International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 11 , November - 2026

Recent Developments and Trends in CAPTCHA: A Review

Pooja Shende[1], Rajeev Pandey[2] and Shikha Agrawal[3]
[1, 2, 3] University Institute of Technology, RGPV
Bhopal, Madhya Pradesh, India

Abstract. The Completely Automated Public Turing test to Tell Computers and Humans Apart, or CAPTCHA, has changed significantly since it was first developed and is now a crucial line of defense against automated bots. This study examines the most recent developments in CAPTCHA design, their ability to fend off online attacks, and the difficulties associated with developing artificial intelligence (AI) methods. The paper examines the future direction of CAPTCHA technology and provides insights into new CAPTCHA types, their usability, and the best way to balance security and accessibility. The goal of recent advancements has been to create increasingly complex and intuitive CAPTCHA variants, such as behavior-based gamified audio-based and image-based systems. In an attempt to achieve a balance between security and accessibility, these developments address problems such as the computational overhead of difficult problems and usability for people with disabilities. However, because AI has made it possible for bots to circumvent conventional CAPTCHAs, it has also created new difficulties, particularly in domains like machine learning and adversarial networks. This article examines the most recent advancements in CAPTCHA technology and assesses how well they defend against contemporary threats. It also discusses recent research that aims to improve security and user experience. The purpose of this paper is to give a summary of the current state of advanced CAPTCHA and point out its flaws.

Keywords: CAPTCHA, Artificial Intelligence, reCAPTCHA, CNN, Automatic Speech Recognition, Text Recognition, Gaming CAPTCHA.

1 Introduction

Since its introduction in 2000, CAPTCHA technology has been essential in preventing automated abuse of online services [1]. Alphanumeric character distortion was used by traditional text-based CAPTCHAs to distinguish between humans and bots. However, many of the earlier CAPTCHA techniques are no longer reliable due to advances in AI. This study examines recent developments and trends in CAPTCHA with a focus on improved security and user experience [2]. But as the internet grew,

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 11 , November - 2026

so did the sophistication of malicious bots. The creation of more reliable alternatives became crucial as sophisticated AI and machine learning models started to perform better than humans when answering conventional CAPTCHAs. Over time, CAPTCHA technology has evolved to incorporate interactive puzzles, image-based obstacles, voice recognition exercises, and more. The goal of each iteration was to outperform bots with the least amount of annoyance to human users.

1.1 Evolution of CAPTCHA

The continuous conflict between security and developing technology is reflected in the evolution of CAPTCHA. CAPTCHAs were first created in 2000 as text-based challenges to differentiate humans from machines. Since then, they have developed into image-based tasks such as item identification and audio CAPTCHAs for accessibility. Invisible CAPTCHAs expedite the process even further, whereas behavioral CAPTCHAs, such as Google's reCAPTCHA v3, examine user behavior to identify bots without upsetting users [3]. Biometric and other techniques have been developed as a result of bots becoming increasingly skilled at responding to conventional CAPTCHAs as AI technologies like machine learning and neural networks advance [4]. As CAPTCHAs are incorporated into more complete security models to strike a balance between user convenience and strong protection, this arms race is still ongoing.

1.1.1 Text Recognition based CAPTCHA

When text-based CAPTCHAs were first introduced in the early 2000s, they were the first to be widely used. They were intended to differentiate humans from bots by displaying distorted alphanumeric characters for users to recognize and enter. Because optical character recognition (OCR) methods at the time had problems reading noisy or distorted text, these systems relied on human interpretation [4].



Fig.1. Text Recognition based CAPTCHA [6]

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 11 , November - 2026

The distorted string CAPTCHA, which is an unintelligible string that can be decoded using OCR technology and is comparable to traditional CAPTCHA, is shown in detail in Figure 1. Despite their initial simplicity and effectiveness, they are now more susceptible to automated attacks due to advances in machine learning and optical character recognition (OCR) technology. For those with visual impairments, text-based CAPTCHAs also created accessibility issues. Consequently, more advanced techniques such as behavioral or image-based CAPTCHAs have largely replaced them [5].

