Assignment 2

r12922054 資工所 邱信瑋

Pseudocodes of Fast Gradient Sign Method

Algorithm 1 Fast Gradient Sign Method

```
$x$ ← Input data
$y$ ← Labels for Input data $x$
$\vartheta$ ← parameters of model
procedure FGSM:
    $\tilde{y} = feedforward(x)$
    $J(\vartheta,x,y) = loss(y, \tilde{y})$
    $\nabla_x J(\vartheta,x,y)$ ← backpropagates the gradient back to the input data
    $sign(\nabla_x J(\vartheta,x,y))$ ← get the gradient direction
    $pertured\_image = x + \varepsilon * sign(\nabla_x J(\vartheta,x,y))$, $\varepsilon \epsilon [0, 1]$ ← The function then creates perturbed image
```

Experiment Setting

I. Hardware Specification

- CPU : Intel(R) Core(TM) i7-6700K CPU 4.00GHz
- GPU : NVIDIA GeForce RTX 2070 8GB

II. Package Version

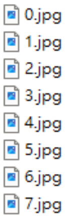
- python 3.10.13
- torch 1.11.0+cu113
- torchvision 0.12.0+cu113
- numpy 1.26.0
- tqdm 4.66.1
- matplotlib 3.8.0
- Pillow 10.0.1

III.All the experiment parameters and details in q2

In this paragraph, I will describe the details of this implementation, as follows.

1. How to convert testing data to image and save it?

First, reading data from *json* file and the data format is list. I converted the data format from *list* to *numpy*. The reason for doing this is to facilitate subsequent feeding of the model. Second, I used the *pillow* package, *Image* to convert the information in *numpy arrays* into images and save them in JPEG format, see Figure 1.



```
0.jpg
1.jpg
2.jpg
3.jpg
4.jpg
5.jpg
6.jpg
7.jpg
```

Figure 1: testing image with JPG format.

2. How to construct custom dataset and Why we need to do this?

The reason why we need to create a Custom dataset is because when we use *Pytorch* to train or test the model, we need to use the function it provides, *Dataloader*, which requires the input parameters to be paired with the data and its label.

As for how to create a Custom dataset, first create a Custom dataset class. Its input parameters are a list of data and a list of its corresponding labels. As for the source of the label for this job, I manually labeled it myself. In addition, it is worth noting that I Complete the transform in Custom dataset

3. What have I tried for this assignment?

(a) In this assignment, in addition to implementing the original correct method: denormalizing the data and adding noise to the original image, I also tested not denormalizing the data and directly using the values after Normalization to add noise.There will be differences in the results.

4. Some processing needs to be done on the testing data.

(a) Because the value of the training data is between 0-1, it is necessary to normalize the value of the testing data to 0-1.

5. Show the results

I use *matplotlib.pyplot* to finish this implementation, see below.

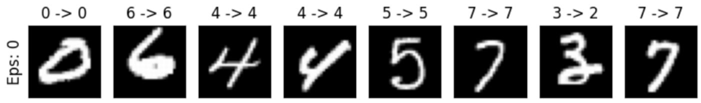


Figure 2: epsilon = 0.

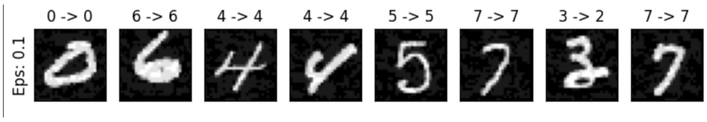


Figure 3: epsilon = 1.

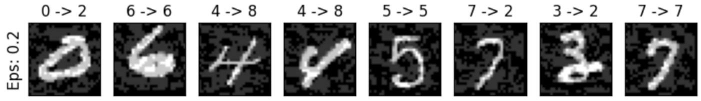


Figure 4: epsilon = 2.

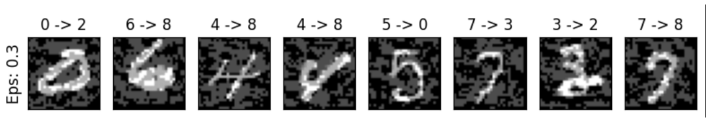


Figure 5: epsilon = 3.

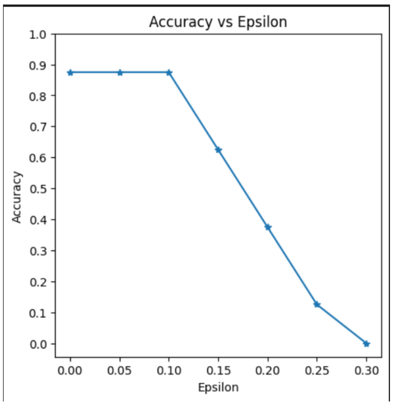


Figure 6: Accuracy with different epsilon