

# Erstellung von Irrbildern zur Überlistung einer Verkehrsschilder erkennenden KI

## Ausarbeitung

Master-Studiengang *Informatik*

Technische Hochschule Georg Simon Ohm

von

Leonhard Applis, Peter Bauer, Andreas Porada und Florian Stöckl

Abgabedatum: 15.01.2019

# Abstract

to be done

**title:** Fooling an TrafficSign-AI

**authors:** Leonhard Applis, Peter Bauer, Andreas Porada und Florian Stöckl

# Kurzfassung

Diese Arbeit zeigt anhand von mehreren wissenschaftlichen Ansätzen, wie Convolutional Neural Networks zur Erkennung und korrekten Klassifikation von Straßenschildern überlistet werden können. Im Bereich des Autonomen Fahren wurden mit Neuronalen Netzen die Erkennungsrate drastisch gesteigert, allerdings sind diese immer noch fehleranfällig gegenüber gezielt erzeugten Irrbildern. Selbst ohne Informationen über die unterliegende Architektur (sog. Black-Box Angriffe), sollen Angriffe durch anderweitig erzeugte Irrbilder möglich sein. Die vorgestellten Verfahren *Degeneration*, *Saliency Maps* und *Gradient Ascent* werden erfolgreich angewendet, um mithilfe eines eigenen Neuronalen Netz welches als *Substitute* dient, Irrbilder für Angriffe auf ein unbekanntes Neuronales Netz zu erzeugen. Ein Angriff gilt als "erfolgreich", wenn das Bild mit einer Konfidenz größer als 90% als Straßenschild erkannt ist, welches ein menschlicher Betrachter nicht als solches erkennen würde.

Titel: Erstellung von Irrbildern zur Überlistung einer Verkehrsschilder  
erkennenden KI

Autoren: Leonhard Applis, Peter Bauer, Andreas Porada und Florian Stöckl

# Inhaltsverzeichnis

<b>Abbildungsverzeichnis</b>	<b>V</b>
<b>Abkürzungsverzeichnis</b>	<b>1</b>
<b>1 Einleitung</b>	<b>2</b>
1.1 Problemstellung . . . . .	3
1.2 Ziel der Arbeit . . . . .	3
1.3 Aufbau der Arbeit . . . . .	4
<b>2 Anforderungsanalyse und Rahmenbedingungen</b>	<b>6</b>
2.1 Rahmenbedingungen des Informaticups . . . . .	6
2.2 Eigenschaften des bereitgestellten Neuronalen Netz . . . . .	6
<b>3 Technisches Konzept</b>	<b>7</b>
3.1 Verwendete Technologien . . . . .	7
3.2 Transferierbarkeit von Angriffen auf ein Blackbox Modell . . . . .	9
3.3 Implementierung eines eigenen Modells zur Klassifizierung von Straßen- schildern (Aphrodite) . . . . .	9
<b>4 Degeneration</b>	<b>11</b>
4.1 Konzept . . . . .	11
4.2 Implementierung Remote . . . . .	14
4.3 Ergebnisse Remote . . . . .	16
4.4 Implementierung Lokal . . . . .	20
4.4.1 Batch-Degeneration . . . . .	22
4.4.2 Parallel-Degeneration . . . . .	23
4.4.3 Tree-Degeneration . . . . .	24

<b>5</b>	<b>Saliency Maps</b>	<b>26</b>
5.1	Konzept . . . . .	26
5.2	Implementierung . . . . .	27
5.3	Ergebnisse . . . . .	28
<b>6</b>	<b>Gradient Ascent</b>	<b>31</b>
6.1	Konzept . . . . .	31
6.2	Implementierung . . . . .	31
6.3	Ergebnisse . . . . .	32
<b>7</b>	<b>Fazit</b>	<b>35</b>
7.1	Zusammenfassung . . . . .	35
7.2	Diskussion . . . . .	35
7.3	Weiterführende Arbeiten . . . . .	36

# Abbildungsverzeichnis

4.1	Degeneration Tiefe 600 . . . . .	16
4.2	Degeneration Tiefe 4000 . . . . .	17
4.3	Plot Degeneration . . . . .	17
4.4	Degeneration overfit . . . . .	18
4.5	Batch-Degeneration-Plot . . . . .	22

# Abkürzungsverzeichnis

<b>DBMS</b>	Database Management System
<b>ETL</b>	Extract-Transform-Load
<b>KI</b>	Künstliche Intelligenz
<b>SQL</b>	Structured Query Language
<b>NN</b>	Neurales Netz
<b>DNN</b>	Deep Neural-Network
<b>CNN</b>	Convolutional Neural-Network
<b>GTSRB</b>	German Traffic Sign Recognition Benchmark
<b>PPM</b>	Portable Pixmap Image
<b>PNG</b>	Portable Network Graphic

# 1 Einleitung

Der Traum von einem autonom gelenkten Automobil ist so alt wie das Automobil selbst [?]. Fabian Dröger schreibt dazu in seinem Beitrag „Das automatisierte Fahren im gesellschaftswissenschaftlichen und kulturwissenschaftlichen Kontext“ in dem Sammelwerk „Autonomes Fahren“ von Markus Maurer et al., wie die zunehmende Anzahl an Verkehrstoten in den USA zu Beginn des 20. Jahrhunderts in Verbindung mit den technischen Errungenschaften in der frühen Flugzeug- und Radiotechnik den Wunsch nach einem selbstfahrenden Automobil aufkommen ließen. Die Vision war, dass ein Automobil ähnlich wie ein Flugzeug durch einen Autopiloten in der Spur gehalten und gesteuert werden könnte. Für die Ansteuerung der mechanischen Teile setzte man auf eine Fernsteuerung mit Funk, die zu dieser Zeit im Bereich der *Radioguidance* erforscht wurde.

Der aktuelle Stand der Technik zeigt, dass sich die Umsetzung dieser Vision schwieriger gestaltet, als zunächst angenommen. Anstelle einer autonomen Steuerung finden sich in heutigen Automobilen verschiedene Techniken zur Erhöhung der Fahrsicherheit und des Komforts. Beispiele sind Spurhalteassistenten, automatische Abstandshalter oder Einparkhilfen. Diese Funktionen unterstützen einen menschlichen Fahrer, ermöglichen jedoch noch kein selbstständiges Fahren.

Es wird aber weiterhin an der Entwicklung eines autonomen Fahrzeugs geforscht, wie die Vergabe von Forschungsgeldern[?] und Berichte von Automobilherstellern[?] und der Presse[?] zeigen. Die Forschung im Bereich Künstliche Intelligenz (KI) hat mittlerweile einen Stand erreicht, der für die Automatisierung des Autos genutzt werden kann. Ein besonderer Fokus liegt hierbei auf dem Erkennen von Bildern aus der Umwelt mittels KI. Im Straßenverkehr ist besonders die Erkennung von Straßenschildern von Bedeutung.



## 1.1 Problemstellung

Im Bereich der Bilderkennung erreichen neuronale Netze bahnbrechende Erfolge. Im Zuge der Forschung trat allerdings ein neues Phänomen auf, die sogenannten *Adversarial Attacks* [?].

Innerhalb dieser Angriffe werden gezielt Gewichte stimuliert, um gewünschtes Feedback des neuronalen Netzes zu erzielen. Die dabei erzeugten Fragmente haben selten etwas mit einem *echten* Bild zu tun - sie wirken entweder wie Rauschen oder moderne Kunst.

Da diese präparierten Bilder eben nicht aussehen, wie beispielsweise ein Verkehrsschild, kann ein Mensch schwer erkennen ob ein Angriff unternommen wird.

Durch den steigenden Einsatz von Machine Learning in verschiedenen sensiblen Sektoren des täglichen Lebens, wie selbstfahrenden Autos, Terrorismusbekämpfung oder Betrugserkennung können Angriffe verheerende Schäden erzeugen und stellen ein lohnendes Ziel dar.

Vor allem im Bereich des autonomen Fahrens, welcher ohnehin geprägt ist durch die Debatte über *Vertrauen in Technik* [?], können erfolgreiche Angriffe zu einem forschungsschädlichen Misstrauen führen - und das gesamte Themengebiet frühzeitig begraben.

Um gegen Adversarial Attacks vorzugehen, werden zunächst einige dieser *Irrbilder* benötigt. Anschließend können, um das neuronale Netz zu härten, Tests durchgeführt werden und die Angriffe berücksichtigt werden.

Diese Irrbilder zu erzeugen stellt das Kernziel dieser Arbeit dar.

