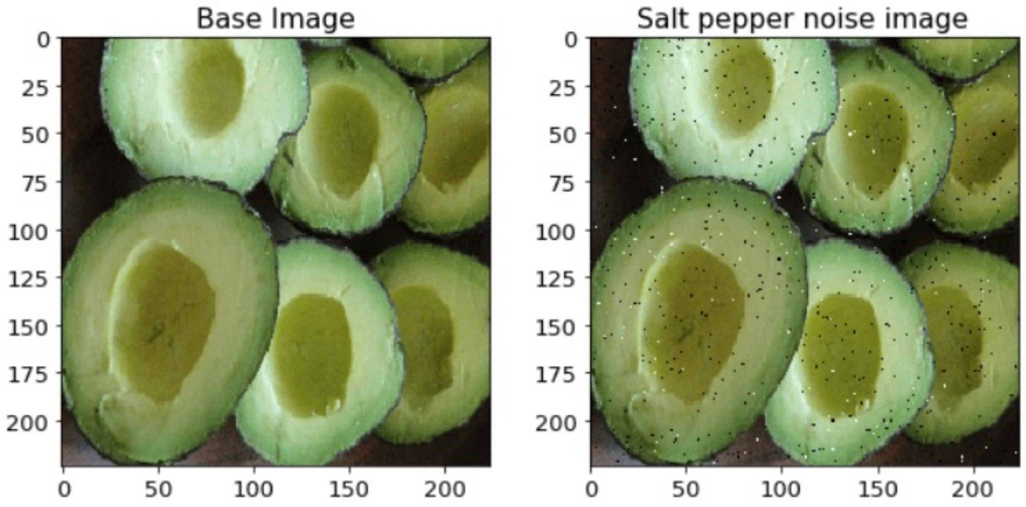
Data Augmentation

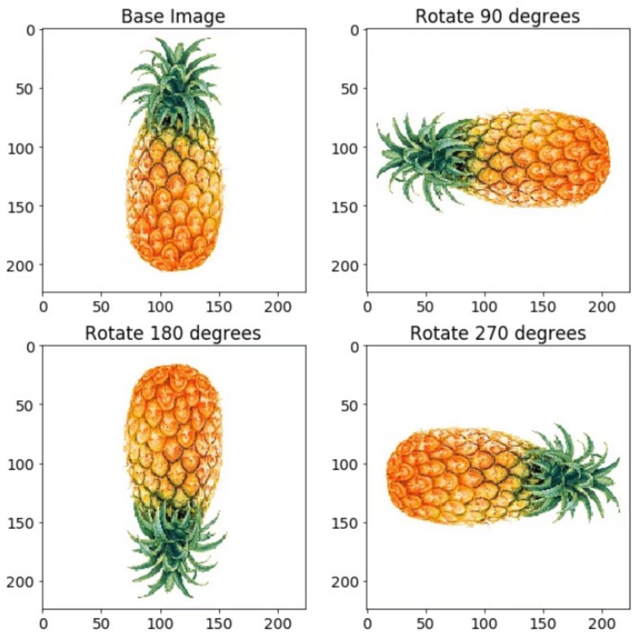
Chia-Cheng Kuo

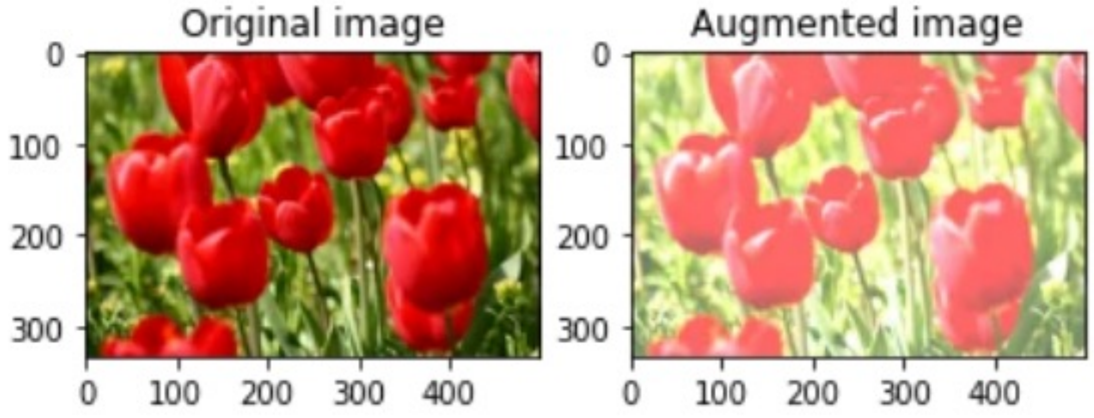
2022/09/14

Image

- Add noise
- Crop
- Flip
- Rotate
- Scale
- Brightness
- Contrast
- Color augmentation
- Saturation



