International Journal of Basic and Applied Sciences, 14 (1) (2025) 32-39

International Journal of Basic and Applied Sciences

Website: www.sciencepubco.com/index.php/IJBAS
https://doi.org/10.14419/fab5t109
Research paper

AI-driven biometric CAPTCHA: defending against automated threats in web security

Dr. Neha P. Bora [1]*, Pradyumna M. Bora [2], Dr. Vaishali S. Tidake[3], Ghanshyam P. Dhomse [4], Deepali P. Pawar [5]

[1,4,5] *Assistant Professor, Department of Computer Engineering, SNJB's Late Sau. K. B. Jain, College of Engineering, Chandwad Dist. Nashik, Maharashtra, India*
[2] *Assistant Professor, Department of Mechanical Engineering, SNJB's Late Sau. K. B. Jain, College of Engineering, Chandwad Dist. Nashik, Maharashtra, India*
[3] *Associate Professor, Department of Computer Engineering, MVPS's KBT College of Engineering, Nashik, Maharashtra, India*
**Corresponding author E-mail: mutha.nccoe@snjb.org*

Received: March 16, 2025, Accepted: April 8, 2025, Published: April 14, 2025

Abstract

Web security is a critical aspect of modern life, as the increasing reliance on internet services exposes systems to various cyber threats. Au-Automated hacking tools exploiting registration systems with false information often led to bandwidth issues and Distributed Denial of Service (DDoS) attacks. CAPTCHA remains a widely used mechanism for distinguishing between humans and automated systems. However, simple CAPTCHAs are easily bypassed by advanced AI, while complex ones can frustrate genuine users. This research presents an innovative B3DA (Biometric 3D Animated) CAPTCHA algorithm that integrates AI for Face Recognition with randomly generated Three-dimensional animated characters. The proposed solution creates CAPTCHAs that are intuitive for people to handle but pose significant challenges in the context of automated systems. By combining handwritten 3D animated characters into randomized strings, the B3DA CAPTCHA algorithm enhances security and usability. Experimental results validate the algorithm's robustness against bot-driven attacks, demonstrating its ability to withstand sophisticated breaches while leveraging machine learning for continuous improvement. The B3DA CAPTCHA algorithm offers a transformative approach to CAPTCHA design, effectively balancing user convenience and resistance to automated hacking tools, marking a significant advancement in web security solutions.

Keywords: *Artificial Intelligence; B3DA; CAPTCHA; DDOS; OCR.*

1. Introduction

The critical role that the Internet plays in our day-to-day activities emphasizes how important it is that all users prioritize Internet security. Customers of many companies and organizations can access the internet. However, sometimes malicious automated malware targets websites to cause servers to slow down. Users are often asked to provide personal information, like addresses, mobile numbers, and email addresses, while registering or filling out forms. Malicious automated tools send large volumes of fake information from non-existent users, which can slow down or crash servers. The expectation was always that genuine users, i.e., humans, would complete tasks honestly. However, automated programs can submit forms with inaccurate information, wasting disk space and significantly slowing down servers. These attacks, typically executed using computer programs [23], can disrupt services such as university result announcements or railway ticket reservations. This action saturates the system with irrelevant information, making it difficult for authentic users to retrieve their exam results. Let us now examine an additional example of a railway reservation website where a hacker can purchase a significant quantity of Tatkal tickets using automated hacking software, thereby preventing regular people from acquiring the tickets [32]. CAPTCHA is used to deter non-human behavior on websites and distinguish between computer and human users. CAPTCHA, or the Completely Automated Public Turing test to Tell Computers and People Apart, prevents bots from answering questions that humans can easily answer. [23]. While modern AI and image recognition systems can hack simple text CAPTCHAs, even complicated ones with severe distortion remain difficult for users to solve.

Fig. 1: CAPTCHA [39].

The user will be prompted to enter the characters shown in the image by the CAPTCHA system. The researchers distorted the image box to resemble character shapes, thereby hindering automated character recognition by computer algorithms. Additionally, noise was added in the form of lines, dots, dashes, and arcs. This method's primary benefit is that human users can respond quickly to inquiries that current computer algorithms are unable to answer or cannot.
Our proposed solution introduces a new method for implementing CAPTCHA using biometric 3D animated technology, aiming to be user-friendly while impervious to computer programs and automated software. In the paper, the next session is the Literature Survey, then Methodology and implementation algorithm, and later session discusses test results and solving time comparison with other CAPTCHA.

