

Forum:[Hack Forums](#)

Thread: [object detector hack](#)

rmccrm - October 10, 2018, 1:45 am

Hi guys,

I've seen a new hack published on git-hub, describing a new hack on faster R-CNN object detector algorithm, which is the algorithm that defines what object are in a picture. this algorithm is in use especially in autonomous cars and allows the car to maneuver depending on the objects on road. I understood that it's a crazy hack because it's riding on a extremely sophisticated system (black box of car).

Given the ability to directly manipulate image pixels in the digital input space, an adversary can easily generate imperceptible perturbations to fool a Deep Neural Network (DNN) image classifier, as demonstrated in prior work. In this work, we propose ShapeShifter, an attack that tackles the more challenging problem of crafting physical adversarial perturbations to fool image-based object detectors like Faster R-CNN. Attacking an object detector is more difficult than attacking an image classifier, as it needs to mislead the classification results in multiple bounding boxes with different scales. Extending the digital attack to the physical world adds another layer of difficulty, because it requires the perturbation to be robust enough to survive real-world distortions due to different viewing distances and angles, lighting conditions, and camera limitations. We show that the Expectation over Transformation technique, which was originally proposed to enhance the robustness of adversarial perturbations in image classification, can be successfully adapted to the object detection setting. ShapeShifter can generate adversarially perturbed stop signs that are consistently mis-detected by Faster R-CNN as other objects, posing a potential threat to autonomous vehicles and other safety-critical computer vision systems.

Do you guys have any idea how did they manipulated this system? I'm really curious because i think this is the next gen of hacking, and a freaking new world to discover...

the code is on Git-hub under the name robust-physical-attack