## 1.2 Ziel der Arbeit

Ziel dieser Arbeit ist es, Methoden und Herangehensweisen vorzustellen, um die Aufgabenstellung des Informaticup 2019 zu erfüllen:

Hyperlink!

Hierbei soll ein neuronales Netz, welches sich hinter einer Webschnittstelle verbirgt und Verkehrsschilder erkennt, erfolgreich *überlistet* werden - es sollen absichtlich Bilder erzeugt werden, welche für den Menschen keine Verkehrsschilder sind aber mit einer Konfidenz von über 90% als solche erkannt werden.

Die gefundenen Methoden sollen reproduzierbar sein und in einem Maße flexibel, um beliebig viele Irrbilder zu erzeugen.

Der erweiterte Rahmen dieser Arbeit umfasst eine Dokumentation der Methoden sowie Verbesserungen und Schlussfolgerungen aus den Implementierungen zu ziehen.

Ebenfalls geliefert werden alle Elemente, um die erzielten Ergebnisse zu reproduzieren und variieren.

Nicht Ziel dieser Arbeit ist, einen Überblick über neuronale Netze, künstliche Intelligenz oder Bildbearbeitung zu vermitteln.

Ebenfalls außerhalb dieser Arbeit liegt eine Auswertung, welche Bilder von einem Menschen als Verkehrsschilder erkannt werden. Die Aussagen über solche stützen sich ausschließlich auf die persönliche Einschätzung des Projektteams.

## 1.3 Aufbau der Arbeit

Innerhalb dieser Arbeit werden zunächst in Kapitel 2 Informationen über die Webchnittstelle gesammelt und aufbereitet.

Im Abschnitt 2.2 werden hierfür zunächst die German Traffic Sign Recognition Benchmark (GTSRB) vorgestellt, welche für das Training der Webschnittstelle verwendet wurden. Dieses Datenset bildet ebenfalls einen zentralen Ausgangspunkt für einige der verfolgten Ansätze.

Anschließend werden in Abschnitt 3.2 die Eigenschaften des Modells zusammengefasst. Diese bestehen zum einen aus den offiziellen Angaben der Gesellschaft der Informatiker, zum anderen aus gewonnenen Erkenntnissen. Dieses Kapitel bildet die Grundlage, um die Schnittstelle einzuschätzen.

Anschließend werden verschiedene Lösungsansätze vorgestellt, beginnend mit der *Degeneration* in Kapitel 4.

Dieser Ansatz verändert iterativ ein Verkehrsschild, und behält die Änderungen bei, sollte der erzielte Score im akzeptablen Bereich liegen. Mit passender Bildver-

änderungen erzielen höhere Iterationen unkenntliche Ergebnisse.

Innerhalb des Kapitels wird zunächst im Abschnitt 4.1 die Idee anhand von Pseudocode weiter erläutert und anschließend in Abschnitt 4.2 die Implementierung für die Webschnittstelle gezeigt. Die Ergebnisse liegen gesondert im Abschnitt 4.3 vor.

Neben der Implementierung für die Webschnittstelle werden zum Abschluss des Kapitels in Abschnitt 4.4 noch weitere Verbesserungen für eine lokale Implementierung vorgestellt, welche allerdings nicht für die Webschnittstelle tauglich waren.

Desweiteren werden in Kapitel 5 verschiedene Methoden zur Erzeugung von sog. *Saliency Maps* (dt. Ausprägungskarte) vorgestellt. Unveränderte Bilder mit einer hohen Konfidenz werden ausgewählt, um die einzelnen Pixel hervorzuheben, welche für die Klassifikation den höchsten Einfluss hatten.

In Kapitel 6 wird das Verfahren des *Gradient Ascent* beschrieben und evaluiert. Dabei wird mithilfe einer *targeted Backpropagation* für jede Klasse ein Bild erzeugt, der die Funktion in Richtung der Zielklasse maximiert, bis die enthaltenen Merkmale eine hohe Konfidenz in der gewünschten Klasse ermöglichen.

Abschluss dieser Arbeit bildet im Kapitel 7 ein Fazit über die gefundenen Methoden, sowie ein Ausblick auf weiterführende Arbeiten.

## 2 Anforderungsanalyse und Rahmenbedingungen

### 2.1 Rahmenbedingungen des Informaticups

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

### 2.2 Eigenschaften des bereitgestellten Neuronalen Netz

33 verschiedene aufgezeichnete klassenlabels (im vergleich GTSRB datensatz 43)

1. Aus der aufgabenstellung 64x64x3
2. bilder aus dem GTSRB [quelle] datensatz
3. Gekürzte Klassen: Aus der analyse geht die Vermutung hervor, dass nur 33 Klassen unterschieden werden, keine 43 wie im orginal datensatz
4. Softmax-Ausgabefunktion
5. Interpolationsfunktion (vllt mit einem Bild in 3 Interpolationsversionen und jeweiligen Score)
6. Overfitting bei Trainingsdaten
7. unzuverlässigkeit bei nicht-Schildern (z.B. OhmLogo)

## 3 Technisches Konzept

### 3.1 Verwendete Technologien

Die Umsetzung der Implementierung erfolgt innerhalb der webbasierten, interaktiven Entwicklungsumgebung Jupyter Notebook <sup>1</sup> (in der Version 5.7.4) zusammen mit der objektorientierten höheren Programmiersprache Python <sup>2</sup> (in der Version 3.6.5).

Jupyter Notebook bietet aufgrund seiner plattformübergreifenden Einsatzmöglichkeit und Kompatibilität zu allen gängigen Webbrowsern eine hohe Flexibilität, was die Darstellung und Ausführung von Python-Code angeht. Darüber hinaus bietet Python eine hohe Verfügbarkeit von Open-Source-Repositories im Bereich Datenverarbeitung, Machine Learning und Deep Learning ???. Die Programmiersprache wurde ferner im Rahmen der StackOverflow Befragung 2017 von den befragten Softwareentwicklern zur fünftbeliebtesten Technologie des Jahres 2017 gewählt ???. Nicht zuletzt ist Python und die inbegriffenen umfangreichen Standardbibliotheken auf allen gängigen Plattformen, wie beispielsweise Linux, Apple MacOS und Microsoft Windows, kostenlos und in quell- oder binärform verfügbar ??.

Als Paketmanager wurde die frei verfügbare Anaconda Distribution in der derzeit aktuellsten Version 2018.12 gewählt, da sie eine vereinfachte Paketinstallation und -verwaltung ermöglicht. Darüber hinaus bietet Anaconda die Möglichkeit Jupyter Notebooks sowie Python und dessen verfügbare Pakete in verschiedenen Entwicklungs- und Testumgebungen isoliert voneinander zu verwalten und zu betreiben ???. Schließlich erlaubt "Anaconda Accelerate" den programmatischen Zugriff auf numerische Softwarebibliotheken zur beschleunigten Codeausführung auf Intel Prozessoren sowie NVIDIA Grafikkarten ??.

---

<sup>1</sup><https://jupyter.org/>

<sup>2</sup><https://www.python.org/>

Name	Version	Beschreibung
Keras	2.2.4	Enthält Funktionen für Deep-Learning Anwendungen [7]
Torchvision	0.2.1	Enthält Datensätze, Modellarchitekturen und gängige Bildtransaktionsoperationen für Computer-Vision Anwendungen [8]
OpenCV	3.4.2	Enthält Funktionen für echtzeit Computer-Vision Anwendungen [9]
NumPy	1.15.3	Enthält Funktionen zur effizienten Durchführung von Vektor- oder Matrizenberechnungen [10]
Requests	2.18.4	Enthält Funktionen zur Vereinfachung von HTTP Requests [11]
Pillow	5.2.0	Enthält Funktionen zum laden, modifizieren und speichern von verschiedenen Bilddateiformaten [12]
Matplotlib	2.2.3	Enthält Funktionen zum Plotten von Graphen oder Bildern [13]
SciPy	1.1.0	Enthält wissenschaftliche und technische Funktionen zur Datenverarbeitung [14]

Tabelle 3.1: Paketabhängigkeiten der implementierten Software

Zur fehlerfreien Ausführung des Codes (Saliency Map Verfahren beziehungsweise Gradient Ascent Verfahren) müssen sowohl Python 3.6.5 als auch folgende Python-Bibliotheken in der wie folgt spezifizierten Version in der zur Laufzeit verwendeten Anaconda Environment vorliegen, wie in Tabelle ?? aufgeschlüsselt.