1.1. OCR and non-OCR based CAPTCHA

Users can generate words by interpreting distorted and visually modified text using OCR technology, but this method is slower for humans compared to computer programs. OCR software struggles with visually altered text, especially on thin paper, making some word forms only partially recognizable. However, as AI and neural networks improve OCR capabilities, the security of OCR-based CAPTCHAs is becoming more vulnerable [24]. For instance, Yahoo faced CAPTCHA circumvention by a software program with a 30% success rate, prompting designers to add random interference to images for enhanced verification, resulting in more complex CAPTCHAs [25].

Fig. 2: Complicated CAPTCHA [40].

2. Literature review

To prevent automated mail account registration, Luis von Ahn, Manuel Blum, Nicholas Hopper, and John Langford created the first CAPTCHA in 2000 for the Carnegie Mellon University Yahoo website [23]. The original purpose of the three-part Further Literature Review was to stop automated bots from flooding online polls.

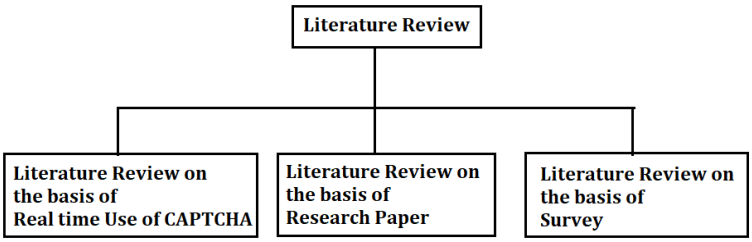

Fig. 3: Literature Review.

2.1. Review based on real time use of CAPTCHA

Simple Text based	Complex Text based CAPTCHA	Audio based	Graphical/ Images based	Puzzle/Logic/ Math/Game based
				
Good CAPTCHA but 90% success in cracking through OCR	More difficulty for human users to recognize	Background noise Similar sound words Difficult to non-English human	Large solving time Occupy more space More loading time	Intelligence required Large solving time Occupy more space More loading time

Fig. 4: Different CAPTCHA Types.

2.2. Review based on research paper

K. Sukhani et al. discussed methods to bypass reCAPTCHA v2 [1,31], Khawandi et al. studied OCR & Non-OCR methods for breaking CAPTCHA [2], M. Jadhav et al. recommended CAPTCHA for people with vision impairments [3], Various CAPTCHA approaches were reviewed by Shivani and R. K. Challa [4], Sheheryar et al. predicted more CAPTCHA schemes will break with AI advancements [5], Y. Zhang et al. proposed deep learning for CAPTCHA security [6], Possible attacks on text CAPTCHAs were demonstrated by Azad and Jain [7], Y. S. Aljarbou highlighted issues with Puzzle, Video, and Audio CAPTCHAs [8], to get around language-based CAPTCHA restrictions and OCR technology, The authors, Aldosari and Al-Daraiseh, developed a CAPTCHA technique based on handwritten characters drawn from four languages: English, French, Spanish, and Arabic. Their system utilizes image processing and machine learning to create complex

CAPTCHA images, enhancing security against automated attacks [9], Cao Lei proposed a finger-guessing game as CAPTCHA [10], NC Mutha et. al. introduced 3D animated handwritten CAPTCHA[11,15], S. Singhal et al. broke CAPTCHA on irctc.co.in [12]., C. J. Chen et al. addressed noisy points in image CAPTCHA [13], Ali et al. developed a puzzle based CAPTCHA system [14], Rao et al. suggested handwritten CAPTCHA images as a solution [16], G. Goswami et al. proposed a CAPTCHA algorithm for better accuracy [17], D. D'Souza et al. introduced AVATAR CAPTCHA [18], J. Cui et al. introduced 3D animated moving CAPTCHA [19], J. Cui wt. et. al. presents a novel CAPTCHA implementation based on 3D animation [20, 21]. Chew and Tygar proposed an image-based CAPTCHA [22]. A text-based CAPTCHA was proposed by L. von Ahn et al. based on challenging AI challenges. [23]. By allowing object detection even when visual noise is present, the paper offers a method for getting around visual CAPTCHA systems. It introduces an approach that uses clutter elimination and object detection methods to bypass the CAPTCHA challenges [24]. In order to prevent bots, recent developments have investigated behavioural biometrics (such as keyboard dynamics and mouse movement patterns) [27] and voice-based CAPTCHA systems (such as speaker verification) [28]. Combining these non-visual methods with visual biometric systems like B3DA CAPTCHA may improve multi-modal authentication and offer inclusive solutions for individuals with visual impairments. While earlier CAPTCHA systems relied on image distortion and noise to confuse automated systems, recent advancements in deep learning have significantly undermined these techniques. For instance, Meng et al. demonstrated that CNNs could successfully bypass voice CAPTCHAs, while Zhang et al. utilized vision transformers to break text-based CAPTCHAs with high accuracy [28,29]. Similarly, GANs have been employed to synthesize realistic CAPTCHA challenges, further aiding adversarial training. These studies highlight a growing trend of AI-driven CAPTCHA circumvention, reinforcing the need for multimodal solutions like B3DA, which combines biometric verification and animated character recognition to enhance resilience against such attacks. Psychological research can guide the design of CAPTCHAs that align with human cognitive strengths (e.g., pattern recognition, memory) while exploiting the weaknesses of automated systems. Neuroscience helps in understanding how humans perceive motion, depth, and patterns, especially in 3D environments. Deep learning techniques can simulate human perceptual thresholds and eye-tracking behaviour to fine-tune CAPTCHA designs that are intuitive for humans but adversarial for AI. The paper by X. Nian et al. (2023) presents a deep learning-based method that uses object detection techniques to effectively break text CAPTCHAs, highlighting security vulnerabilities in these commonly used systems.