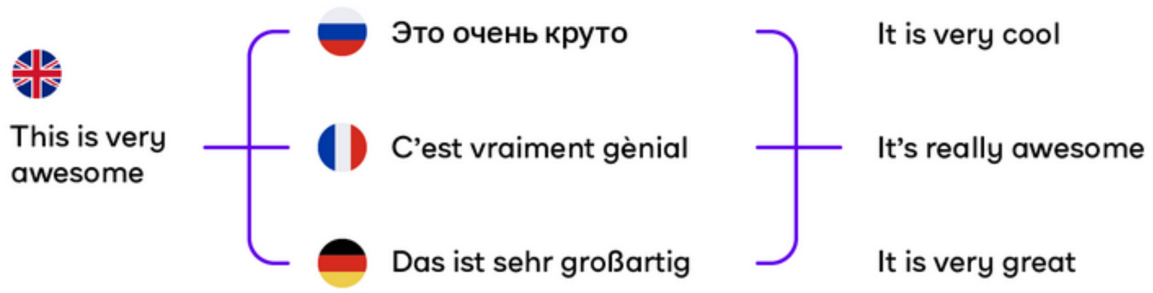


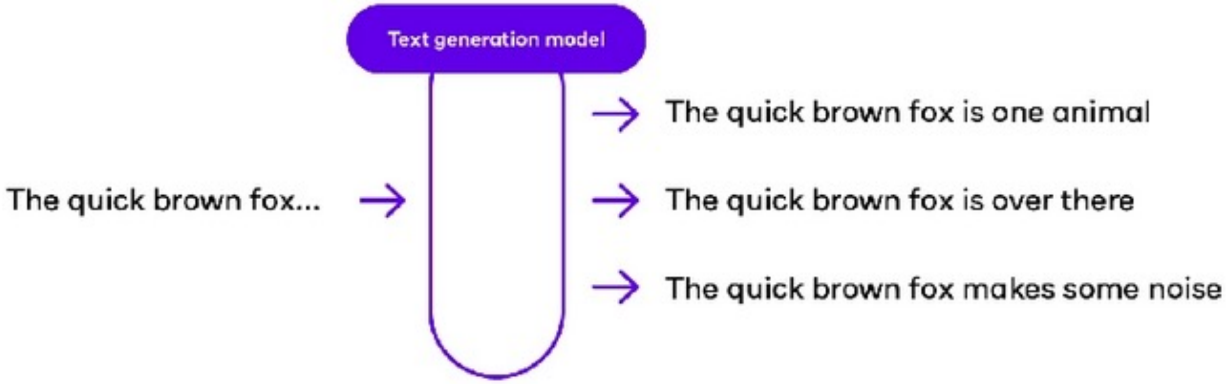


Natural Language Model

- Synonym replacement