Um die Voraussetzungen zur benötigten Python Version respektive der erforderlichen Python-Bibliotheken zu erfüllen, muss beim ersten Öffnen des Jupyter Notebooks zum Saliency Map Verfahren beziehungsweise zum Gradient Ascent Verfahren immer der Code zur Rubrik “Managing Anaconda Environment” zuerst ausgeführt werden. Andernfalls kann die korrekte Ausführung von weiteren Teilen des Codes in nachfolgenden Rubriken nicht gewährleistet werden.

## 3.2 Transferierbarkeit von Angriffen auf ein Blackbox Modell

Eine Herausforderung des Wettbewerbs ist der Umgang mit dem zu täuschenden Neuronalen Netz. Die oberflächliche Analyse der Web-Schnittstelle ermöglicht keine genauen Informationen über die verwendete Architektur oder anderen Details. Dennoch wurde bereits bestätigt, dass es selbst für "Blackbox" Modelle möglich ist, Irrbeispiele und Bilder zu erzeugen.

Papernot et al.[?] bestätigten, dass Täuschungen auf ein bekanntes Netz mit hoher Wahrscheinlichkeit auch auf fremden Modellen fehlklassifiziert werden, also, dass die Ergebnisse nicht nur ein zufälliges Ereignis aufgrund von Overfitting des spezifischen Neuronalen Netzes sind. Die Ergebnisse wurde an verschiedenen Modelltypen getestet (bspw. **SVM!** (SVM!), Deep Neural-Network (**DNN**)) und zeigten immer eine - in ihrer Ausprägung schwankende- Korrelation zwischen Fehlklassifikation auf einem fremden Modell im Vergleich zu bekannten Modellen.

Diese Ergebnisse führten zu dem Entschluss, ein eigenes Neuronales Netz zu modellieren, welches als Substitute (dt. Ersatz) dient.

## 3.3 Implementierung eines eigenen Modells zur Klassifizierung von Straßenschildern (Aphrodite)

Für die Umsetzung der verschiedenen Ansätze wird ein selbst modelliertes Neuronales Netz (**NN**) als Substitute verwendet.

Das (am meisten verwendete) Modell *Aphrodite* umfasst vier Convolutional-Layer, drei Dense-Layer und zuletzt im Ausgabelayer eine Softmax-Funktion für die 43 Klassen. Ein detaillierter Aufbau des Netzes befindet sich im Anhang.

Für das Training wurden die **GTSRB**-Trainings- und Test-Daten verwendet. Diese wurden um die richtige Auflösung zu erreichen auf 64x64 interpoliert.

Da nicht sicher war, welche Interpolationsfunktion innerhalb der Remote-Schnittstelle

Netzzusammenfassung  
als Tabelle in  
den Anhang

Link in den  
Anhang

verwendet wurde, wurde für das Training jedes Bild mehrfach interpoliert und ebenfalls mehrfach für das Training verwendet. Für die Testdaten wurde eine zufällige Interpolationsfunktion ausgesucht.

*Aphrodite* erreichte eine Genauigkeit von 96.5 % auf die Trainingsdaten. Eine Übersicht über die Trainingsparameter findet sich im Repository unter /Degeneration-Code/Training.py.

Der Name Aphrodite wurde gewählt, um dem ersten Modell (Model A) innerhalb des Projektes einen sprechenden Namen zu geben.

Sollte man  
das anders  
schreiben?  
Oder packen  
wir das file in  
den Anhang?



## 4 Degeneration

Innerhalb dieses Kapitels wird der Ansatz der *Degeneration* vorgestellt.

Die Benennung schöpft sich aus der Nähe zu genetischen Algorithmen, allerdings aus einer invertierten Perspektive: Um auf unbekannte Modelle einzugehen, wird hierbei von einem korrekt erkannten Bild *weggearbeitet*.

genauer, was das ist?

Zunächst wird das Konzept anhand von Pseudocode genauer erläutert. Anschließend wird die Implementierung des Algorithmus für die Verwendung der unbekannten Trasi-AI vorgestellt, und den Abschluss dieses Kapitels bildet eine lokale Implementierung zuzüglich einiger Verbesserungen, welche sich aufgrund der Limitierungen des Zugriffs auf die *remote-AI* nicht angeboten haben.

### 4.1 Konzept

Die Grundlegende Idee des Algorithmus bezieht sich darauf, ein Urbild  $i$  zu einem Abbild  $\hat{i}$  zu manipulieren, welches von dem unbekannten Klassifizierungsalgorithmus weiterhin korrekt erkannt wird.

Abhängig von der Stärke der Manipulation soll eine *Tiefe* gewählt werden, ab welcher der Algorithmus beendet wird. Als Beispiele der Manipulation seien insbesondere Rauschen und Glätten genannt, allerdings auch Kantenschärfung und Veränderungen der Helligkeit und anderer Metaparameter.

Mit fortschreitender Tiefe wird nahezu jedes Bild unkenntlich. Zusätzlich sollten allerdings weitere Parameter als Abbruchkriterien aufgenommen werden, konkret eine Anzahl an Gesamt-Iterationen und ein Abbruch, sollten keine weiteren Fortschritte erreicht werden.

**Pseudocode**

Folgende Parameter erwartet unsere (generische) Implementierung des Degeneration-Algorithmus:

- Einen Eingabewert  $i$
- Eine Manipulations-Funktion  $a : i \rightarrow \hat{i}$
- Eine Klassifizierungsfunktion  $p : i \rightarrow \mathbb{R}$
- Eine gewünschte Tiefe  $d$  (empfohlen, nicht notwendig)
- Eine Iterationszahl  $its$  (empfohlen, nicht notwendig)
- Ein Schwellwert  $t$ , um wie viel % die Vorhersage schlechter sein darf, als das vorhergegangene Bild

Auf einige der Punkte wird in den Anmerkungen gesondert eingegangen.

```
input :  $i, a, p, d, its, t$   
output:  $\hat{i}, \text{score}$   
 $depth \leftarrow 0, loop \leftarrow 0$  ;  
 $s \leftarrow p(i)$  ;  
 $ii \leftarrow i, is \leftarrow s$  ;  
while  $depth < d \parallel loop < its$  do  
     $ai \leftarrow a(i)$  ;  
     $as \leftarrow p(ai)$  ;  
    if  $as \geq is - t$  then  
         $is \leftarrow as$  ;  
         $ii \leftarrow ai$  ;  
         $depth++$  ;  
    end  
     $loop++$  ;  
end  
return  $ii, is$  ;
```

**Algorithm 1:** Degeneration

**Anmerkungen**

Die Manipulationsfunktionen müssen genau ein Bild der Größe  $(x,y)$  erhalten und genau ein Bild der Größe  $(x,y)$  wiedergeben, und (für die generischen Implementierungen) keine weiteren Parameter erhalten.

Zusätzlich sollte die Manipulationsfunktion zufällige Elemente erhalten. Sollte eine einfache, idempotente Glättungsfunktion den Schwellwert nicht erfüllen, so wird niemals eine größere Tiefe erreicht.

Tiefe, Schwellwert und Manipulationsfunktion müssen aufeinander abgestimmt werden. Es gibt einige Funktionen, welche eine starke Veränderung hervorrufen, und für welche eine geringe Tiefe bereits ausreicht. Auf der anderen Seite dieses Spektrums können Funktionen, welche lediglich minimale Änderungen vornehmen, schnell große Tiefen erreichen, ohne ein merklich verändertes Bild hervorzurufen zu haben.

Diese Parameter auszubalancieren obliegt dem Nutzer.

Bei der Auswahl der Parameter sollte zusätzlich überschlagen werden, wie groß die letztendliche Konfidenz ist, falls die maximale Tiefe erreicht wird.

Innerhalb der Implementierungen sollte zusätzlich eine *verbose*-Funktion eingebaut werden. Hiermit kann zum einen ein ergebnisloser Versuch frühzeitig erkannt werden, und zusätzlich, ob der Algorithmus sich festgefahren hat. Üblicherweise kann man erkennen, wenn die Manipulationsfunktion *zu stark* ist (bzw. der Schwellwert zu niedrig gewählt wurde).

Der oben genannte Algorithmus lässt sich auch für Text- oder Sprach-basierte Klassifikationen adaptieren.

Hierfür müssen lediglich andere Manipulations- und Klassifizierungs-Funktionen gewählt werden.