2.3. Review based on survey

With the intent to find bottlenecks in strengthening the CAPTCHA leading to compromise of the data security of the web portals, a survey was conducted. For this purpose, we visited a nearby web development IT company, Coexis Tech, to observe and discuss CAPTCHA generation in 'sign in/sign up' forms, along with the issues and challenges faced by the software developers. One Google form is shared with them, and the response received is as follows:

Summary: Survey responses and discussions revealed that the image CAPTCHA they employ takes a long time, roughly 30 to 35 seconds, and that 25% of users still fail to complete the CAPTCHA on their first try. Also, the image CAPTCHA occupies more space on a website. The discussion concluded the need for a simple, less time and space-consuming CAPTCHA with higher security.

Identified Gaps: Existing CAPTCHA systems fall short of fulfilling all the desired criteria for an ideal solution. Many of them prove unsuitable for a wide range of users. Although traditional text-based CAPTCHAs are generally favoured, alternative formats tend to receive less user approval. The study highlights that the growing sophistication of image recognition, bots, and artificial intelligence makes simple CAPTCHAs less reliable. However, increasing their complexity may hinder human interaction. These limitations underscore the necessity for a novel and more effective CAPTCHA design.

Problem Statement: Harmful automated hacking software attempts to overload website resources and create traffic by using a program to submit false information, leading to server slowdowns and wasted disk space. CAPTCHA, a Fully Automated Public Turing Test to Tell Computers and Humans Apart, provides a solution. Basic text AI can readily decode CAPTCHAs, but humans find it challenging to understand complex CAPTCHAs. It will become more challenging to discern between humans and robots as AI and machine learning develop and allow bots to impersonate humans and solve CAPTCHA. The demand for creative CAPTCHA designs has increased as a result.

3. Methodology and algorithm

The development of CAPTCHA is predicated on a few methods, including:

1) Face capture using biometrics
2) Characters with handwritten 3D effects
3) Motion Pictures
4) Method of Display

3.1. Mathematical module

F(n): H(n) ∨ G(n)

Where,

F(n): CAPTCHA Function

H(n): Human Face Capturing

G(n): B3DA Algorithm

G(n): q ^ r ^s

q: Handwritten 3D effect Characters

r: Animation

s: Display Technique

Fig. 5: Mathematical Module.

When it comes to fending off attacks by bots or programs on systems without cameras, B3DA CAPTCHA is a fair technique. However, industries including banking [34], defence, and train reservation systems are employing cameras to increase security. When these cameras are paired with human face identification, security is increased by a factor of two. Computer vision frequently uses a shape predictor algorithm to identify and forecast points (landmarks) on an object, usually human faces. These points, like the corners of the eyes, the nose tip, or the shape of the jaw, are typically preset.

3.2. Algorithm

Step 1:
Using pen tablets, enter 3D biometric handwritten characters (A-Z) into a database. Create a variety of 3D designs while taking depth into account, and store several character pictures under a single index.

Fig. 6: Datasets.

Step 2:
Verify human or robot identity visually, akin to checking visitors at the doorstep, by employing a frontal face detection method with a camera setup.
Step 3:
Utilize the Shape predictor algorithm to identify single human faces from frontal views and mark facial landmarks accordingly.

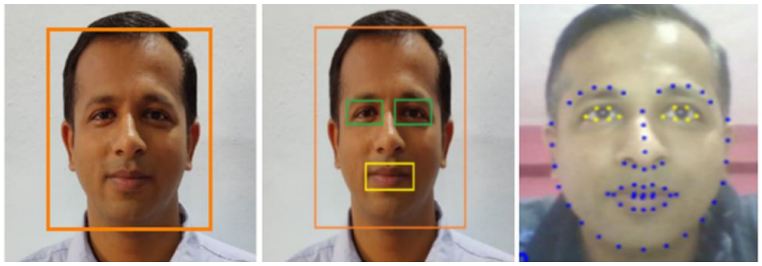

Fig. 7: Facial Landmark Detection.

