下載ILSVRC2012 資料集產生對抗式樣本

models資料夾下載cnn模型的權重:

<https://github.com/ylhz/tf_to_pytorch_model>

修改attack.py 第12行

Ex: import methods\_TGRv1 as methods (用TGRv1產生對抗式樣本)

python attack.py --attack TGR --batch\_size 1 --model\_name vit\_base\_patch16\_224

評估對抗式樣本對vit模型的攻擊率

bash run\_evaluate.sh model\_vit\_base\_patch16\_224-method\_TGR

評估對抗式樣本對cnn模型的攻擊率

python evaluate\_cnn.py

Code refer to: [Towards Transferable Adversarial Attacks on Vision Transformers](https://github.com/zhipeng-wei/PNA-PatchOut) , [tf\_to\_torch\_model](https://github.com/ylhz/tf_to_pytorch_model) and [TGR](https://github.com/jpzhang1810/TGR)