Bulletin of Electrical Engineering and Informatics
Vol. 15, No. 4, August 2026, pp. 3347~3355
ISSN: 2302-9285, DOI: 10.11591/eei.v15i4.10147

A novel CAPTCHA mechanism: virtual keyboard for robust user authentication

Jyoti B Deone, Jyoti Kundale, Sumedha Bhagwat
Department of Information Technology, Ramrao Adik Institute of Technology, D Y Patil Deemed to be University, Navi Mumbai, India

Article Info

Article history:

Received Feb 24, 2025
Revised Mar 11, 2026
Accepted Apr 19, 2026

Keywords:

Authentication
CAPTCHA
Optical character recognition
Security
Threats

ABSTRACT

In the current digital age, the growing prevalence of cybersecurity threats has heightened the importance of securing online platforms. Completely automated public turing test to tell computers and humans apart (CAPTCHA) mechanisms are commonly employed to protect these platforms from spam, a prevalent type of online identity theft, and to strengthen defenses against automated attacks. This study introduces an innovative method to improve security against such automated threats. A key feature of the proposed system is the implementation of a virtual keyboard, which plays a central role in user authentication. The system utilizes a text recognition algorithm to authenticate users in real-time, effectively minimizing the risk of unauthorized access and ensuring enhanced security. Furthermore, the system is capable of detecting and managing imprecise user inputs, thereby increasing its reliability. Experimental findings highlight the system's efficacy in mitigating comment spam on blogs, demonstrating its robustness against optical character recognition (OCR)-based attacks. Achieving an 87% success rate in user authentication, the system proves to be a strong defense against automated threats, reinforcing its overall security framework. This study underscores the potential of the proposed approach to advance cybersecurity measures for online platforms.

Corresponding Author:

Jyoti B Deone
Department of Information Technology, Ramrao Adik Institute of Technology
D Y Patil Deemed to be University
Navi Mumbai, India
Email: jyoti.deone@rait.ac.in

1. INTRODUCTION

Completely automated public turing test to tell computers and humans apart (CAPTCHA) is a fundamental security measure employed to differentiate between human users and automated bots. Its purpose is to present challenges or tasks that are straightforward for humans to solve but challenging for automated programs to bypass or interpret [1]. The primary goal of CAPTCHA is to protect online platforms from spam bots that attempt to submit forms, post unwanted content, or extract sensitive information. The importance of CAPTCHA cannot be overstated in today's digital landscape, where cybersecurity threats are increasingly sophisticated. As computer vision and machine learning technologies evolve, bots become more adept at circumventing traditional CAPTCHA methods. This ongoing evolution underscores the need for continuous innovation in CAPTCHA design to maintain its effectiveness against emerging threats [2], [3].

Traditional text-based CAPTCHA systems face multiple vulnerabilities. Optical character recognition (OCR) technology has advanced significantly, enabling automated bots to decipher distorted text with increasing accuracy. Additionally, CAPTCHA farms—where human workers are employed to solve CAPTCHAs in bulk for malicious actors—pose a significant threat to conventional authentication systems.

These farms exploit the human-solvable nature of CAPTCHAs while bypassing their intended security purpose, making them available as a service to attackers. In recent years, advancements in artificial intelligence have introduced new challenges to CAPTCHA security. Adversaries leverage sophisticated algorithms to bypass text-based CAPTCHAs, highlighting the limitations of conventional approaches [4], [5]. To address these challenges, novel approaches like graphical CAPTCHA authentication have emerged, integrating graphical elements and synthetic artifacts to enhance security while ensuring a seamless user experience. This study aims to address the shortcomings of existing CAPTCHA schemes by proposing a novel graphical CAPTCHA authentication system [6], [7].