Step 4:
Using the facial landmark algorithm (ranges 36-48), determine whether or not human eyes are open. Assuming that eyes are open by default, look for blinks to verify the existence of humans.

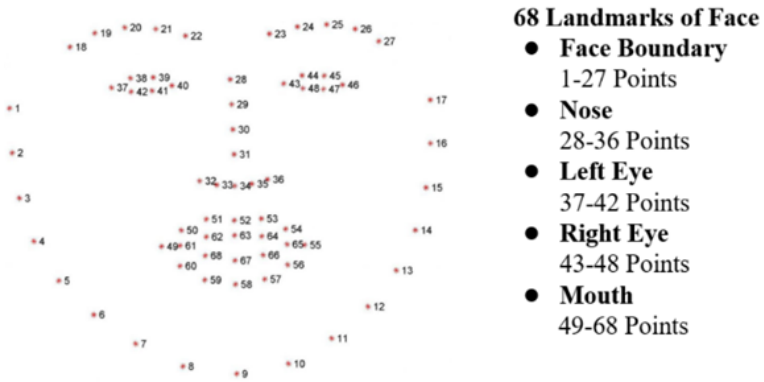

Fig. 8: 68 Landmarks of Faces.

Step 5:
Using a random variable generator technique, create random CAPTCHAs on the screen that are difficult for automated systems to get past by showing characters in a box with limited size and animation effects.

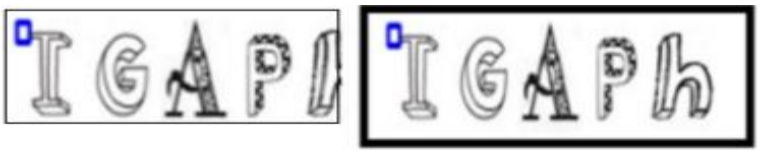

Fig. 9: Randomly Generated B3DA CAPTCHA.

Step 6:
After user input, compare entered CAPTCHA text with database records, verify blinking in human face detection, and either accept the form or refresh CAPTCHA for further attempts, leveraging AI and ML to enhance CAPTCHA security against bot attacks.

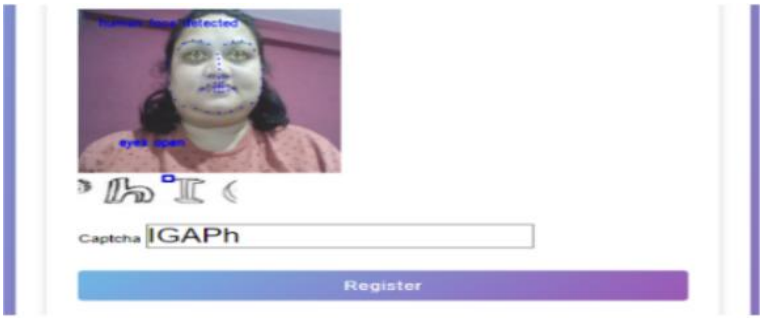

Fig. 10: Upshot of Website.

4. Experiments and results

B3DA CAPTCHA's robustness was verified by the cybersecurity & Testing Company Lumiverse Solutions is a private limited company that continuously works towards building the best security framework to shelter businesses ' data-centric treasures based in Nashik, India. Two Test Comparisons are done, one with Handwritten CAPTCHA [16] and one with Strong multilingual CAPTCHA [9].
500 CAPTCHA samples were tested using online OCR tools
For this CAPTCHA recognition test, Lumiverse experts employ the following OCRs:
1: OCR, 2: OCR, 3: OCR, and 4: OCR are the aliases for the websites
www.onlineocr.net [35], www.free-online-ocr.com [36], www.newocr.com [37], and www.i2ocr.com [38]
Case 1:
Comparisons are made between Handwritten CAPTCHA and B3DA CAPTCHA
A performance evaluation of the proposed CAPTCHA generation algorithm was conducted using 500 distinct samples. Multiple online OCR tools were employed to assess recognition accuracy. Initial testing with handwritten CAPTCHA samples served as a baseline, where high recognition rates indicate vulnerability. The same OCR tools were then applied to B3DA CAPTCHA samples, showing a substantial increase in robustness: OCR-1 incorrect recognition accuracy increased from 74.5% to 98.8%, OCR-2 from 83.4% to 99%, and OCR-3 from 88.9% to 99.6%. Since CAPTCHA systems aim to prevent automated decoding.

