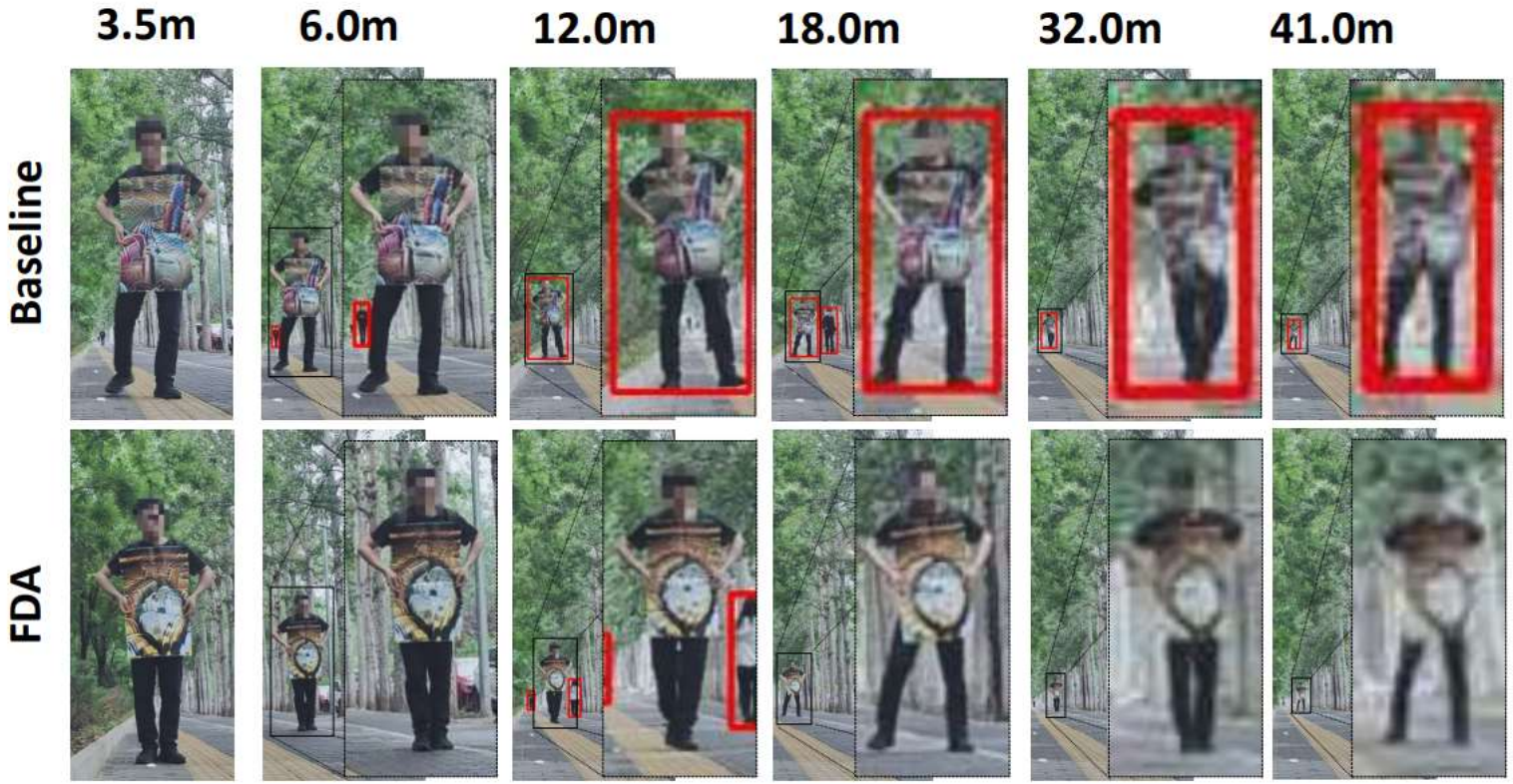
Full-Distance Evasion of Pedestrian Detectors in the Physical World

Zhi Cheng[1], **Zhanhao Hu**[2], **Yuqiu Liu**[3], **Jianmin Li**[1], **Hang Su**[1], **Xiaolin Hu**[*1]

