Temporary MS Word

README

For GitHub Repository: KradNosnatef/CS612\_Project

# CS612 Group Project Very First README

Reference: <https://github.com/SoftWiser-group/FTrojan>

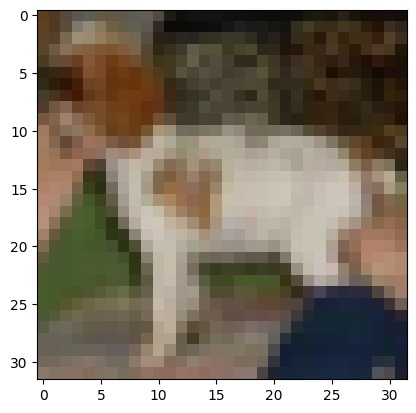
## Abstract

This is a study program for implementing a backdoor detector to identify backdoor embedded in the neural network.

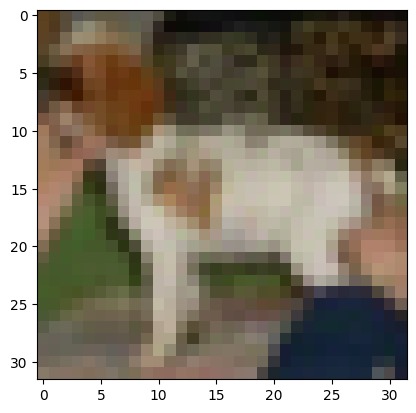
Currently we are using FTrojan FIBA as our test object and our test dataset is CIFAR-10.

## Implementation of FTrojan FIBA

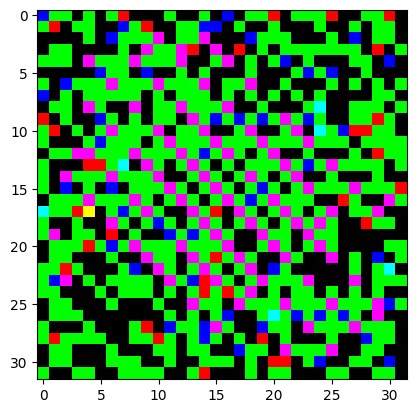
As an FIBA, FTrojan impose trigger by inserting information into the frequency domain, After this information being restored to the spatial domain, generally it will be difficult to be detected by the naked eye:



Original Image



Poisoned Image



Trigger

We trained model using the default settings of the original author. The model got 84% correct on the CIFAR-10 test dataset and got more than 99% ASR when we poisoned the test image