740 Deep Learning Project README File

1 Initial Setup

Please first begin by following these steps:

1. Please download `740_deeplearning` folder at this link: https://drive.google.com/drive/folders/1O2IX9ZFRE3by3s9HXRDFgXQ47FzPM8Nu?usp=share_link
2. Please create a folder named `740_deeplearning` on your Google Drive, and upload the downloaded content into it.
3. Please open a new notebook in Google Colab by clicking on the `File` tab and then `New notebook`.
4. Please change the runtime of the Google Colab to GPU by following these steps:
   (a) Open the Google Colab notebook.
   (b) In the top menu bar, click on `Runtime`.
   (c) Select `Change runtime type` from the dropdown menu.
   (d) In the pop-up window, choose `GPU` from the `Hardware accelerator` dropdown menu.
   (e) Click on `SAVE` to apply the changes.
5. In the following sections, we provide instructions on how to run ResNet, AutoAttack, Anomaly Detection, and our Novelty work. For each step, we have created a Jupyter Notebook. You need to copy and paste the content of each Jupyter notebook into a `New notebook` in Google Colab and execute each cell sequentially.
6. Please note that each Jupyter Notebook includes some initialization steps for mounting Google Drive and other setup procedures in the first cell.

2 ResNet Training

The `Model-cifar-ResNet18` folder contains the ResNet-18 model for training on CIFAR-10 and CIFAR-100 datasets. To train the model, follow these steps:

1. Copy and paste the contents of either `train_ResNet_18_CIFAR_10.ipynb` or `train_ResNet_18_CIFAR_100.ipynb` (based on the desired dataset) from the `740_deeplearning/Model-cifar-ResNet18` folder into a new Google Colab notebook.

2. The first cell imports Google Drive and copy the contents of the `740_deeplearning` folder into the Colab environment:

```
!rm -rf sample_data/
from google.colab import drive
drive.mount('/content/drive')
!cp -r /content/drive/MyDrive/740_deeplearning/* /content/
```

3. After training, the model will be saved as a `.pt` file.

3 Autoattack

To run Autoattack on the CIFAR-10 or CIFAR-100 datasets, follow these steps:

1. Copy and paste the contents of either `CIFAR_10_AutoAttack.ipynb` or `CIFAR_100_AutoAttack.ipynb` (based on the desired dataset) from the `740_deeplearning` folder into a new Google Colab notebook.

2. The results will be saved in the `Standard` folder for each dataset and norm.

4 Anomaly Detection

The `Anomaly_detection` folder contains the PANDA and FITYMI algorithms for anomaly detection.

PANDA Algorithm

To run the PANDA algorithm, follow these steps:

1. Copy and paste the contents of the `PANDA.ipynb` notebook from the `Anomaly_detection/PANDA` folder into a new Google Colab notebook.

2. The first cell set up the Google Colab environment:

```
!rm -rf sample_data/
from google.colab import drive
drive.mount('/content/drive')
!cp -r /content/drive/MyDrive/740_deeplearning/standard/* /content/
!cp -r /content/Anomaly_detection/PANDA/code/* /content/
!pip install faiss-gpu
```

3. The log files for different datasets and norms will be saved in separate folders.

FITYMI Algorithm

To run the FITYMI algorithm, follow these steps:

1. Copy and paste the contents of the `FITYMI.ipynb` notebook from the `Anomaly_detection/FITYMI` folder into a new Google Colab notebook.

2. The first cell set up the Google Colab environment:

```
from google.colab import drive
drive.mount('/content/drive')
!git clone https://github.com/sajjad2014/FITYMI.git
!cp -r /content/drive/MyDrive/740_deeplearning/* /content/
!cp -r /content/FITYMI/* /content/
!cp -r /content/drive/MyDrive/740_deeplearning/Anomaly_detection/FITYMI/* /content/
!cp -r /content/drive/MyDrive/740_deeplearning/standard/* /content/
!pip install -r requirements.txt
!wget https://storage.googleapis.com/vit_models/imagenet21k/ViT-B_16.npz -P pretrained_
!pip install faiss-gpu
!pip install ml_collections
```

3. The log files for different datasets and norms will be saved in separate text documents.

5 Novelty Algorithm

1. Copy and paste the contents of the `AutoAttack_cifar10_vgg.ipynb` notebook from the `Novelty` folder into a new Google Colab notebook.

2. The first cell set up the Google Colab environment:

```
from google.colab import drive
drive.mount('/content/drive')
!cp -r /content/drive/MyDrive/740_deeplearning/* /content/
!cp -r /content/drive/MyDrive/740_deeplearning/Novelty/* /content/
```

3. You can change `model_path` and `save_dir` to run different models such as HRANK, CRANK, and unpruned vgg networks.