This folder contains the source code for our Fake Gradient:

Experiment Environment:

This code is developed with Python 3.7 Pytorch 1.0 and OpenCV4.0

The DNN models used here are from the torchvision libraries.

The files are organized as below:

Fake Gradient:

|

|

|---------***ModelModify.py***: contains the core functions that modify the model

|

|---------***DeepFoolB.py***: the original code of Deepfool

|

|---------***DeepFoolC.py***: the original code of Deepfool with minor modification for

| displaying the parameters of the modified model

|

|---------***HeatMapShow.py***: contains functions to process and visualize the

| gradient/perturbation

|

|---------***AnalysisWeight.py***: Code to analyze the weights of fully connected layer

|

|---------***MM21\_classifiactionResult.py***: The code to analyze the overhead

|

|

|---------***MM21\_FakeGradient\_DeepFool\_XXXX.py***: The code to analyze defense

| accuracy based on Model XXXX