Autonomous Vehicle AI Analysis

Ankit Patel, Cristian Vives, Dr. Joseph Ernst, Mark Rogers, Di Jin
Hume Center Colloquium, April 18th 2018

Objective

Investigate how adversarial artificial intelligence prevention can help ensure the safety of future vehicles

Project Background

Using Python and TensorFlow to classify a large traffic sign dataset using a convolutional neural network (CNN)

Adversarial Phase: manipulate images within dataset to test vulnerabilities of machine learning and our CNN model and ensure accuracy

Sample Images from the dataset

Number of different classes: 2

Data Processing

Over 7000 raw images varying in size

All images gray scaled to reduce channels

Images were upscaled by padding or downscaled

Used a Binary Classification System with respect to number of unique classes

References

1. Andreas Møgelmose, Mohan M. Trivedi, and Thomas B. Moeslund, "Vision based Traffic Sign Detection and Analysis for Intelligent Driver Assistance Systems: Perspectives and Survey," *IEEE Transactions on Intelligent Transportation Systems,* 2012.

Creating the Neural Network

5 layers (Convolutional, Flattening, Pooling, Fully Connected)

Weights, biases, and filters to create the feature maps

Centered around TensorFlow and Estimator API

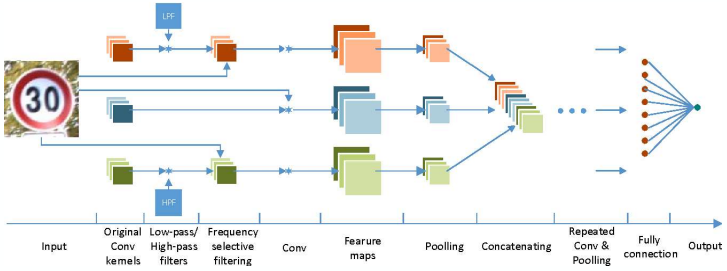


Figure 1.“Under the Hood” structure of the CNN

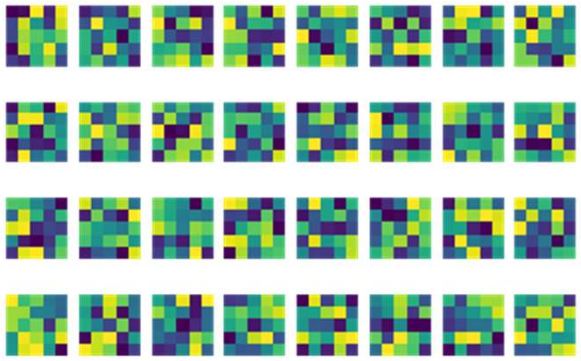


Figure 2. Output of filters of the primary layer

Key features of CNN

Dropout: Randomly ignoring neuron nodes during the training phase to prevent overfitting

Estimator API: Allows for high-level implementation of machine learning model

Training and Testing Neural Network

Images were split 80/20 to between training and testing

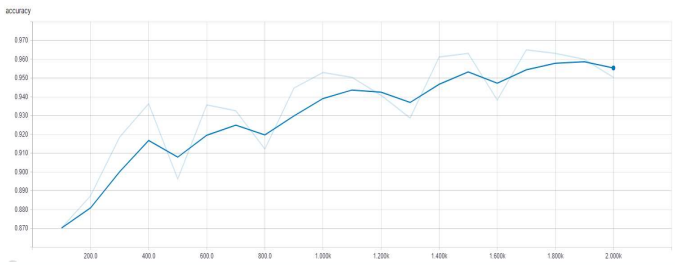


Figure 3. Accuracy vs. Number of steps

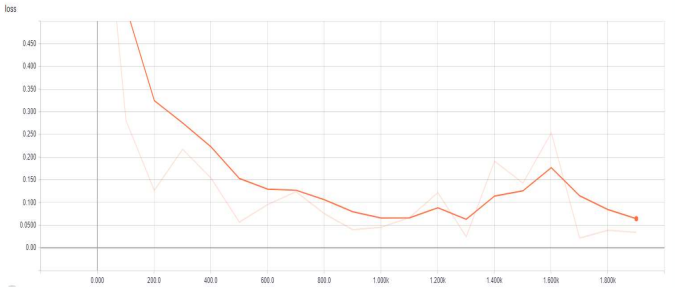
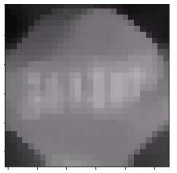


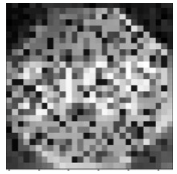
Figure 4. Computed loss vs. Number of steps

Adversarial Phase

Original
Result: Stop Sign



Blurred 70%
Result: Stop Sign



Salt and Pepper
Result: Not a Stop Sign