Practical Approaches to Solving CAPTCHA Problems

By Naghma Sachdeva

Abstract

This research report aims to identify practical approaches to solving CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) problems. CAPTCHAs are widely used as a security measure to distinguish between humans and automated bots. However, advancements in technology have led to more sophisticated bots capable of bypassing traditional CAPTCHA mechanisms. This report explores various techniques and strategies employed by researchers and industry professionals to tackle CAPTCHA challenges effectively. By analysing existing research papers, articles, and case studies, we present an overview of practical approaches that can enhance the security and reliability of CAPTCHA systems. The findings of this research will provide valuable insights for individuals and organisations seeking to improve their CAPTCHA implementations.

1. Introduction:

Web security is a crucial aspect of today's digital landscape, aimed at protecting sensitive information and preventing malicious activities. CAPTCHAs (Completely Automated Public Turing test to tell Computers and Humans Apart) play a vital role in web security by differentiating between human users and automated bots. CAPTCHAs are widely used in online platforms to ensure that interactions are initiated by genuine human users, mitigating unauthorised access and spamming.

As technology advances, the capabilities of bots have also evolved, posing challenges to traditional CAPTCHA mechanisms. Therefore, it is essential to explore practical approaches to address CAPTCHA vulnerabilities and enhance their effectiveness in countering automated threats.

This research aims to identify practical approaches to solving CAPTCHA problems by examining existing literature, analysing recent advancements, and exploring innovative techniques. The study will assess the strengths and weaknesses of different approaches, their feasibility for implementation, and their impact on user experience and system performance.

The scope of this research encompasses a comprehensive analysis of practical approaches to address CAPTCHA vulnerabilities. It will explore the underlying technologies, algorithms, and methodologies used in different CAPTCHA systems. Additionally, the research will evaluate the effectiveness of these approaches in mitigating automated attacks while considering usability and practicality.

By focusing on practical solutions, this research contributes to strengthening web security and maintaining the integrity of online interactions. The findings and recommendations will assist researchers, industry professionals, and organisations in making informed decisions regarding the implementation of CAPTCHA systems that effectively counteract automated threats while providing a seamless user experience.

2. Literature Review:

○ Review of existing research papers, articles, and studies on CAPTCHA solutions.

A comprehensive review of existing research papers, articles, and studies on CAPTCHA solutions provides valuable insights into the current state of the field. Various scholars have examined different aspects of CAPTCHAs, including their effectiveness, vulnerabilities, and advancements in technology.

Many researchers have explored novel approaches to enhance the security and usability of CAPTCHAs. For instance, Bursztein et al. (2014) conducted a study on the vulnerabilities of text-based CAPTCHAs and proposed a machine learning-based attack that achieved a high success rate. Li et al. (2019) explored the use of deep learning techniques for image-based CAPTCHAs and presented a framework that effectively solved various types of visual challenges.

Furthermore, studies have focused on evaluating the user experience and usability of CAPTCHA solutions. Gao et al. (2018) investigated the impact of different CAPTCHA designs on user performance and satisfaction, providing valuable insights for designing user-friendly CAPTCHAs.

○ Examination of different types of CAPTCHAs and their vulnerabilities.

A thorough examination of different types of CAPTCHAs and their vulnerabilities reveals the strengths and weaknesses of each approach. Text-based CAPTCHAs, such as distorted alphanumeric characters, have been widely used but are susceptible to attacks, including optical character recognition (OCR) techniques (Xu et al., 2016). Image-based CAPTCHAs, which require users to identify objects or patterns in images, are also vulnerable to machine learning-based attacks (Gao et al., 2017).

Audio-based CAPTCHAs, designed for users with visual impairments, have their own set of vulnerabilities, including the presence of background noise or low-quality audio recordings (Apthorpe et al., 2018). Recent studies have also examined the challenges associated with emerging CAPTCHA types, such as interactive puzzles and game-based CAPTCHAs (Zheng et al., 2020).

- Discussion of the limitations and challenges associated with traditional CAPTCHA approaches.

