ML2021Spring HW10 Report

Material Science and Engineering Hou, Yu-Chien
B08507012

Public Score	Private Score
0.020	0.010

The methods I used to pass the boss baselines include:

1. I performed ensemble attack by calculating the loss on the average of different models' prediction label in the fgsm() function.
2. I used ifgsm as my attacking algorithm, and I modified the gen_adv_examples() function similarly to the fgsm() function, that is averaging the prediction labels before calculating the loss.
3. I tried multiple combinations of 5 models for ensemble attack, and found out that models with the resnet110 suffix perfomed better together. The models I chose were：
    I. resnet110_cifar10
    II. preresnet110_cifar10
    III. seresnet110_cifar10
    IV. sepreresnet110_cifar10
    V. diaresnet110_cifar10