Outline:

1. What is a reasonable threat model for transportation?

an attacker might not have control over a vehicle’s systems, but can modify the objects in the physical world that a vehicle might depend on to make crucial safety decisions.

1. What should be considered for the attack in real life (for camera)?

(1) sensor imperfection 🡺 Perturbation could not be too small.

(2) perturbation in the background is not realistic 🡺 the background has already changed, depending on the different viewpoint. (Spatial constraint)

(3) imperfect fabrication.

1. What is Physical Perturbations (RP2)?

creating a visible, but inconspicuous perturbation that only perturbs the object (e.g. a road sign) and not the object’s environment. (white-box attack) 🡺 mask: In addition to providing spatial locality, the mask also helps generate perturbations that are visible but inconspicuous to human observer. 🡪 using L1 favoring the sparse perturbation, then using L2 with the region from L1.

1. the non-printability score is:

一張含有 文字, 字型, 白色, 設計 的圖片

自動產生的描述

1. The objective function:



1. What are the focus of the experiments in this paper?

we focus on angles and distances because they are the most rapidly changing elements for our use case.

1. attack success rate:

一張含有 字型, 筆跡, 文字, 白色 的圖片

自動產生的描述

1. Two types of the experiments: Stationary (Lab)/ Drive-by (field).
2. Poster-printing attack: reproducing the old work but only applying to the surface of the objects.
3. Sticker-attacks: more effective.
4. Overall results: over 60 % of success for target-attack but no real experiment with cars.

Ideas:

This paper shows how we could use just a simple sticker or a poster to impact the classifier of the cameras and then give the wrong road sign to the drivers in the white-box attack form. Also, it points of the overall high percent of success of the target attack. The interesting thing for me is that the perturbation is hidden under the graffiti, making this attack highly possible in the real world and dangerous. On one side, the human cannot easily see this attack. On the other side, this kind of attack could cause a huge deviation. Therefore, I firmly believe that there must be more improvements on the training of the models nowadays.