Paper: <https://arxiv.org/pdf/1710.11342.pdf>

Code: <https://github.com/zhengliz/natural-adversary>

1. From terminal/cmd:

**ssh** [**daryln@10.4.0.15**](mailto:daryln@10.4.0.15) **or ssh daryln@<server ip address>**

1. In server
   1. If container is not already running

command to run:

**docker run -it -p 8893:8893 --name naturalgan -v /home/daryln/adversarial\_attacks/natural-adversary:/home --gpus '"device=1"' tensorflow/tensorflow:1.15.0-gpu**

* 1. If container is already running (should already be named)
     1. **docker start naturalgan**
     2. **docker attach naturalgan**

1. Natural Generative Adversarial Network attack directory is under /home as natural-adversary
2. Install required libraries: (pip install …)
   1. keras==2.1.2
   2. scipy==0.17.0
   3. pillow==6.2.2
   4. matplotlib==2.2.5
   5. scikit-learn==0.20.4
3. **mkdir original\_examples** and copy contents of **examples/** over to the former to store the original adversarial examples previously generated
4. Run attack using

**python mnist\_natural\_adversary.py**

1. The adversarial images will be generated as .png files under “examples” directory.

To view the imageset

To view them, it is recommended to open a Jupyter notebook for this. There is already one generated in the directory (**compare\_adversarial\_images.ipynb)**.

To use Jupyter

Command to run: **jupyter lab --no-browser --ip=0.0.0.0 --port=8893 --allow-root**

Open the notebook and the code should already be written for you.