1 2 3

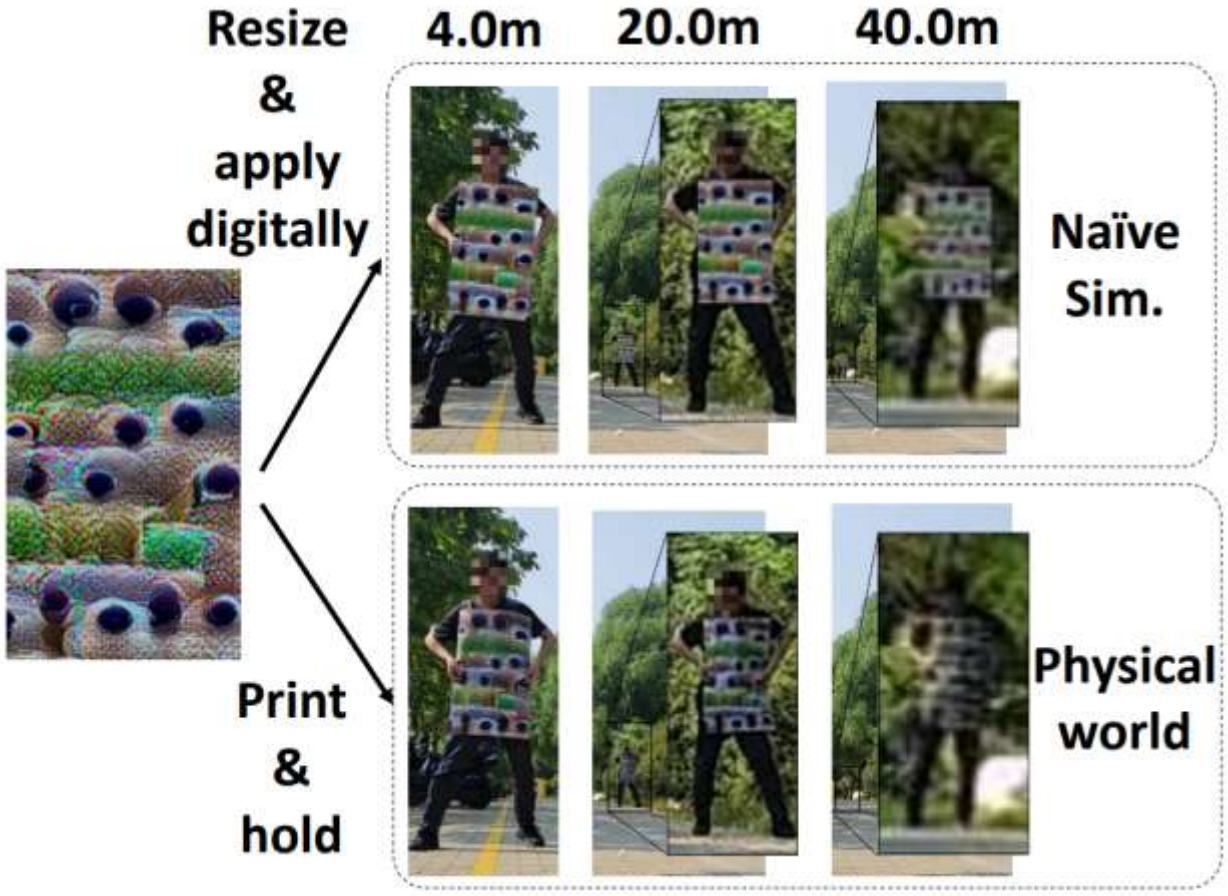
Introduction



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

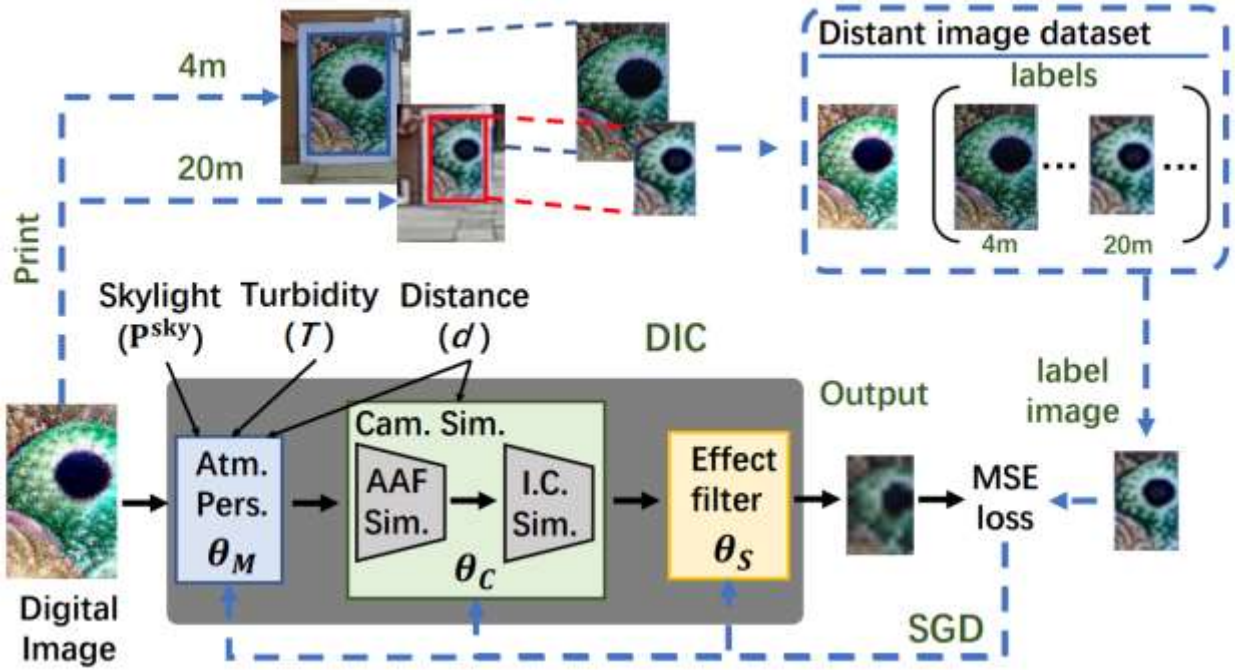
Our full-distance attack method overcame this limitation with a **distant image converter** and a **multi-frequency optimization technique**

