學期學習進度

張定堯、張之芃、王定偉

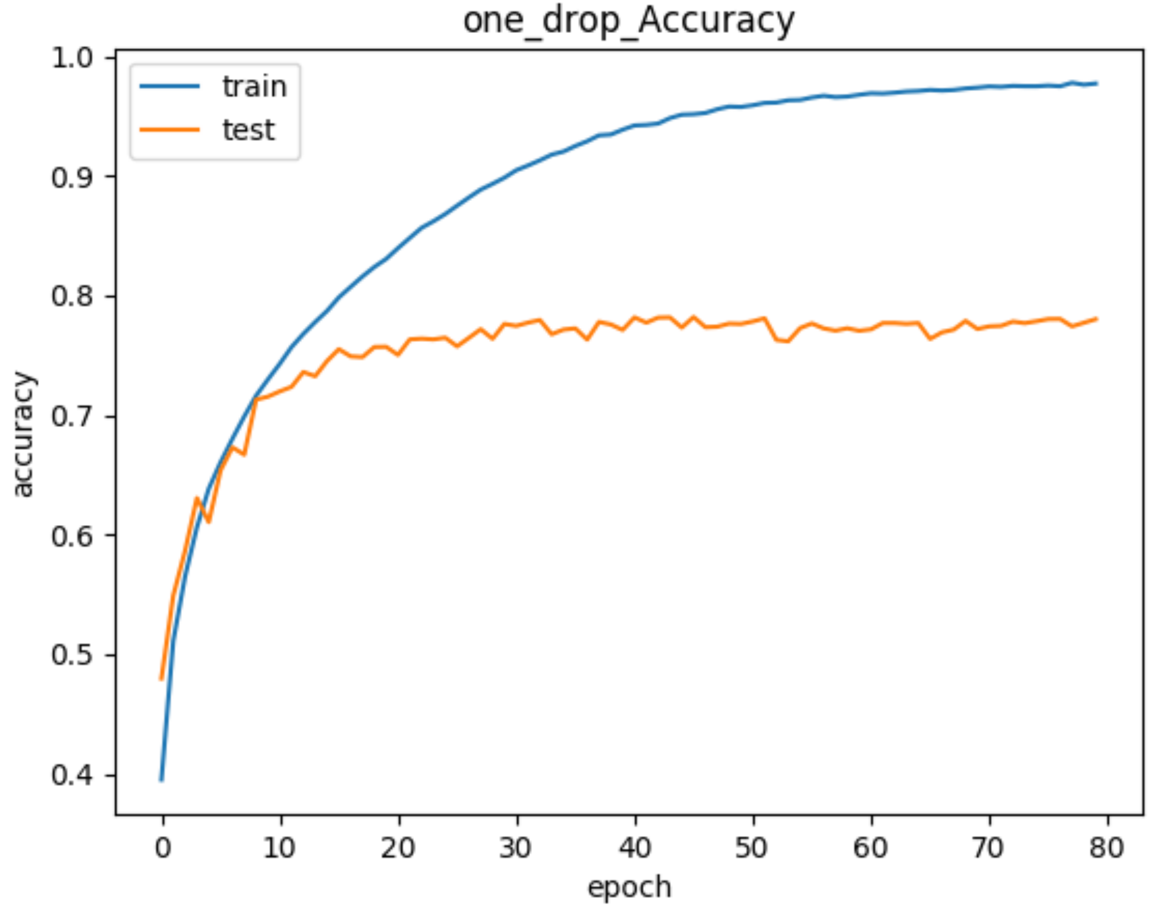
3/15 ~ 3/29

- 學習
  - Linear Regression
  - Gradient Descent
  - Logistic Regression
- 實作
  - Spam Classification (垃圾郵件分類)
    - Use the vector of emails and Logistic Regression to train model
  - Kaggle : Predict survival on Titanic
    - Form the vector of passengers from their personal information, and calculate their survival possibility

