Homework #4 for CS 419— Computer Security

1 Backpropagation (30 points)

Backpropagation is one of the most important algorithm in Deep Neural Network training. Here is how it works: `https://cs231n.github.io/optimization-2/`. Please use a simple **CNN** to explain one training iteration using the backpropagation algorithm.

Note: model arch can be simple without max pooling layers.

2 Self-supervised learning (10 points)

Labeling training data is time consuming and error pruning. A possible way to avoid such problems is to perform self-supervised learning. For example, in NLP (Natural Language Processing), we mask one or a few words in a sentence and ask the model to predict the masked words so that we can train word vectors that carry semantics (e.g., king - man + women = queen). However, this will be difficult for computer vision tasks. Please try to think a way to perform such self-supervised learning.

Note: you should intuitively explain how it works, design a loss function and explain how it can achieve the goal. You do not need to design a model.

3 DeepFake (30 points)

Please try to use DeepFake techniques (e.g., `https://faceswap.dev//`) to generate a 30-second long video, and submit a final video with the original framews on the left hand side and deepfake video on the right hand side (timeline should be aligned).

Note: this is used for learning purpose only! Do not overuse this technique or try to use it for illegal purposes.