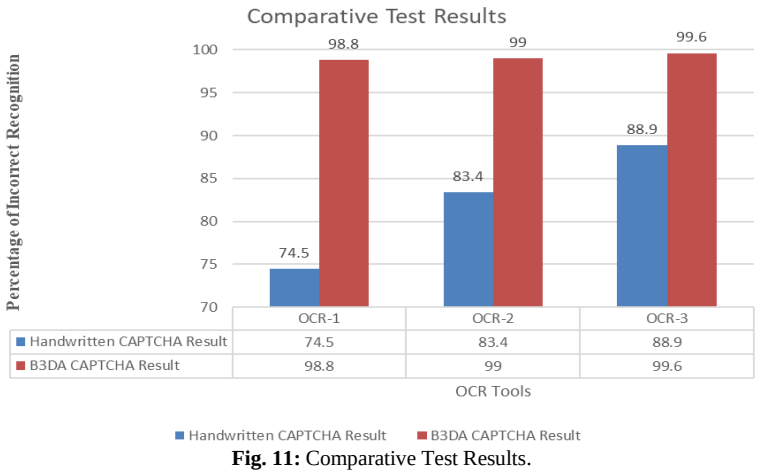

Fig. 11: Comparative Test Results.

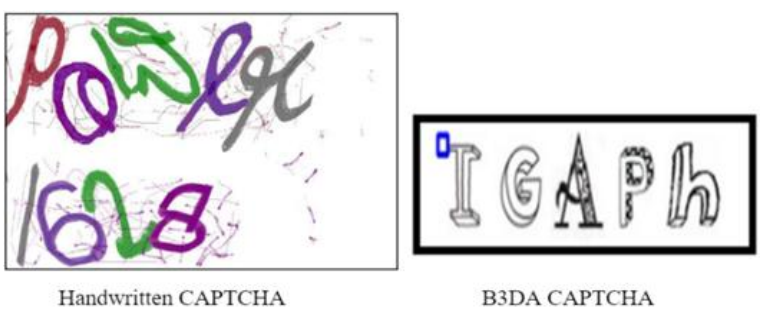

Fig. 12: Comparative Display of CAPTCHA [16].

Case 2: Comparisons are done between Strong multilingual CAPTCHA and B3DA CAPTCHA [9].
www.i2ocr.com alias 4: OCR

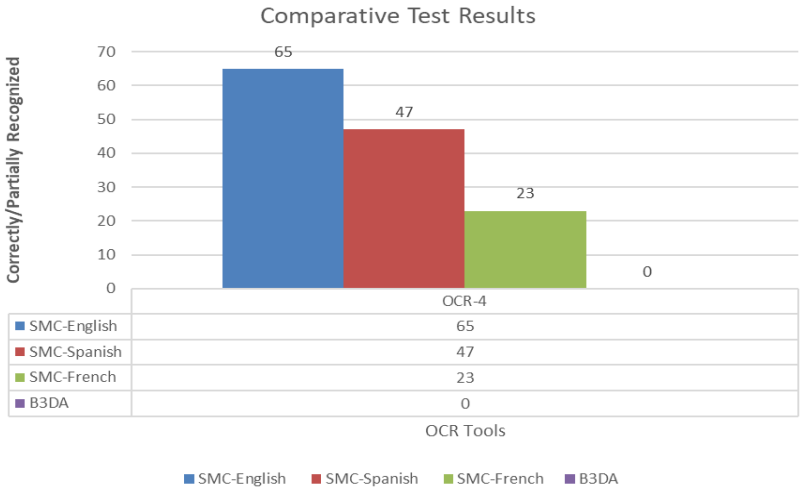

Fig. 13: Comparative Test Results.

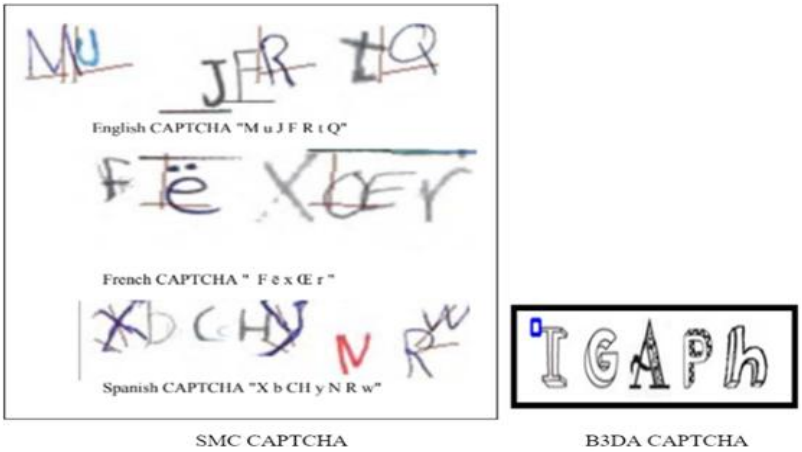

Fig. 14: Comparative Display of CAPTCHA [9].