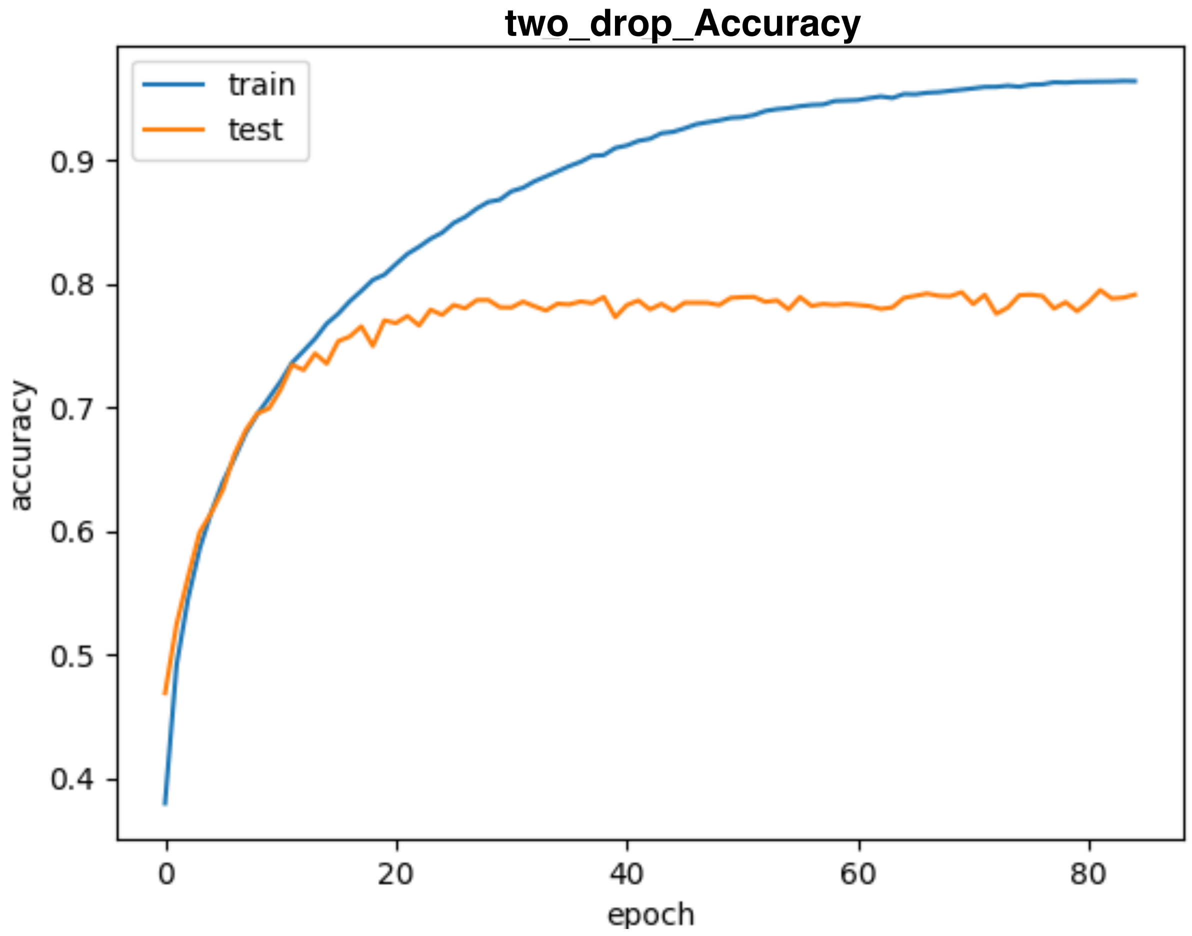
3/30 ~ 4/19

- 學習
  - Deep Learning
  - Convolutional Neural Network (CNN)
  - Tips for deep learning, e.g. Adaptive learning rate, drop out
- 實作
  - Picture Classification with mnist and cifar-10 using Keras
    - Compare the accuracy and loss between different models

