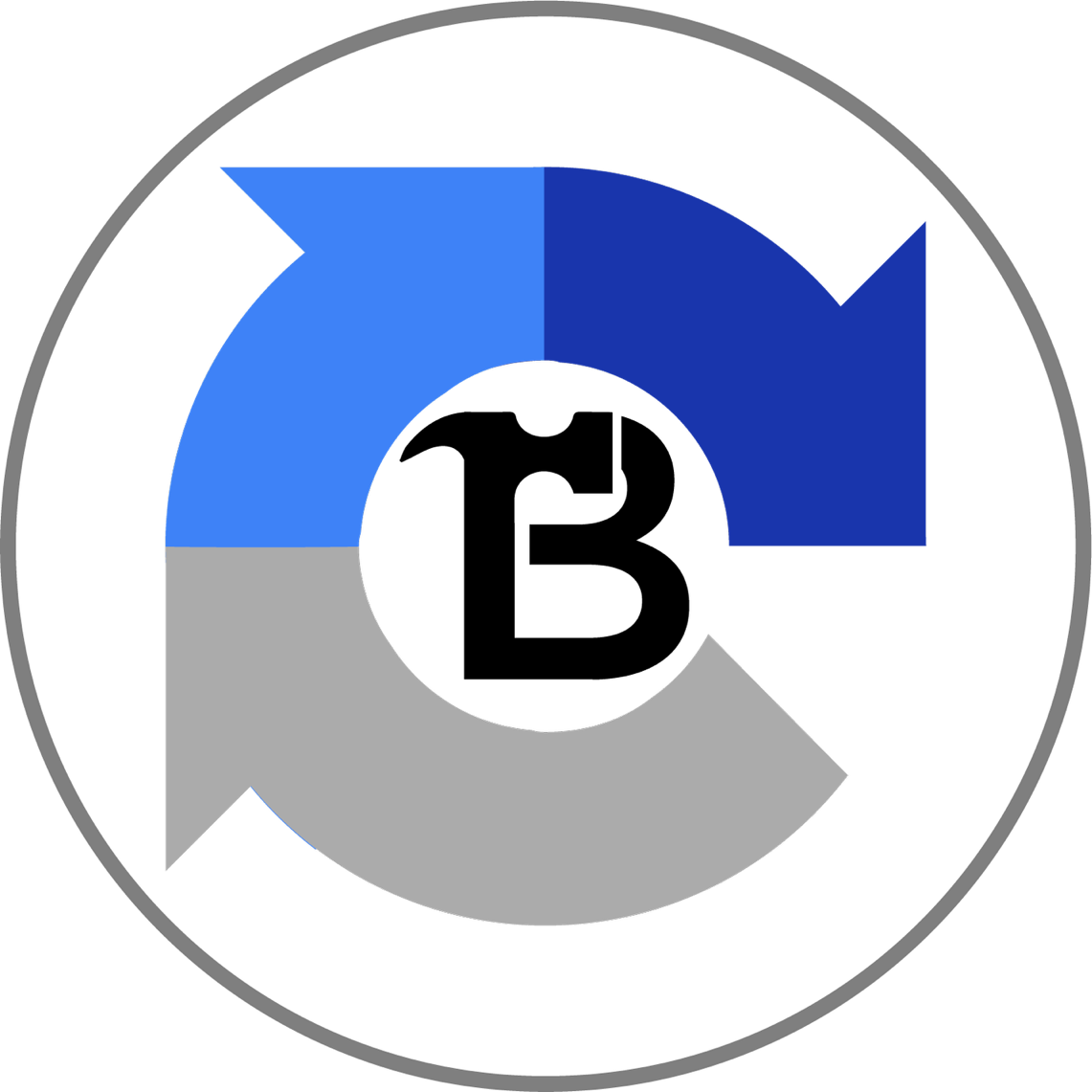
*Research Document*

Version 1.0 – 24th May 2023



*Breaking Captcha – Hardhat Enterprises 2023*

Table of Contents

[1. Introduction 2](#_Toc136074617)