1.1.2 Image Recognition based CAPTCHA

Concerns regarding the usability and security of CAPTCHAs are increasing as a result of their recent failure. Since general vision issues are thought to be more difficult than text recognition, many designs these days concentrate on image-based recognition rather than character recognition. In response to the shortcomings of text-based CAPTCHAs, image-based CAPTCHAs which take advantage of people's natural ability to identify objects in visual content emerged in the 2010s. These CAPTCHAs, which rely on people's higher visual acuity than bots, usually ask users to identify particular objects or patterns in a collection of images, like "Select all images with traffic lights.". Image-based CAPTCHAs were made popular by Google's reCAPTCHA v2, which combined visual barriers with user behavior analysis, including engagement patterns, to increase security [4].

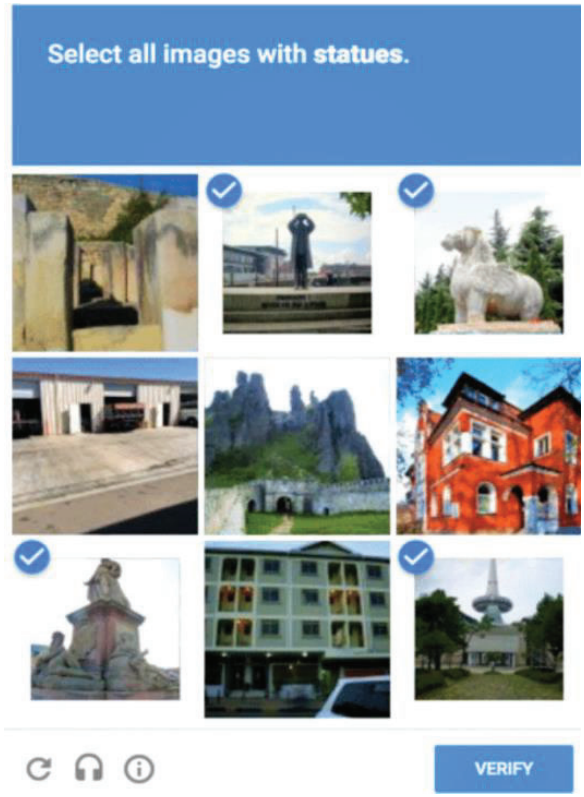


Fig.2. Image Recognition based CAPTCHA [7]

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 11 , November - 2026

An image processing technique that is currently popular in the field of image processing can be used to crack the picture recognition CAPTCHA shown in Figure 2. However thanks to advancements in computer vision and deep learning particularly convolutional neural networks (CNNs) bots can now effectively solve these issues. Additionally they make them difficult for visually impaired users to use which has led to the development of alternatives like behavioral models and audio CAPTCHAs.

1.1.3 Audio CAPTCHA

The audio-based CAPTCHA recognition system that can be cracked using machine learning-based speech recognition is shown in Figure 3. The purpose of audio-based CAPTCHAs is to make CAPTCHA systems accessible to people who are blind or visually impaired. Participants in these tasks have to recognize spoken words, numbers, or phrases that are hidden by background noise. These CAPTCHAs rely on people's ability to identify speech patterns despite noise distortions or multiple voices. Although audio-based CAPTCHAs increase accessibility, they are vulnerable to improvements in automated speech recognition (ASR) systems that are more adept at deciphering audio [8]. Additionally, because they may be challenging for users with hearing impairments or in noisy environments, multi-modal CAPTCHA systems combine them with text- or image-based alternatives. Despite these shortcomings audio CAPTCHAs remain a crucial component of inclusive security frameworks [9].

