Handbuch

Installation:

Referenzplattform: Windows 10 x64, Release 1803 (10.0.17134.319) oder neuer

Voraussetzungen unter Python 3.7.0:

numpy==1.15.4
torch==1.0.0
matplotlib==2.2.3
requests==2.19.1
torchvision==0.2.1
Pillow==5.4.1

1. Downloaden des Anaconda-Installers: Anaconda installer für Windows.

2. Installieren von Anaconda:

Doppelklicken der .exe Datei.
Folgen Sie den Anweisungen auf dem Bildschirm.
Wenn Sie unsicher über Einstellungen sind, akzeptieren Sie die Standardeinstellungen.

2.1 Eventuell müssen die Umgebungsvariablen für Anaconda wie folgt eingefügt werden:

1. Geben Sie „Systemumgebungsvariablen bearbeiten“ in die Windowssuche ein.
2. Klicken sie auf den Reiter „Erweitert“ und dann auf „Umgebungsvariablen...“
3. Bearbeiten Sie die Benutzervariale „Path“.
4. Fügen Sie den Anaconda-Pfad ähnlich wie in *Abbildung 1* ein.

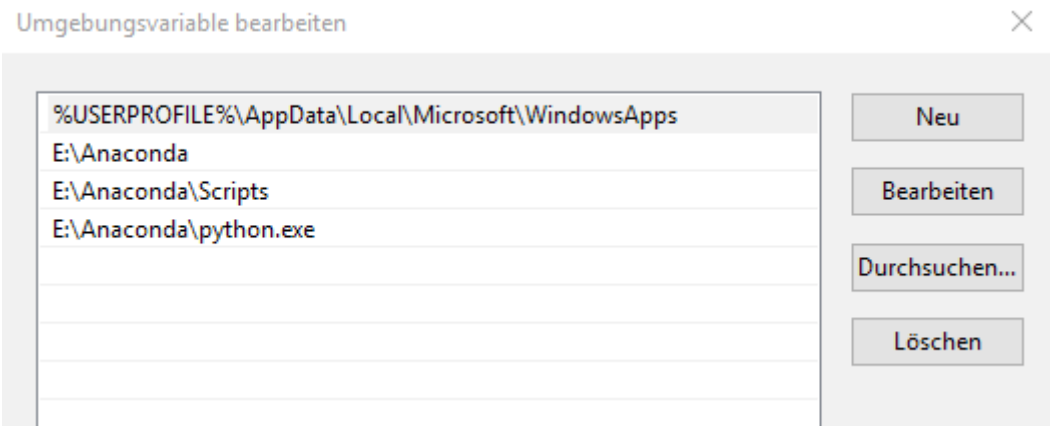

Abbildung 1: Path-Variablen einfügen

3. Installieren der Requirements:

Manuell über Anaconda

oder

über die Konsole mit der mitgelieferten Textdatei requirements.txt :

```
conda install --yes --file requirements.txt
```

pytorch installation:

```
conda install pytorch torchvision -c pytorch
```

Betrieb:

Es sollte folgende Ordnerstruktur vorliegen:

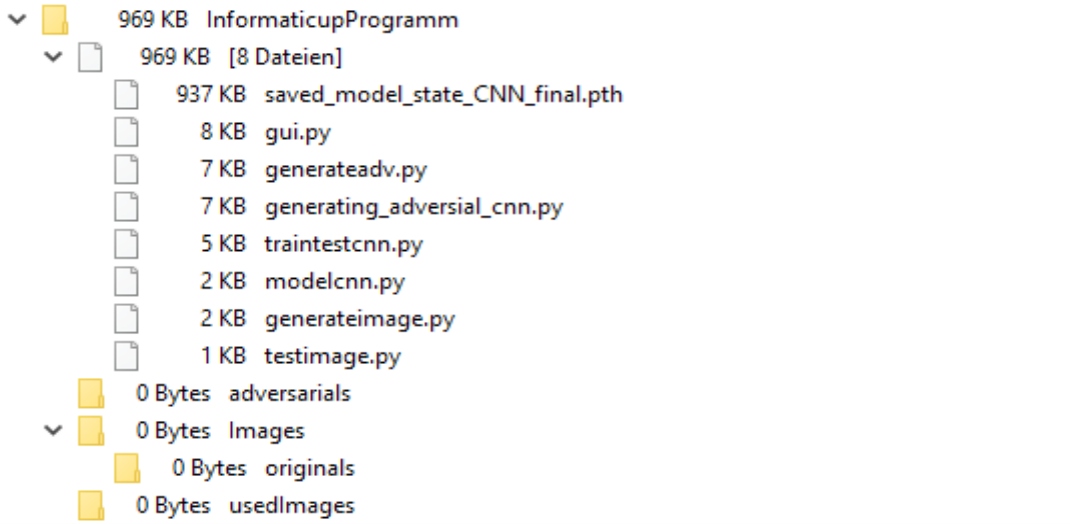

Abbildung 2: Die Ordnerstruktur

1. Über das GUI:

