GTSRB Neural Network and Verification

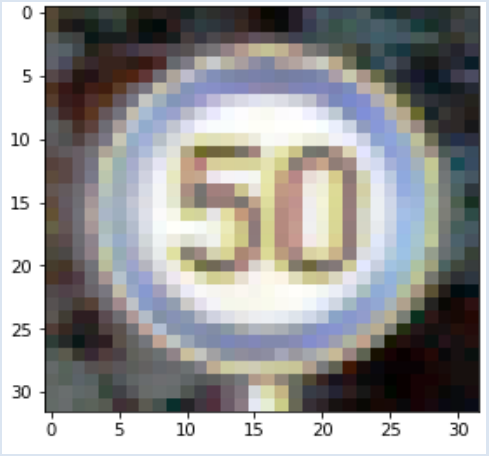
Karman Nagra

Tel (615) 343-7472 | Fax (615) 343-7440
1025 16th Avenue South Nashville, TN 37212
www.isis.vanderbilt.edu

VANDERBILT UNIVERSITY

Dataset

- Image Classification Network
- 43 image classes for German road signs
- Training data with 39209 rgb images
- Test data with 12630 rgb images
- https://sid.erda.dk/public/archives/daaeac0d7ce1152aea9b61d9f1e19370/published-archive.html



Model Structure

```
Model: "sequential"
_________________________________________________________________
Layer (type)                 Output Shape              Param #
=================================================================
conv2d (Conv2D)              (None, 32, 32, 32)        896
_________________________________________________________________
conv2d_1 (Conv2D)            (None, 30, 30, 32)        9248
_________________________________________________________________
dropout (Dropout)            (None, 30, 30, 32)        0
_________________________________________________________________
conv2d_2 (Conv2D)            (None, 30, 30, 64)        18496
_________________________________________________________________
conv2d_3 (Conv2D)            (None, 28, 28, 64)        36928
_________________________________________________________________
dropout_1 (Dropout)          (None, 28, 28, 64)        0
_________________________________________________________________
conv2d_4 (Conv2D)            (None, 28, 28, 128)       73856
_________________________________________________________________
conv2d_5 (Conv2D)            (None, 26, 26, 128)       147584
_________________________________________________________________
dropout_2 (Dropout)          (None, 26, 26, 128)       0
_________________________________________________________________
flatten (Flatten)            (None, 86528)             0
_________________________________________________________________
dense (Dense)                (None, 512)               44302848
_________________________________________________________________
dropout_3 (Dropout)          (None, 512)               0
_________________________________________________________________
dense_1 (Dense)              (None, 43)                22059
=================================================================
Total params: 44,611,915
Trainable params: 44,611,915
Non-trainable params: 0
```

Results

- Training time ~90 minutes
- Test dataset accuracy: ~95%

Verification Applications

- Adversarial Perturbations
- Analyzing Adversarial Attacks Using FoolBox.
- Generate adversarial perturbations for the nnv tool.