Bosch's Model Extraction Attack For Video Classification

Team 17

Inter IIT Tech Meet 10.0

Folder Structure

- **BlackBox_P1**: Contains scripts for training the extracted model from SwinT victim under the Black Box setting. Refer to `setup_readme` within the folder for detailed instructions on running the code for training.

- **BlackBox_P2**: Contains scripts for training the extracted model from MoViNet victim under the Black Box setting. Refer to `setup_readme` within the folder for detailed instructions on running the code for training.

- **GreyBox_P1**: Contains scripts for training the extracted model from SwinT victim under the Grey Box setting. Refer to `setup_readme` within the folder for detailed instructions on running the code for training.

- **GreyBox_P2**: Contains scripts for training the extracted model from MoViNet victim under the Grey Box setting. Refer to `setup_readme` within the folder for detailed instructions on running the code for training.

Each of the above folders have the last obtained checkpoint of the extracted models stored in the `checkpoints` subfolder.

- **Evaluation_All** - Contains Jupyter Notebooks for evaluation. Refer to `eval_readme` within the folder to get information on the setup and run environment.

Running Environment

Training codes were run on a single server equipped with NVIDIA V100 GPU. Evaluations codes were run on Google Colaboratory with a Pro Plus subscription.