Full-Distance Evasion of Pedestrian Detectors in the Physical World

Zhi Cheng¹, Zhanhao Hu², Yuqiu Liu³, Jianmin Li¹, Hang Su¹, Xiaolin Hu^{*1}



Introduction



Existing methods for generating adversarial patterns for evading pedestrian detection commonly fail at medium to long distances

Our full-distance attack method overcame this limitation with a **distant image converter** and a **multi-frequency optimization technique**

Distant image converter (DIC) motivation



- There is commonly an **appearance gap** between simulated distant adversarial patterns and their physical world counterparts
 - leading to incorrect optimization

DIC design **Camera simulation** Distant image dataset 4m labels 20m Print 20m 4m Skylight Turbidity Distance (Psky) DIC (T)(d)label Output image J Cam. Sim. Effect Atm. MSE AAF I.C. filter Pers. Sim. Sim. OSS θ_M θ_{S} 0c Digital SGD Image

Atmospheric perspective





Simulating blurring performed by AAF Simulating blurring performed by IC lo Input l_d Output Averaging in Distance IC sensor Averaging in AAF sim. locations d IC sim.

Effect filters



Sharpening & contrast



Full distance attack (FDA) pattern optimization



Multi-frequency optimization

- Restricting the overall pattern of the FDA pattern to be optimized for performing long distance attack
- Restricting its textures to be optimized for performing short distance attacks

DIC experiments



FDA experiments





Clothing attacks