## 4.2 Implementierung Remote

Im Rahmen des Wettbewerbs wurde mit einer Rest-API gearbeitet, welche besondere Herausforderungen mit sich bringt:

Marker nach  
oben

- Anfragen können fehlschlagen
- zwischen Anfragen muss ein Timeout liegen
- Mehrere Nutzer, welche die API beanspruchen, blockieren sich

Zusätzlich wurde der Grundalgorithmus um die *Verbose*-Funktion und eine *History* erweitert. Mithilfe der *History* können anschließend hilfreiche Plots erstellt werden.

Diese wurden für den untenstehenden Code weggelassen.

Ebenso ist anzumerken, dass ignoriert wurde, welche Klasse zuerst erzeugt wurde. Solange irgendeine Klasse mit einer passenden Konfidenz gefunden wurde, wird dies als hinreichend erachtet. Im Normalfall bleibt es allerdings bei derselben Klasse.

Die Klassifizierungsfunktion wird innerhalb der Remote-Degeneration durch einige Hilfsfunktionen umgesetzt. Diese bereiten ein als *Bytearray* vorliegendes Bild entsprechend auf und senden es an das Trasi-Webinterface (Die Methode *Scorer.Send\_ppm\_image(i* und gibt ein JSON-Array der Scores wieder.

Die Hilfsmethode *Scorer.get\_best\_score(response)* gibt den höchsten gefunden Score wieder.

```

# Parameters :
#   An image (as 64x64x3 Uint8 Array),
#   a function to alter the image ,
#   a threshold how much the image can be worse by every step
#   The # of Iterations i want to (successfully) alter my image
#   The # of loops which i want to do max
def remoteDegenerate(image, alternationfn = _noise, decay = 0.01, iterations = 100, maxloops = 1000):
    # First: Check if the credentials are correct and the image is detected
    initialResp = Scorer.send_ppm_image(image)
    if(initialResp.status_code!=200):
        return
    totalLoops = 0 # Counts all loops
    depth = 0 # Counts successfull loops
    lastImage = image
    lastScore = Scorer.get_best_score(initialResp.text)
    # To check if we put garbage in
    print("StartConfidence:",lastScore)
    #We stop if we either reach our depth , or we exceed the maxloops
    while(depth<iterations and totalLoops<maxloops):
        totalLoops+=1
        # Alter the last image and score it
        degenerated = alternationfn(lastImage.copy())
        degeneratedResp = Scorer.send_ppm_image(degenerated)
        if (degeneratedResp.status_code==200):
            degeneratedScore= Scorer.get_best_score(degeneratedResp.text)
        else:
            print("Error, status code was: ", degeneratedResp.status_code)
        # If our score is acceptable (better than the set decay) we keep it
        if(degeneratedScore>=lastScore-decay):
            lastImage=degenerated
            lastScore=degeneratedScore
            depth+=1
        #We are working remote , we need to take a short break
        time.sleep(1.1)
    return lastScore,lastImage

```

## 4.3 Ergebnisse Remote

In diesem Abschnitt werden die mit der Degeneration erzielten Ergebnisse in Bezug auf die Trasi-Schnittstelle vorgestellt. Zunächst werden einige positive Beispiele (Erfolge) gezeigt, anschließend einige Probleme die aufgetreten sind und zuletzt noch ein kurzes Zwischenfazit gezogen.

### Positive Ergebnisse

Die zuverlässigsten Ergebnisse wurden mit einfachem Rauschen erzeugt. Die Abbildung 4.1 zeigt, dass zunächst vor allem die Pixel außerhalb des eigentlichen Schildes verändert werden - ein erwartetes Verhalten. Die farbstarken bunten Pixel sind hierbei entstanden, da Werte welche die gültige Reichweite  $[0,255]$  verlassen, wieder zyklisch zurück in den Farbbereich geholt werden. Sollte ein Farbwert durch das Rauschen einen Wert  $-2$  erreichen, wird er auf 253 gesetzt.

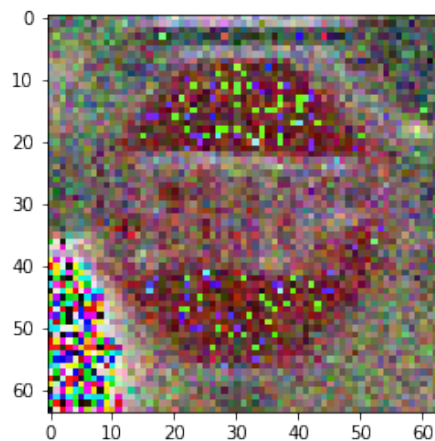


Abbildung 4.1: Rausch - Degeneration mit 600 Iterationen

Während die Abbildung 4.1 noch als Verkehrsschild zu erkennen ist, führt ein längeres ausführen der Degeneration zu einem Ergebniss wie in Abbildung 4.2. Um dieses Ergebnis zu erzielen wurden 4400 sekunden benötigt, also ca. 73 Minuten.

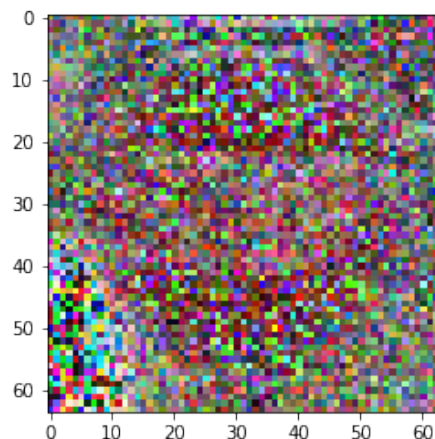


Abbildung 4.2: Rausch - Degeneration mit 4000 Iterationen

Die Plots in Abbildung 4.3 stellen den Verlauf des Algorithmus dar: Das erste Diagramm zeigt einen Verlauf der aktuellen *Tiefe* über die Iterationen dar, der zweite die jeweils produzierten Genauigkeit der jeweiligen Iteration (nicht nur die der akzeptierten), und der letzte Plot visualisiert diejenigen Iterationen, an welchen eine Änderung stattgefunden hat (weißer Strich) oder keine (schwarzer Strich). Innerhalb der Implementierung werden ebenfalls standartmäßig diese Plots erzeugt.

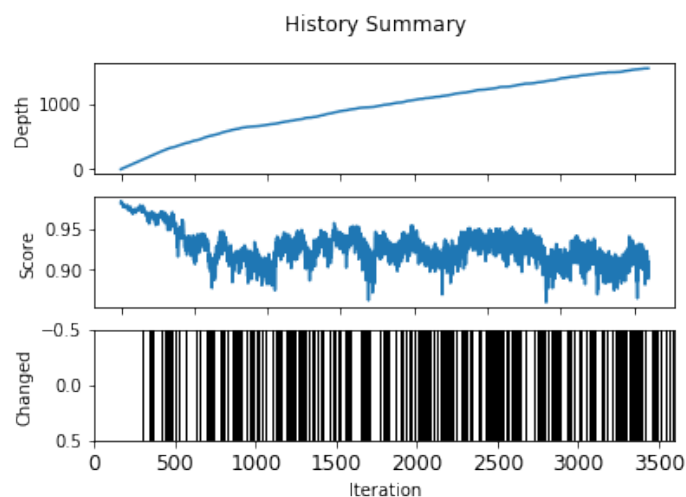


Abbildung 4.3: Plot der Rausch-Degeneration

Es wurden ebenfalls einige sehr positive Ergebnisse mit einer Mischung aus star-

kem Rauschen und Glätten erzeugt, allerdings waren diese nicht zuverlässig reproduzierbar.

### Negative Ergebnisse

Es gab zwei primäre Fehlerquellen in Bezug auf die Remote-Degeneration: Die Auswahl von Bildern, welche im GTSRB-*Training*-Set waren, sowie die Auswahl ungeeigneter Manipulationsfunktionen.

Die AI innerhalb der Schnittstelle scheint sich die Bilder aus dem Trainingsset *gemerkt* zu haben. Bereits minimale, unwichtige Änderungen des Schildes (z.B. einfügen einiger blauer Punkte im Hintergrund) führen zu einer drastischen Verschlechterung des Ergebnisses. Dieses starke *Ausschlagen* des Scores machte die Benutzung der Degeneration unbrauchbar.

