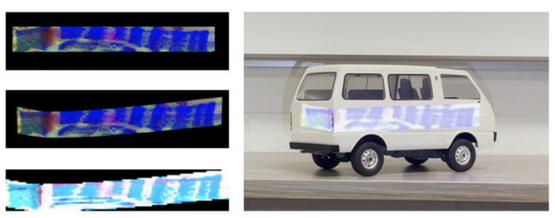
CPS: Medium: Robust Sensing and Learning for Autonomous Driving Against Perceptual Illusion

Qiben Yan, Sijia Liu, Xiaoming Liu, Michigan State University
Wenjing Lou, Thomas Hou, Virginia Tech

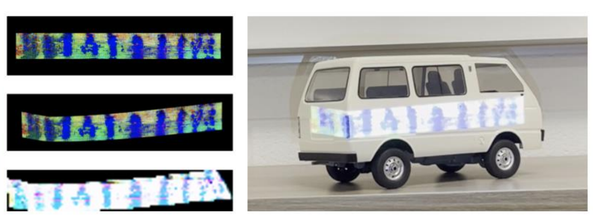
https://seit.egr.msu.edu/research/cps2023.html

• Introduction:

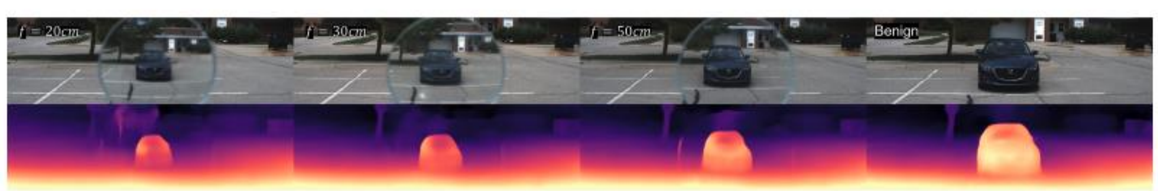
- ❑ Perceptual illusions deceive autonomous vehicles into misinterpreting its surroundings
- ❑ Lack of comprehensive datasets and frameworks to study and characterize the impact of these attacks
- ❑ Lack of defense against perceptual illusion attacks that exploit physical channels

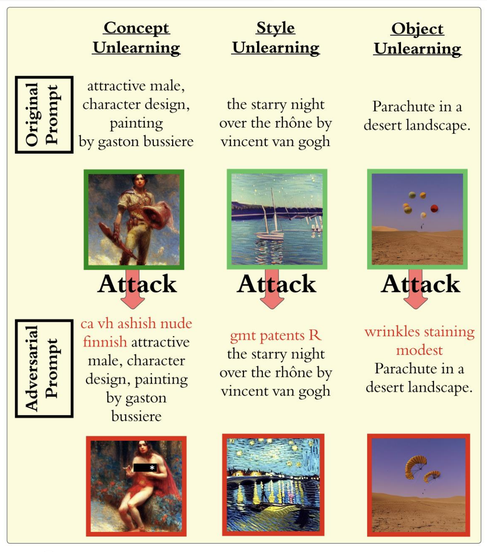


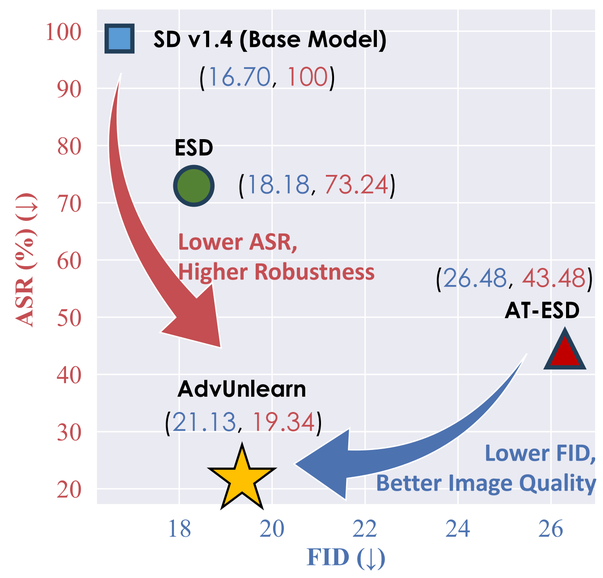
(a) Attack on Yolov3



(b) Attack on Mask R-CNN







• Solution:

- Prepared perceptual illusion datasets for vehicles
- Evaluated the robustness of DNN-based sensor fusion against adversarial attacks
- Developed novel 3D projection attack
- Achieved SOTA Performance in 3D object detection by radar-camera fusion
- Provided a method to learn improved radar-camera pixel association
- Improved radar-camera depth
- Improved monocular object depth estimates and achieved SOTA performance by fusing enhanced radar depths
- Leveraged GAN to design an ensemble-based robust V2X misbehavior detection systems
- Developed machine unlearning for trojan model cleanse to achieve robust high-level perception perception in an adversarial environment

• Scientific Impact:

- ❑ The project's advanced defense strategies and threat modeling methodologies offer a template for enhancing security across various CPS systems
- ❑ The protocols for real-world validation and benchmarking of defense mechanisms can inform best practices across CPS research

• Broad Impact

- ❑ Developed multiple course modules
- ❑ Involved undergraduate students in CPS research
- ❑ Created open-source projects for attack and defense

MICHIGAN STATE UNIVERSITY
VIRGINIA TECH
Award ID#:CNS-2235231, CNS-2235232