TP APPC : Exemples Adversaires

Stéphane Canu

4 Décembre 2023, ITI, INSA Rouen

Le but du TP est d'étudier et de comparer différentes méthodes de génération d'exemples adversaires

Ex. 1 — Génération d'exemples adversaires

1. Choisisez un réseaux de neurones pour lequel vous voulez générer un exemple adversaire, par exemple sur le site `https://robustbench.github.io/`
2. Choisissez une méthode de génération d'exemples adversaires, par exemple sur le site `https://adversarial-attacks-pytorch.readthedocs.io`
3. Générez un exemple adversaire et commentez vos résultats