- Random insertion
- Random swap
- Random deletion

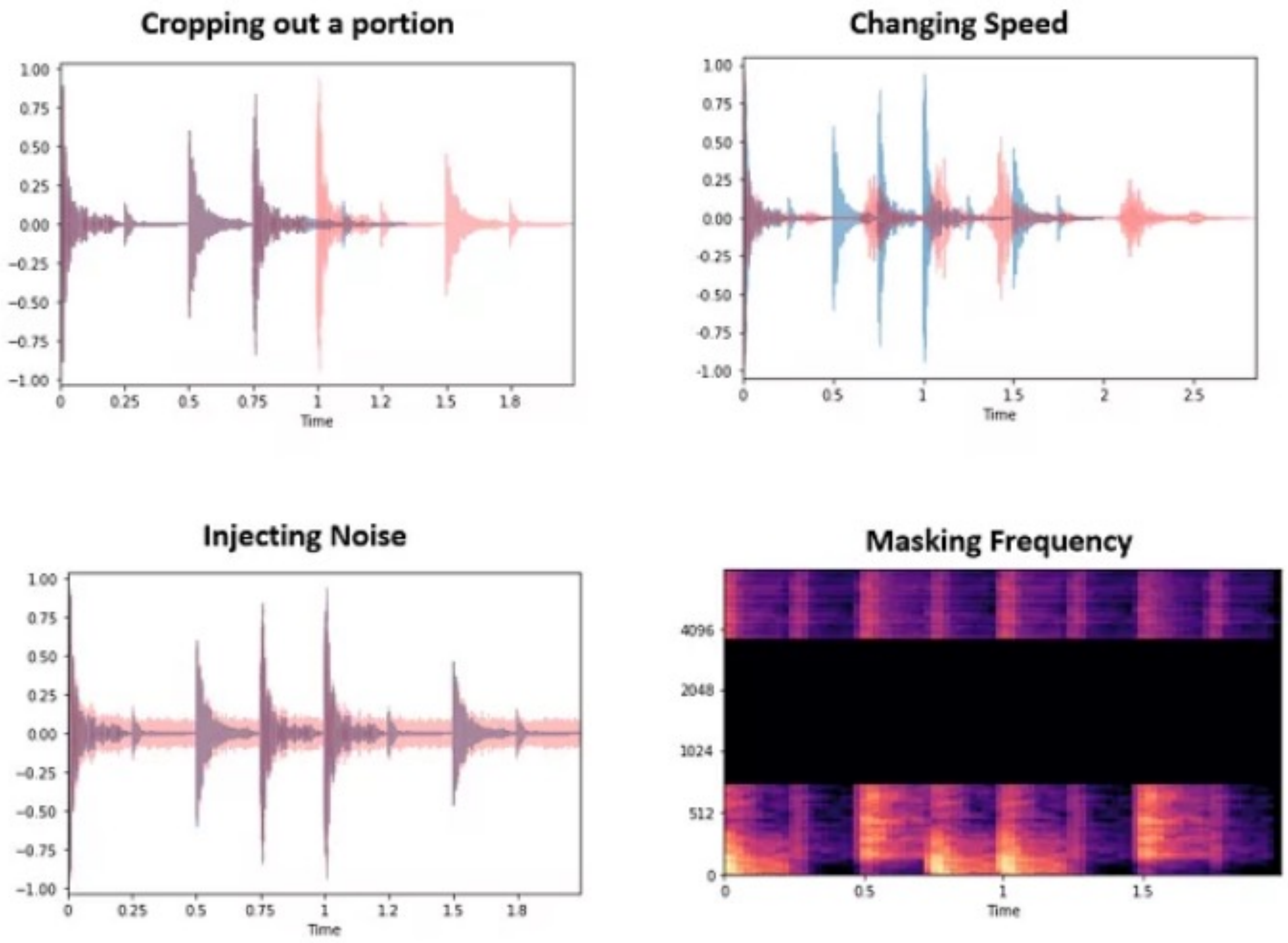
- **Back Translation**
- **Text Generation (GAN)**





