Physical Adversarial Attacks on an Aerial Imagery Object Detector: Supplementary Material

Andrew Du[†] Bo Chen[†] Tat-Jun Chin[†] Yee Wei Law[‡] Michele Sasdelli[†]
Ramesh Rajasegaran[†] Dillon Campbell[†]
[†]The University of Adelaide [‡]University of South Australia

8. Supplementary Material

A demo video and additional quantitative results are provided below.

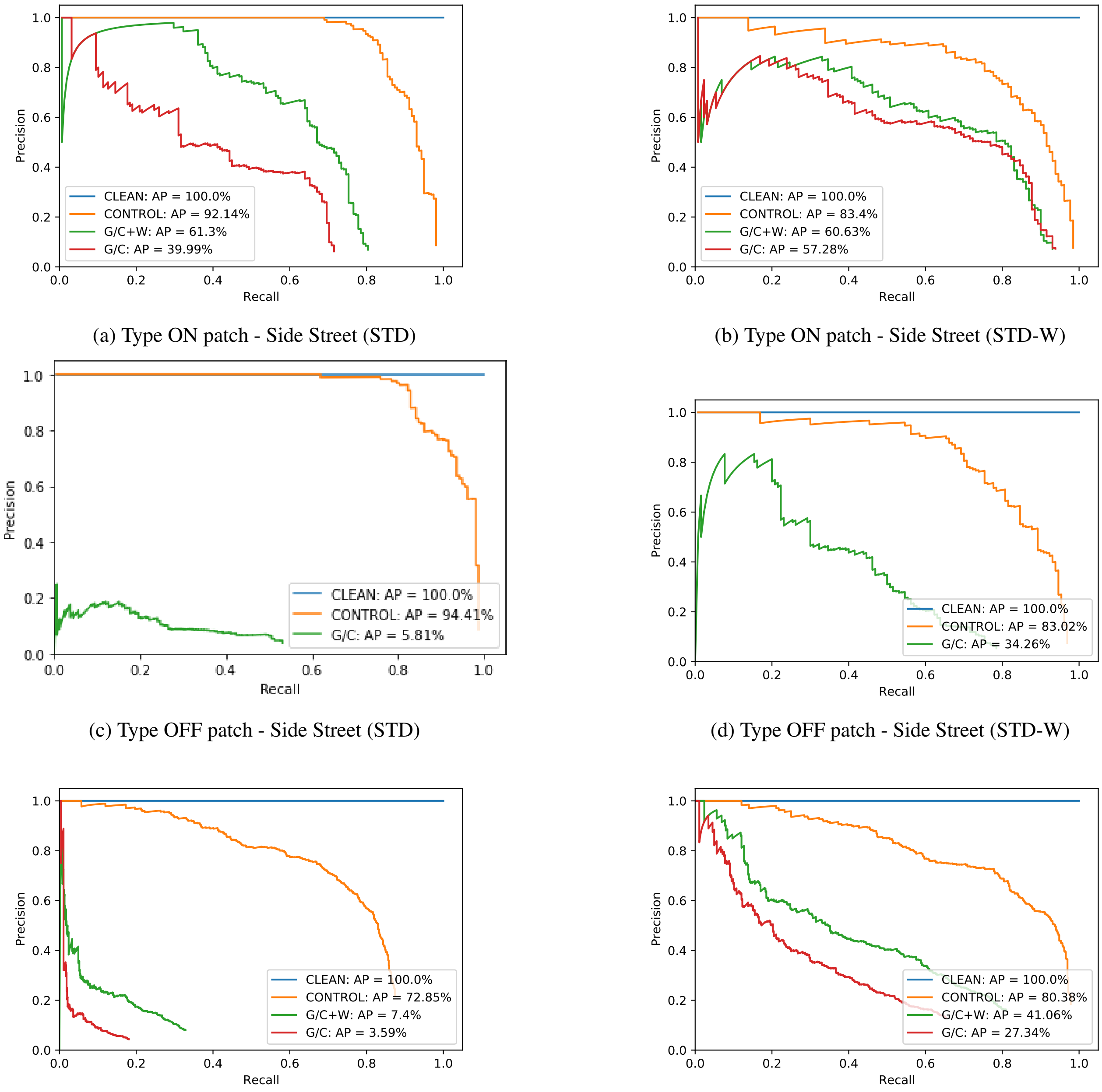
8.1. Demo video

We provide a demo video at `https://youtu.be/5N6JDZf3pLQ` of a grey car being attacked with a patch in the Side Street scene and a blue car being attacked with a patch in the Car Park scene. The colour of a bounding box indicates the objectness score: green is for a score of above 0.8, red is for a score of between 0.5 and 0.8, and grey is for a score of below 0.5.

8.2. Additional quantitative results

Since we were not interested in misclassifying cars, we only provide the precision-recall curves and average precision (AP) values (see Fig. 10) of the car detector (Sec. 4.1) when it is attacked with patches optimised under different variants of the pipeline (Sec. 4.3). The CLEAN curve is the evaluation of testing images with no patches applied. The CONTROL curve is with patches with random intensity patterns applied. The G/C+W curve is with patches optimised with geometric, colour-space and weather augmentations applied (full pipeline), and the G/C curve is with patches optimised with only geometric and colour-space augmentations. These patches were also evaluated under two testing regimes. STD are testing images with no weather effects applied and STD-W is with weather effects applied.

Similar to the results in Table 1, Fig. 10 shows that, while both G/C and G/C+W were significantly more effective (lower AP) than Control, G/C visibly outperforms G/C+W. Again, this indicated the lack of value in performing weather augmentations during training and further motivated us to ignore G/C+W for training Type OFF patches for Side Street. Type OFF G/C patches were also found to outperformed Type ON G/C patches for the same scene (Side Street).



(a) Type ON patch - Side Street (STD)

(b) Type ON patch - Side Street (STD-W)

(c) Type OFF patch - Side Street (STD)

(d) Type OFF patch - Side Street (STD-W)

(e) Type ON patch - Car Park (STD)

(f) Type ON patch - Car Park (STD-W)

Figure 10: The precision-recall curves as well as AP values of the car detector for different variants of the pipeline and testing regimes.