Concluding Remark: The results were excellent. B3DA CAPTCHA is easy for humans to identify, fast and secure, and challenging for bots to break; we recommend its use as a more secure CAPTCHA.

5. Solving time for CAPTCHA

A CAPTCHA-breaking service and Amazon Mechanical Turk employees were tested by Stanford University researchers [26] on 21 common CAPTCHA varieties (eight audio and thirteen text images) of different difficulty levels. Findings showed text image CAPTCHA took 9.8 seconds on average, while audio CAPTCHA were much tougher at 28.4 seconds.
A similar study on B3DA CAPTCHA showed significantly better results compared to other schemes in the Stanford University study. The study involved 50 teaching staff, 50 non-teaching staff, and 50 students for human evaluation.

Comparative Average solving time for each scheme

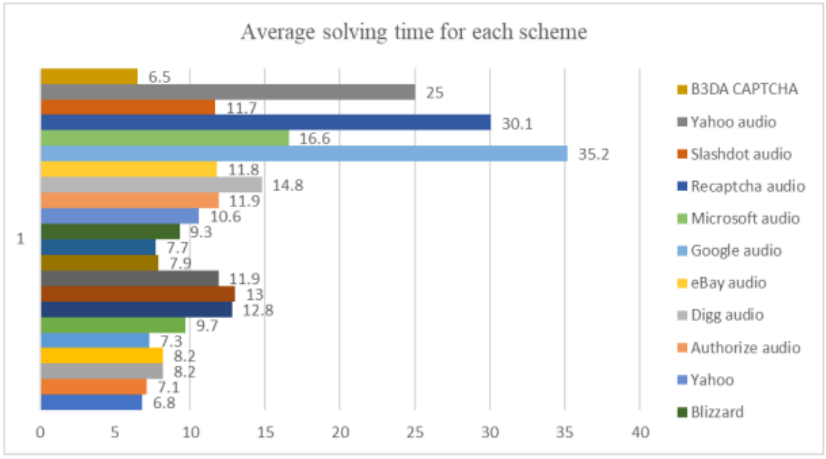

Fig. 15: Solving Time of CAPTCHA.

CAPTCHA Schemes	Time Required to Solve CAPTCHA in sec
Authorize	6.8
Baidu	7.1
Captchas.net	8.2
Digg	8.2
eBay	7.3
Google	9.7
mail.ru	12.8
Microsoft	13
Recaptcha	11.9
Skyrock	7.9
Slashdot	7.7
Blizzard	9.3
Yahoo	10.6
Authorize audio	11.9
Digg audio	14.8
eBay audio	11.8
Google audio	35.2
Microsoft audio	16.6
Recaptcha audio	30.1
Slashdot audio	11.7
Yahoo audio	25
B3DA CAPTCHA	**6.5**

Fig. 16: Average Solving Time for Each Scheme [26].

6. Discussion & conclusion

Using computer vision algorithms, facial landmark identification, and live detection, CAPTCHAs that require users to identify and match human faces in a sequence of images are effective techniques for stopping automated spam and abuse. By making it harder for bots to pass for real users, the B3DA CAPTCHA algorithm adds an extra degree of protection. It does this by combining biometrically produced characters with randomly chosen 3D effects for a brief animated CAPTCHA frame. When compared to pictures or other CAPTCHAs, solving time and space on websites is also decreased. Website and application developers who wish to increase the accuracy with 98% of their security against automated attacks and bots should consider the B3DA CAPTCHA algorithm as a viable solution because it is simple to implement utilizing AIML libraries. The machine learning algorithm that underpins the suggested B3DA CAPTCHA system is made to adapt to new data patterns over time. Due to its flexibility, the underlying CAPTCHA dataset can be strengthened and updated dynamically, thereby increasing its resistance to new AI-based threats.

7. Future directions

With the above conclusion, it is important to understand that the future capabilities of AI remain highly unpredictable, and exploration of the AI threat becomes a part of future work as under:

1) Systematic testing of CAPTCHA robustness against generative AI and deepfake technologies.
2) Using concepts from neuroscience and psychology to increase usability without sacrificing security.
3) Creation of legal and ethical standards for the application of behaviour-based and biometric CAPTCHA systems.