Distant image converter (DIC) motivation

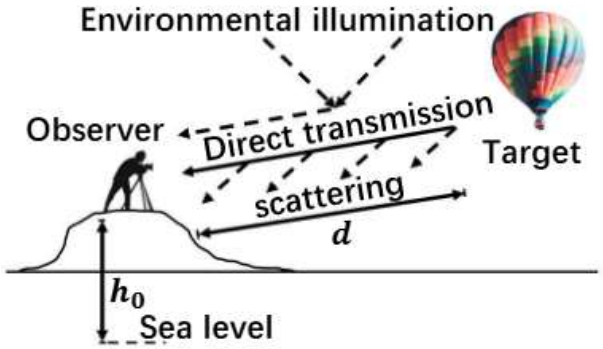


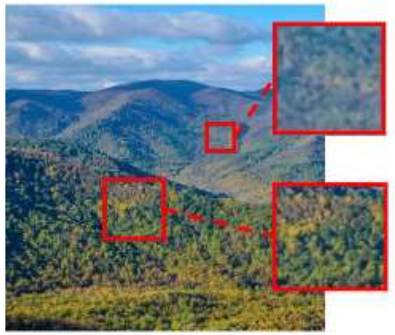
- There is commonly an **appearance gap** between simulated distant adversarial patterns and their physical world counterparts
  - leading to **incorrect optimization**