By incorporating visually complex elements and intuitive challenges, this system seeks to provide robust security against automated attacks while ensuring accessibility and user-friendliness. There are various CAPTCHA methods available, including image-based, voice-based, video-based, text-based, audio-based, and puzzle-based approaches. The most commonly used is text-based CAPTCHA, but text-based CAPTCHAs have significant drawbacks, including vulnerability to OCR attacks [8], [9]. In text-based CAPTCHA systems, challenges include easy verification by OCR techniques and difficulty for visually impaired users. In the case of image-based CAPTCHAs, recognition can sometimes be difficult [10]. Not every person understands English, as they may speak their local language, which is a major issue related to audio-based CAPTCHAs. Due to video size and web performance degradation, video-based CAPTCHAs are not suitable for all cases [11]. Our proposed system specifically addresses the CAPTCHA farm problem by implementing several countermeasures: i) using a specialized virtual keyboard that prevents standard automated input methods, ii) incorporating dynamic image distortion that makes pattern recognition difficult even for human-assisted attacks, and iii) implementing time-based validation and error-tracking mechanisms that detect suspicious solving patterns characteristic of farm operations. The virtual keyboard also provides protection against shoulder surfing attacks by displaying a randomized layout and requiring on-screen interaction, making it difficult for observers to capture authentication credentials.

2. BACKGROUND AND LITERATURE REVIEW

Traditional text-based CAPTCHA systems are increasingly vulnerable to OCR and deep learning–based attacks, as CNNs can accurately recognize distorted characters [12], GANs can denoise and segment CAPTCHA images [13] and ensemble models can adapt to new designs with high success rates [14]. To counter this, recent research introduces rotating 3D artifacts of varying sizes combined with letters or numbers, which significantly confuse machine learning models [15] and exploit artifacts that disrupt visual recognition algorithms [16] while remaining highly usable for humans, achieving nearly 98% user success. Earlier defenses relying on added noise and distortion often reduced readability without fully preventing attacks, underscoring the need for balanced, multi-layered solutions. Advanced systems such as reCAPTCHA, developed at Carnegie Mellon University [17], and techniques used by Google, including mouse-movement analysis and cookie-based verification, demonstrate how combining visual and behavioral cues can improve CAPTCHA robustness while preserving usability.

2.1. Limitations of existing system

Recent research indicates that many real-world CAPTCHA implementations exhibit lower than-desired security levels, revealing shortcomings in existing resistance methods. In this context, we aim to identify and outline several key issues that contribute to these security concerns:

- OCR threat: OCR technology poses a significant threat to CAPTCHA security. OCR can analyze and interpret text within images, making it capable of deciphering traditional text-based CAPTCHAs [3], [18]. This undermines the effectiveness of CAPTCHAs in distinguishing humans from bots. Implementations must consider techniques that counter OCR, such as using distorted text or graphical challenges that are difficult for OCR algorithms to interpret accurately.
- CAPTCHA farms: CAPTCHA farms represent a significant vulnerability where human workers are employed to solve CAPTCHAs in bulk for malicious actors. These farms operate as services that attackers can purchase to bypass CAPTCHA protections, effectively circumventing the security measure regardless of its complexity. Traditional CAPTCHAs that are designed to be human-solvable become exploitable through this model.
- Implementation errors: flaws in CAPTCHA system design or implementation can introduce vulnerabilities that attackers exploit. This includes coding errors, misconfigurations, or inadequate security measures that compromise the integrity of CAPTCHA challenges. Regular security audits and testing can help identify and mitigate implementation flaws.
- Adaptability and learning curve: introducing new CAPTCHA methods may require users to adapt to unfamiliar authentication processes. Effective education and user guidance are crucial to facilitate

successful adoption and minimize user frustration. Ensuring that CAPTCHAs are intuitive and user-friendly encourages user acceptance and compliance.
- Forgetfulness: CAPTCHAs that rely on recalling specific images or color sequences can be challenging for users, leading to frequent authentication failures. Designing CAPTCHAs with simpler and more memorable challenges reduces the likelihood of user errors and enhances overall usability.