Acknowledgement

We, authors, express our gratitude to the editor and anonymous reviewers for their insightful feedback that has helped to elevate this work. Funding organizations from the governmental, private, or nonprofit sectors did not specifically award money for this study.

References

[1] K. Sukhani, S. Sawant, S. Maniar, and R. Pawar, "Automating the bypass of image-based CAPTCHA and assessing security," in 12th International Conference on Computer Communication and Network Technology (ICCCNT), 2021, pp. 01–08. https://doi.org/10.1109/ICCCNT51525.2021.9580020.

[2] S. Khawandi, A. Ismail, and F. Abdallah, "Different implemented CAPTCHAs and breaking methods," International Research Journal of Engineering and Technology (IRJET), vol. 6, no. 2, 2019. [Online]. Available: https://www.researchgate.net/publication/335961595_Different_Implemented_Captchas_and_Breaking_Methods.

[3] M. Jadhav, N. Kulkarni, and O. Walhekar, "Doodling based CAPTCHA authentication system," in Asian Conference on Innovation Technology (ASIANCON), 2021, pp. 1–5. https://doi.org/10.1109/ASIANCON51346.2021.9544570.

[4] K. Shivani and R. K. Challa, "CAPTCHA: A systematic review," in IEEE International Conference on Advent Trends in Multidisciplinary Research and Innovation (ICATMRI), 2020, pp. 1–8. https://doi.org/10.1109/ICATMRI51801.2020.9398494.

[5] M. A. Sheheryar, P. K. Mishra, and A. K. Sahoo, "A review on CAPTCHA generation and evaluation techniques," ARPN Journal, vol. 11, pp. 5800–5811, 2016.

[6] Y. Zhang et al., "A survey of research on CAPTCHA designing and breaking techniques," in 18th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/13th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE), 2019, pp. 75–84. https://doi.org/10.1109/TrustCom/BigDataSE.2019.00020.

[7] S. Azad and K. Jain, "CAPTCHA: Attacks and weaknesses against OCR technology," Global Journal of Computer Science and Technology: Neural & Artificial Intelligence, vol. 13, no. 3, pp. 14–18, 2013.

[8] Y. S. Aljarbou, "Improving current CAPTCHA systems," in 2nd International Conference on Computer Applications & Information Security (ICCAIS), 2019, pp. 1–6. https://doi.org/10.1109/CAIS.2019.8769466.

[9] M. H. Aldosari and A. A. Al-Daraiseh, "Strong multilingual CAPTCHA based on handwritten characters," in 7th International Conference on Information and Communication Systems (ICICS), 2016, pp. 239–245. https://doi.org/10.1109/IACS.2016.7476118.

[10] C. Lei, "Image CAPTCHA technology research based on the mechanism of the finger-guessing game," in Third International Conference on Cyberspace Technology (CCT 2015), 2015, pp. 1–4. https://doi.org/10.1049/cp.2015.0843.

[11] N. P. Bora and D. C. Jain, "A web authentication biometric 3D animated CAPTCHA system using artificial intelligence and machine learning approach," Journal of Artificial Intelligence and Technology, vol. 3, no. 3, pp. 126–133, 2023. https://doi.org/10.37965/jait.2023.0216.

[12] S. Singhal, A. Sharma, S. Garg, and N. Jatana, "Vulnerabilities of CAPTCHA used by IRCTC and an alternative approach of Split Motion Text (SMT) CAPTCHA," in 4th International Conference on Reliability, Infocom Technologies and Optimization (ICRITO), 2015, pp. 1–6. https://doi.org/10.1109/ICRITO.2015.7359287.

[13] C. J. Chen, Y. W. Wang, and W. P. Fang, "A study on CAPTCHA recognition," in Tenth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, 2014, pp. 395–398. https://doi.org/10.1109/IIH-MSP.2014.105.

[14] F. A. B. H. Ali and F. B. Karim, "Development of CAPTCHA system based on puzzle," in 1st International Conference on Computer, Communications, and Control Technology (I4CT), 2014, pp. 426–428. https://doi.org/10.1109/I4CT.2014.6914219.

[15] N. C. Mutha and D. S. D. Sharma, "3D handwritten animated CAPTCHA algorithm: Web security," International Journal of Engineering Research and Technology (IJERT), vol. 2, no. 10, pp. 2071–2076, 2013.

[16] M. Rao and N. Singh, "Random handwritten CAPTCHA: Web security with a difference," International Journal of Information Technology and Computer Science, vol. 4, pp. 53–58, 2012. https://doi.org/10.5815/ijitcs.2012.09.07.

