ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

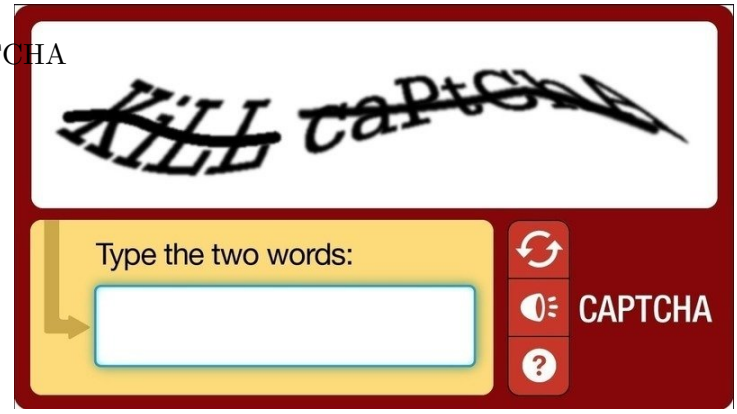
Distributed Computing

Prof. R. Wattenhofer

Generating CAPTCHAs with Deep (Reinforcement) Learning

Everyone knows them and everyone hates them: CAPTCHAs, which stands for **C**ompletely **A**utomated **P**ublic **T**uring test to tell **C**omputers and **H**umans **A**part.

Of course, CAPTCHAs are anything but perfect, and it is only a matter of time until any given CAPTCHA system can be broken, i.e., be solved by a computer. This leads to a classic arms race between the good and bad guys. Companies like Google come up with new CAPTCHA systems, and "hackers" come up wtih new ways to solve them automatically.



In this thesis we want to automatically generate new CAPTCHA systems in order to make it harder for the bad guys to come up with new solvers. One of the biggest challenges is that CAPTCHAs need to be difficult to solve for machines/algorithms, but remain easily solvable for humans. We envision, for example, using reinforcement learning techniques such as self-play and sparse human input to generate new CAPTCHAs from existing ones. We could also tackle this problem from the perspective of generative models, e.g., GANs. Another aspect of this project could be adversarial learning, i.e., applying small perturbations to the input in order to fool a classifier. Concretely, we would "adversarially" change existing CAPTCHAs in order to confuse automatic CAPTCHA solvers, while ensuring that the CAPTCHA is still easily solvable by humans.

If any of this sounds interesting to you, do not hesitate to contact us.

Requirements: Knowledge in Deep Learning, or solid background in Machine Learning. Implementation experience is an advantage. You should be able to read and understand the first 12 chapters of the "Deep Learning Book" by Goodfellow et al. (available for free online from MIT press). If you are interested in the topic but new to deep learning we expect you to complete an introductory deep learning course before applying for the thesis, such as Andrew Ng's coursera course (use the free trial!)[1] or this Udacity course[2].

- If you are interested, we can provide you with a list of interesting papers to get you started.

Interested? Please contact us for more details!

[1] `https://www.coursera.org/specializations/deep-learning`
[2] `https://classroom.udacity.com/courses/ud730`

Contacts

- Gino Brunner: `brunnegi@ethz.ch`, ETZ G63
- Oliver Richter: `richtero@ethz.ch`, ETZ G63