2.2. Purpose of the study

The objectives of this study are:
- To enhance cybersecurity by implementing graphical authentication at the CAPTCHA level, using visual challenges to improve security and user experience while reducing automated bot attacks and mitigating CAPTCHA farm exploitation.
- To address shoulder surfing vulnerabilities through the implementation of a specialized virtual keyboard that provides superior security compared to standard keyboards.
- To provide a comparative analysis of the proposed virtual keyboard against standard keyboards and compare the method with existing image-based CAPTCHA protection methods.
- To ensure the system integrates seamlessly with existing security protocols and offers customizable options to meet specific application requirements, ensuring flexibility, and adaptability.

3. METHOD

CAPTCHAs play a crucial role in preventing bots from accessing various computer services and gathering sensitive information. They also help by providing a layer that can differentiate between bots and valid users. However, attackers can use OCR bots to bypass these layers, and CAPTCHA farms can exploit human-solvable challenges [19]. To address these challenges, our proposed graphical CAPTCHA authentication system incorporates images of daily-use objects into CAPTCHAs, making it difficult for attacking bots to solve them while remaining easy for humans to decipher. Our approach aims to introduce a new type of CAPTCHA scheme that emphasizes user engagement by using graphical images like "daily-use objects." The following steps are shown in Figure 1:

a. Step 1: the first module applies "salt and pepper" noise and lines to the base image, adding random black and white pixels and graphical elements. This noise increases the CAPTCHA's complexity, making it harder for automated recognition (e.g., OCR) but still readable by humans [3].
b. Step 2: the altered image from Step 1 is then shown in a graphical user interface (GUI). This GUI presents the CAPTCHA to the user, allowing them to view the distorted image and attempt to identify the object.
c. Step 3: a virtual keyboard is available in the GUI for user input, prohibiting physical keyboard use. The virtual keyboard is designed with special characters to add complexity beyond typical keyboards and provides protection against shoulder surfing attacks through its randomized layout and on-screen interaction requirement.
d. Step 4: the user analyzes the CAPTCHA and inputs their answer. For example, if the word "BOTTLE" is embedded within the visual noise, the user identifies it and types "BOTTLE" using the virtual keyboard. This input is converted to lowercase to make the system case insensitive.
e. Step 5: the system then validates the user's input by comparing it to the correct answer stored in the database. This validation confirms whether the user is human or possibly an automated bot. Time-based validation and pattern analysis help detect CAPTCHA farm activities.
f. Step 6: once the CAPTCHA is validated, the user gains access to the system's protected areas or functions, such as logging in or completing a particular task. Figure 1 describes the system architecture using a graphical representation. This work aims to create a distinctive and robust CAPTCHA by utilizing graphical images and a virtual customized keyboard, as depicted in the system architecture shown in Figure 1. Subsequently, this system is subjected to testing on various OCR websites [11], [20]. In addition, the images underwent testing with human subjects to assess the system's functionality in real-world conditions.

This work aims to create a distinctive and robust CAPTCHA by utilizing graphical images and a virtual customized keyboard, as depicted in the system architecture shown in Figure 1. Subsequently, this system is subjected to testing on various OCR websites. In addition, the images underwent testing with human subjects to assess the system's functionality in real world conditions.

a. Image distortion

In this phase of CAPTCHA generation, we modify the base image to challenge automated recognition systems like OCR while remaining easy for humans. We introduce noise elements like salt and pepper noise, scattering black and white pixels randomly to disrupt patterns. Additionally, graphical elements such as overlapping lines add visual complexity and distortion shown in Figure 2. These alterations aim to thwart OCR algorithms while ensuring real users can still decipher the content [21]. This approach underscores the balance

between security and usability in CAPTCHA design, enhancing resistance to automated attacks while preserving accessibility for human users.