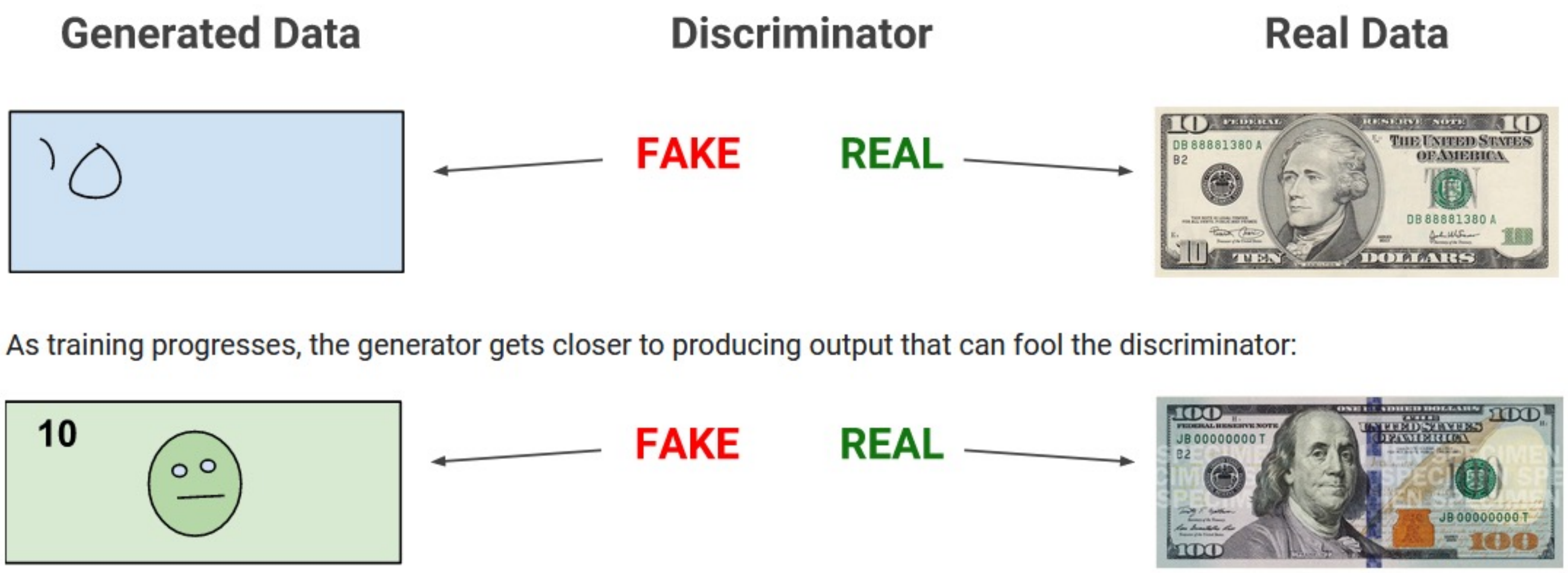
Audio Data

- Crop audio
- Change speed
- Add noise
- Masking frequency



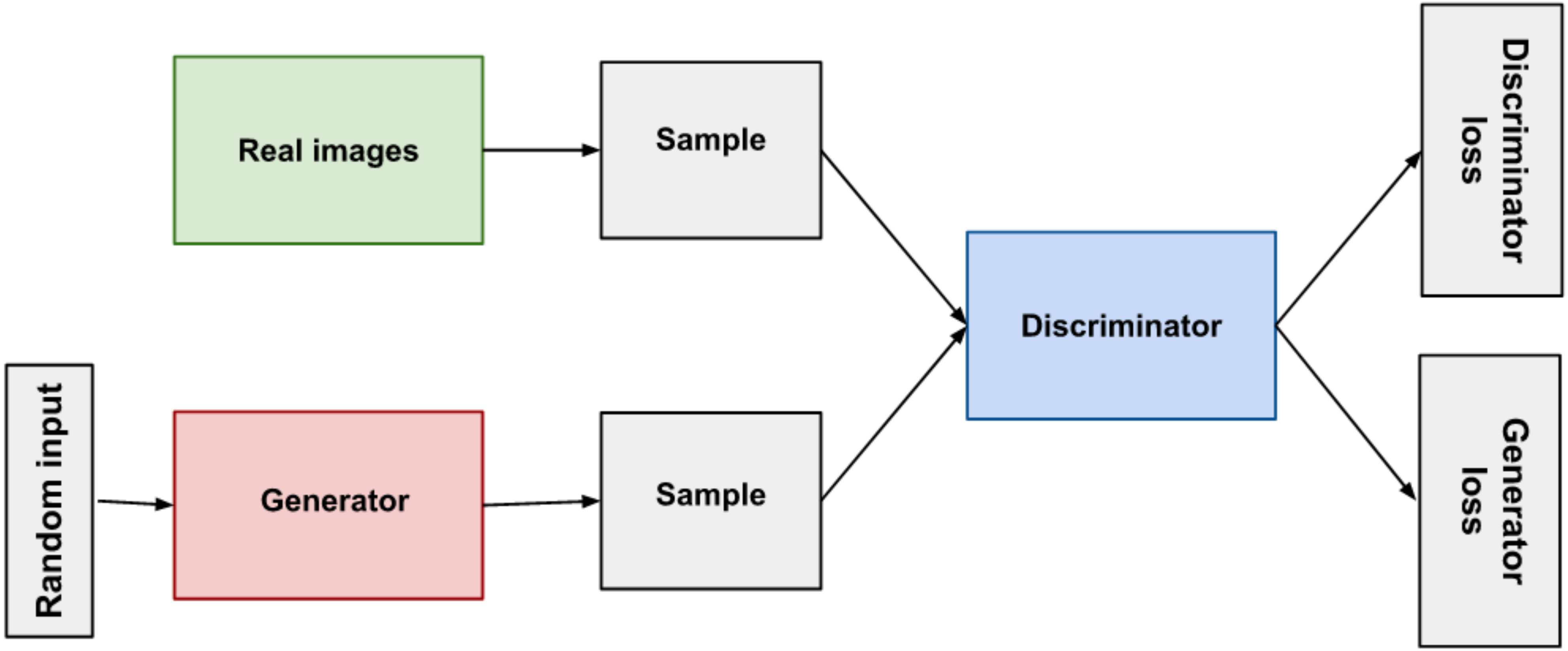
Generative adversarial network (GAN)

- Generator: generate data
- Discriminator: distinguish real and fake data (classifier)