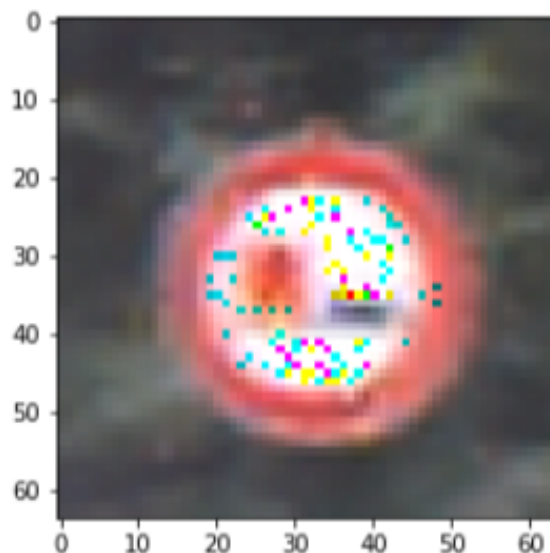


Abbildung 4.4: Rausch-Degeneration auf Trainingsbild - 36000 Iterationen

Dieses Problem hat sich herauskristallisiert, als über einen längeren Zeitraum (10 Stunden) kein Bild erzeugt wurde, welches auch nur leicht verändert wurde. Die einzigen Änderungen, welche erzielt wurden, waren innerhalb des weißen Bereiches des Überholverbotsschildes wie in Abbildung 4.4. Es wurden aber ebenfalls keine Änderungen vorgenommen außerhalb des Schildes, wo diese zu erwarten wären und bei vorhergehenden Versuchen auch zu beobachten waren (vgl. Abbildung 4.1).



Dieses Problem tritt ausschließlich (allerdings zuverlässig) bei der Verwendung von Bildern aus dem Trainingsset auf. Es tritt nicht auf sobald man Bilder aus dem Test-Set verwendet oder *GTSRB-fremde* Bilder (vorausgesetzt, sie besitzen eine akzeptable Startkonfidenz).

Innerhalb der lokalen Implementierung ist dieses Problem ebenfalls aufgetreten, konnte allerdings behoben werden, sobald man das Overfitting erkannt hatte.

### Fazit

Innerhalb dieses kurzen Zwischenfazits sollen noch einmal die Vor- und Nachteile der Degeneration zusammengefasst werden:

Vorteile	Nachteile
<b>Model-Agnostic:</b> Der Algorithmus funktioniert unabhängig und ohne Wissen über das zugrundeliegende Modell	<b>Zeitintensiv:</b> v.A. die Remote-Variante benötigt größere Zeitspannen
<b>Kontext-Unabhängig:</b> Die Herangehensweise ist nicht auf Bilderkennungen limitiert	<b>Vorwissen benötigt:</b> Der Sinn des zugrundeliegenden Modells muss bekannt sein, und ein geeignetes Startbild muss ausgewählt werden
<b>Erweiterbar:</b> Die Manipulationsfunktionen können weiter ausgebaut werden und haben noch großes Potenzial	Die Degeneration erzielt bei empfindlichen Modellen schlechter Ergebnisse - gerade <i>professionelle</i> Modelle sollten lange brauchen, um so überlistet zu werden
<b>Simpel:</b> Der Algorithmus ist einfach implementiert und erläutert, er benötigt keine höhere Mathematik oder Vorwissen zur Thematik <i>Machine Learning</i> und der Modelle/Verfahren im Speziellen	Im Remote-Umfeld kann die Degeneration als DDoS wahrgenommen werden und entsprechend frühzeitig unterbunden werden.

Caption und Label

Als besonderen Fall sind solche Modelle zu nennen, die mit jeder Anfrage *hinzulernen*:

Diese sind entweder besonders anfällig gegenüber der Degeneration, weil sie die bereits veränderten Bilder als *korrekte* klassifizieren und somit den Entstehungsprozess der Degeneration verinnerlichen, oder sie *härten* sich mit jedem Versuch gegen die neuen Änderungen und sind de facto immun gegen diesen Angriff.

Solche Modelle sind selten im Einsatz, weil zuviel Schabernack damit getrieben werden kann. Hierfür brauche ich noch eine Quelle

## 4.4 Implementierung Lokal

### Anpassungen und Verbesserungen

Innerhalb dieses Abschnittes werden zunächst die Änderungen bei der lokalen Verwendung des Algorithmus kurz behandelt, und anschließend zwei konzeptionelle Verbesserungen vorgestellt: Parallel- und Batch-Varianten des Algorithmus.

Auf weitere Code-Beispiele wird im Rahmen des Umfangs verzichtet - sie befinden sich im Anhang.

#### Anpassungen

Für die lokale Implementierung wurde zunächst ein eigenes Modell (von Grund auf) trainiert mithilfe der GTSRB-Daten. Das *Scoring* der Remote-Implementierung wird durch die *predict()*-Funktion des Models ersetzt.

Als zusätzliche Erweiterung wurde für die lokale Implementierung umgesetzt, dass sich der Nutzer für eine bestimmte Klasse entscheiden kann, auf welche die Degeneration ausgelegt ist. Es wird also zuverlässig bspw. ein Stoppschild erzeugt, und kein beliebiges Schild mit hohem Score.

Des Weiteren entfällt die Wartezeit, welche für die Schnittstelle benötigt wurde, sowie die Wartezeit. Letzteres erhöht die Geschwindigkeit des Algorithmus maßgeblich.

Eine zusätzliche, passive Verbesserung wurde erzielt, indem die Verwendung der *GPU-Acceleration* von Tensorflow eingebunden wurde. Diese beschleunigte nicht nur das Training des lokalen Models maßgeblich, sondern auch die Vorhersagen, insbesondere für die Batch-Variante, wurden um ein vielfaches ( $\approx$ Faktor 20) schneller.

Quelle? Oder Ausarbeiten?

### Fazit

Das wichtigste Fazit, welches im Umgang mit der lokalen Implementierung gezogen werden konnte, ist die nicht-verwendbarkeit der lokalen Bilder für die Schnittstelle. Während dies ursprünglich die Motivation war, schnell lokal Irrbilder zu erzeugen und Remote zu verwenden, stellte sich heraus das die lokalen Irrbilder keine guten Scores an der Schnittstelle erzielten und vice versa.

Es ist anzunehmen, das die Modelle dieselben stärken haben (Verkehrsschilder korrekt zu erkennen), allerdings unterschiedliche *Schwächen*. Die erzeugten Irrbilder scheinen im Model selbst zu fußen und sind somit hochgradig spezifisch.

Die meisten stark veränderten Bilder, welche i.A. nicht mehr vom Menschen als Verkehrsschilder erkannt werden, erzeugen bei der jeweilig erstellen AI Werte >90%, und bei der anderen Implementierung zuverlässig einen Score von  $\approx 30\%$ .

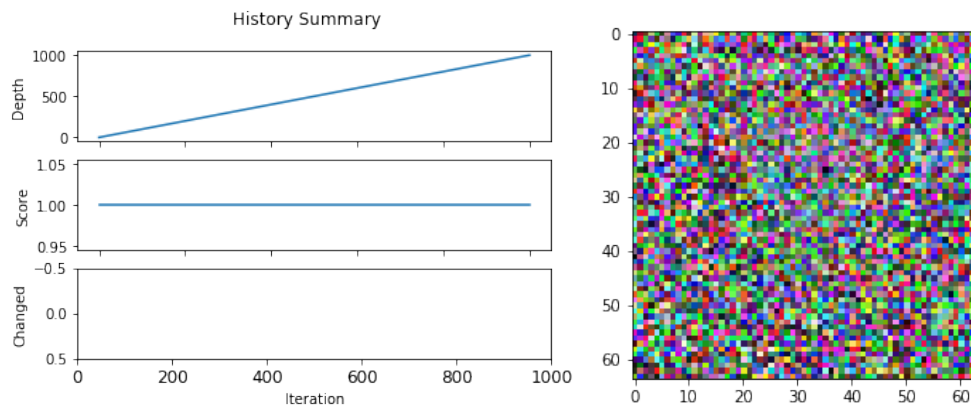
Für ein Bild, welches an sich nichts mehr mit einem Verkehrsschild zu tun hat, sind dies immernoch unwahrscheinlich hohe Werte, und die Zuverlässigkeit mit der dieser Zusammenhang auftritt, lässt einen leichten, inhaltlichen Zusammenhang der Bilder erahnen.

Beispielbild,  
Remote 90  
% und Lokal  
30% oder vice  
versa

### 4.4.1 Batch-Degeneration

Innerhalb des Batch-Variante wird anstatt eines einzelnen Bildes ein Array aus  $n$  veränderten Bildern erzeugt.

Diese werden alle bewertet und falls das beste Bild des Batches den Threshold erfüllt wird mit dem besten Bild weitergearbeitet.



Nähe zu genetischen Algorithmen herausbringen, Quelle!