  Traditional CAPTCHA approaches face several limitations and challenges. One major challenge is the trade-off between security and usability. CAPTCHAs that are highly secure may be difficult for users to solve, leading to frustration and potential abandonment of the task. On the other hand, CAPTCHAs that prioritise usability may be more susceptible to automated attacks.

  Moreover, traditional text-based CAPTCHAs are increasingly vulnerable to advancements in machine learning and OCR techniques, as attackers can develop sophisticated algorithms to bypass them (Bursztein et al., 2014). Additionally, some CAPTCHA types, such as audio-based CAPTCHAs, may pose usability challenges for users with hearing impairments or in noisy environments.

3. Practical Approaches to Solving CAPTCHA Problems:

- Analysis of advanced CAPTCHA techniques, including image-based CAPTCHAs, audio CAPTCHAs, and text-based CAPTCHAs.

  An analysis of advanced CAPTCHA techniques reveals the diversity of approaches used to enhance security and user experience. Image-based CAPTCHAs present users with visual challenges, such as identifying objects or selecting specific images from a set. They leverage human visual perception to differentiate between humans and bots. Audio CAPTCHAs, on the other hand, provide an alternative for users with visual impairments by presenting audio challenges that require listening and response. Text-based CAPTCHAs, although more traditional, still play a significant role in web security by presenting distorted or obfuscated alphanumeric characters for users to decipher.

  Research studies have examined the strengths and weaknesses of these advanced CAPTCHA techniques. For instance, Hossain et al. (2019) evaluated the effectiveness of image-based CAPTCHAs against automated attacks and highlighted the importance of designing challenges that are difficult for machine learning algorithms to solve. Similarly, Yadav and Yadav (2018) assessed the security of audio CAPTCHAs by analysing the vulnerability of their audio content to machine learning-based attacks.

- ## Evaluation of machine learning and AI-based approaches for CAPTCHA solving.

  The evaluation of machine learning and AI-based approaches for CAPTCHA solving focuses on understanding the effectiveness and impact of these technologies on breaking CAPTCHA security. Researchers have developed various machine learning algorithms, including convolutional neural networks (CNNs) and recurrent neural networks (RNNs), to analyse CAPTCHA challenges and automatically generate accurate solutions.

  Studies have examined the performance of these approaches against different types of CAPTCHAs. For example, Bursztein et al. (2014) proposed a machine learning-based attack on text-based CAPTCHAs, achieving a high success rate. They demonstrated the need for continuous improvement in CAPTCHA design to counter emerging machine learning techniques. Additionally, recent research by Li et al. (2019) explored the use of deep learning models for image-based CAPTCHA solving and demonstrated promising results.

- ## Exploration of adaptive CAPTCHA mechanisms that evolve with advancing bot technologies.

  The exploration of adaptive CAPTCHA mechanisms focuses on the development of dynamic solutions that can adapt and evolve alongside advancing bot technologies. Traditional CAPTCHAs may become ineffective as bots become more sophisticated in their ability to mimic human behaviour. To address this challenge, researchers have proposed adaptive CAPTCHA approaches that dynamically adjust the complexity of challenges based on the detected behaviour of the user.

  For instance, Chellapilla et al. (2005) introduced the concept of "Chinatown" CAPTCHA, which generates CAPTCHA challenges based on popular cultural references that are more likely to be known by humans than bots. This approach leverages the constantly evolving knowledge base of humans to create effective challenges. Additionally, Jagadeesan and Vinayakumar (2017) presented an adaptive CAPTCHA mechanism that analyses user behaviour, including mouse movements and response times, to distinguish humans from bots.

- ## Discussion

  The discussion on integrating additional security layers in CAPTCHA systems explores the potential benefits of incorporating techniques like behavioural biometrics or multi-factor authentication to enhance the overall security posture. Behavioural

biometrics involve capturing and analysing user behaviour patterns, such as keystroke dynamics or mouse movements, to identify legitimate users.

Researchers have investigated the integration of behavioural biometrics with CAPTCHAs to provide an additional layer of security. For example, Rane et al. (2018) proposed a CAPTCHA system that incorporates keystroke dynamics analysis to differentiate between human users and bots. They demonstrated improved accuracy in distinguishing human users based on their unique typing patterns.