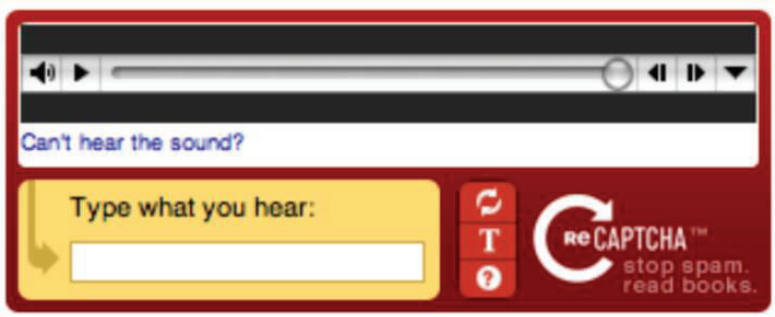


Fig.3. Audio Recognition based CAPTCHA [10]

1.1.4 Gamified CAPTCHA

Simple drag-and-drop games have become very popular since the appearance of Figure 4. It can be resolved by employing a dynamic cognitive approach and image recognition for path detection. Gamified CAPTCHAs combine security and user experience by providing dynamic and engaging challenges that require users to solve puzzles or complete basic tasks. Unlike traditional CAPTCHAs these tasks could involve dragging objects to predefined locations aligning shapes or completing a jigsaw puzzle. This ensures that only humans can complete the task while also

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 11 , November - 2026

making the process more enjoyable [11]. Gamified CAPTCHAs use natural interactions to make them more accessible and less annoying than traditional methods [12]. They may still be susceptible to sophisticated AI and bots that have been trained on human interaction patterns, though their implementation can be resource-intensive [13]. Despite these challenges gamified CAPTCHAs offer a novel approach to balancing security and usability in modern applications.

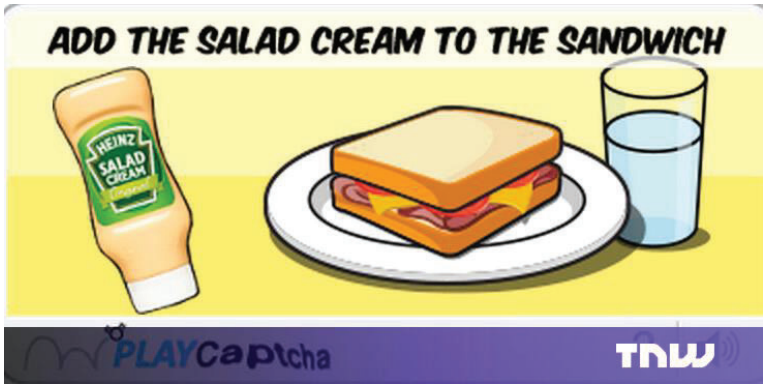


Fig.4. Gamified CAPTCHA [14]

1.1.5 Invisible CAPTCHA

ReCAPTCHA can be solved with a keylogger that uses mouse coordinates to copy the CAPTCHA track, as shown in Figure 5. Modern CAPTCHA solutions that eliminate visual barriers for the majority of users and use background user behavior analysis to differentiate between humans and bots are known as invisible CAPTCHAs. For example Googles Invisible reCAPTCHA uses browser activity click patterns and mouse movements to create a risk score. Only those who are suspected are then challenged with additional confirmation. This seamless approach improves accessibility and usability over traditional CAPTCHAs because legitimate users rarely encounter interruptions. However because of the extensive monitoring and profiling it raises privacy concerns and sophisticated bots that mimic human behavior might still be able to circumvent it [15]. Despite these concerns invisible CAPTCHAs represent a significant improvement in the security of online applications.

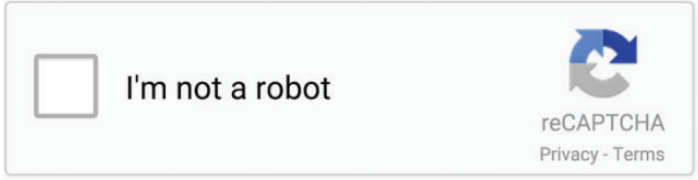


Fig.5. re-CAPTCHA [16]

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 11 , November - 2026

1.2 Visual Conceptual based Model

The User Interface (UI) Layer, which displays the CAPTCHA challenge (text image or audio) and an input field for user response; the Challenge Generation system, which generates interactive puzzles or randomly distorted text images to thwart automated bots; the Validation System, which compares the user's response with stored or dynamically generated values; and Security Mechanisms, which include behavior tracking time-based expiry and AI-based detection to thwart automated attacks, are the various interconnected components of a Visual Conceptual Model for CAPTCHA. A user requests access, a CAPTCHA appears, the user responds, and the system verifies the response. This is how the process is organized. Access is allowed if the input is accurate; if not, the user must try again or submit to further verification.