DIC design

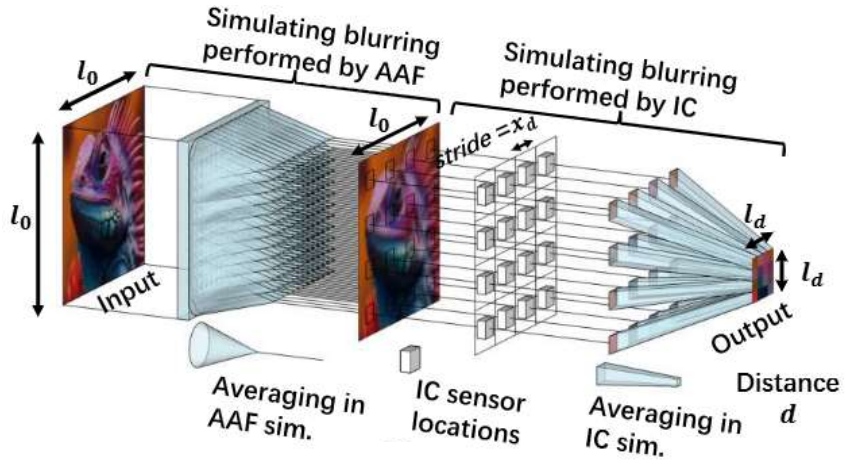


Atmospheric perspective





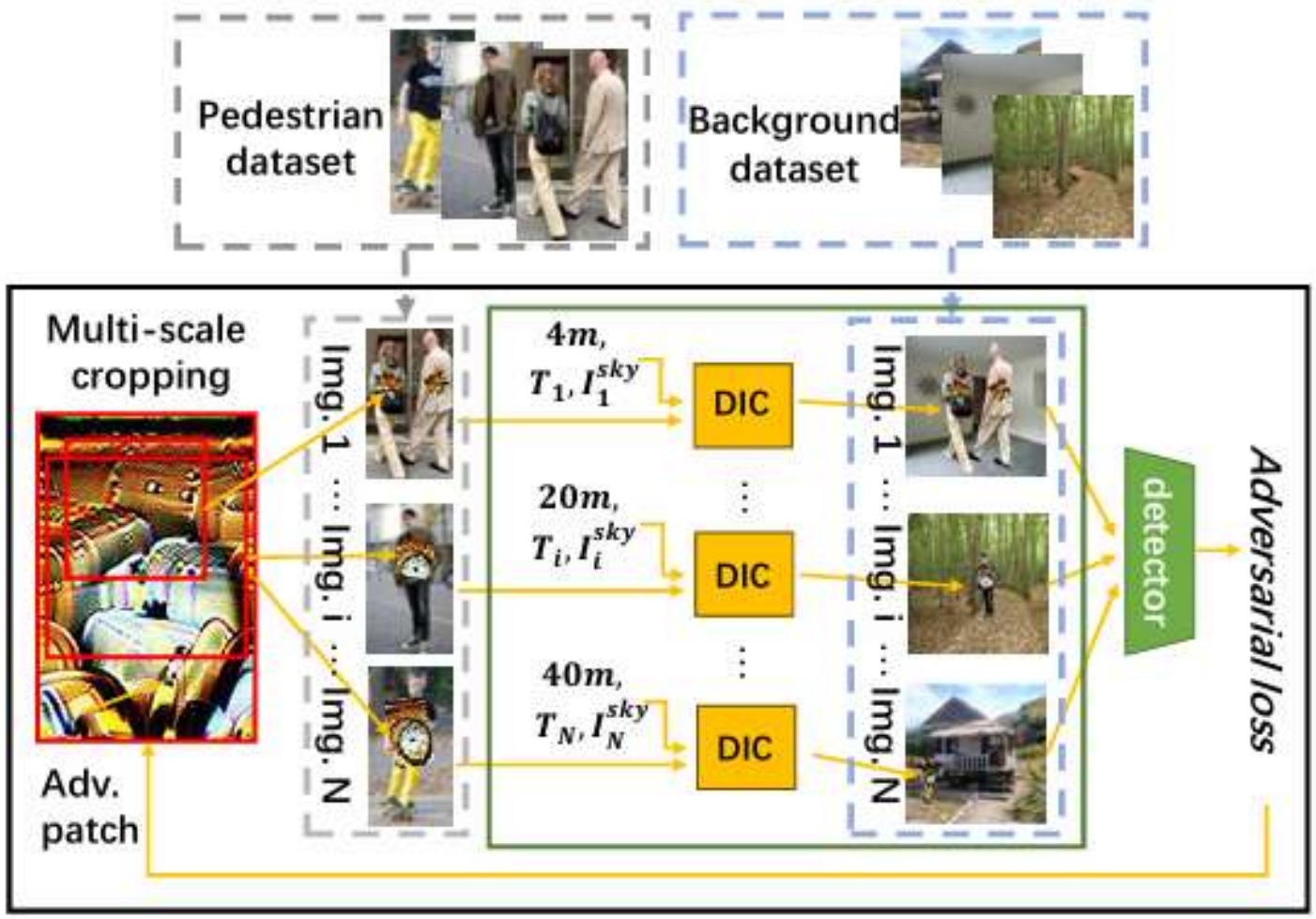
Camera simulation



Effect filters

Sharpening & contrast

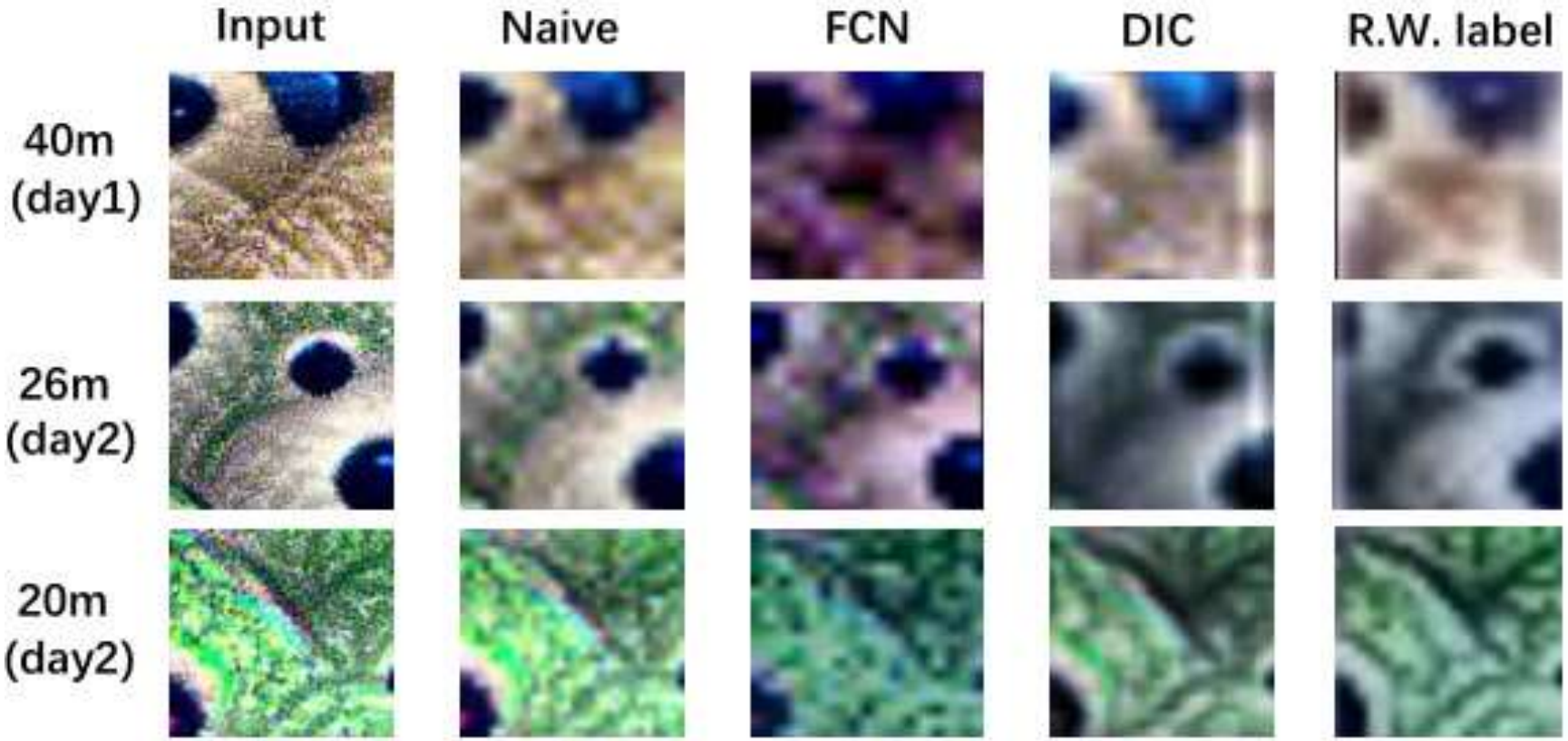
Full distance attack (FDA) pattern optimization



Multi-frequency optimization

