Part 1: Attack

- 根據你最好的實驗結果，簡述你是如何產生 transferable noises, JudgeBoi 上 Accuracy 降到多少 (1pt)

我將 `model_lists = ['resnext29_16x64d_cifar10','resnext29_32x4d_cifar10','preresnet56_cifar10','preresnet110_cifar10', 'preresnet164bn_cifar10','seresnet110_cifar10','sepreresnet56_cifar10','sepreresnet110_cifar10', 'diaresnet56_cifar10','resnet1001_cifar10','diapreresnet56_cifar10', 'resnet1202_cifar10', 'resnet56_cifar10','resnet110_cifar10','diapreresnet110_cifar10']` 中的一共 15 個 Model 做 Ensemble，透過各自產生的結果做加權平均產生 Transfer noises，JudgeBoi 上的 Accuracy 為：0.09。

Part 2: Defense

當 source model 為 resnet110_cifar10(from Pytorchcv), 使用最原始的 fgsm 攻擊在 dog2.png 的圖片。

1. 請問被攻擊後的預測的 class 是錯誤的嗎？(1pt) 有個話：變成哪個 class? 沒有的話：則不用作答

   錯誤的。變成 cat 的 class。

2. 實作 jpeg compression (compression rate=70%) 前處理圖片, 請問 prediction class 是錯誤的嗎？同第一題作答 (1pt)

   沒有，預測的 class 是正確的，仍然是 dog。

3. Jpeg compression 為什麼可以抵擋 adversarial attack, 讓模型維持高正確率？(1pt) a. 圖片壓縮時讓色彩更鮮豔 b. 圖片壓縮時把雜訊減少 c. 圖片壓縮讓圖片品質下降 d. 圖片壓縮時雜訊反而變大

   Ans: (b)