2 Related Work

Sivakorn et al. [17] cracked traditional text-based CAPTCHA systems using deep learning, particularly convolutional neural networks (CNNs), as "I Am Robot: (Deep) Learning to Break Text-based CAPTCHAs.". The authors show that CNNs can solve CAPTCHAs with high accuracy, including ones with noise distortions and overlapping characters, after being trained on a sizable synthetic dataset of CAPTCHA images. Their study demonstrates how deep learning models can easily get around text-distortion-based CAPTCHA protections, jeopardizing the security of many online services that rely on these systems to thwart bot attacks. The study highlights the increasing susceptibility of text-based CAPTCHAs to machine learning-based attacks and proposes that in order to counter these sophisticated methods, new CAPTCHA designs that may incorporate multiple modalities and human behavior analysis are required. Ye et al. [18] look into how "Generative Adversarial Networks (GANs)" might be used to solve text-based CAPTCHAs, which are frequently designed to prevent automated attacks. The authors suggest a GAN-based model that uses adversarial training to improve both the generator that creates the CAPTCHA-like images and the discriminator that assesses them. Their method works better than conventional machine learning methods for decoding CAPTCHAs with distortions and noise. The model's outstanding generalization across different CAPTCHA types draws attention to how susceptible conventional text-based CAPTCHA systems are to malicious attacks. The study highlights the increasing challenge of preserving CAPTCHA security in the face of cutting-edge machine learning techniques by arguing that future CAPTCHA designs must be more complex and multi-modal in order to withstand such attacks. H. Gao, H. et al. [19] in particular, examines the use of CAPTCHAs as a security measure to distinguish automated bots from human users in artificial intelligence (AI)-based problems. By concentrating on challenging AI tasks that are beyond the capabilities of current machine learning models, such as visual pattern recognition and natural language processing, the authors suggest leveraging problems that are challenging for machines but simple for humans. According to the article, CAPTCHAs can successfully thwart

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 11 , November - 2026

automated attacks and bot activity while maintaining accessibility for authorized human users because they are built around these intricate concerns. The paper argues for stronger AI-driven security measures by examining different CAPTCHA system implementations and the trade-offs between security and usability.

Table 1. Comparitive Analysis.

References	Focus	Technique	Problem Statement	Accuracy in %
[20]	An innovative concept called Drag and Drop has been introduced to counter laundry and OCR-based attacks.	Use your mouse to recognize people.	Redirection and money laundering attacks are two potential threats that the Drag and Drop (DnD) technique effectively combats.	87
[21]	The major goal is to introduce a new 3D CAPTCHA that offers better defense against bots.	OCR	Automating the identification process is more difficult for bots due to the complexity of the 3D world.	80
[22]	The main goal is to create a new image-based CAPTCHA that requires human expertise to pass.	Use two factors in your design.	The suggested CAPTCHA has an easy-to-understand interface that is clear and efficient.	72.61
[23]	To offer a CAPTCHA that combines pre-tagged images with geometric modifications to increase security.	Geometric adjustments	A clever and practical way to improve the security of image-based CAPTCHAs is through geometric modifications.	90
[24]	Creating grayscale human face images for image-based CAPTCHAs that are difficult for bots to figure out.	ULDP-WULDP	Avatar CAPTCHA offers robustness and an improved user experience.	85.52
[25]	To develop FRCAPTCHA, a system based on human face	Face recognition	FR-CAPTCHA offers accuracy on par with a human and is incredibly resistant to automated	94

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 11 , November - 2026

	pairings that match an image.		bots.	
[26]	To provide a strong framework that makes image-based problems more difficult, thereby increasing security.	SelAttack	The security issues that actual image-based CAPTCHAs encounter are addressed by the suggested approach.	90
[27]	A new CAPTCHA known as IMPTCHA was developed in order to recognize human users.	Semantic graphs	By using images instead of distorted text to label pictures, the proposed methodology yields useful results.	98.18
[28]	By forcing the deepfake model to produce stuff that is beyond its capabilities, the tactic aims to identify the adversary..	RTDF	This approach makes passive detection easier and tests AI's ability to create content rather than just classify it.	91