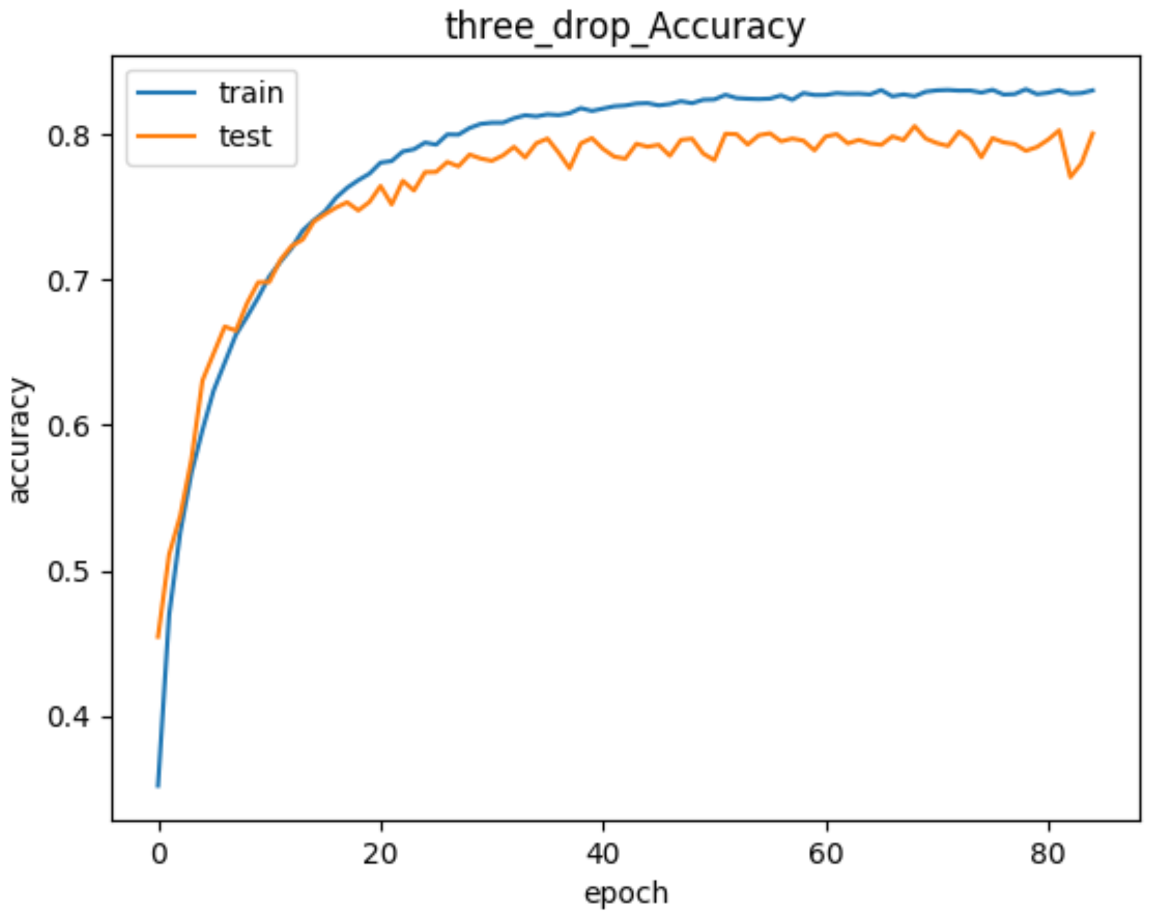
0.25



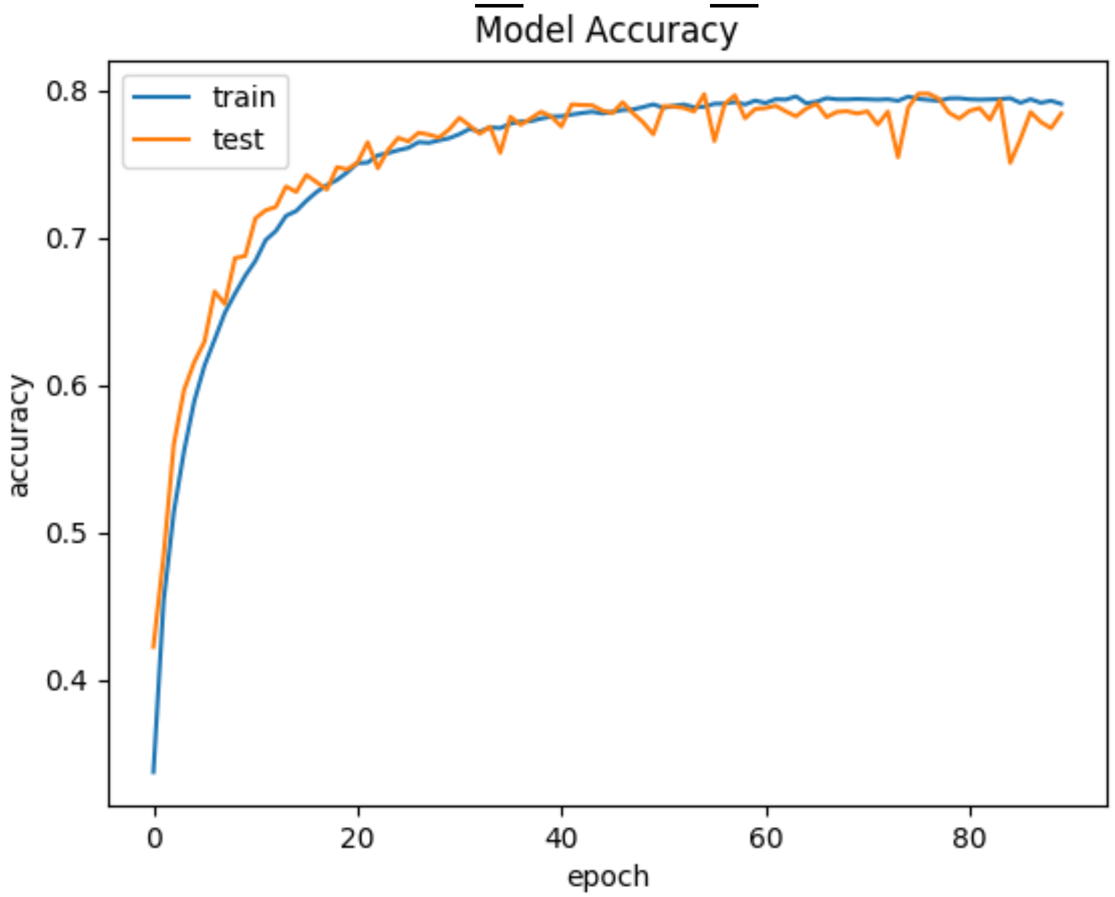
0.25_0.25



0.25_0.25_0.25

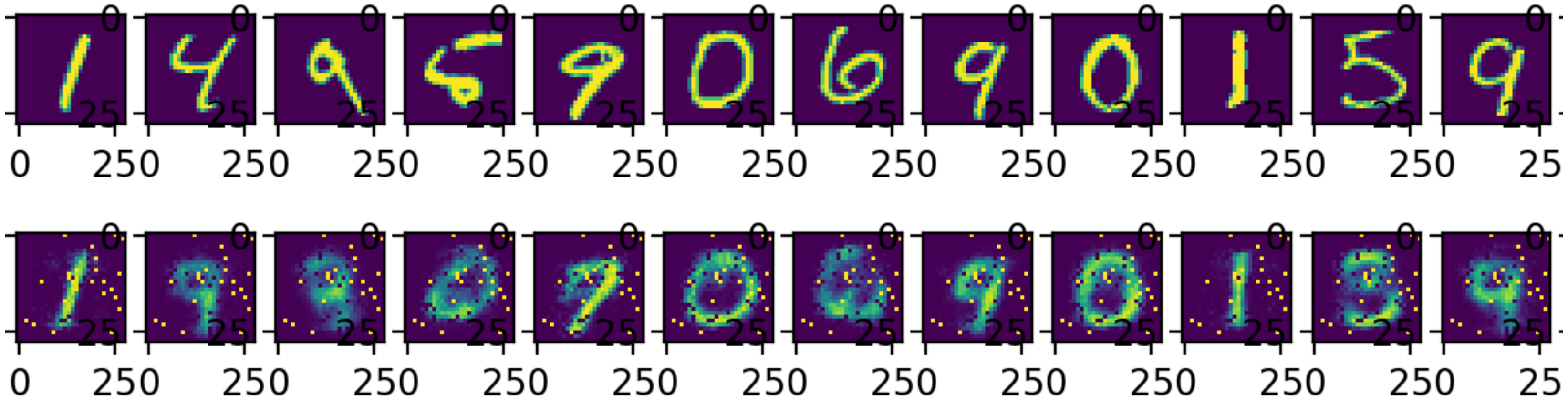


