TECHNISCHE HOCHSCHULE NÜRNBERG
GEORG SIMON OHM

Erstellung von Irrbildern zur Überlistung einer Verkehrsschilder erkennenden KI

IT-Projekt Bericht

Studiengang *Informatik*

Technische Hochschule Georg Simon Ohm

von

Leonhard Applis, Peter Bauer, Andreas Porada und Florian Stöckl

Abgabedatum:	15.03.2019
Gutachter der Hochschule:	Prof. Dr. Gallwitz

Eidesstattliche Erklärung

Wir versichern hiermit, dass der IT-Projekt Bericht mit dem Thema

Erstellung von Irrbildern zur Überlistung einer Verkehrsschilder erkennenden KI

selbständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe. Die Arbeit wurde bisher keiner anderen Prüfungsbehörde vorgelegt und auch nicht veröffentlicht.

Wir versichern zudem, dass die eingereichte elektronische Fassung mit der gedruckten Fassung übereinstimmt.

Nürnberg, den 19. Dezember 2018

Leonhard Applis, Peter Bauer, Andreas Porada und Florian Stöckl

Abstract

To be done

title:	Fooling an TrafficSign-AI
author:	Leonhard Applis, Peter Bauer, Andreas Porada und Florian Stöckl
reviewer DHBW:	Prof. Dr. Gallwitz

Kurzfassung

To be done

Titel:	Erstellung von Irrbildern zur Überlistung einer Verkehrsschilder erkennenden KI
Author:	Leonhard Applis, Peter Bauer, Andreas Porada und Florian Stöckl
Prüfer der Hochschule:	Prof. Dr. Gallwitz

Inhaltsverzeichnis

Abbildungsverzeichnis VI

1 Einleitung 1
- 1.1 Motivation . . . 1
- 1.2 Ziel der Arbeit . . . 1
- 1.3 Aufbau der Arbeit . . . 1
- 1.4 Verwandte Werke und Primärquellen . . . 1
- 1.5 Rahmenbedingungen des Informaticups . . . 1

2 Gegneranalyse 2
- 2.1 Ursprungsdaten . . . 2
- 2.2 Modellschätzungen . . . 2

3 AI-Greyboxing 3
- 3.1 Konzept . . . 3
- 3.2 Implementierung und erste Ergebnisse . . . 3
- 3.3 Fehler- und Problemanalyse . . . 3

4 Degeneration 4
- 4.1 Konzept . . . 4
- 4.2 Implementierung Remote . . . 4
- 4.3 Ergebnisse Remote . . . 4
- 4.4 Implementierung Lokal . . . 4
- 4.5 Anpassung und Verbesserung Lokal . . . 4
  - 4.5.1 Batch-Degeneration . . . 5
  - 4.5.2 Parallel-Degeneration . . . 5

5 Saliency Maps ANPE 6

6 Fazit 7
6.1 Zusammenfassung 7
6.2 Weiterführende Arbeiten 7

Literaturverzeichnis 8

Abbildungsverzeichnis

1 Einleitung

1.1 Motivation

Optische Täuschungen, Irrbilder, Rahmenbedingungen

1.2 Ziel der Arbeit

1.3 Aufbau der Arbeit

1.4 Verwandte Werke und Primärquellen

1.5 Rahmenbedingungen des Informaticups

2 Gegneranalyse

In das Kapitel kommen die Dinge die wir über die Trasi-AI wissen

Anderer Chapter-Title

2.1 Ursprungsdaten

Hier gehen wir kurz auf die Trainingsdaten ein die wir haben, zeigen ein paar Bilder und wie fürchterlich hässlich die sind in 64x64

2.2 Modellschätzungen

Hier kommen unsere Erfahrungen, die wir mit dem Modell gemacht haben

1. Gekürzte Klassen: Aus unserer MongoDB können wir ziemlich sicher sagen, dass wir nur 33 Klassen von Trasi haben, keine 43. Wir können nachsehen welche fehlen
2. Softmax-Ausgabefunktion
3. Interpolationsfunktion (vllt mit einem Bild in 3 Interpolationsversionen und jeweiligen Score)
4. Overfitting bei Trainingsdaten
5. unzuverlässigkeit bei nicht-Schildern (z.B. OhmLogo)

3 AI-Greyboxing

3.1 Konzept

Wichtigste Inhalte:

1. hübsches Diagramm was für Komponenten
2. Stichpunktartige Beschreibung der Komponenten
3. Workflow durch Setup (Gen - Score - DB - Training - AI)
4. Workflow Ansatz in betrieb (Gen - AI - Scorer)

3.2 Implementierung und erste Ergebnisse

Code zeigen? MongoDB sagen?

3.3 Fehler- und Problemanalyse

Schätzen, das man aus Pixelbrei nichts lernen kann.

4 Degeneration

4.1 Konzept

Hier kommt die Idee, der Pseudocode und die Voraussetzungen damit es klappt

4.2 Implementierung Remote

Hier kommt der konkrete Code, das trennen der Alternation-Funktionen und einige sonstige Ideen hin

4.3 Ergebnisse Remote

Hier kommen ein paar Beispiele und Plots.

Auch hierhin kommt ein Fazit welche AlternationFunktionen wie gut waren und das die Trainingsbilder nicht geeignet waren

Sehr wichtig sind die benötigten Zeiten.

4.4 Implementierung Lokal

Ich weiß nicht ob das ein extra Punkt ist, aber an sich würde ich hier das Model bei uns kurz vorstellen

4.5 Anpassung und Verbesserung Lokal

Hier kommen zunächst so Dinge wie "wait"rauszunehmen aber GPU-Acceleration würde ich auch hernehmen.

4.5.1 Batch-Degeneration

Ist noch ein To-Do: Degenerieren von 100 Bildern, Wahl des "besten". Mach ich noch.

4.5.2 Parallel-Degeneration

Nur Ansatz: Hat nicht geklappt das zu basteln weil numpy Arrays echt nervig sind bei Parallelverarbeitung.

Vorstellen kann man das allerdings kurz. Konflikt mit GPUAcceleration.

5 Saliency Maps ANPE

Hier kommt Andreas und Peters Teil.

Das File zu Evolutionären Algorithmen ist noch vorhanden, nur nicht eingebunden.

6 Fazit

6.1 Zusammenfassung

6.2 Weiterführende Arbeiten

Literaturverzeichnis