Using Machine Learning To Solve Text-Based CAPTCHAs

Turhan Kimbrough
Department of Computer Science
Towson University
Towson, Maryland
tkimbr1@students.towson.edu

***Abstract*—CAPTCHA is an acronym for the "Completely Automated Public Turing test to tell Computers and Humans Apart". It is a mechanism which is used to distinguish real human users from bots. CAPTCHAs come in a variety of forms, including the deciphering of obfuscated text, transcribing of audio messages, tracking mouse movement, and more. This research will focus on automating the process of deciphering text-based CAPTCHAs using machine learning techniques. Specifically, supervised learning is used to develop neural networks capable of over 99% accuracy for certain datasets. The goal of this research is to demonstrate the weaknesses associated with text-based CAPTCHA mechanisms, especially with the prevalence of machine learning tools.**

***Keywords*—machine learning, neural networks, supervised training, CAPTCHA**

I. Introduction

CAPTCHA is an acronym for the "**C**ompletely **A**utomated **P**ublic **T**uring test to tell **C**omputers and **H**umans **A**part", which is a challenge-response test used in computing services to verify that the user is a human. The premise of a CAPTCHA is to provide a test which is relatively easy for a human to solve, but difficult for bots. This is one of many mechanisms used to combat against the growing usage of malicious software automation. Due to the ubiquity of automation software, cybercriminals have been able to easily create bots to perform malicious acts. These acts include denial-of-service attacks, autonomous social media communication agents, scalping scarce merchandise, and more.

Due to the wide availability of CAPTCHA-generating software, they have become a popular mechanism to integrate into websites. In particular, text-based CAPTCHAs are often available as a low-cost and simple solution. Text-based CAPTCHAs typically consist of alphanumeric characters in an image, which has been manipulated to prevent it from being easily parsed by a machine. Users are then challenged to decipher the text in the CAPTCHA, and if the answer is correct, they can continue using the service. CAPTCHAs are typically available from content management systems (such as WordPress) or can be integrated into a website via API.

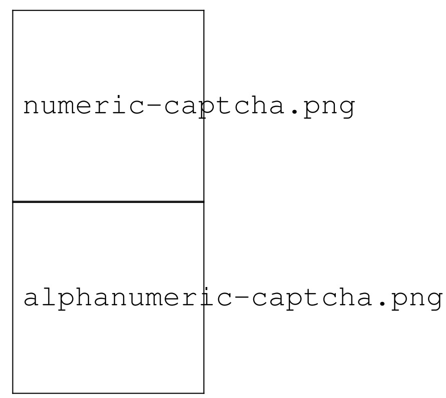

Fig. 1. Example of a text-based CAPTCHA.

While this mechanism can mitigate the majority of software bots, it is not effective against bots utilizing machine learning technology. This research paper demonstrates that a machine learning agent is capable of solving CAPTCHAs with the use of an open-source framework, several libraries, and supervised learning. The goal of this research is to highlight the vulnerabilities which are present in simple CAPTCHA mechanisms. This paper will cover background/related work, the methodology used for solving CAPTCHAs, challenges which were present, key contributions, results, and a section covering future work.

II. Background/Related Work

In this section, there will be a brief review of similar work which has been done on using machine learning to solve CAPTCHA tests.

A. Solving reCAPTCHAs With Reinforcement Learning

Researchers at [] have demonstrated the ability to solve mouse-based reCAPTCHAs using reinforcement learning. Google's reCAPTCHA mechanism is more difficult to solve compared to traditional CAPTCHAs due to its usage of mouse-tracking to determine if the user is a human. While the exact algorithm is unknown due to the closed-source nature of the reCAPTCHA technology, the researchers uses a black-box approach to solve reCAPTCHAs.

The approach models mouse movements as transitions on a 2-dimensional grid of pixels. The *Markov Decision Process* is used to generate a series of movements (up, down, left, right), which is combination of random and controlled outcomes. The mouse-control agent is then trained through reinforcement learning to generate a series of movements which mimic the behavior of humans. This methodology was able to achieve a success rate of 97.4% on a 100x100 grid and 96.7% on a 1000x1000 display.

III. Methodology

IV. Challenges

V. Key Contributions

VI. Results

VII. Future Work

References

[1] G. Eason, B. Noble, and I. N. Sneddon, "On certain integrals of Lipschitz-Hankel type involving products of Bessel functions," Phil. Trans. Roy. Soc. London, vol. A247, pp. 529–551, April 1955.

[2] J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.

[3] I. S. Jacobs and C. P. Bean, "Fine particles, thin films and exchange anisotropy," in Magnetism, vol. III, G. T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271–350.

[4] K. Elissa, "Title of paper if known," unpublished.

[5] R. Nicole, "Title of paper with only first word capitalized," J. Name Stand. Abbrev., in press.

[6] Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, "Electron spectroscopy studies on magneto-optical media and plastic substrate interface," IEEE Transl. J. Magn. Japan, vol. 2, pp. 740–741, August 1987 [Digests 9th Annual Conf. Magnetics Japan, p. 301, 1982].

[7] M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.