[2. Objectives 2](#_Toc136074618)

[3. Methodology 3](#_Toc136074619)

[4. Research Articles 3](#_Toc136074620)

[4.1. A survey of CAPTCHA technologies to distinguish between human and computer. 3](#_Toc136074621)

[4.2. Gotta CAPTCHA'Em all: a survey of 20 Years of the human-or-computer Dilemma 4](#_Toc136074622)

[4.3. Human-artificial intelligence approaches for secure analysis in CAPTCHA codes 4](#_Toc136074623)

[4.4. A deep learning-based attack on text CAPTCHAs by using object detection techniques 4](#_Toc136074624)

[4.5. A Security Analysis of Captchas With Large Character Sets 5](#_Toc136074625)

[4.6. An End-to-End Attack on Text CAPTCHAs 5](#_Toc136074626)

[4.7. aaeCAPTCHA: The Design and Implementation of Audio Adversarial CAPTCHA 6](#_Toc136074627)

[4.8. Automatic Generation and Evaluation of Usable and Secure Audio reCAPTCHA 6](#_Toc136074628)

[4.9. Blind and Human: Exploring More Usable Audio CAPTCHA Designs 6](#_Toc136074629)

[5. Potential Applications 7](#_Toc136074630)

[6. Future Directions 7](#_Toc136074631)

[7. Conclusion 8](#_Toc136074632)

[8. References 8](#_Toc136074633)

## Introduction

The arrival of automated processes in various aspects of technology has prompted the need for improved methods of verifying human users and distinguishing them from bots that can potentially cause harm. Google reCAPTCHA has emerged as a widely adopted solution to address this challenge, but it is not immune to vulnerabilities. Breaking Captcha aims to develop an innovative platform that automates the process of solving Google reCAPTCHAs, with the dual goals of advancing research in this area and contributing to improved security measures.

## Objectives

Breaking Captcha has established the following key objectives:

a. Research Tool Development: Breaking Captcha aims to create an advanced platform that automates the solving of Google reCAPTCHAs. This platform will serve as a valuable research tool for academics, developers, and security professionals, enabling them to streamline their work whilst also allowing the testing that enables our team to aid improve security measures.

b. Security Enhancement: Breaking Captcha recognises the importance of maintaining a secure online environment. Through extensive research, the platform aims to identify vulnerabilities within reCAPTCHA mechanisms, contribute to the enhancement of security measures employed by Google and other stakeholders, and assist in the development of more robust anti-bot technologies.

c. User Convenience: In addition to its research focus, Breaking Captcha strives to develop a user-friendly interface that allows users to effortlessly solve reCAPTCHAs. This ensures a seamless browsing experience while maintaining adequate security measures.

## Methodology

The development of Breaking Captcha involves a rigorous and research-driven methodology:

a. Data Collection: A comprehensive dataset of Google reCAPTCHAs will be gathered for analysis and model training purposes. This dataset will encompass various types of reCAPTCHAs, including text-based, image-based, and audio-based challenges. The dataset will be diverse and representative to ensure accurate model training.

b. Machine Learning Models: Cutting-edge machine learning techniques, such as deep learning, convolutional neural networks (CNNs), and recurrent neural networks (RNNs), will be employed to train models capable of accurately solving reCAPTCHAs. These models will undergo iterative refinement, fine-tuning, and optimisation to improve their performance and adaptability to new challenges.

c. Research Validation: Breaking Captcha will conduct comprehensive evaluations and tests to validate the effectiveness and reliability of the developed models. These evaluations will focus on solving reCAPTCHAs accurately and efficiently while also assessing potential weaknesses in the system. The research findings will be documented and published to contribute to the wider research community.

d. Security Audits: Breaking Captcha's commitment to enhancing security involves performing rigorous security audits of the reCAPTCHA system. Vulnerabilities and potential attack vectors will be identified and reported to relevant stakeholders, to foster collaboration and improve security measures across the board.