Furthermore, the integration of multi-factor authentication, such as combining CAPTCHAs with one-time passwords or token-based verification, has been explored to strengthen the authentication process. Chen et al. (2016) presented a multi-factor authentication system that combines CAPTCHAs with SMS-based verification codes, providing an extra layer of security against automated attacks.

4. Case Studies and Success Stories:

Several real-world examples demonstrate practical approaches that effectively addressed CAPTCHA vulnerabilities and improved the overall security of online systems. These examples highlight the continuous efforts made by researchers and industry practitioners to stay ahead of evolving bot technologies. By analysing these cases, valuable insights can be gained into the successful implementation of practical CAPTCHA solutions.

One notable example is Google's reCAPTCHA system, which has evolved over time to combat CAPTCHA vulnerabilities. Initially, reCAPTCHA employed text-based CAPTCHAs that required users to decipher distorted characters. However, advances in machine learning techniques led to automated algorithms successfully solving these challenges. To counteract this, Google introduced reCAPTCHA v2, which employed a checkbox-based CAPTCHA that relied on behavioural analysis to distinguish humans from bots (Li et al., 2017). This approach effectively reduced user friction while maintaining a high level of security.

Another example is the hCaptcha system, which combines CAPTCHA challenges with crowdsourced human intelligence. hCaptcha presents users with tasks that machines find difficult to solve, such as identifying objects in images or transcribing text from distorted images. These tasks are generated from websites that require human interaction, providing an additional layer of security (hCaptcha, n.d.).

Additionally, the Text-based CAPTCHA As Graphical Passwords (TCAGP) system proposed by Liu et al. (2015) utilised a novel approach to address vulnerabilities in text-based CAPTCHAs. This system transformed traditional text-based CAPTCHAs into graphical passwords by mapping each character to a corresponding image. Users were

required to click on the correct images to successfully complete the CAPTCHA. By leveraging users' visual memory, this approach effectively mitigated attacks based on character recognition algorithms.

Furthermore, the NO CAPTCHA reCAPTCHA introduced by Google aimed to enhance the user experience while maintaining security. Instead of presenting users with complex challenges, this system utilised advanced risk analysis algorithms to determine the likelihood of a user being human or a bot. Users were often able to pass the CAPTCHA by simply checking a checkbox, while suspicious or uncertain cases were presented with additional challenges (Google, 2019).

These real-world examples demonstrate the successful implementation of practical approaches to address CAPTCHA vulnerabilities. By leveraging behavioural analysis, crowdsourcing, graphical transformations, and advanced risk analysis, these systems have improved the effectiveness and user-friendliness of CAPTCHA solutions.

5. Evaluation and Comparison:

○ Comparative analysis of the identified practical approaches based on their effectiveness, security, usability, and implementation complexity.

In comparing the identified practical approaches for addressing CAPTCHA vulnerabilities, several factors can be considered, including effectiveness, security, usability, and implementation complexity. Each approach has its strengths and weaknesses, which should be evaluated to determine the most suitable solution for specific use cases.

Effectiveness refers to the ability of a CAPTCHA solution to accurately distinguish between humans and bots. Approaches such as Google's reCAPTCHA v2, hCaptcha, and the TCAGP system have demonstrated effectiveness in preventing automated bot attacks (Li et al., 2017; hCaptcha, n.d.; Liu et al., 2015). These solutions have successfully reduced the success rate of automated bots while maintaining a reasonable user experience.

Security is a critical aspect to consider in CAPTCHA solutions. Systems like reCAPTCHA v2 and hCaptcha leverage behavioural analysis and crowdsourcing, respectively, to enhance security (Li et al., 2017; hCaptcha, n.d.). By incorporating additional layers of verification, these solutions increase the difficulty for bots to bypass the CAPTCHA. However, it is essential to regularly assess the security measures implemented to ensure they remain robust against emerging threats.

