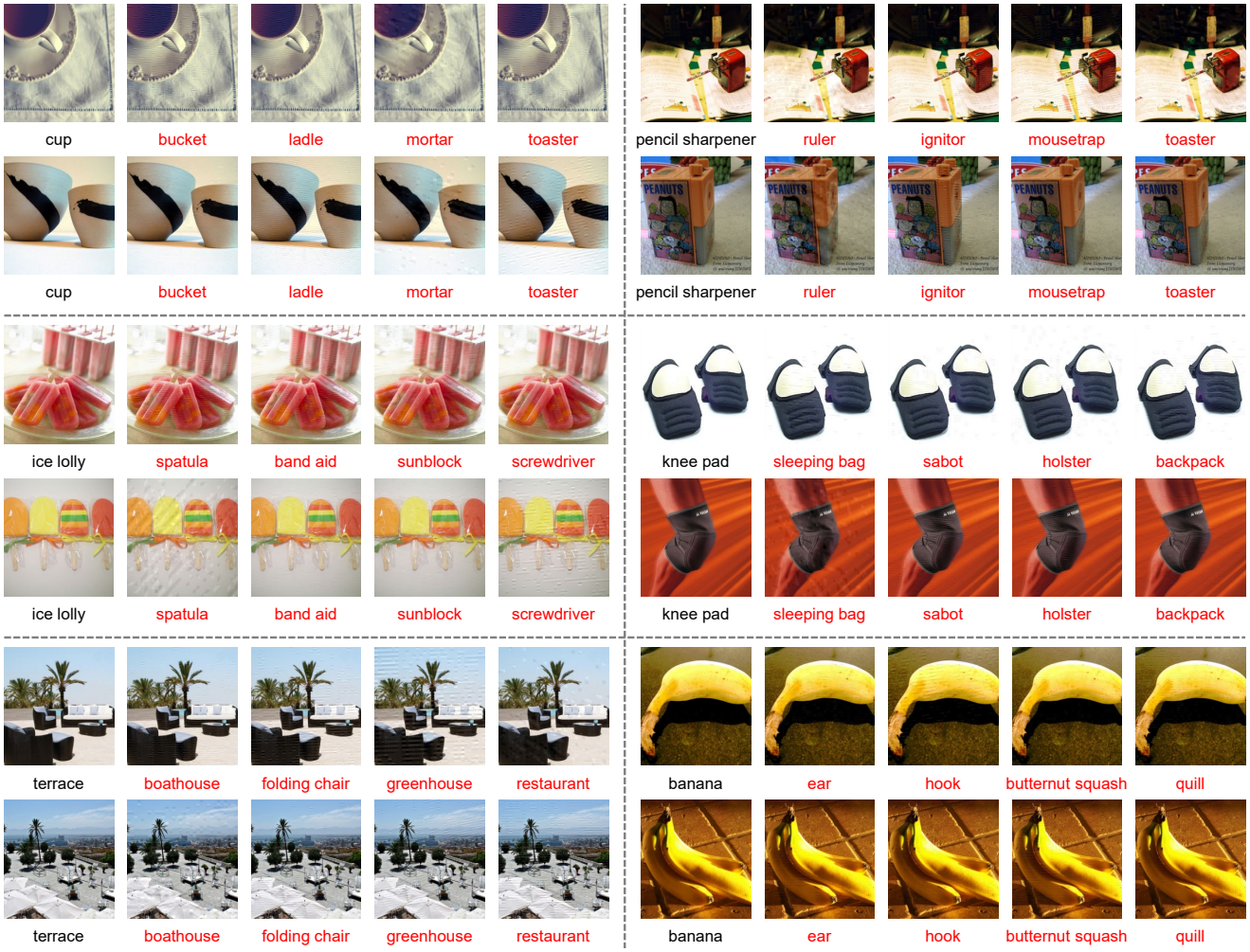

Figure D2. Visualization results corresponding to the affinity targets listed in Tab. 2.