Lucas Guichard
50221623

CYBER PHYSICAL SYSTEM SECURITY

Prac Assignment #3

Deadline : 06.18 (Sun.) 23:59 pm
Report file type: Only PDF

Instructions

- (Basic 7pt)
  - Change the estimator to “FRCNN” to perform “Object Detection” and “Dpatch Attack” during the code by the 13th week of practice
- (Advanced 3pt)
  - Evaluate the impact of “DPatch” using “Average Precision” among YOLO's performance evaluation methods

You will find my code below with my results. All the code is documented for you to understand how I proceed this assignment.

Furthermore, I make different tests and find that I need to use a max_iter above or equal to 100 and a prediction threshold equal to 0.3. Otherwise, the two Average Precisions computed (one for the original image and one for the adversarial image) were two close.

This results show that FRCNN is not “that” vulnerable to the DPatch attack.