Grey Box Model Extraction on SwinT

Team 17

A. Training

Setup

- Download the entire folder on your local drive.
- Navigate to the folder directory, and setup the virtual environment as:

  ```
  >python -m venv v1
  >source v1/bin/activate
  ```

- Install necessary dependencies

  ```
  >pip install -U torch==1.8.0+cu101 torchvision==0.9.0+cu101 torchtext==0.9.0
  torchaudio==0.8.0 -f https://download.pytorch.org/whl/torch_stable.html
  >pip install mmcv-full==1.4.0 -f
  https://download.openmmlab.com/mmcv/dist/cu101/torch1.8.0/index.html
  >pip install av
  >pip install git+https://github.com/wilson1yan/VideoGPT.git
  >pip install scikit-video
  >pip install --upgrade --no-cache-dir gdown
  ```

  Note that the above versions have been chosen corresponding to the CUDA version on our device (=CUDA 11.2).

- Run `generate_samples.py` script to generate samples for training the extracted model.
- Run `create_dataset.py` script to transform the generated dataset in the required structure, and incorporate the class label predictions from the victim model. Essentially, this script uses the videos generated in the earlier step, and stores them in a subfolder whose name corresponds to the class label index predicted by the victim.
- Run `train.py` script to train the model on the generated dataset in the above steps. The checkpoints will be stored in the folder `checkpoint` in the base directory

Training was done on a Linux server equipped with NVIDIA Tesla V100 32GB.