Mitigating Backdoor Training Parameters

Environment Settings

- Framework version (PyTorch version):
- CUDA version (if applicable):
- GPU used (Newt/Floo/local - specifics):

Dataset Settings

- Data preprocessing techniques applied (if any):
- Data augmentation techniques (if any):

Model Architecture

- Base model: Backdoored VGG16 on GTSRB
- Any modifications to the architecture:

Neural Cleanse Detection Parameters

- Threshold used for MAD anomaly detection:
- Number of optimization iterations:
- Batch size:
- Optimizer:
- Learning rate:
- Learning rate schedule (if any):
- Weight decay:
- Loss function:
- Early stopping criteria (if used):

Random Seeds

- Random seed for model initialization (if applicable):
- Random seed for weight initialization (if applicable):
- Random seed for data augmentation (if applicable):

Additional Notes: please write any other techniques and methods used.