[17] G. Goswami, R. Singh, M. Vatsa, B. Powell, and A. Noore, "Face recognition CAPTCHA," in IEEE Fifth International Conference on Biometrics: Theory, Applications, and Systems (BTAS), 2012, pp. 412–417. https://doi.org/10.1109/BTAS.2012.6374608.

[18] D. D'Souza, P. C. Polina, and R. V. Yampolskiy, "Avatar CAPTCHA: Telling computers and humans apart via face classification," in IEEE International Conference on Electro/Information Technology, 2012, pp. 1–6. https://doi.org/10.1109/EIT.2012.6220734.

[19] J. Cui, J. Mei, W. Zhang, X. Wang, and D. Zhang, "A CAPTCHA implementation based on moving objects recognition problem," in International Conference on E-Business and E-Government, 2010, pp. 1277–1280. https://doi.org/10.1109/ICEE.2010.326.

[20] J. Cui, J. Mei, X. Wang, D. Zhang, and W. Zhang, "A CAPTCHA implementation based on 3D animation," in International Conference on Multimedia Information Networking and Security, 2009, pp. 179–182. https://doi.org/10.1109/MINES.2009.298.

[21] M. Chew and J. D. Tygar, "Image recognition CAPTCHAs," in Proceedings of the 2004 International Conference on Financial Cryptography, 2004, pp. 268–279. https://doi.org/10.1007/978-3-540-30144-8_23.

[22] L. von Ahn, M. Blum, and J. Langford, "Telling humans and computers apart automatically," Communications of the ACM, vol. 47, no. 2, pp. 56–60, 2004. https://doi.org/10.1145/966389.966390.

[23] von Ahn L, Blum M & Langford J (2004), Telling humans and computers apart automatically. Communications of the ACM 47(2), 56–60. https://doi.org/10.1145/966389.966390.

[24] Mori G & Malik J (2003), Recognizing objects in adversarial clutter: Breaking a visual CAPTCHA. Proceedings of the 2003 IEEE Computer Society Conference on Computer Vision and Pattern Recognition, Vol. 1, Madison, WI, USA. https://doi.org/10.1109/CVPR.2003.1211347.

[25] Claburn T (n.d.), Yahoo's CAPTCHA security reportedly broken. Available online: https://www.informationweek.com/government/yahoo-s-captcha-security-reportedly-broken.

[26] Bursztein E, Bethard S, Fabry C, Mitchell JC & Jurafsky D (2010), How good are humans at solving CAPTCHAs? A large-scale evaluation. Proceedings of the 2010 IEEE Symposium on Security and Privacy, pp. 399–413. https://doi.org/10.1109/SP.2010.31.

[27] Yampolskiy, R. V. (2012). *Human computer interaction-based CAPTCHA: A survey*. International Journal of Human-Computer Studies, 70(11), 831–866. https://doi.org/10.1016/j.ijhcs.2012.05.009.

[28] Meng, X., Liu, X., & Wang, Y. (2021). *Voice CAPTCHA authentication via deep learning*. Computers & Security, 104, 102202. https://doi.org/10.1016/j.cose.2021.102202.

[29] Zhang, H., Liu, J., Wang, Y., & Liu, X. (2022). CAPTCHA breaking using vision transformers. Pattern Recognition Letters, 155, 50-57. https://doi.org/10.1016/j.patrec.2021.12.010.

[30] X. Nian, J. Liu, Y. Han, and Y. Zhang, "A deep learning-based attack on text CAPTCHAs using object detection techniques," IET Information Security, vol. 17, no. 2, pp. 85–94, Mar. 2023, https://doi.org/10.1049/ise2.12047.

[31] reCAPTCHA (n.d.), available online: https://www.google.com/recaptcha/about.

[32] IRCTC Train Search (n.d.), available online: https://www.irctc.co.in/nget/train-search.

[33] NLP CAPTCHA (n.d.), available online: https://nlpcaptcha.in/en/index.html.

[34] SBI Online (n.d.), available online: https://www.onlinesbi.com.

[35] Online OCR (n.d.), available online: https://www.onlineocr.net.

[36] Free Online OCR (n.d.), available online: www.free-online-ocr.com.

[37] New OCR (n.d.), available online: https://www.newocr.com.

[38] i2OCR (n.d.), available online: http://www.i2ocr.com.

[39] CAPTCHA (n.d.), available online: http://www.captcha.net/.

[40] HubSpot Blog (n.d.), Control spam by integrating Google Invisible reCAPTCHA on your WordPress site. available online: https://blog.hubspot.com/website/control-spam-integrating-google-invisible-recaptcha-wordpress-site.