The security accuracy and user experience of CAPTCHA techniques have greatly improved, as Table 1 demonstrates. Automated attacks are successfully thwarted by high-performing techniques like FR-CAPTCHA (94%) and IMPTCHA (98.18%), which use facial recognition and semantic graphs, respectively. Modern techniques like RTDF and SelAttack demonstrate flexibility in handling new threats like deepfakes and the complexity of the real world. While techniques like 3D CAPTCHA and two-factor design demonstrate creativity, their lower accuracy (80% and 72.61%) emphasizes the need for improvement. All things considered, contemporary CAPTCHAs are developing into reliable systems that strike a compromise between security and usability, opening the door for future intelligence-based anti-bot defenses.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 11 , November - 2026

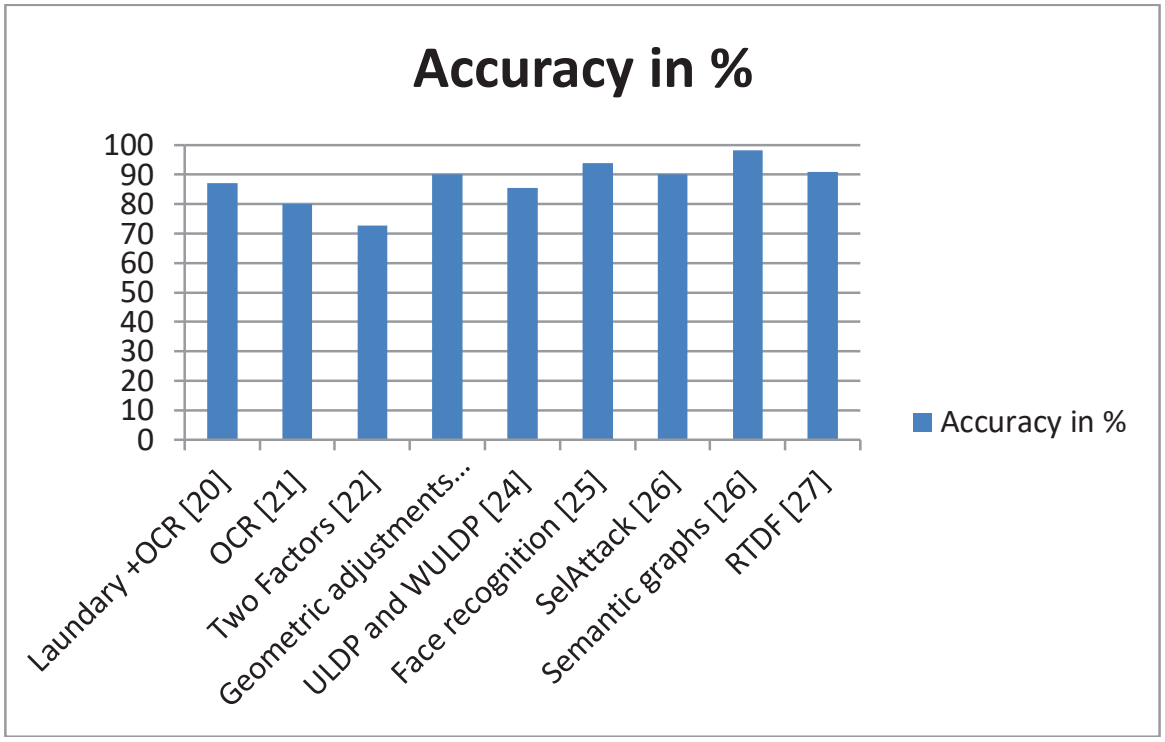


Fig.6. Result Comparison

When accuracy is specified, Figure 6 contrasts the results of a number of previously used CAPTCHA systems. Real-world CAPTCHA usability problems are frequently caused by user annoyance with excessively complicated or distorted text, challenging image selection tasks, and accessibility problems for people with cognitive or visual impairments. Many CAPTCHAs are difficult to read which makes it more difficult for users to finish tasks and discourages them from using forms or transactions. Additionally because mobile users cannot use touch-based interactions and have small screens some CAPTCHA issues are more challenging for them to solve. Even though audio CAPTCHAs are made to be accessible they often have background noise or poor clarity which aggravates users even more. Modern systems like Google reCAPTCHA use behavioral analysis and AI-driven risk assessments to reduce user friction while maintaining security.

