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: VGG16 pretrained on GTSRB
- Any modifications to the architecture:

Backdoor Implementation

- Trigger pattern description in words (must be ≤16 pixels): (e.g. black cross on top center of the image)
- Poisoning ratio (% of training data poisoned): (e.g. my source class [1] has 1500 samples. I poisoned 400 samples. Poisoning ratio = 27%)

Training Hyperparameters

- Number of epochs:
- 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.