https://developers.google.com/machine-learning/gan/gan_structure

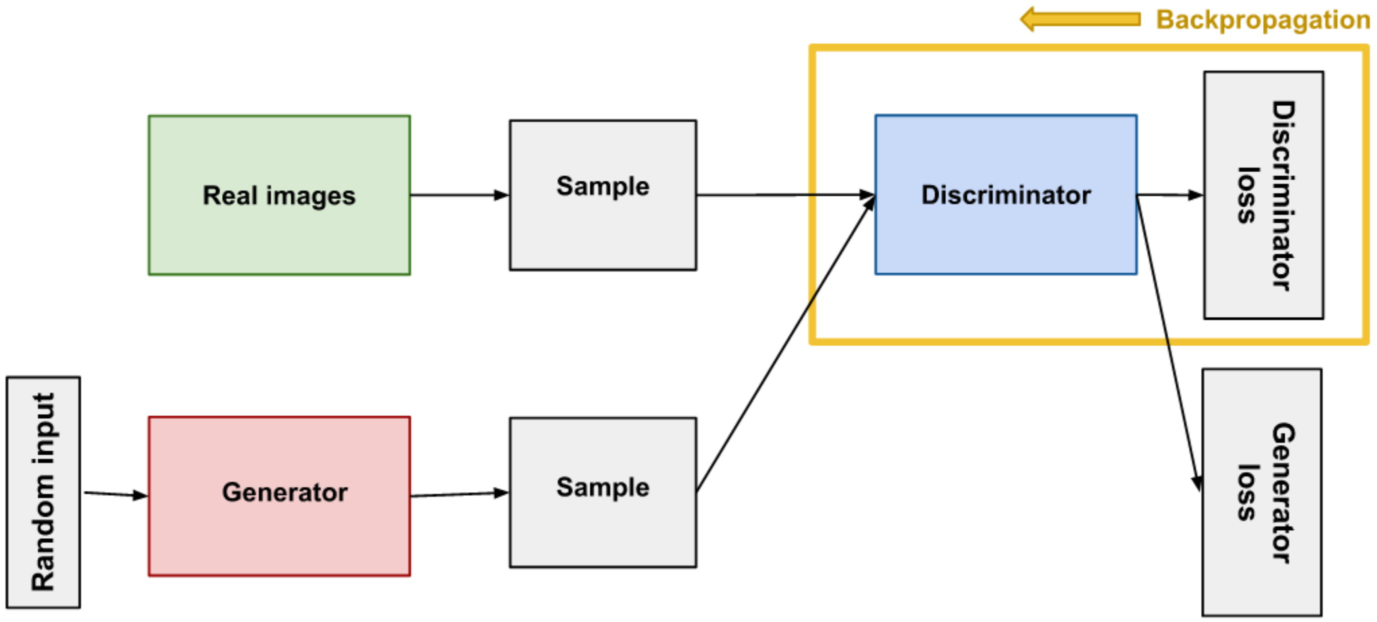
GAN structure



Training Discriminator

- Take training data from real data and fake data from generator

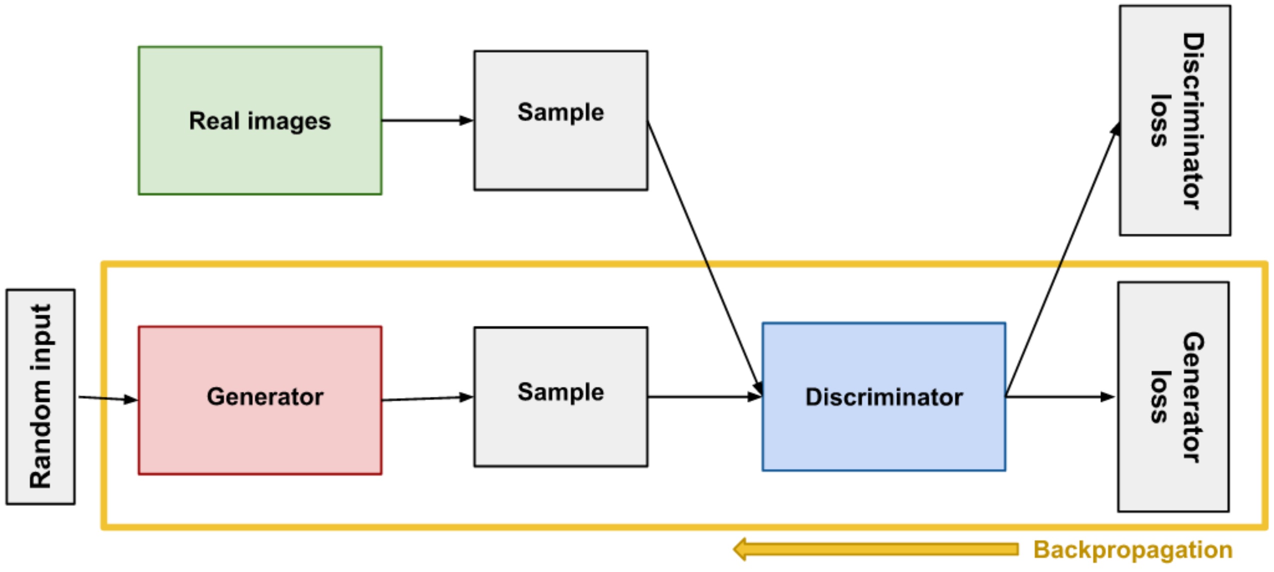
1. Discriminator classifies real data and fake data.
2. Calculate discriminator loss.
3. Discriminator updates weights through backpropagation.



