REVAMP Automated Simulations of Adversarial Attacks on Arbitrary Objects in Realistic Scenes

Swiftly explore physically realizable adversarial objects

Matthew Hull **Jay** Wang **Polo** Chau

Georgia Tech

An open-source Python library for easily creating attack scenarios with arbitrary objects in realistic scenes.

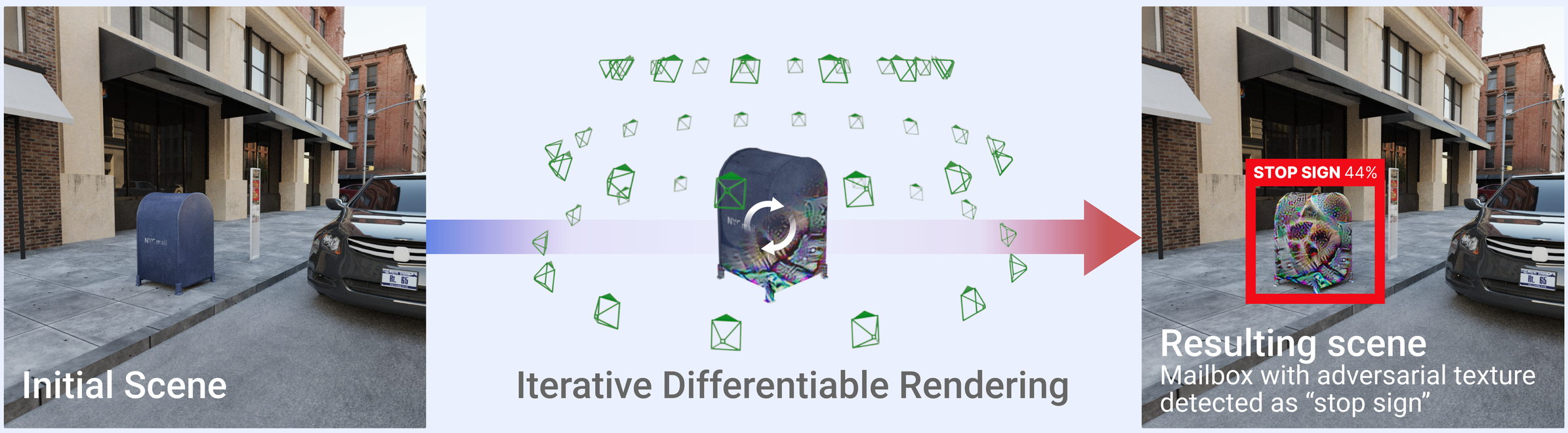
Code & Paper

github.com/poloclub/revamp

Demo Video

youtu.be/NA0XR0XkS1E

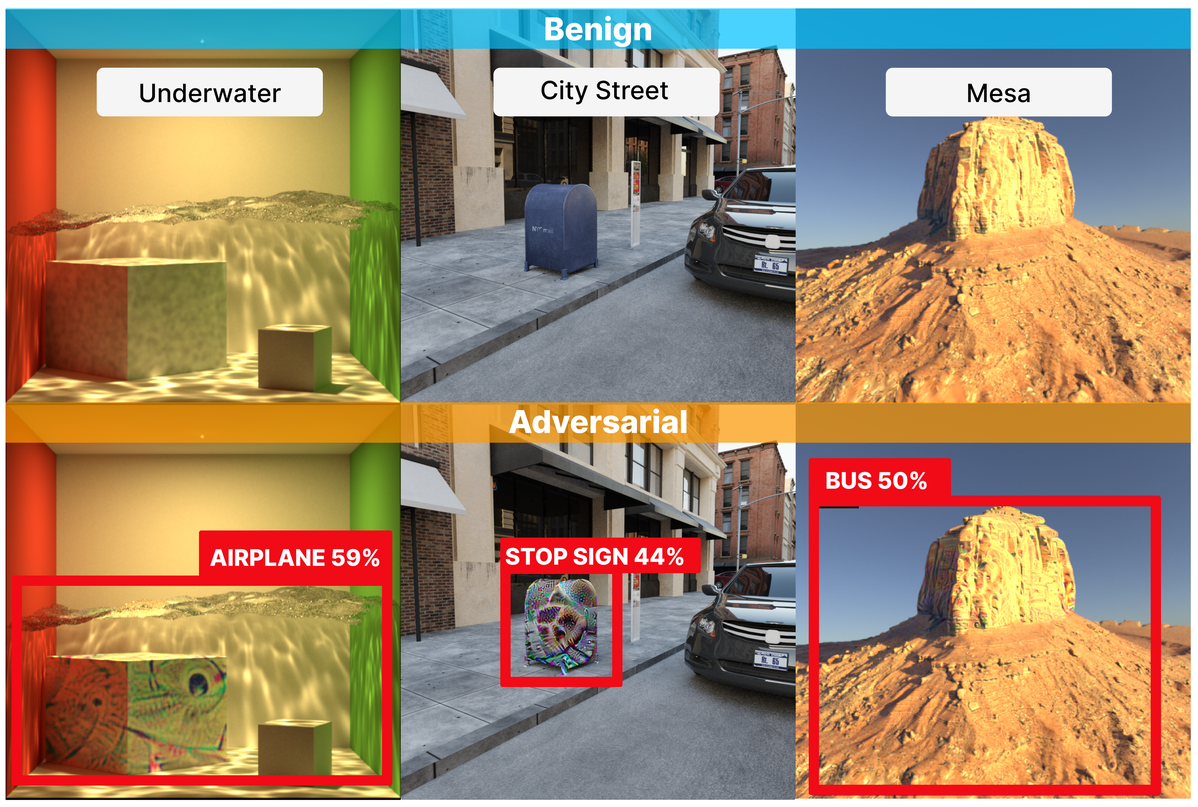
With a single REVAMP command, the mailbox in a realistic scene is iteratively perturbed via differentiable rendering to induce a stop sign STOP misdetection across camera positions




```
python revamp.py scene=city texture=mail_box attack_class=stop_sign multicam=64
```

Easily customize and configure attack scenarios

Explore attacks in varying lighting and environmental conditions



Top Row: Benign examples for 3 different scenes. Bottom Row: Perturbed texture maps on an underwater cube with light distortions perturbed as an airplane, a mailbox on a city street attacked to appear as a stop sign, and a mesa attacked to appear as a bus

Paper

https://arxiv.org/pdf/2310.12243.pdf