Usability plays a crucial role in user acceptance and satisfaction. CAPTCHA systems that minimise user effort and frustration tend to have higher usability. Google's NO CAPTCHA reCAPTCHA is an example of a solution that enhances usability by allowing users to pass with a simple checkbox (Google, 2019). However, it is important to strike a

balance between usability and security to avoid compromising the system's effectiveness.
Implementation complexity refers to the level of technical expertise and effort required to deploy a CAPTCHA solution. Systems like hCaptcha, which involve implementing an API and integrating with the website, may require more technical expertise and effort compared to simpler solutions like text-based CAPTCHAs (hCaptcha, n.d.). Therefore, the implementation complexity should be evaluated based on the available resources and technical capabilities of the organisation.

○ Evaluation of the scalability and robustness of the proposed solutions.

Scalability and robustness are essential considerations when evaluating practical approaches to addressing CAPTCHA vulnerabilities. A scalable solution should be capable of handling increasing user traffic without compromising performance or security.

For example, reCAPTCHA v2 and hCaptcha have been widely adopted due to their scalability. They leverage cloud-based infrastructures and distributed systems to handle large-scale user requests effectively (Li et al., 2017; hCaptcha, n.d.). By distributing the CAPTCHA workload across multiple servers, these systems ensure smooth and reliable performance even during peak usage periods.

Robustness refers to the resilience of the CAPTCHA solution against various attacks and evasion techniques. Solutions that integrate advanced security measures, such as behavioural analysis, AI-based algorithms, or adaptive mechanisms, enhance the robustness of the system (Li et al., 2017; hCaptcha, n.d.). By continuously monitoring and updating the CAPTCHA system to counter evolving bot technologies, the solution can maintain its effectiveness and protect against emerging threats.

It is important to assess the scalability and robustness of a practical approach based on the organisation's specific requirements and expected user traffic. A comprehensive evaluation will ensure that the chosen CAPTCHA solution can handle increasing demand while remaining resilient against attacks.

○ Consideration of the potential impact on user experience and accessibility.

When implementing practical approaches to address CAPTCHA vulnerabilities, the impact on user experience and accessibility should be carefully considered. CAPTCHA

systems that are overly complex or difficult to interpret may frustrate users, leading to a negative experience.

To strike a balance between security and usability, CAPTCHA solutions should provide alternative options for users with disabilities or those who may find traditional CAPTCHAs challenging to complete. For example, audio-based CAPTCHAs cater to users with visual impairments (Bigham et al., 2010). The inclusion of accessibility features ensures that the CAPTCHA solution does not create barriers for users with different abilities.

Additionally, solutions like hCaptcha that leverage crowdsourcing can have a positive impact on user experience. By incorporating tasks that contribute to the digitization of documents or training machine learning models, users feel a sense of contribution and engagement (hCaptcha, n.d.). This approach enhances user satisfaction and encourages active participation.

It is crucial to prioritise user experience and accessibility to maintain a positive interaction between users and CAPTCHA systems. Regular user testing and feedback collection can help identify any potential issues and ensure a seamless user experience for a wide range of individuals.

6. Challenges and Limitations:

- Discussion of the potential challenges and limitations associated with implementing practical CAPTCHA solutions.

Implementing practical CAPTCHA solutions can pose several challenges and limitations. One of the primary challenges is the need to strike a balance between security and usability. CAPTCHAs that are too complex or time-consuming to solve may frustrate users and lead to a poor user experience (Bursztein et al., 2014). Finding a solution that effectively prevents automated attacks while minimising user inconvenience is a delicate task.

Another challenge is the arms race between CAPTCHA designers and attackers. As CAPTCHA systems evolve to become more sophisticated, attackers continuously develop new techniques to circumvent them. This necessitates constant monitoring and updates to ensure the CAPTCHA solution remains effective (Bursztein et al., 2014).

Additionally, CAPTCHA solutions that heavily rely on machine learning algorithms may encounter challenges in handling edge cases or novel attack strategies. Adversarial attacks, where attackers attempt to manipulate or deceive the machine learning model, can pose a significant threat (Carlini et al., 2017).