Training Generator

- Random Input: random noise

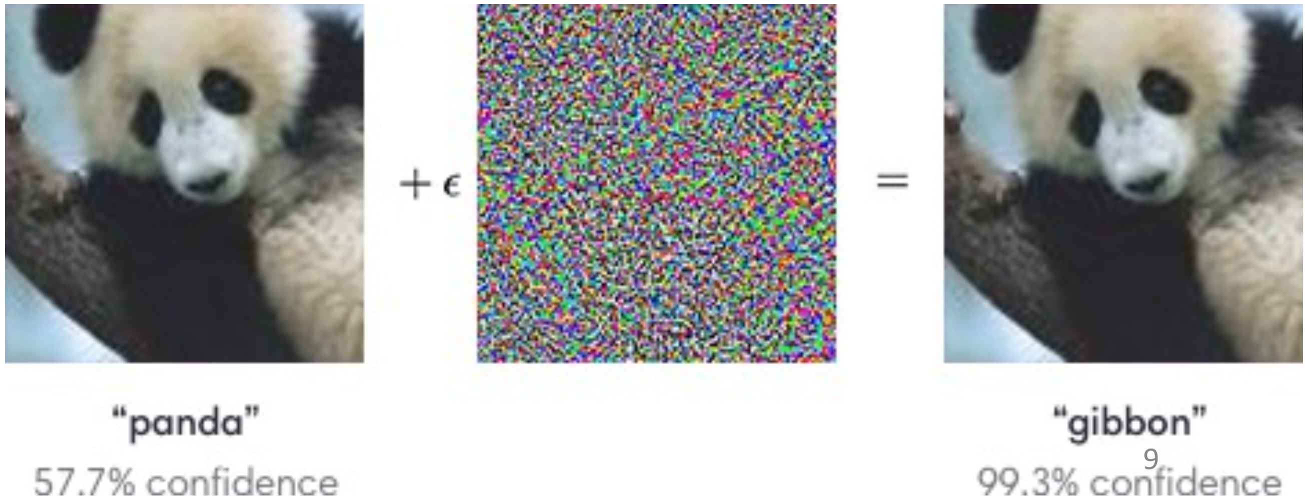
1. Generate output from random noise input.
2. Discriminator classify real or fake.
3. Calculate loss from discriminator classification.
4. Backpropagate discriminator and generator for gradients.
5. Use gradients to change only the generator weights (discriminator fixed).



Adversarial Examples can be Effective Data Augmentation for Unsupervised Machine Learning

Chia-Yi Hsu[1], Pin-Yu Chen[2], Songtao Lu[2], Sijia Liu[3], Chia-Mu Yu[1]
[1]National Yang Ming Chiao Tung University
[2] IBM Research
[3] Michigan State University

- Adversarial Example
  -> for supervised learning models.
- Goal: data augmentation for unsupervised ML. (Unsupervised Adversarial Example, UAE)