0.25_0.25_0.5



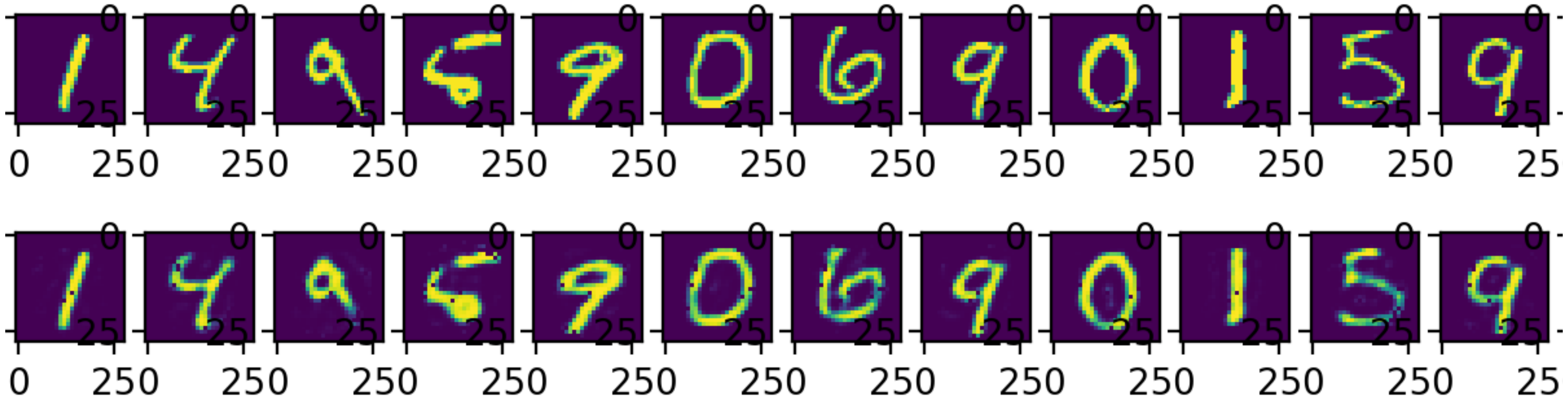
4/20 ~ 5/17

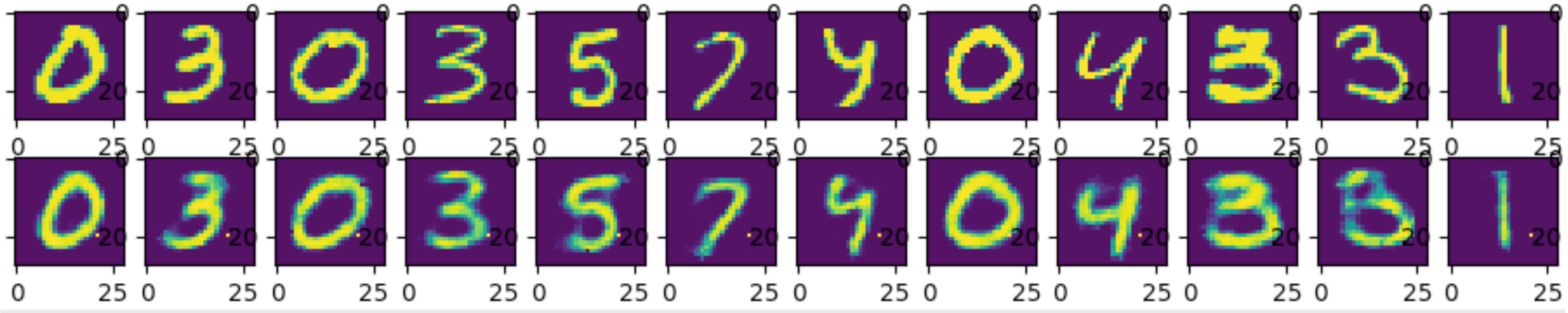
- 學習
    - Semi-supervised Learning
    - Unsupervised Learning
    - Deep Auto-encoder
- 實作
    - Unsupervised Learning : Auto-encoder
        - Compare the outputs between different models