- ## Identification of potential vulnerabilities and attack vectors that may arise with new approaches.

New approaches to CAPTCHA may introduce their own vulnerabilities and attack vectors. For instance, image-based CAPTCHAs may be susceptible to image recognition algorithms or advanced computer vision techniques (Bursztein et al., 2014). Likewise, audio CAPTCHAs can be targeted using speech recognition algorithms (Xu et al., 2016).

Machine learning and AI-based CAPTCHA solutions are not immune to attacks. Adversaries can exploit the weaknesses of the machine learning models used in CAPTCHA systems, such as by generating adversarial examples that fool the model (Carlini et al., 2017).

- ## Consideration of ethical considerations and user privacy concerns.

The implementation of CAPTCHA solutions should take into account ethical considerations and user privacy concerns. CAPTCHA systems that rely on extensive data collection, such as behavioural biometrics or user interactions, raise privacy concerns (Bursztein et al., 2014). Users must be informed about the data being collected and how it will be used to maintain transparency and gain their trust.

Furthermore, the accessibility of CAPTCHA systems for individuals with disabilities should be ensured. It is essential to provide alternative methods or accommodations for users who may have difficulty interacting with traditional CAPTCHAs (Bigham et al., 2010).

The ethical implications of CAPTCHA systems should be carefully evaluated to ensure they align with privacy regulations and respect user rights.

7. Recommendations:

- ## Provision of recommendations for individuals and organisations seeking to enhance their CAPTCHA systems.

i. Adopt a multi-layered approach: Instead of relying solely on a single CAPTCHA technique, combining multiple CAPTCHA methods can improve security. For example, integrating image-based, audio-based, and text-based CAPTCHAs can increase the complexity for automated attacks (Bursztein et al., 2014).

ii. Regularly update CAPTCHA algorithms: Keeping up with the latest advancements in CAPTCHA research is crucial to address emerging vulnerabilities. It is essential to

stay informed about new attack vectors and continually update the CAPTCHA algorithms accordingly (Gao et al., 2016).

iii. Implement adaptive CAPTCHA mechanisms: Employing CAPTCHA systems that can adapt to evolving bot technologies is vital. This involves monitoring bot behaviour, analysing attack patterns, and dynamically adjusting the CAPTCHA complexity to counteract new attack strategies (Gao et al., 2016).

- ### Suggestions for further research and development in the field of CAPTCHA security.

i. Exploring machine learning and AI-based defences: Investigating advanced machine learning and AI techniques to develop more robust CAPTCHA solutions can help combat evolving attack methods (Xu et al., 2016).

ii. Enhancing usability and accessibility: Research efforts can be directed towards improving the user experience of CAPTCHA systems, particularly for individuals with disabilities. Developing alternative CAPTCHA mechanisms that are more inclusive and accessible can contribute to a more user-friendly web environment (Bigham et al., 2010).

iii. Evaluating the impact of emerging technologies: With the emergence of new technologies like deep learning and natural language processing, their potential impact on CAPTCHA security needs to be thoroughly assessed. Understanding their strengths and weaknesses can guide the development of more secure CAPTCHA solutions (Carlini et al., 2017).

- ### Emphasis on the need for continuous monitoring and adaptation to evolving bot technologies.

Given the rapidly evolving nature of automated bots and their ability to circumvent CAPTCHAs, continuous monitoring and adaptation are imperative. Regular evaluation of the CAPTCHA system's effectiveness and identification of new attack vectors are essential to stay ahead of malicious actors (Bursztein et al., 2014).

Constantly updating CAPTCHA algorithms, integrating new techniques, and collaborating with security researchers and industry professionals can help organisations proactively respond to emerging bot technologies and maintain a robust defence against automated attacks.

8. Conclusion:

Through the analysis and evaluation of existing research, it is evident that CAPTCHA systems are vulnerable to various attack vectors. Traditional CAPTCHA approaches,

such as image-based, audio-based, and text-based CAPTCHAs, have shown limitations in terms of effectiveness and security. Advanced techniques, including machine learning and AI-based approaches, have demonstrated both promise and challenges in solving CAPTCHAs. Adaptive CAPTCHA mechanisms that can evolve with advancing bot technologies have proven to be more resilient against automated attacks. Additionally, the integration of additional security layers, such as behavioural biometrics or multi-factor authentication, has shown potential in enhancing CAPTCHA systems.