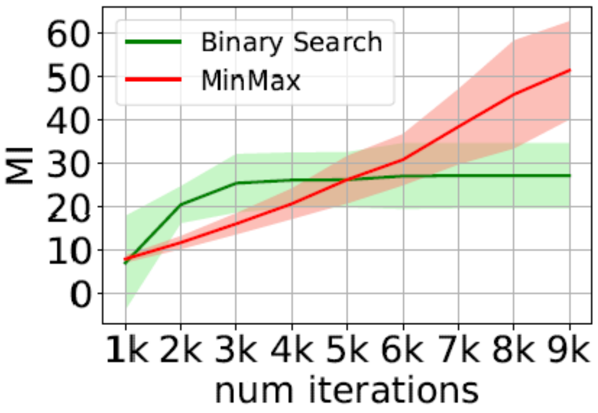


Key Idea

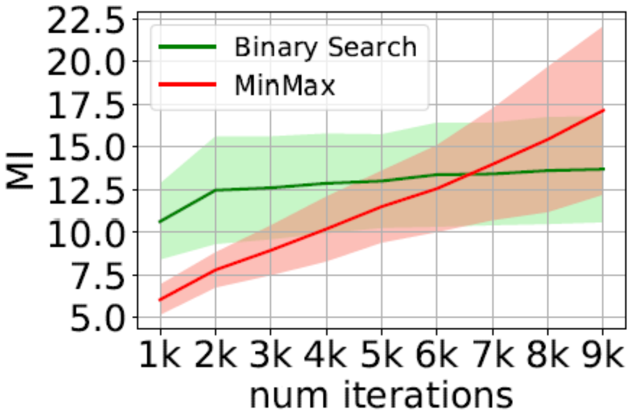
- MINE, Mutual Information Neural Estimator
  - MI -> Mutual dependence between 2 RV.
  - MINE -> maximize MI using model parameterized by neural network.
  - Can improve representation learning.
  - Problem: applies batch of data samples, not single data sample
  - Solution: Per-sample MINE
- MinMax Algorithm.
  - Reformulate attack generation via MINE
  - More efficient in finding MINE-based adversarial examples than penalty-based algorithm.
- Per-sample MINE + MinMax -> MINE based Supervised or Unsupervised Adversarial Examples

Evaluation

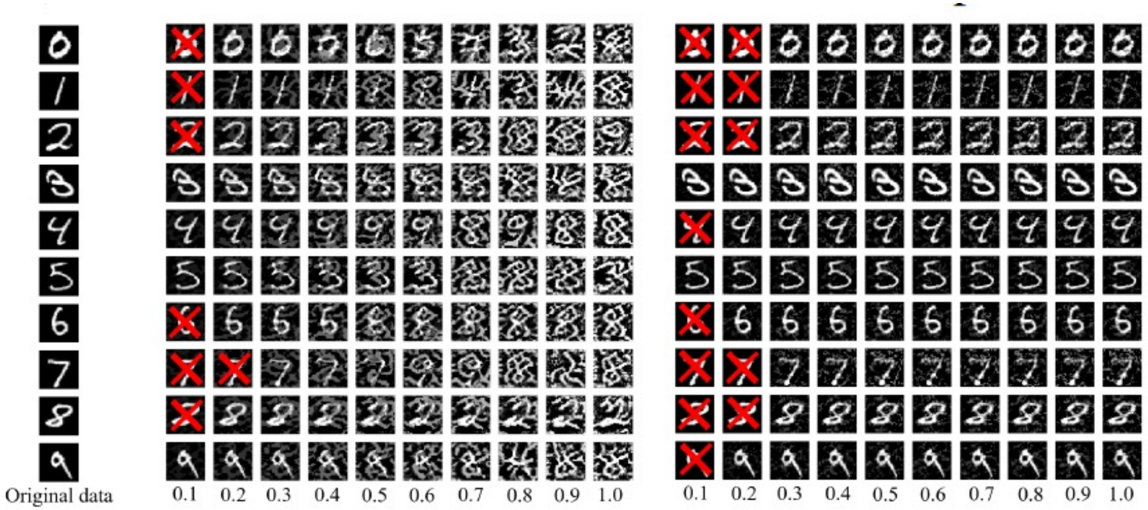
- Tested on MNIST, SVHN, Fashion MNIST, Isolet, Coil-20, Mice Protein, Human Activity Recognition.
- MinMax vs Penalty-based algorithm -> MI continue to improve
- MinMax vs PGD attack -> better picture quality.



(a) MNIST



(b) CIFAR-10



(a) (b) PGD attack (c) MinMax attack

Evaluation

Improves

- Data reconstruction
- Representation learning
- Constrastive Learning

Conclusion

- Data Augmentation
  - Img, txt, audio data
- GAN
- Adversarial Examples can be Effective Data Augmentation for Unsupervised Machine Learning
  - Adversarial Examples
  - Per-sample MINE + MinMax -> MINE based UAE