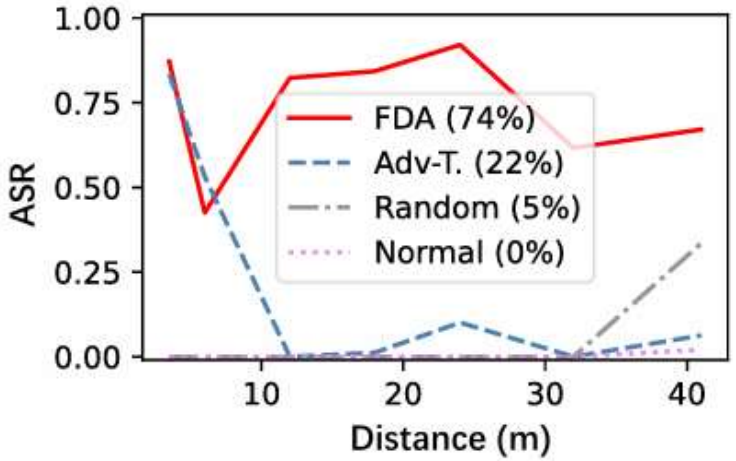
- Restricting the **overall pattern** of the FDA pattern to be optimized for performing **long distance** attack
- Restricting its **textures** to be optimized for performing **short distance attacks**

DIC experiments



FDA experiments

Patch attacks



Clothing attacks