## Research Articles

The Breaking Captcha team utilised a comprehensive range of research articles to form the foundation of our knowledge and inform our approach. These articles encompassed various topics related to automated Google reCAPTCHA solving, surveys of technology distinguishing human and machine, human-artificial intelligence approaches, object detection techniques as well as a variety of audio and text captcha research. Key articles examined the intricacies of reCAPTCHA challenges and explored the vulnerabilities and limitations of the reCAPTCHA system. Additionally, research articles on user experience provided valuable insights for Breaking Captcha's methodology. By drawing upon these research articles, the team ensured a well-informed and evidence-based approach to their work, leading to advancements in automated reCAPTCHA solving. Below are some of the many research articles available to our team during our time throughout Trimester 1, 2023.

All other research articles we possessed are located in MS Teams -> Breaking Captcha -> Files -> Research.

### A survey of CAPTCHA technologies to distinguish between human and computer.

*Xu, X., Liu, L. and Li, B., 2020.*

Abstract:

“CAPTCHA, Completely Automated Public Turing test to tell Computers and Humans Apart, is widely used as a security mechanism to classify human and computer. This security mechanism is based on the Turing Test, which has been conceived to ensure network security. Usability is another fundamental issue, which can avoid human users proceeding tedious and time-consuming operation. CAPTCHA design should consider security and usability simultaneously” (Xu et al 2020).

<https://deakin365.sharepoint.com/:b:/r/sites/HardhatEnterprises2-BreakingCAPTCHA/Shared%20Documents/Breaking%20CAPTCHA/research/A%20survey%20of%20CAPTCHA%20technologies%20to%20distinguish%20between%20human%20and%20computer.pdf?csf=1&web=1&e=sCjJWX>

### Gotta CAPTCHA'Em all: a survey of 20 Years of the human-or-computer Dilemma

*Guerar, M., Verderame, L., Migliardi, M., Palmieri, F., Merlo, A., 2021.*

Abstract:

“A recent study has found that malicious bots generated nearly a quarter of overall website traffic in 2019. These malicious bots perform activities such as price and content scraping, account creation and takeover, credit card fraud, denial of service, and so on. Thus, they represent a serious threat to all businesses in general, but are especially troublesome for e-commerce, travel, and financial services. One of the most common defence mechanisms against bots abusing online services is the introduction of Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA), so it is extremely important to understand which CAPTCHA schemes have been designed and their actual effectiveness against the ever-evolving bots” (Guerar et al 2021).

<https://deakin365.sharepoint.com/:b:/r/sites/HardhatEnterprises2-BreakingCAPTCHA/Shared%20Documents/Breaking%20CAPTCHA/research/Gotta%20CAPTCHA%20%E2%80%99Em%20All-%20A%20Survey%20of%2020%20Years%20of%20the%20Human-or-computer%20Dilemma.pdf?csf=1&web=1&e=bAidAW>

### Human-artificial intelligence approaches for secure analysis in CAPTCHA codes

*Dinh, N., Ogiela, L., 2022.*

Abstract:

“CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) has long been used to keep automated bots from misusing web services by leveraging human-artificial intelligence (HAI) interactions to distinguish whether the user is a human or a computer program. Various CAPTCHA schemes have been proposed over the years, principally to increase usability and security against emerging bots and hackers performing malicious operations. However, automated attacks have effectively cracked all common conventional schemes, and the majority of present CAPTCHA methods are also vulnerable to human-assisted relay attacks. Invisible reCAPTCHA and some approaches have not yet been cracked” (Dinh & Ogiela 2022).

