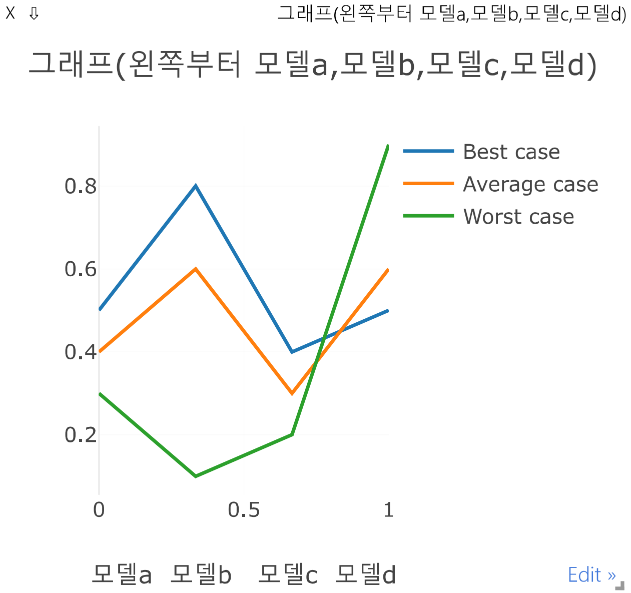
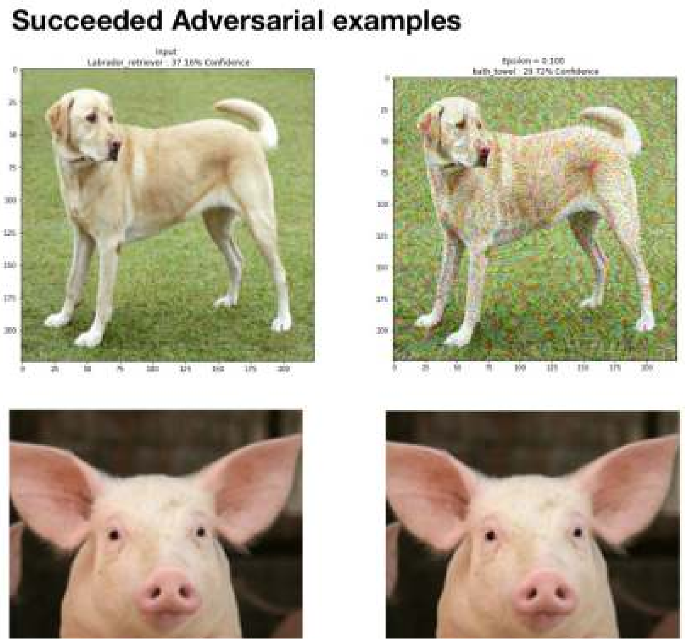
visdom | Environment main × | View current ▾ | Filter text | online



Top-5 Accuracy against attacks

```
-----------------------------------
|| top-5 | bst | avg | wst ||
||모델 a | 0.5 | 0.4 | 0.3 ||
||모델 b | 0.8 | 0.6 | 0.1 ||
||모델 c | 0.4 | 0.3 | 0.2 ||
||모델 d | 0.5 | 0.6 | 0.9 ||
-----------------------------------
```

0.5


Succeeded Adversarial examples
Input
Labrador_retriever : 37.16% Confidence
Epsilon = 0.100
bath_towel : 23.72% Confidence

46 /100 try harder!

Your model is significantly weak aganinst 모델b attack,and 모델d attack.But relatively robust against 모델a attack, and 모델c attack

This weekness can be caused from setting hyper parameters,maybe input bias,or input capacity etc.

if you think none of this are your issues we recommend adversarial training with provided our adversarial examples.

Try again with adversarilly trained model and check out the result