Können Computer CAPTCHAs lösen?

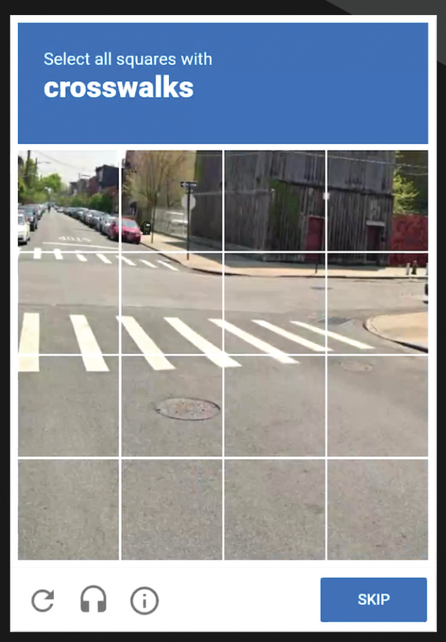
Jan Kümmerle
Betreuungsperson: Gérald Huber

Leitfrage:
Kann ein Computer ein CAPTCHA lösen, welches eigentlich genau dazu konzipiert wurde, nur von Menschen gelöst werden zu können?

Teilfragen:

- Mit welcher Objekterkennungsmethode schafft es ein Computer, die meisten CAPTCHAs vollständig richtig zu lösen, also den Test zu bestehen?
- Wie gut schneiden die Computermodelle im Vergleich mit Menschen ab?

Methode:



Beispiel-CAPTCHA mit Fussgängerstreifen [1]

Modelltraining:
Die Computermodelle wurden auf das Lösen von CAPTCHAs mit Fussgängerstreifen trainiert.

Es wurden die folgenden drei Objekterkennungsmethoden getestet:

- Histogram of Oriented Gradients
- Neuronale Netzwerke
- Segmentierungsmodelle

Diese drei Methoden wurden anschliessend ausgewertet und miteinander verglichen.

Um ein Computermodell trainieren zu können, braucht es einen Datensatz. Dieser wird in mehreren Schritten erstellt, die man unter **ELON** zusammenfassen kann:
Erlangen von Daten, **L**abeling der Daten, **O**rganisation der Daten, **N**ormalisierung der Daten.

Der Datensatz, der in dieser Arbeit verwendet wurde, besteht aus 1240 Bildern.

Von den drei getesteten Objekterkennungsmethoden, wurden jeweils verschiedene Modelle getestet, damit die Methoden so gut wie möglich optimiert waren. Es wurden dabei bereits bestehende Modelle trainiert, damit ein möglichst breites Spektrum abgedeckt werden konnte.

Auswertung:

- Perfekte Genauigkeit (*pG*):

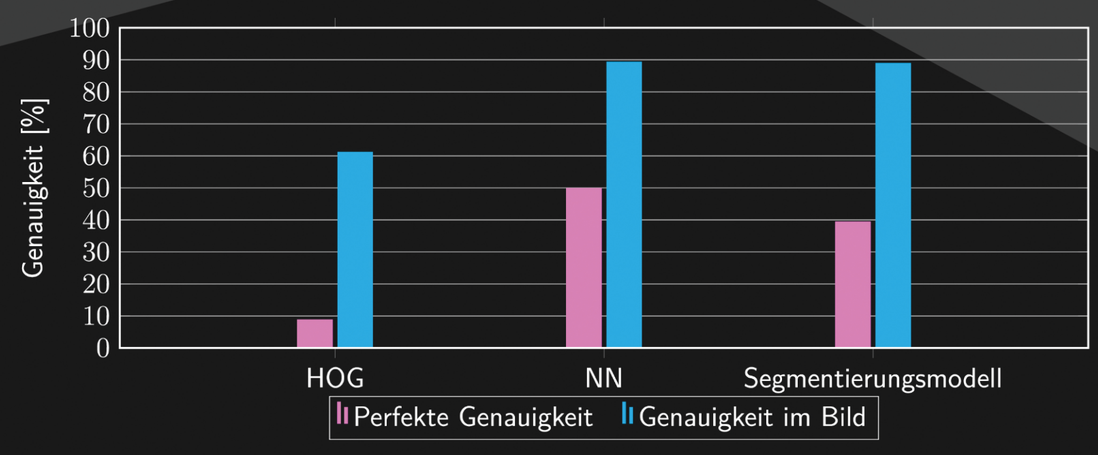
$$pG = \frac{\text{Anzahl komplett richtiger Bilder}}{\text{Gesamtanzahl Bilder im Testdatensatz}}$$

- Genauigkeit im Bild (*GiB*):

$$GiB = \frac{1}{N} \sum_{i=1}^{N} \frac{\text{Anzahl richtige Kästchen im } i\text{-ten Bild}}{\text{Gesamtanzahl Kästchen im } i\text{-ten Bild}}$$

Resultate:

- Das Histogram of Oriented Gradients (HOG) schnitt mit einer *pG* von gerade 8.87% mit Abstand am schlechtesten ab.
- Die neuronalen Netzwerke (NN) erreichten eine *pG* von 50%. Es wurde also jedes zweite CAPTCHA vollständig richtig gelöst, was sehr eindrücklich ist, da Computer diesen Test gar nicht lösen können sollten.
- Das beste Segmentierungsmodell erreichte eine respektable *pG* von 39.52%, die aber trotzdem etwas schlechter ist als die *pG* des neuronalen Netzwerkes.



Vergleich mit Menschen:

Neun Probanden lösten dieselben 124 Test-CAPTCHAs, die von den Computermodellen gelöst wurden. Die Resultate wurden gespeichert und anschliessend miteinander verglichen.

Von den Menschen wurden gerade mal 51.88% aller CAPTCHAs gleich gelöst. Es gab dabei viele CAPTCHAs, die von allen gleich gelöst wurden, aber auch viele, die von praktisch allen unterschiedlich gelöst wurden.

Die Menschen waren also nur gerade 1.88% besser als die Computer, was mehr oder weniger vernachlässigbar ist.

Zudem brauchten die Menschen durchschnittlich pro CAPTCHA knapp über fünf Sekunden, während das beste Computermodell gerade mal 0.09 Sekunden brauchte. Die Menschen sind also auch deutlich langsamer.

Fazit:

Die Ergebnisse zeigen, dass Computer mittlerweile CAPTCHAs fast so gut lösen können wie Menschen. Das beste Modell, ein neuronales Netzwerk, konnte jedes zweite CAPTCHA richtig lösen und benötigte dabei pro Bild deutlich weniger Zeit als die Menschen.

Es stellt sich nun also die Frage, wie sicher CAPTCHAs überhaupt noch sind, um Menschen von Computern zu unterscheiden. In Zukunft werden aber auf jeden Fall neue Methoden für diese Unterscheidung erfunden werden müssen, da Computermodelle wie diese nur noch besser werden.

Quelle:
[1]: https://patrickhlauke.github.io/recaptcha/

Kantonsschule Zimmerberg
Lang- und Kurzgymnasium