3 Conclusion

Given the increasing use of automated technologies the concept of CAPTCHA is crucial to website security. As a result developing robust and secure CAPTCHA frameworks has become a primary goal of CAPTCHA research with significant advancements in recent years. Several CAPTCHA frameworks are compared and examined in this study with an emphasis on their effectiveness. The inaccessibility of many graphically distorted CAPTCHAs is a source of criticism. However audio-based CAPTCHA was developed to address the challenges faced by visually impaired individuals. To improve accessibility and explore the potential of audio-based CAPTCHA for all users more research is needed. The study's overall findings

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 11 , November - 2026

demonstrate how quickly CAPTCHA technology is developing and how important it is to assess and contrast various CAPTCHA frameworks in order to identify the most successful and efficient for visually impaired users. Researchers and practitioners in the domains of human-computer interaction (HCI) and CAPTCHA development are anticipated to gain from the findings. With the advent of behavioral analysis and risk-based authentication, CAPTCHA technology is moving away from traditional text and image-based challenges and toward more AI-driven and user-friendly methods. While AI improves verification techniques through sophisticated machine learning and fraud detection, it also enables attackers to create increasingly complex bots that can get around conventional CAPTCHAs. Because of this, AI is essential to CAPTCHA security. The largest challenge is still striking a balance between security and usability because complicated CAPTCHAs irritate users and increase abandonment rates, while simpler ones are more likely to be easily circumvented by AI-powered bots. By evaluating browsing habits and allocating risk scores, innovations such as Google reCAPTCHA v3 aim to reduce user interaction while preserving security. Future advancements will probably concentrate on adaptable and undetectable authentication methods that guaranty a flawless user experience without sacrificing security.

References

1. Von Ahn, L., Blum, M., & Langford, J. (2003). "Telling humans and computers apart automatically." *Communications of the ACM*, 46(5), 56-60.
2. Goodfellow, I., et al. (2014). "Generative Adversarial Nets." *Advances in Neural Information Processing Systems*.
3. Akhawe, D., & Felt, A. P. (2013). Alice in Warningland: A Large-Scale Field Study of Browser Security Warning Effectiveness. *USENIX Security Symposium.*
4. Bursztein, E., Martin, M., & Mitchell, J. (2011). Text-based CAPTCHA Strengths and Weaknesses. *Proceedings of the 18th ACM Conference on Computer and Communications Security.*
5. Mori, G., & Malik, J. (2003). Recognizing Objects in Adversarial Clutter: Breaking a Visual CAPTCHA. *IEEE Computer Vision and Pattern Recognition (CVPR).*
6. J.J. (2022, October 7). 3 things to consider before you implement CAPTCHA for accessibility. Medium. https://uxdesign.cc/3-things-to-consider-before-you-implement-captcha-for-accessibility-7b4fe01cd747
7. Noury, Zahra & Rezaei, Mahdi. (2020). Deep-CAPTCHA: a deep learning based CAPTCHA solver for vulnerability assessment. 10.31219/osf.io/km35b.
8. Tam, H., Florencio, D., & Herley, C. (2008). Secure CAPTCHAs Using Audio and Images. Proceedings of the 17th International Conference on World Wide Web (WWW).
9. Bigham, J. P., & Cavender, A. C. (2009). Evaluating Existing Audio CAPTCHAs and an Interface Optimized for Non-Visual Use. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems.
10. Ahmed, Tanvir & Tushar, Kaiser & Islam, Sunjida & Rahman, Md.Mahbubur. (2016). Siimple, Robust & User Friiendlly CAPTCHA 'InstaCap' for Web Securiity. International Journal of Hybrid Information Technology. 9. 163-182. 10.14257/ijhit.2016.9.1.15.
11. Chew, M., & Baird, H. S. (2003). BaffleText: A Human Interactive Proof. International Journal on Document Analysis and Recognition (IJDAR).