<https://deakin365.sharepoint.com/:b:/r/sites/HardhatEnterprises2-BreakingCAPTCHA/Shared%20Documents/Breaking%20CAPTCHA/research/Human-artifcial%20intelligence%20approaches%20for%20secure%20analysis%20in%20CAPTCHA%20codes.pdf?csf=1&web=1&e=F3svdU>

### A deep learning-based attack on text CAPTCHAs by using object detection techniques

*Nian, J., Wang, P., Gao, G., Guo, X., 2021.*

Abstract:

“Text-based CAPTCHAs have been widely deployed by many popular websites, and many have been attacked. However, most previous cracks were based on classification algorithms that typically rely on a series of preprocessing operations or on many training samples, thus making such attacks complicated and costly. In this study, a simple, generic, fast and end-to-end attack based on advanced object detection technologies is introduced. The proposed attack combines a feature extraction module, a character location and recognition module and a coordinate matching module. The experiments show that the attack can break a wide range of real-world text CAPTCHAs deployed by the 50 most popular websites on Alexa.com and that the method achieves a high attack accuracy with only 2000 samples at an attack speed of less than 0.10 s” (Nian et al 2021).

<https://deakin365.sharepoint.com/:b:/r/sites/HardhatEnterprises2-BreakingCAPTCHA/Shared%20Documents/Breaking%20CAPTCHA/research/attack/A%20deep%20learning%E2%80%90based%20attack%20on%20text%20CAPTCHAs%20by%20using%20object%20detection%20techniques.pdf?csf=1&web=1&e=pW6d5z>

### A Security Analysis of Captchas With Large Character Sets

*Wang, P., Gao, H., Rao, Q., Luo, S., Yuan, Z., Shi, Z., 2020.*

Abstract:

“Captcha, which can prevent computer programs from attacking websites, has been the most important security technology for many years. The most popularly deployed Captcha is the text-based scheme. The vast majority of the existing text Captchas are designed with English letters and Arabic numerals. Recently, text Captchas with large character sets are being increasingly popular. From the perspective of attackers, larger character set means greater solution space and better theoretical security. However, the security of Captchas with large character sets in real world has never been studied comprehensively. In this article, we introduce a simple, fast, and effective deep learning method to attack these newly emerging Captchas. Taking 11 Chinese Captchas as representatives, we ran our experimental attack on each of them” (Wang et al 2020).

<https://deakin365.sharepoint.com/:b:/r/sites/HardhatEnterprises2-BreakingCAPTCHA/Shared%20Documents/Breaking%20CAPTCHA/research/attack/A%20Security%20Analysis%20of%20Captchas%20With%20Large%20Character%20Sets.pdf?csf=1&web=1&e=hB9Y1o>

### An End-to-End Attack on Text CAPTCHAs

*Zi, Y., Gao, H., Cheng, Z. and Liu, Y., 2019.*

Abstract:

“Text-based CAPTCHAs are the most widely used CAPTCHA scheme. Most text-based CAPTCHAs have been cracked. However, previous works have mostly relied on a series of preprocessing steps to attack text CAPTCHAs, which was complicated and inefficient. In this paper, we introduce a simple, generic, and effective end-to-end attack on text CAPTCHAs without any preprocessing. Through a convolutional neural network and an attention-based recurrent neural network, our attack broke a wide range of real-world text CAPTCHAs that are deployed by the top 50 most popular websites ranked by Alexa.com. In addition, this paper comprehensively analysed the security of most resistance mechanisms of text-based CAPTCHAs through experiments” (Zi et al 2019).

<https://deakin365.sharepoint.com/:b:/r/sites/HardhatEnterprises2-BreakingCAPTCHA/Shared%20Documents/Breaking%20CAPTCHA/research/attack/An%20End-to-End%20Attack%20on%20Text%20CAPTCHAs.pdf?csf=1&web=1&e=98xOtI>

### aaeCAPTCHA: The Design and Implementation of Audio Adversarial CAPTCHA

*Hossen, I. and Hei, X., 2022.*

Abstract:

