Advanced Machine Learning
Assignment 1

Group members

Shubhangi Sanyal (MDS202238) Subhashree Saha (MDS202243) Samriddha Adhikary (MDS202229)

October 14, 2023

1 Data Preprocessing

- The pixel values of input images were converted to tensors and then normalized.

2 DNN vs. CNN

- Designed and trained both Deep Neural Network (DNN) as well as Convolutional Neural Network (CNN) to classify the datasets.
- CNN tends to give better accuracy than traditional DNN for both the datasets because CNNs are specifically designed to capture spatial hierarchies and local patterns in images through shared weight parameters in convolutional layers, making them more effective at feature extraction and pattern recognition in visual data.

2.1 Effect of image scrambling

- CNNs rely on the spatial relationships between pixels in an image to learn and identify features. When the pixels of the images are scrambled, the spatial relationships gets destroyed, making it very challenging for the network to recognize patterns and features in the image.So, the accuracy of CNN drops for both the datasets after scrambling. Whereas, DNNs do not have convolutional layers and are not that much affected by image scrambling.
- From the tables below, it can be observed that CNNs show a greater decrease in accuracy when the input image pixels are permuted. This proves that convolutional neural networks can "visualize" information better than dense neural networks.

Table 1: DNN vs. CNN on Fashion MNIST

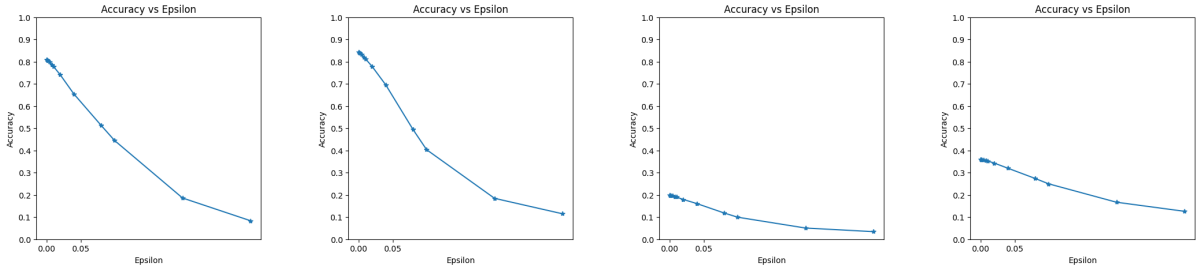
Neural Network	**Accuracy**	**Time needed**
DNN	85%	173.65s
CNN	90%	175.41s
DNN after image scrambling	87%	173.33s
CNN after image scrambling	87%	188.39s

Table 2: DNN vs. CNN on Sign Language MNIST

Neural Network	**Accuracy**	**Time needed**
DNN	59%	136.74s
CNN	88%	129.04s
DNN after image scrambling	47%	127.24s
CNN after image scrambling	64%	131.67s

2.2 FGSM attack

Demonstrating the effect of FGSM attack on Neural Networks



(a) DNN (Fashion MNIST) (b) CNN (Fashion MNIST) (c) DNN (Sign Language MNIST) (d) CNN (Sign Language MNIST)

- For both datasets, it is observed that as epsilon increases, accuracy drops. Additionally, CNN has a greater curvature since it remembers more features.

3 External Packages Used

1. `numpy` - For mathematical calculations, and array handling
2. `tensorflow` - For model tracking, performance monitoring, and model retraining
3. `math` - For mathematical operations
4. `matplotlib` - To visualize graphs, plots, and images
5. `tensorflow_datasets` - a collection of datasets ready to use, with TensorFlow
6. `random` - generating pseudorandom integers from a specified range to pick the number from
7. `torch` - For developing and training neural network based deep learning models
8. `torchvision` - provides additional functionalities to manipulate and process images with standard image processing algorithms
9. `time` - To calculate the time taken by the neural networks for training and testing