# Untitled

## 1. Install Git LFS

要將大型檔案（如 model.h5）上傳到 GitHub 時會需要用到此工具。

```
curl -s https://packagecloud.io/install/repositories/github/git-lfs/script
sudo apt install git-lfs
git lfs install
```

```
git lfs track model.h5
git add .gitattributes
git add model.h5
git commit -m "Add model.h5"
git push origin master
```

---

## 2. Install python3 & keras & tensorflow

這裡安裝 predict.py 需要用到的 python library，由於參考了 Hint 的範例程式，所以順便安裝 tensorflow。

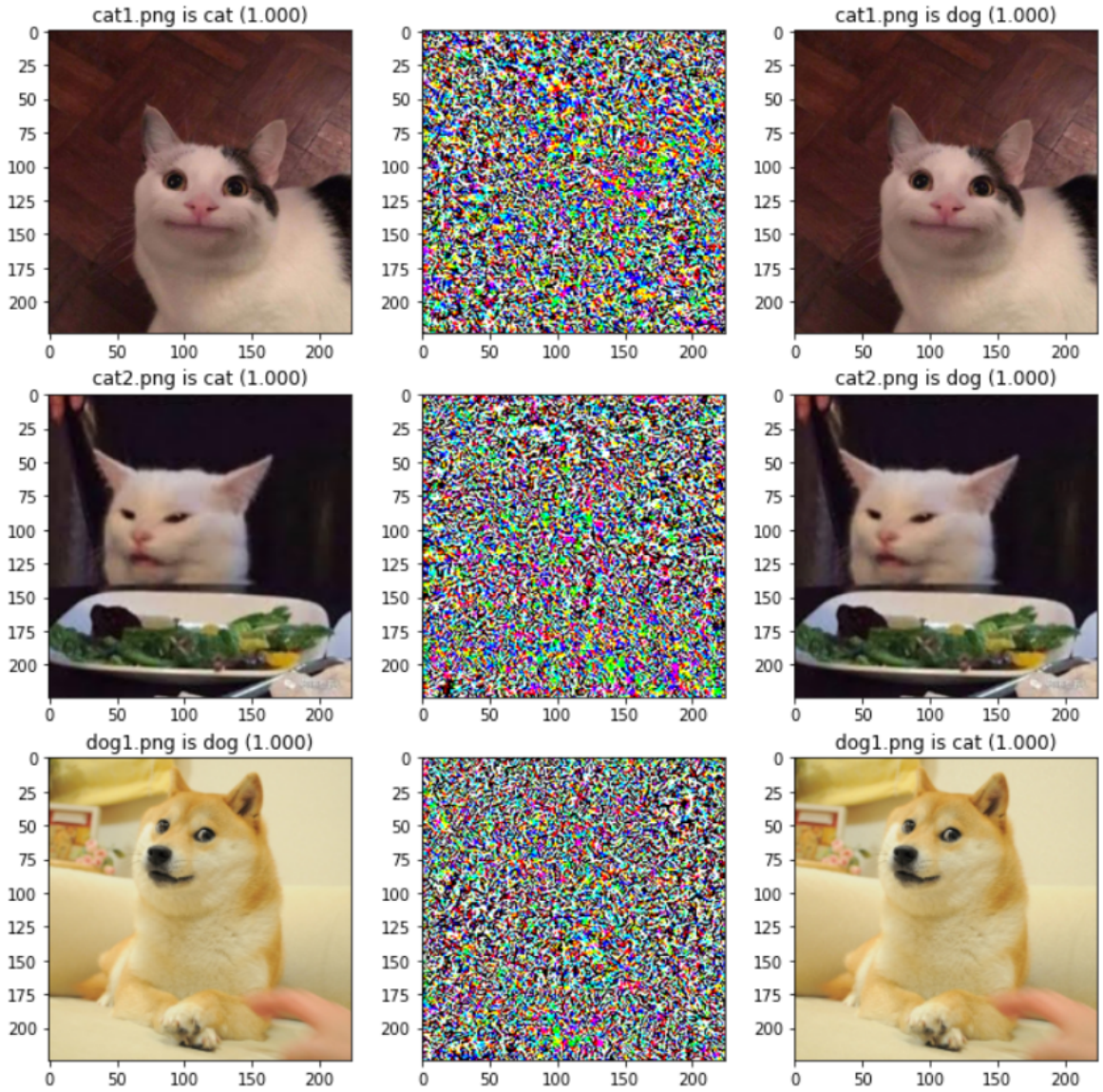
```
sudo apt install python3-pip
pip3 install --upgrade pip
pip3 install keras tensorflow-gpu
```

---

## 3. FGSM

請參閱 fgsm.ipynb 的程式碼，我將整個流程分為三部份，第一部份 (function part1) 使用 model.h5 對原始的圖片做預測，目的是為了要作為對照組跟後面的部份做比較，第二部份 (function part2) 建立遮罩來合成 adversarial image。第三部份 (function part3) 將原始圖片與遮罩做合併，並再做一次預測，可以發現肉眼看起來沒差的圖片，卻能使 AI 做出錯誤的判斷。

**cat1.png, cat2.png, dog1.png 的 adversarial 版本分別存成 adversarial_cat1.png, adversarial_cat2.png, adversarial_dog1.png**




## Reference

**git-lfs/git-lfs**

https://github.com/git-lfs/git-lfs/wiki/Installation

**Git Large File Storage**

https://git-lfs.github.com/

**Adversarial example using FGSM | TensorFlow Core**

https://www.tensorflow.org/tutorials/generative/adversarial_fgsm