“CAPTCHAs are designed to prevent malicious bot programs from abusing websites. Most online service providers deploy audio CAPTCHAs as an alternative to text and image CAPTCHAs for visually impaired users. However, prior research investigating the security of audio CAPTCHAs found them highly vulnerable to automated attacks using Automatic Speech Recognition (ASR) systems. To improve the robustness of audio CAPTCHAs against automated abuses, we present the design and implementation of an audio adversarial CAPTCHA (aaeCAPTCHA) system in this paper. The aaeCAPTCHA system exploits audio adversarial examples as CAPTCHAs to prevent the ASR systems from automatically solving them. Furthermore, we conducted a rigorous security evaluation of our new audio CAPTCHA design against five state-of-the-art DNN-based ASR systems and three commercial Speech-to-Text (STT) services. Our experimental evaluations demonstrate that aaeCAPTCHA is highly secure against these speech recognition technologies, even when the attacker has complete knowledge of the current attacks against audio adversarial examples” (Hossen & Hei 2022).

<https://deakin365.sharepoint.com/:b:/r/sites/HardhatEnterprises2-BreakingCAPTCHA/Shared%20Documents/Breaking%20CAPTCHA/research/defence/aaeCAPTCHA-%20The%20Design%20and%20Implementation%20of%20Audio%20Adversarial%20CAPTCHA.pdf?csf=1&web=1&e=zVBLNp>

### Automatic Generation and Evaluation of Usable and Secure Audio reCAPTCHA

*Jain, M., Tripathi, R., Bhansali, I. and Kumar, P., 2019.*

Abstract:

“CAPTCHAs are challenge-response tests to differentiate humans from automated agents, with tasks that are easy for humans but difficult for computers. The most common CAPTCHAs require humans to decipher characters from an image and are unsuitable for visually impaired people. As an alternative, audio CAPTCHA was proposed, which require deciphering spoken digits/letters. However, current audio CAPTCHAs suffer from low usability and are insecure against Automatic Speech Recognition (ASR) attacks. In this work, we propose reCAPGen, a system that uses ASR for generating secure CAPTCHAs.” (Jain et al 2019).

<https://deakin365.sharepoint.com/:b:/r/sites/HardhatEnterprises2-BreakingCAPTCHA/Shared%20Documents/Breaking%20CAPTCHA/research/defence/Automatic%20Generation%20and%20Evaluation%20of%20Usable%20and%20Secure%20%20Audio%20reCAPTCHA.pdf?csf=1&web=1&e=kXNUzg>

### Blind and Human: Exploring More Usable Audio CAPTCHA Designs

*Fanelle, V., Karimi, S., Shah, A., Subramanian, B. and Das, S., 2020*

Abstract:

“For people with visual impairments (PVIs), audio CAPTCHAs are accessible alternatives to standard visual CAPTCHAs. However, current audio CAPTCHA designs are slower to complete and less accurate than their visual counterparts. We designed and evaluated four novel audio CAPTCHAs that we hypothesised would increase accuracy and speed. To evaluate our designs along these measures, we ran a three-session, within-subjects experiment with 67 PVIs from around the world — the majority being from the U.S. and India. Thirty-three participants completed all three sessions, each separated by one week. These participants completed a total of 39 distinct audio CAPTCHA challenges across our prototype designs and the control, all presented in random order. Most importantly, all four of our new designs were significantly more accurate and faster than the control condition, and were rated as preferable over the control.” (Fanelle et al 2020).

<https://deakin365.sharepoint.com/:b:/r/sites/HardhatEnterprises2-BreakingCAPTCHA/Shared%20Documents/Breaking%20CAPTCHA/research/defence/Blind%20and%20Human-%20Exploring%20More%20Usable%20Audio%20CAPTCHA%20Designs.pdf?csf=1&web=1&e=BxUMRJ>

## Potential Applications

Breaking Captcha's research-driven approach to automated reCAPTCHA solving has several potential applications, including:

a. Research Community: Breaking Captcha's platform serves as an invaluable research tool for academics and researchers. It automates the process of solving reCAPTCHAs, allowing researchers to focus more on their core work and enhancing their productivity.

b. Security Improvement: By identifying vulnerabilities and weaknesses in the reCAPTCHA system, Breaking Captcha contributes to the enhancement of security measures. The research findings can aid in the development of more effective anti-bot technologies and fortify online platforms against automated attacks.

c. User Convenience: Breaking Captcha's user-friendly interface and automated reCAPTCHA solving provide everyday users with a seamless browsing experience. Users can navigate websites without the need to manually solve reCAPTCHAs, streamlining their online interactions and enhancing convenience.

