RAUCA: A Novel Physical Adversarial Attack on Vehicle Detectors via Robust and Accurate Camouflage Generation

Jiawei Zhou[1], Linye Lyu[1], Daojing He[1], Yu Li[1]

[1]School of Computer Science and Technology, Harbin Institute of Technology, Shenzhen 518055, P.R. China

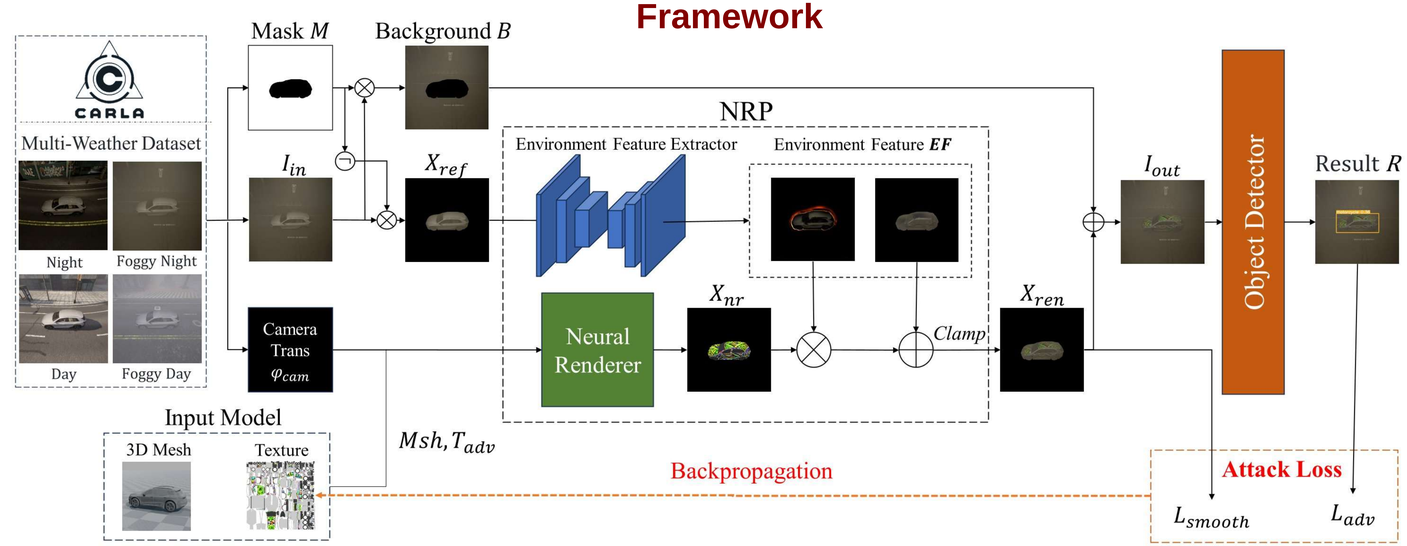
Background

- **Adversarial camouflage** is a widely used physical attack against vehicle detectors for its superiority in multi-view attack performance.
- Existing methods often **struggle to capture environmental characteristics** during the rendering process or produce adversarial textures that can **precisely map to the target vehicle**, resulting in suboptimal attack performance.
- Moreover, these approaches **neglect diverse weather conditions**, reducing the efficacy of generated camouflage across varying weather scenarios.

Key Contributions

- We present the **Robust and Accurate UV-map-based Camouflage Attack (RAUCA)**, a framework for generating physical adversarial camouflage against vehicle detectors. It enhances the effectiveness and robustness of the adversarial camouflage through a novel rendering component and a multi-weather dataset.
- We propose the **Neural Renderer Plus (NRP)**, a novel neural rendering component that allows for the optimization of textures that can be accurately mapped to vehicle surfaces and can render images with environmental characteristics such as lighting and weather.
- We incorporate a **multi-weather dataset** with ample environmental effects into the camouflage generation process. Our experiments show that the use of this dataset substantially enhances the attack robustness when using NRP for rendering.

Framework

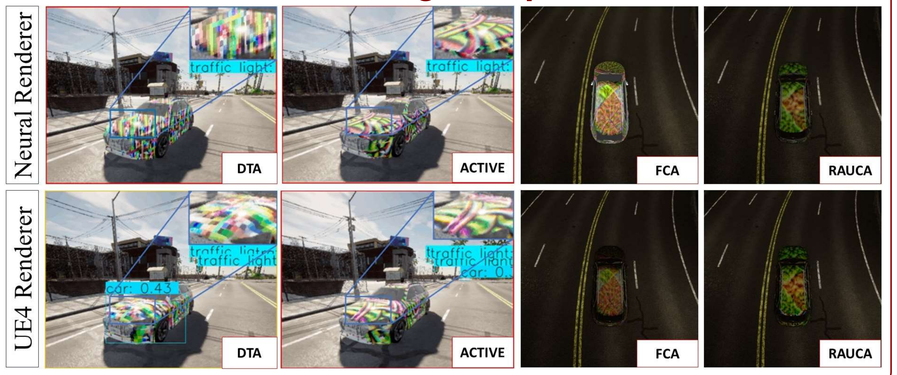


$$H_d(x) = \mathrm{IoU}\left(H_b(x), gt\right) * H_c(x) * H_o(x)$$
$$L_{adv}(x) = -\log\left(1 - \max\left(H_d(x)\right)\right)$$

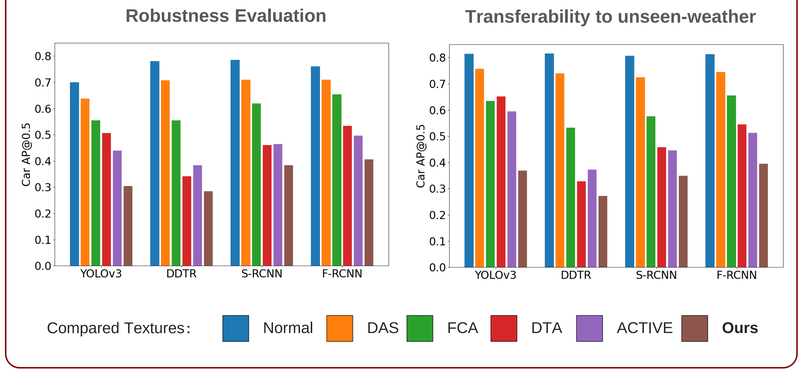
$$L_{sm} = \sum_{i,j} \left(x_{i,j} - x_{i+1,j}\right)^2 + \left(x_{i,j} - x_{i,j+1}\right)^2$$

$$L_{total} = \alpha L_{adv} + \beta L_{sm}$$

Rendering Comparison



Evaluation Results



Phyisical Evaluation Samples