Abbildung 4.5: Verlauf der Batch-Degeneration mit Batchsize=10 und Tiefe=1000

Abbildung 4.5 zeigt den deutlich besseren Verlauf der Batch-Degeneration gegenüber der unveränderten Implementierung in Abbildung 4.3. Auffallend ist die durchgängige Veränderung und die gleichbleibend hohe Konfidenz von mehr als 99.9% <sup>1</sup>.

Dieses Verhalten für Remote einzusetzen ist möglich, allerdings wurde aufgrund der Wartezeit zwischen den Anfragen davon abgesehen.

Diese Variante profitiert maßgeblich von der *GPU-Acceleration* innerhalb Tensorflows.

Selbst ohne die Verwendung des CUDA-Frameworks ist ein Tensorflow-Model auf Batch-Verarbeitung ausgelegt.

Die optimale Batchgröße zu finden ist Systemabhängig und sollte kurz getestet werden. Insgesamt benötigt die Batch-Degeneration trotzdem maßgeblich mehr Zeit: Für das Beispiel in Abbildung 4.5 wurden ca. 15 Minuten benötigt, was knapp

<sup>1</sup>Innerhalb des Plots wird es auf 1 gerundet

5 mal so lange ist wie die ursprüngliche Implementierung.

**Anmerkung:** Ein prinzipielles Problem der Batch-Degeneration liegt in der Zufälligkeit der Manipulationsfunktion. Als Beispiel sei einfaches Rauschen gewählt worden.

Ein naheliegendes Verhalten für den Algorithmus ist, von den 100 erzeugten Bildern dieses auszuwählen, welches das geringste Rauschen aufweist, und als solches am wenigsten verändert wurde. Im Normalfall weist das am wenigsten veränderte Bild den nächsten Score auf.

Glücklicherweise ist dies ein hypothetisches Problem, und in der tatsächlichen Implementierung nicht aufgetreten. Dennoch sollte es vor Allem für die Manipulationsfunktion berücksichtigt werden. Im Falle einer Manipulationsfunktion, welche konstante Elemente beinhaltet (zum Beispiel Glätten oder statische Veränderungen der Helligkeit) fördert die Batch-Degeneration den selektiven Ansatz.

#### 4.4.2 Parallel-Degeneration

Die Parallel-Variante stützt sich auf die Idee, mehrere Threads zu starten, welche gleichzeitig eine Degeneration durchführen.

Sobald ein einzelner Thread die gewünschte Tiefe erreicht hat, wird der Prozess beendet.

Die Implementierung der Parallel-Degeneration ist aufgrund mehrerer technischer Gründe gescheitert:

- **Modelgröße:** Jeder Thread braucht ein eigenes Model, welches allerdings zu groß war. Naive Benutzung eines gemeinsamen Models führen zu Race-Conditions, *geschickte* Benutzung des Models führen zu einem Verhalten wie innerhalb der Batch-Variante
- **Numpy-Arrays:** Die Bilder für die lokale Degeneration lagen als Numpy-Arrays vor, welche ein besonderes Verhalten und eine besondere Benutzung innerhalb der Parallelverarbeitung benötigen <sup>2</sup>.

---

<sup>2</sup>Dieses Problem ist sicherlich lösbar - allerdings tief verankert im Bereich der Parallelverarbeitung und somit nicht im Scope dieser Arbeit

- **Grafikkarteneinbindung:** Sobald die GPU-Acceleration innerhalb Tensorflows eingerichtet ist, werden (nahezu alle) Anfragen an die Grafikkarte weitergeleitet. Diese unterstützt das parallele Verhalten der einzelnen Threads nicht.

Die Probleme sind Hardware- oder Frameworkbezogen. Je nach Umfeld können diese somit entfallen. Race-Conditions entfallen beispielsweise, sollte man in der Cloud arbeiten.

Diese Variante war für die Remote-Implementierung nicht umsetzbar, da gleichzeitige Anfragen (mit dem selben API-Key) fehlschlagen. Ein internes Scheduling der Anfragen führt nicht zu schnelleren Ergebnissen.

#### 4.4.3 Tree-Degeneration

Diese Variante führt eine Merkstruktur ein, welche die bisherigen Ergebnisse und Schritte zwischenspeichert.

Das bisherige Verhalten entspricht dem einer Liste, bei welcher lediglich der letzte Knoten verwendet wird. Mit dem jeweils letzten Bild wird weitergearbeitet, bis entweder ein neues korrektes Bild erzeugt wurde, oder der Algorithmus endet.

Schaubild:  
Liste vs. Tree

Die Variation beinhaltet das Führen eines *Retry-Counters* welcher bei jedem Versuch von einem Knoten erhöht wird. Sollte eine gewisse Anzahl an Versuchen ergebnislos bleiben, wird der aktuelle Knoten verworfen und der Vorgänger benutzt.

Dieses Verhalten führt, je nach gewählter Maximalanzahl Kinder eines Knotens, zu einem (Binär-)Baum. Das Abbruchkriterium der Tiefe kann weiterhin beibehalten werden und entspricht der Tiefe des Baumes. Im Falle eines Versuch- oder Zeitbedingten Abbruchs wird das Bild mit der bisher größten Tiefe ausgegeben.

Die Entwicklung dieser Variante entstand durch Beobachtung, dass die Geschwindigkeit der Degeneration stark abhängig sind vom Ausgangsbild. Es kann ein Bild

erreicht werden, welches sehr *sensibel* wahrgenommen wird und deutlich schwerer Änderungen *toleriert*.

Die Batch-Degeneration ist mit dieser Variante frei kombinierbar.

## 5 Saliency Maps

Das Saliency Map Verfahren wurde erstmals von den Neurowissenschaftlern Itti et al. [?] in ihrer Studie vorgeschlagen. Die Studie beschreibt eine Methode zur Extraktion von einzigartigen Merkmalen, wie beispielsweise Farben, Farbintensitäten und Strukturen, sogenannten High-Level Features, aus Bildern, die wiederum in sogenannten Saliency Maps topografisch visualisiert werden. Diese High-Level Features sind nichts anderes als spezifische Pixel im Bild auf Mikroebene (Low-Level Features), welche die optisch ansprechendsten respektive bedeutendsten Stellen in einem Bild repräsentieren.

Um also spezifischen Bildmerkmalen eine semantische Bedeutung zuzuordnen, werden beispielsweise Farbbilder anhand des Saliency Map Verfahrens in Schwarzweißbilder umgewandelt, um die stärksten darin vorhandenen Farben zu analysieren und zu extrahieren.

### 5.1 Konzept

Bei Convolutional Neural-Network (CNN) werden Merkmale von Eingabebildern extrahiert, indem zunächst im Input-Layer Low-Level Features und mit jeder weiteren Schicht des Netzwerks immer komplexere Merkmale (High-Level Features), wie etwa Kanten, Rundungen oder Strukturen erlernt werden [?].

Diese Kenntnis um CNN und Saliency Maps machten sich Simonyan et. al. erstmalig im Kontext von Deep Learning zunutze, um die gelernten Merkmale des zugrunde liegenden CNN anhand von Saliency Maps zu visualisieren [?]. Die in der Arbeit von Simonyan et. al. erzeugten Bilder sind hierbei nicht oder nur ansatzweise für den Menschen erkennbar, wurden jedoch vom zugrunde liegenden CNN mit einer hohen Konfidenz richtig klassifiziert werden.

Aus dieser Kenntnis ergeben sich folgende Hypothesen:



- Ein Convolutional Neural Network mit beliebiger Architektur, jedoch trainiert mit demselben Datensatz ([GTSRB](#)) wie das Black Box Modell (aus der Aufgabenstellung), lässt sich ähnlich gut angreifen wie das Black Box Modell selbst.
- Saliency Maps repräsentieren die wesentlichen Merkmale, die das Convolutional Neural Network zu den Eingabebildern gelernt hat. Die erzeugten Bilder mit dem Saliency Map Verfahren werden wiederum vom [CNN](#) mit einer hohen Konfidenz richtig klassifiziert, das heißt das jeweils erzeugte Bild wird vom [CNN](#) als Verkehrszeichen erkannt und mit hoher Konfidenz richtig klassifiziert, ist jedoch für den Menschen nicht als solches erkennbar.

## 5.2 Implementierung

Als vorverarbeitenden Schritt werden zunächst alle 12.630 Bilder aus dem [GTSRB](#)-Testdatensatz, welche in 24-Bit Farbtiefe und im Portable Pixmap Image ([PPM](#)) Dateiformat vorliegen, in das Portable Network Graphic ([PNG](#)) Dateiformat konvertiert und im Dateisystem abgespeichert.