## Future Directions

Breaking Captcha remains committed to advancing its research and development efforts to ensure automated reCAPTCHA solving becomes more robust and secure. Future directions include:

a. Collaboration with Stakeholders: Breaking Captcha will actively collaborate with stakeholders to address vulnerabilities, enhance security measures, and contribute to the development of more effective anti-bot technologies. Collaboration will facilitate knowledge exchange and promote industry-wide security improvements.

b. User Feedback Integration: The platform will prioritise user feedback and suggestions to refine the user interface, ensuring it caters to the specific needs and preferences of users. User feedback will be actively incorporated into the design and development processes to enhance usability and user experience.

c. Integration with Other Platforms: Breaking Captcha aims in future to expand its capabilities by integrating with various platforms, such as e-commerce websites, social media platforms, and online forums. This expansion will broaden the reach of automated reCAPTCHA solving, providing convenience to users across a diverse range of online interactions.

## Conclusion

Breaking Captcha's research-driven approach to automated Google reCAPTCHA solving holds great potential for advancing the field, improving security measures, and enhancing user convenience. Through its methodology, Breaking Captcha aims to contribute to the research community, collaborate with stakeholders, and create a more secure and user-friendly online environment. The future directions outlined will guide the company's ongoing efforts to push the boundaries of automated reCAPTCHA solving technology.

## References

Dinh, N. and Ogiela, L., 2022. Human-artificial intelligence approaches for secure analysis in CAPTCHA codes. EURASIP Journal on Information Security, 2022(1), p.8.

Fanelle, V., Karimi, S., Shah, A., Subramanian, B. and Das, S., 2020, August. Blind and human: Exploring more usable audio CAPTCHA designs. In Proceedings of the Sixteenth USENIX Conference on Usable Privacy and Security (pp. 111-125).

Guerar, M., Verderame, L., Migliardi, M., Palmieri, F. and Merlo, A., 2021. Gotta CAPTCHA’Em all: a survey of 20 Years of the human-or-computer Dilemma. ACM Computing Surveys (CSUR), 54(9), pp.1-33.

Hossen, I. and Hei, X., 2022, June. aaecaptcha: The design and implementation of audio adversarial captcha. In 2022 IEEE 7th European Symposium on Security and Privacy (EuroS&P) (pp. 430-447). IEEE.

Jain, M., Tripathi, R., Bhansali, I. and Kumar, P., 2019, October. Automatic generation and evaluation of usable and secure audio ReCAPTCHA. In Proceedings of the 21st International ACM SIGACCESS Conference on Computers and Accessibility (pp. 355-366).

Nian, J., Wang, P., Gao, H. and Guo, X., 2022. A deep learning‐based attack on text CAPTCHAs by using object detection techniques. IET Information Security, 16(2), pp.97-110.

Wang, P., Gao, H., Rao, Q., Luo, S., Yuan, Z. and Shi, Z., 2020. A security analysis of captchas with large character sets. IEEE Transactions on Dependable and Secure Computing, 18(6), pp.2953-2968.

Xu, X., Liu, L. and Li, B., 2020. A survey of CAPTCHA technologies to distinguish between human and computer. Neurocomputing, 408, pp.292-307.

Zi, Y., Gao, H., Cheng, Z. and Liu, Y., 2019. An end-to-end attack on text captchas. IEEE Transactions on Information Forensics and Security, 15, pp.753-766.