Landon Buell

Error Compensation Attacks

Data Analysis Report

19 July 2020

**Error Compensation Attacks - Data Analysis Report**

Convolutional Neural Network with “Approximation Layer” and “Compensation Layer” Objects after Input Layer Object. All sample used are images with shape 32 x 32 x 3 matrices of bytes. A “Mask vector” is hard coded within the program, which is used to determine the indexes of pixels with will be subject to the approximation or compensation.

Approximation Layer Object:

Takes a batch of samples shaped (batch\_size,32,32,3) and tests for a “beta” condition, based on the internal clock. Given the FLOP frequency, the beta condition is set to a microsecond accuracy. If the systems internal clock measures the microsecond counter as an even number when the layer is called, then the ask is used to apply the approximation to the designated pixels. If the microsecond counter is an odd number, no approximation is applied and the batch is passed through the layer untouched. The approximation method approximates all designated bits to *0*.

Compensation Layer Object:

Takes a batch of samples shaped (batch\_size,32,32,3) and always attempts to compensation