DEPENDABLE AND SECURE AI-ML (AI60006)

Assignment 1

Abhinav Bohra **18CS30049** horizontal line

# 1. Constructing adversarial examples

|  |  |
| --- | --- |
| **Before Adding Noise** | **After Adding Noise** |
|  |  |
| **Prediction:** Pomegranate | **Prediction:** Candle |

# 

# 2. Adversarial Training

# Models used: We used two different architectures to train our model: a 2-layer fully connected MLP, also referred to as a **DNN**, and a 6-layer ConvNet, also referred to as a **CNN**.

# 

|  |  |  |
| --- | --- | --- |
| **Original Model without Perturbations** | | |
| Model | Miss-classification Rate | Output Screenshot |
| DNN | 0.0279 | original_preds_dnn |
| CNN | 0.0106 | original_preds_cnn |