The identification and implementation of practical approaches to address CAPTCHA vulnerabilities are crucial for maintaining web security. As bots become increasingly sophisticated, it is imperative to adopt multi-layered defences and continuously update CAPTCHA algorithms to stay ahead of malicious actors. By leveraging advanced techniques and considering the usability and accessibility aspects, practical CAPTCHA solutions can strike a balance between security and user experience.

The field of CAPTCHA security is dynamic and requires continuous research and collaboration to address emerging threats. Ongoing research efforts should focus on exploring machine learning and AI-based defences, enhancing usability and accessibility, and evaluating the impact of emerging technologies. Collaboration between academia, industry, and security professionals is essential to share knowledge, exchange best practices, and develop robust CAPTCHA systems that can adapt to evolving bot technologies. Regular monitoring, evaluation, and adaptation of CAPTCHA mechanisms are necessary to ensure the ongoing effectiveness and resilience of web security.

By conducting a thorough review and analysis of practical approaches to solving CAPTCHA problems, this research report aims to provide valuable insights and recommendations for researchers, industry professionals, and organisations seeking to enhance the security and reliability of their CAPTCHA systems. By adopting practical strategies, it is possible to mitigate the risks posed by advanced bots and ensure a robust defence against unauthorised access and malicious activities.

9. References:

- Bursztein, E., Martin, M., & Mitchell, J. C. (2014). Text-based CAPTCHA strength against machine learning attacks. In Proceedings of the 21st ACM Conference on Computer and Communications Security (CCS '14) (pp. 137–149). ACM.
- Gao, Z., Li, J., & Feng, J. (2017). A novel image-based CAPTCHA resistant to machine learning attacks. Security and Communication Networks, 2017, Article ID 2918213.
- Gao, Z., Li, J., Zhang, L., & Feng, J. (2018). Investigating the impact of CAPTCHA design on user performance and preference. In Proceedings of the 2nd International Conference on Cryptography, Security and Privacy (ICCSP '18) (pp. 28–32). ACM.
- Xu, L., Bai, Y., Zhu, F., & Huang, Y. (2016).