Ein eigenes [CNN](#) Modell („Aphrodite“) wird mit dem [GTSRB](#)-Datensatz trainiert.

Die vorliegenden [PNG](#)-Bilder werden anhand dem „Aphrodite“-Modell klassifiziert: Nur diejenigen Bilder, welche vom „Aphrodite“-Modell mit einer Konfidenz von 100% korrekt klassifiziert wurden (3.063/12.630) werden im Dateisystem in einem eigenständigen Verzeichnis abgespeichert.

Gemäß einer auf die Anforderungen an die Aufgabenstellung abgewandelten Variante zu [Anh \[?\]](#), erfolgt nun die Implementierung der verschiedenen Saliency Map Verfahren.

Hierzu werden zunächst die drei Basismethoden „Vanilla“ [\[?\]](#), „Guided Backpropagation“ [\[?\]](#) und „Integrated Gradient“ [\[?\]](#) implementiert. Unter Hinzufügung von Zufallsrauschen, gemäß [\[?\]](#), werden die Basismethoden verbessert, wie die Gegenüberstellung der Ergebnisse zu den eingesetzten Verfahren in Kapitel [5.3](#) verdeutlicht. Diese optimierten Varianten werden als „Smoothed Vanilla“, „Smoothed Guided Backpropagation“ und „Smoothed Integrated Gradient“ bezeichnet und implementiert.

Jedes der Saliency Map Verfahren wird auf die in Schritt 3 erzeugten Bilder angewendet. Diese Bilder werden nacheinander vom Dateisystem geladen und anschließend auf eine Zielbildgröße von 64 x 64 Pixel skaliert. Zur Extraktion und Visualisierung der gelernten Merkmale des zugrunde liegenden Modells (Aphrodite) zu jedem skalierten Eingabebild, wird das gewählte Saliency Map Verfahren auf jedes Eingabebild, unter Verwendung des trainierten „Aphrodite“-Modells, angewendet. Die damit erzeugten Bilder werden anschließend in einem nach dem verwendeten Saliency Map Verfahren bezeichneten Verzeichnis in der Größe 64 x 64 Pixel im Dateisystem abgespeichert.

Zur abschließenden Evaluierung der erzeugten Bilder am Black Box Modell, werden alle Bilder zu jedem eingesetzten Saliency Map Verfahren im Zyklus von 60 Bilder pro Minute (Übertragungslimit pro Minute an der Remote-Webschnittstelle) an das Trasi-Webinterface gesendet. Die Informationen, das heißt die vom Black Box Modell erkannte Zielklasse und Konfidenz, werden anschließend aus dem HTTP-Responsecode zu jedem übermittelten Bild in zwei verschiedenen Logdateien gespeichert: Die erste Logdatei speichert alle Ergebnisse aus dem jeweiligen HTTP-Responsecode, wohingegen die zweite Logdatei nur gefilterte Ergebnisse, das heißt Konfidenzen von mehr als 90%, zu den übermittelten Bildern enthält.

## 5.3 Ergebnisse

Mit den verschiedenen Saliency Map Verfahren wurden Graustufenbilder erzeugt, in denen die relevanten Bildmerkmale durch helle Pixeleinfärbungen gekennzeichnet sind. Die erzeugten Bilder sind hierbei vom Menschen nicht als Verkehrszeichen wahrnehmbar.

Die mit den Basismethoden „Vanilla“, „Guided Backpropagation“ und „Integrated Gradient“ erzeugt Bilder wurden vom Black Box Modell mit jeweils 45,834911% als „Baustelle“ klassifiziert. Dieses Ergebnis lässt sich möglicherweise auf die besonderen „Faltungseigenschaften“ von Convolutional Neural Networks zurückführen, dass wesentliche bildcharakterisierende Merkmale und die damit verbundene semantische Information aus den erzeugten Bildern verloren ging.

Dahingegen konnten mit den optimierten Saliency Map Verfahren („Smoothed Vanilla“, „Smoothed Guided Backpropagation“ und „Smoothed Integrated Gradi-


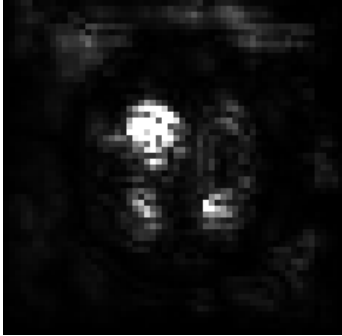
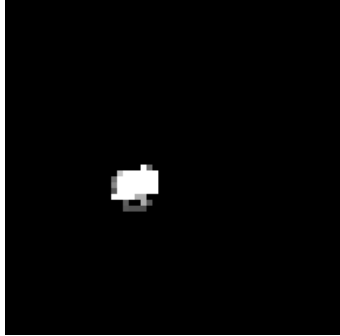
		
5.1a Ursprungsbild Höchstgeschwindigkeit (30)	5.1b Guided Backprop. Überholverbot 0.9155	5.1c Vanilla Saliency Höchstgeschwindigkeit (30) 0.9283

Tabelle 5.1: Ergebnisse von verschiedenen Verfahren am selben Bild.

ent“) Bilder erzeugt werden, die Zielkonfidenzen von mehr als 90% am Black Box Modell erreichten.

Tabelle 5.1 zeigt exemplarisch, wie aus dem Ursprungsbild (5.1a „Höchstgeschwindigkeit (30)“), unter Verwendung des „Smoothed Guided Backpropagation“ Verfahrens, ein Bild erzeugt wurde, das vom Black Box Modell mit 91,55% als „Überholverbot“ klassifiziert wurde (5.1b). Das „Smoothed Vanilla Saliency“ Verfahren erzeugte hingegen aus demselben Ursprungsbild ein Bild, das mit einer Zielkonfidenz von 92,83% vom Black Box Modell als „Höchstgeschwindigkeit (30)“ erkannt wurde (5.1c).

Tabelle 5.2 veranschaulicht weitere Beispiele für erfolgreich erzeugte Bilder, unter Verwendung der optimierten Saliency Map Verfahren. Wieder kann beobachtet werden, dass die erzeugten Bilder zwar mit einer Zielkonfidenz von mehr als 90% vom Black Box Modell klassifiziert wurden, die ursprüngliche Klasse jedoch abweicht.

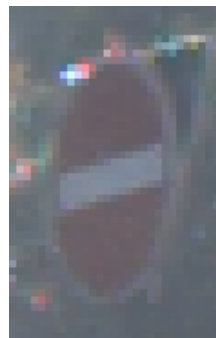
Zusammenfassend konnte hiermit gezeigt werden, dass die in Kapitel 5.1 formulierten Hypothesen zutreffen und sich Bilder – unter Verwendung eines eigens trainierten CNN Modells („Aphrodite“) sowie verschiedener Saliency Map Verfahren – erzeugen lassen, die zwar keine für den Menschen sinnvolle Bedeutung haben, jedoch beim Black Box Modell Zielkonfidenzen von mehr als 90% erreichten.



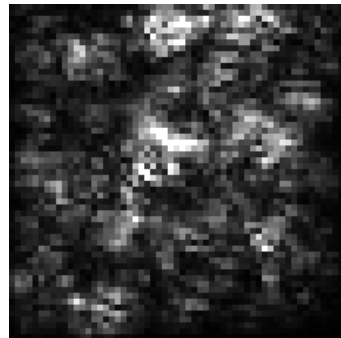
Rechts Vorbei



Guided Backprop.  
Einmalige Vorfahrt  
0.9678



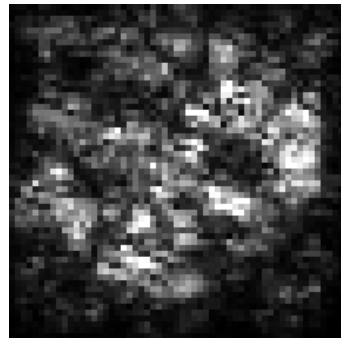
Einfahrt Verboten



Integrated Grad.  
Überholverbot  
0.9571



Kreisverkehr



Integrated Grad.  
Baustelle  
0.9999

Tabelle 5.2: Weitere Beispiele für Irrbilder mit Konfidenz  $>0.9$  inklusive entsprechendem Ursprungsbild und verwendetem Verfahren.

