Outsmarting Biometric Imposters: Enhancing Iris-Recognition System Security through Physical Adversarial Example Generation and PAD Fine-Tuning

Supplementary Material

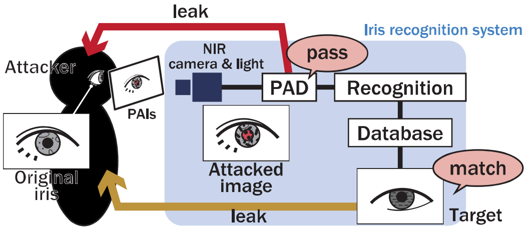


Figure 6. Our attack Scenario.

6. Our Attack Scenario

Figure 6 illustrates our proposed attack scenario. In this scenario, the attacker raises presentation attack instruments (PAIs), displaying the attack image to the capturing system. The target system includes Presentation Attack Detection (PAD) as a preprocessing step and iris recognition as a post-processing step. The attack image bypasses the PAD by evasion attack and proceeds to the recognition. This attack allows the attacker to impersonate or register without suspicion from unnatural actions in the image. In our scenario, the attacker can access the target iris image and the PAD model.

7. Experimental settings

In order to enhance the reproducibility of our results, we explain detail of experimental setting (Section 4.1) including the iris engines, hardware devices, and data employed in the experiments.

7.1. Iris Recognition Engines

We selected the hand-crafted iris recognition engine OSIRIS [43] and the CNN-based T-Center [10] and performed impersonation using internal representation. The publicly available OSIRIS includes Viterbi algorithm-based detection and normalization, feature extraction through six Gabor filters, and Hamming distance matching. T-Center uses a CNN-based feature extraction method, and TinyVGG was trained as a feature extractor on the ND-IRIS-0405 dataset [45, 46] with an applied OSIRIS detector and normalizer. We used 80% of the dataset for training data, same as described in [10]. USITv3 [49] includes several algorithm options for optimization, but we select best eer combination in [49] of contrast-adjusted Hough transform (CAHT) for detection, and quadratic spline wavelet (QWS) algorithms for feature extraction and Hamming-distance matching.

7.2. Physical Environments Settings

In our experiments, four Leimac IDBA-LE375S-IR-850 devices were utilized as NIR lights, with their power level set to 150/255. Table 5 lists the camera and lens settings used in our experiments and shows example images captured with the same iris in each environment. Additionally, we used PAIs, e-Paper, and printed paper as shown in Table 6. We show captured images of Siemens stars with a diameter of approximately 12mm, the same as the iris diameter, using e-Paper and printed paper. The display resolution of e-Paper is coarser than that of printed paper.

Table 5. Capturing environments

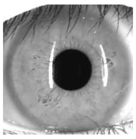
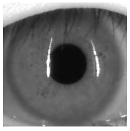
	Camera-1	Camera-2
Camera	Baumer VCXU-91M	Baumer VCXU-65M.R
Sensor	IMX267	IMX178
Shutter	global	rolling
Pixel size	3.45×3.45 [μm]^2	2.4×2.4 [μm]^2
Lens	Kowa LM50JC3M2	Kowa LM35JC3M2
Exposure	12 - 16 [ms]	12 - 16 [ms]
		

Table 6. Difficulty comparison between presentation attack instruments (PAIs) by capturing Siemens stars.

	e-Paper	Paper	digital
Device	Boox Max Lumi	Canon iR-ADV C5560F	
Dpi	207	600