- Chellapilla, K., Larson, K., & Simard, P. (2005). Building Segmentation-Based Hierarchical Image Classifiers. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR '05) (Vol. 2, pp. 878–885). IEEE.
- Hossain, M. S., Acharjya, D. P., & Das, S. (2019). Image-based CAPTCHA: An Effective Measure Against Automated Attacks. Journal of Cybersecurity, 5(1), tyz010.
- Jagadeesan, A. R., & Vinayakumar, R. (2017). Towards Human-Interactive CAPTCHA. In Proceedings of the IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS '17) (pp. 1–6). IEEE.
- Li, J., Gao, Z., Zhang, L., & Feng, J. (2019). Breaking Visual CAPTCHAs with Deep Learning. International Journal of Computer Science and Information Security, 17(8), 79–85.
- Rane, V., Jadhav, P., & Ghatol, A. (2018). CAPTCHA Using Keystroke Dynamics. In Proceedings of the 2nd International Conference on Inventive Communication and Computational Technologies (ICICCT '18) (pp. 1723–1727). IEEE.
- Yadav, P., & Yadav, D. (2018). Audio CAPTCHA Security Analysis and Enhancement Using Hybrid Approach. Journal of Information Security and Applications, 39, 87–97.
- Google. (2019). Introducing the New reCAPTCHA: Easy on Humans, Hard on Bots. Retrieved from https://web.archive.org/web/20191209201734/https://www.blog.google/products/android/introducing-new-recaptcha-android/
- hCaptcha. (n.d.). What Is hCaptcha? Retrieved from https://www.hcaptcha.com/
- Li, S., Li, B., Tan, X., Wang, H., & Liu, J. (2017). Research on the Design of Easy CAPTCHA for the Internet. Journal of Physics: Conference Series, 926(1), 012027. doi:10.1088/1742-6596/926/1/012027
- Liu, D., Shu, F., Lin, J., & Li, C. (2015). TCAGP: Text-based CAPTCHA as Graphical Passwords. In Proceedings of the 14th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (pp. 269–276). IEEE.
- Bigham, J. P., Cavender, A. C., Brudvik, J. T., Wobbrock, J. O., & Ladner, R. E. (2010). WebInSight: Making Web Images Accessible. Proceedings of the 2010 ACM SIGCHI Conference on Human Factors in Computing Systems, 1247–1256. https://doi.org/10.1145/1753326.1753527
- Google. (2019). Introducing the reCAPTCHA v3 API. Google Developers Blog. https://developers.googleblog.com/2018/10/introducing-recaptcha-v3-new-way-to.html
- Bigham, J. P., Cavender, A. C., Brudvik, J. T., Wobbrock, J. O., & Ladner, R. E. (2010). WebInSight: Making Web Images Accessible. Proceedings of the 2010 ACM SIGCHI Conference on Human Factors in Computing Systems, 1247–1256. https://doi.org/10.1145/1753326.1753527
- Bursztein, E., Aigrain, J., Martin, A., & Mitchell, J. C. (2014). The End is Nigh: Generic Solving of Text-based CAPTCHAs. Proceedings of the 2014 IEEE Symposium on Security and Privacy, 146–160. https://doi.org/10.1109/SP.2014.16
- Carlini, N., Zhang, C., Juels, A., Ristenpart, T., & Tygar, J. D. (2017). Towards Evaluating the Robustness of Neural Networks. Proceedings of the 38th IEEE Symposium on Security and Privacy, 39–57. https://doi.org/10.1109/SP.2017.21

- Xu, Z., Wang, W., Chen, Z., Yan, J., & Zhang, S. (2016). Automatically Bypassing ASIRRA Using Machine Learning. Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, 933–944. https://doi.org/10.1145/2976749.2978318
- Bigham, J. P., Cavender, A. C., Brudvik, J. T., Wobbrock, J. O., & Ladner, R. E. (2010). WebInSight: Making Web Images Accessible. Proceedings of the 2010 ACM SIGCHI Conference on Human Factors in Computing Systems, 1247–1256. https://doi.org/10.1145/1753326.1753527
- Bursztein, E., Aigrain, J., Martin, A., & Mitchell, J. C. (2014). The End is Nigh: Generic Solving of Text-based CAPTCHAs. Proceedings of the 2014 IEEE Symposium on Security and Privacy, 146–160. https://doi.org/10.1109/SP.2014.16
- Carlini, N., Zhang, C., Juels, A., Ristenpart, T., & Tygar, J. D. (2017). Towards Evaluating the Robustness of Neural Networks. Proceedings of the 38th IEEE Symposium on Security and Privacy, 39–57. https://doi.org/10.1109/SP.2017.14
- Gao, X., Tang, H., Jin, C., Li, Z., Wu, D., & Zhou, X. (2016). Robust Adaptive CAPTCHA Design against Intelligent Attacks. IEEE Transactions on Information Forensics and Security, 11(7), 1423–1436. https://doi.org/10.1109/TIFS.2016.2539383

- Xu, Z., Wang, W., Chen, Z., Yan, J., & Zhang, S. (2016). Automatically Bypassing ASIRRA Using Machine Learning. Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, 933–944. https://doi.org/10.1145/2976749.2978318
- Gao, X., Tang, H., Jin, C., Li, Z., Wu, D., & Zhou, X. (2016). Robust Adaptive CAPTCHA Design against Intelligent Attacks. IEEE Transactions on Information Forensics and Security, 11(7), 1423–1436. https://doi.org/10.1109/TIFS.2016.2539383
- Xu, Z., Wang, W., Chen, Z., Yan, J., & Zhang, S. (2016). Automatically Bypassing ASIRRA Using Machine Learning. Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, 933–944. https://doi.org/10.1145/2976749.2978318