# 6 Gradient Ascent

## 6.1 Konzept

Mit Zugriff auf die berechneten Gradienten des Modells, können diese verwendet werden um gezielt Bilder zu verändern. Dieses Verfahren wird als *Gradient Ascent* bezeichnet, welches als Pendant zum Gradient Descent, einem Verfahren zum Training von neuronalen Netzen, verstanden werden kann. Demnach bedeutet der Ascent (dt. Aufstieg), dass die Eingabe verändert wird, um die Funktion und Neuronenaktivierung zu maximieren. Mithilfe einer *targeted Backpropagation* werden demnach die Gradienten berechnet, die zum Erreichen einer Zielausgabe (sprich Klasse) am relevantesten sind. Die Gradienten werden dann von dem ursprünglichen Bild (üblicherweise Zufallsgeneriert) mit einem Skalierungsfaktor mathematisch subtrahiert. Dabei kann man beobachten, dass relevante Pixel stärker mutiert werden und unwichtige Pixel weitgehend unverändert bleiben.

Die Methode sollte nach Aussage von Nguyen et al. [?] auf für selbst ausgewählte "echte" Bilder funktionieren. Um jedoch die Erkennbarkeit der ursprünglichen Bilder zu erhalten, sollten kleinere Skalierungsfaktoren verwendet werden. So wird ein "über das Ziel hinausschießen" verhindert und nur so gering wie nötig abgeändert, benötigt dann allerdings auch mehr Iterationsdurchläufe. Diese Implementation wurde allerdings nicht weiter verfolgt, da das Konzept auch mit Zufallsbildern bestätigt werden konnte.

## 6.2 Implementierung

Der verwendete Code zur Erzeugung der Schadbilder mithilfe des Gradient Ascent Verfahrens basiert auf einer modifizierten Version von [?]. Desweiteren wird ein angepasstes Modell basierend auf der AlexNet Architektur verwendet, mit Eingangs-

bedimensionen  $64 \times 64 \times 3$  und einer Softmax Ausgabe von den 43 Klassen des [GTSRB](#) Datensatz. Dieser Datensatz wurde für ein Training des [NN](#) verwendet. Die final verwendete Version unseres AlexNet erreichte in der Validierung eine Genauigkeit von 0.89

Es wird ein zufälliges Bild erzeugt, welches als Eingabeparameter für das trainierte NN verwendet wird. Daraus werden durch Anwendung der *categorical cross entropy* die Gradienten entsprechend für eine Zielklasse berechnet. Diese Gradienten werden nicht verwendet um die Parameter des NN zu ändern (wie es beim Training der Fall wäre), sondern um das eingegebene Bild gezielt zu modifizieren, indem die entsprechenden Pixel der aktivierten Neuronen je nach Aktivierungsstärke den Pixelwerten addiert werden. Dieser Prozess wird iterativ wiederholt, bis das veränderte Bild die gewünschte Mindestkonfidenz einer ausgewählten Klasse erreicht hat.

Die verwendete Implementation modifiziert Bilder, bis im lokalen [NN](#) eine Konfidenz von 1 erreicht wurde. Diese Bilder werden im darauffolgenden Schritt an das Blackbox Modell gesendet und klassifiziert.

Ergebnisbilder mit einer Konfidenz  $>0.9$  für irgendeine Klasse, wurden in eine gesonderte Textdatei mit Referenz auf den Speicherort, die erkannte Klasse und zugehörige Konfidenz abgespeichert.

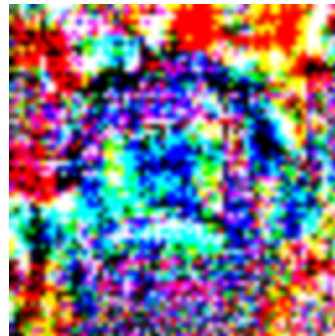
## 6.3 Ergebnisse

Als Ergebnis des Algorithmus wurden 43 Bilder respektive der 43 Klassen des letzten Layers erzeugt. Die Evaluation am zu überlistenden [NN](#) ergab Konfidenzen  $>0.9$  für 20 der 43 Bilder. Durch die Ähnlichkeit zwischen verschiedenen Klassen bzw. Straßenschildern, beispielsweise Höchstgeschwindigkeit 30 und 50, wurden nur 10 verschiedene Klassen in den 20 “erfolgreichen” Bildern erkannt. Nachfolgende Grafiken [6.1](#) zeigen verschieden Beispiele für die erzeugten Bilder mit initialen Zufallswerten. Wieder kam es zu Ergebnissen, welche eine andere Klasse lieferten, als für die Erzeugung verwendet wurde. Das für die Klasse *Links Abbiegen* erzeugte Bild wurde vom Trasi-[NN](#) beispielsweise als *Kreisverkehr* erkannt.

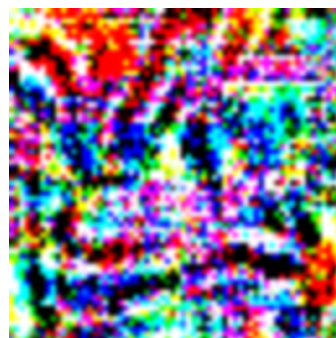
Abschließend kann bestätigt werden, dass das Gradient Ascent verfahren die erzeugung von Täuschungsbildern ermöglicht. Einschränkungen des Verfahrens



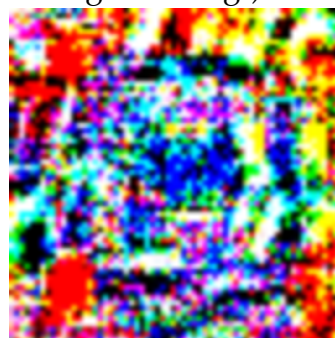
Einfahrt Verboten  
0.9999



Kreisverkehr  
0.9535  
(Ursprünglich als Links  
abbiegen erzeugt)



Rechts Vorbei  
0.9950



Kreisverkehr  
0.9868

Tabelle 6.1: Beispiele für Irrbilder mit Konfidenz  $>0.9$

belaufen sich auf die Architektur und Ähnlichkeit des [NN](#). Es steht die Annahme, dass das verfahren mit größeren Bildern bessere Ergebnisse liefert.



# 7 Fazit

Nach einer abschließenden Zusammenfassung, werden in diesem Kapitel zusätzlich die verschiedenen Ansätze verglichen und bewertet. Aus dieser Diskussion werden die Einschränkungen und Möglichkeiten für weitere Arbeiten angesprochen.

## 7.1 Zusammenfassung

Desweiteren konnten Erfolge mit der Erzeugung von Saliency Maps in den geglätteten Varianten verbucht werden. Somit konnte bestätigt werden, dass die Visualisierung der Relevanten Pixel für ein Bild mit hoher Konfidenz geeignet sind, um als "minimale Beispiele" für das NN verwendet werden können. Die entsprechenden Verfahren erzeugten Täuschungen mit Konfidenzen  $>0.9$ , allerdings lassen sich keine Aussagen über die allgemeine Verlässlichkeit und Zielgerichtetheit treffen.

Zuletzt konnte auch mit dem *Gradient Ascent* Verfahren sehr gute Ergebnisse erzielt werden. für 10 von 43 Klassen konnten Täuschungen mit hohen Konfidenzen am Remote-NN erzielt werden. Es wird vermutet dass die Ausbeute mit weiterer Optimierung vergrößert werden kann oder auch echte Bilder für die Erzeugung der Täuschungen verwendet werden können.

## 7.2 Diskussion

Die Herausforderungen des Wettbewerbs wirken sich auf die Erfolge der Verfahren aus. Es wird vermutet dass beide Verfahren *Saliency Map* und *Gradient Ascent*

bessere ergebnisse liefern Könnten, wenn das verwendete Bild größer als  $64 \times 64$  wäre. Desweiteren kann nichts über die Validierungsgenauigkeit des Trasi-NN gesagt werden, weshalb auch die nicht zielgerichteten Täuschungsbilder als gutes Ergebnis betitelt werden.

Im Vergleich der Methoden *Saliency Map* und *Gradient Ascent*, kann das letztere bevorzugt werden.

hier kommen rein vergleich der ergebnisse (reproduzierbarkeit, gezielt/random, qualität der bilder) - einschränkungen probleme unserer ansätze,  
wichtig: eigene fehler oder einschränkungen der methodik erkennen.

## 7.3 Weiterführende Arbeiten

Die Ergebnisse dieser Arbeit liefern weitere Ansätze für zukünftige Aufgaben. Zum einen können die verwendeten Ansätze individuell weiter Optimiert werden, bezüglich des selbsterstellten lokalen Neuronalem Netz und der Algorithmik bzw. deren Parameter. Desweiteren können verfahren entwickelt werden, die sich aller Methoden gezielt bedienen.