784 > 300 > 100 > 50

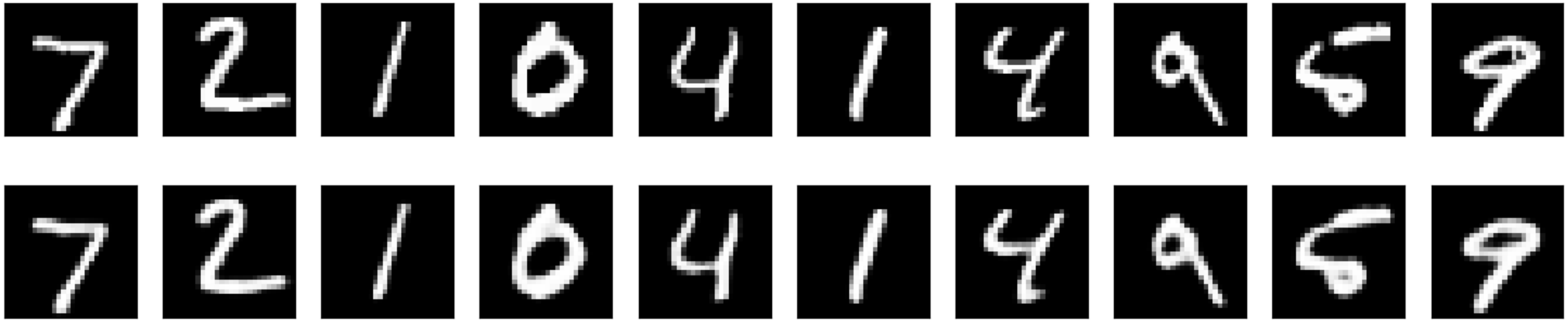
784 > 100



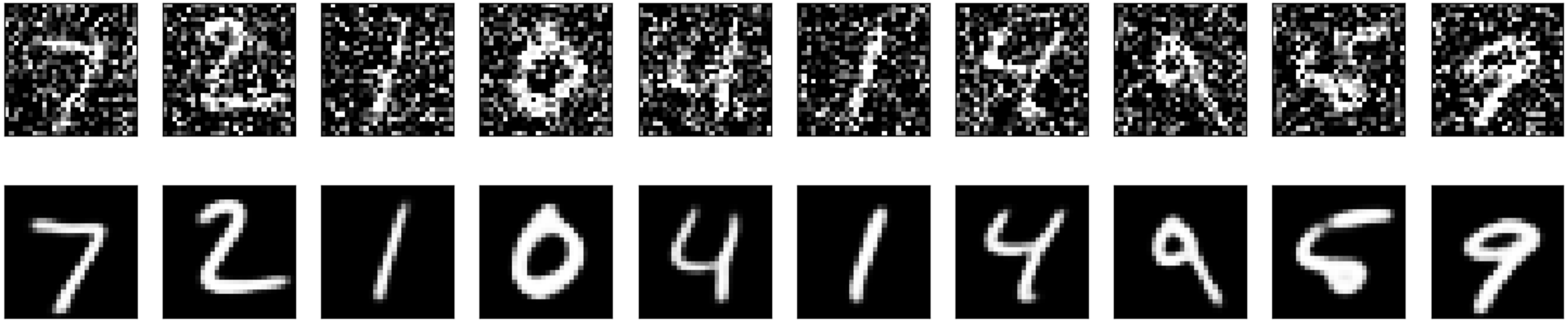


784 > 128 > 64 > 32

Convolutional



Denoising



5/18 - 7/19

- 論文閱讀
  - Automatic Malware Signature Generation and Classification
  - Modeling Password Guessabiliby Using Neural Networks
  - Practical Black-Box Attacks against Machine Learning

7/20 -

- 實作
  - Malware detection based on machine learning
  - Attack against machine learning base malware detection

Progress Schedule

- Attack
  - Implement MNIST attack model
  - Modify previous model against malware detector
- Defense
  - Dataset preparation: obfuscation, packer & static feature (1.5 ~ 2 weeks)
  - Deep Belief Network: implement NN (1 week)
  - Detection: implement classifier (1 week)