   Führen Sie die Datei „gui.py“ über die Konsole mit folgendem Befehl aus:

   python gui.py

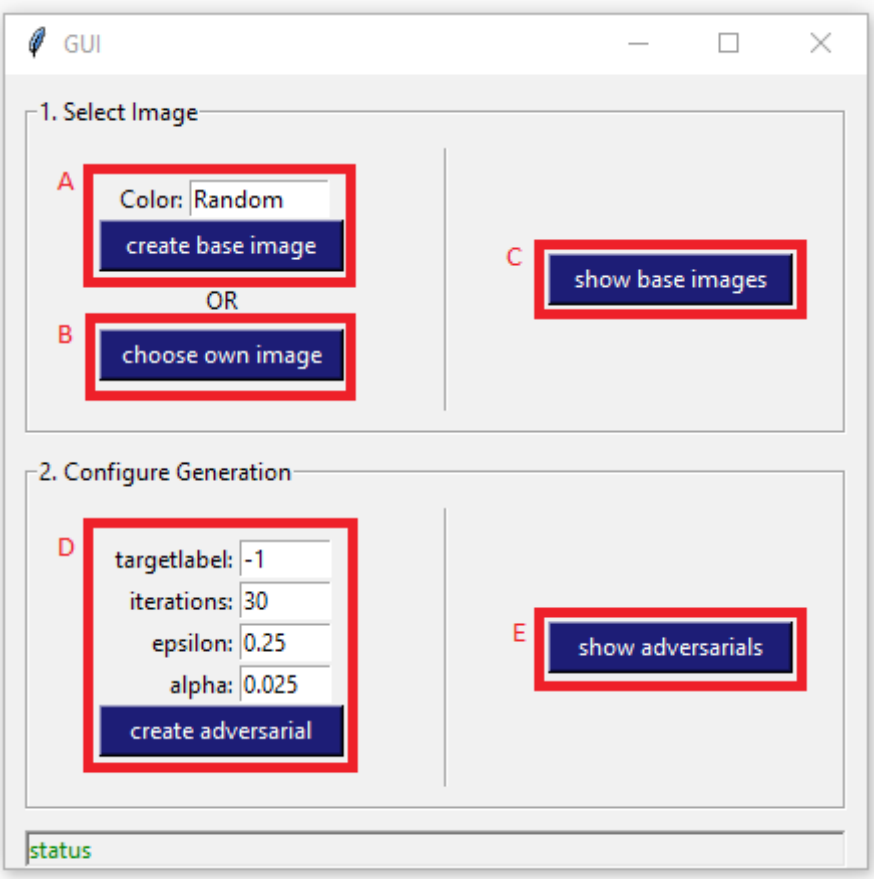

Abbildung 3: Das GUI

2. Erstellen Sie ein zufälliges Bild oder ein Bild einer bestimmten Farbe (Zum Beispiel „Color: red“, siehe *Abbildung 3.A*)

oder

Wählen Sie ein Bild (siehe *Abbildung 3.B*), aus dem ein Irrbild gemacht werden soll. Optional kann man auch ein Bild über den Dateiexplorer manuell in das Verzeichnis verschieben.

3. Klicken Sie auf „show base images“, um zu kontrollieren, dass sich das Bild an der richtigen Stelle befindet. **WICHTIG:** Es darf sich nur ein Bild in dem Ordner befinden, ansonsten kann es zu Fehlern kommen.

4. Generieren Sie aus dem Basisbild das Irrbild. Wählen Sie dazu ein bestimmtes Angriffslabel (*Abbildung 3.D*: targetlabel: 0,1,…,42) oder versuchen Sie es mit allen vorhandenen Straßenschildern (*Abbildung 3.D*: targetlabel: -1). Es können noch verschiedene Einstellungen an

den iterations-, epsilon- und alpha-Werten vorgenommen werden. (Empfohlen werden die Basiseinstellungen in *Abbildung 3.D*)

5. Nach Beendigung der Generierung erscheint ein Fenster mit allen Ergebnissen (*Abbildung 4*). Klicken Sie auf OK.

Abbildung 4: Ergebnisse für die generierten Irrbilder

6. Lassen Sie sich über „show adversarials“ (*Abbildung 3.E*) alle Bilder mit einer Konfidenz von über 95% anzeigen.