EN. 520. 650 Project 2 Spring 2022

1. Download the CIFAR-10 dataset from

<https://www.cs.toronto.edu/~kriz/> [cifar.html](https://www.cs.toronto.edu/%7Ekriz/cifar.html). The dataset description is also there.

The CIFAR-10 dataset consists of 60000 32*×*32 color images 10 classes, with 6000 images per class. There are 50000 training images and 10000 test images. The dataset is divided into five training batches and one test batch, each with 10000 images. The test batch contains exactly 1000 randomly selected images from each class. The training batches contain the remaining images in random order, but some training batches may contain more images from one class than another. However, the training batches in total contain exactly 5000 images from each class.

Build a Deep Convolutional Neural Network, train it on CIFAR-10 training set and test it on CIFAR-10 testing set. You can use any architectures learned in class or come up with your own architecture.

Submission: Please try deep learning method on CIFAR-10 dataset, submit a report detailing the methods employed, experiments performed and results. The project should be done INDIVIDUALLY.

1. In this project you will implement several attack models (noise, semantic, FGSM, PGD and C-W) on the MNIST data and implement one defense mechanism of your choice. Compare the drops in classification performance for three values of noise magnitude

Due 05/11/2021