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 11 , November - 2026

12. Ahn, L. V., & Blum, M. (2004). Peekaboom: A Game for Locating Objects in Images. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems.
13. Gossweiler, R., Kamvar, M., & Baluja, S. (2009). What's Up CAPTCHA? A CAPTCHA Based on Image Orientation. Proceedings of the 18th International Conference on World Wide Web (WWW).
14. Ong, J. (2013, October 9). Future Ad Labs signs Heinz and Reckitt Benckiser as launch partners for its gamified CAPTCHA. *TNW | Insider*. https://thenextweb.com/news/future-ad-labs-signs-heinz-and-reckitt-benckiser-as-launch-partners-for-its-gamified-captcha.
15. Bursztein, E., Martin, M., & Mitchell, J. (2014). The End is Nigh: Exploring the Collapse of HTTPS Visual Indicators. Proceedings of the USENIX Security Symposium.
16. Ridloghfry. (2024, November 18). Integrating Google reCAPTCHA into Your Next.js Application: A Step-by-Step Guide. *Medium*. https://blog.devgenius.io/integrating-google-recaptcha-into-your-next-js-application-a-step-by-step-guide-f7df3f7c57e0.
17. Sivakorn, S., Polakis, I., & Keromytis, A. D. (2016). "I Am Robot: (Deep) Learning to Break Text-based CAPTCHAs." Proceedings of the ACM Conference on Computer and Communications Security (CCS).
18. Ye, G., Yang, S., Wang, X., et al. (2018). Yet Another Text CAPTCHA Solver: A Generative Adversarial Approach. IEEE Transactions on Information Forensics and Security.
19. Gao, H., Yan, J., et al. (2013). Network and Distributed System Security Symposium (NDSS).
20. Arpan Desai, Pragnesh Patadia (2009, November). Drag & Drop: A better approach to captcha. In 2009, A.D Patel Institute Of technology, Sardar Patel University, Gujarat, India (pp. 1-4) IEEE.
21. Montree Imsamai, Suphakant Phimoltares (2010, April) 3D CAPTCHA: A Next Generation of the CAPTCHA. In 2010, 2010 International Conference on Information Science and Applications, Seoul, Korea (pp. 1–5) IEEE
22. Shardul Vikram, Yinan Fan, Guofei Gu (2011, December) Semage: A new image based two factor captcha. In 2011, Texas A&M University College Station, Texas (pp. 1-9) ResearchGate
23. Maryam Mehrnejad, Abbas Ghaemi Bafghi, Ahad Harati, Ehsan Toreini (2012, January) SEIMCHA: A New Semantic Image CAPTCHA Using Geometric Transformations. In 2012, Computer Department Ferdowsi University, Mashhad, Iran (pp. 1-12) ISC
24. Darryl Felix D'Souza (2014, December) Avatar telling computers and humans apart via face classification and mouse dynamics. In 2014, University of Louisville (pp. 1-10) ResearchGate
25. Gaurav Goswani, Brian M. Powell, Mayank Vatsa, Richa Singh, Afzel Noore (2014, April) FR-CAPTCHA: CAPTCHA Based on Recognizing Human Faces. In 2014, IIT, Delhi, India (pp. 1–4) ResearchGate. PLOS
26. Haiqin Weng, Binbin Zhao, Shouling Ji*, Jianhai Chen, Ting Wang, Qinming He, Raheem Beyah (2019, June) Towards Understanding the security of modern image captcha & unground captcha solving services. In 2019, College Of Computer science & Technology, Zhejiang University, China (pp. 1-25) IEEE
27. Reza Shali (2020, December) IMPTCHA: A creative image captcha. In 2020, Faculty Of Comp
28. Lior Yasur, Guy Frankovits, Fred M. Grabovski, Yisroel Mirsky (2023, January) Deepfake CAPTCHA: A Method for Preventing Fake Calls, In 2023, Ben -Gurion University of the Negev, Israel (pp. 1 – 12) ACM Digital Library, ISBN

(This work is licensed under a Creative Commons Attribution 4.0 International License.)