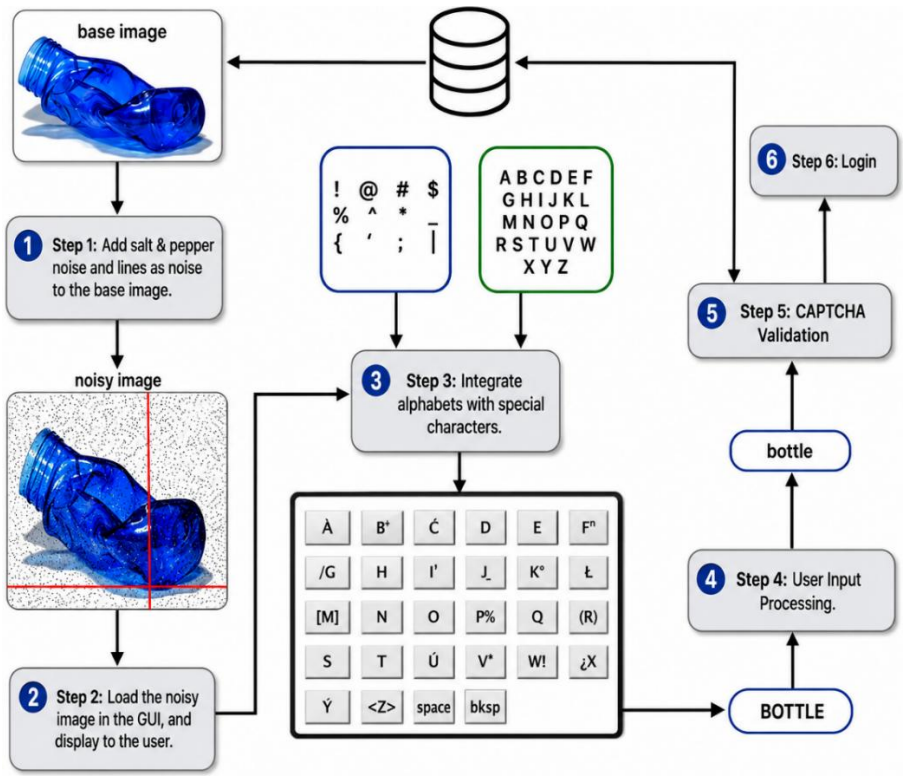

Figure 1. System architecture

Figure 2. Comparison between base and distorted image

b. Display distorted image

In this module, the distorted image generated in Step 1 is displayed to the user through a user-friendly graphical interface. This interface facilitates user interaction by presenting the distorted image clearly and allowing users to decipher its contents. Users can engage with the interface to understand and respond to the graphical challenge effectively [22].

c. Virtual keyboard integration

In the graphical CAPTCHA interface, a virtual keyboard, as shown in Figure 3, is integrated to facilitate user input. This specialized keyboard includes unique characters, setting it apart from conventional keyboards. Users interact with this virtual keyboard to enter responses, while simultaneous disabling of the physical keyboard enhances security [23], [24]. By employing this approach, the system prevents automated bots from exploiting standard keyboard input methods during CAPTCHA challenges, thereby ensuring the effectiveness of the authentication process. The virtual keyboard's distinct design contributes to the system's resilience against automated attacks and provides significant advantages over standard keyboards in preventing shoulder surfing attacks through its randomized layout and on-screen interaction requirement. This makes it difficult for observers or recording devices to capture authentication credentials, reinforcing the security measures in place for user verification [25].

Figure 3. Virtual keyboard

d. User interaction and input

Users interact with the graphical CAPTCHA by deciphering the presented challenge and entering their responses using the virtual keyboard. The input provided by users is processed for validation in a case-insensitive manner, ensuring that variations in text casing do not affect the verification process, thereby enhancing user convenience during authentication shown in Figure 4.

e. Validation process

The user's input is validated by comparing it with the expected solution stored in the database. This comparison assesses the accuracy of the user's response to determine if they are human or potentially an automated bot. An incorrect response counter tracks errors, triggering a block and initiating a 60-second cooldown period if the error threshold is exceeded, preventing potential abuse of the authentication system shown in Figure 5.

Figure 4. CAPTCHA validation page

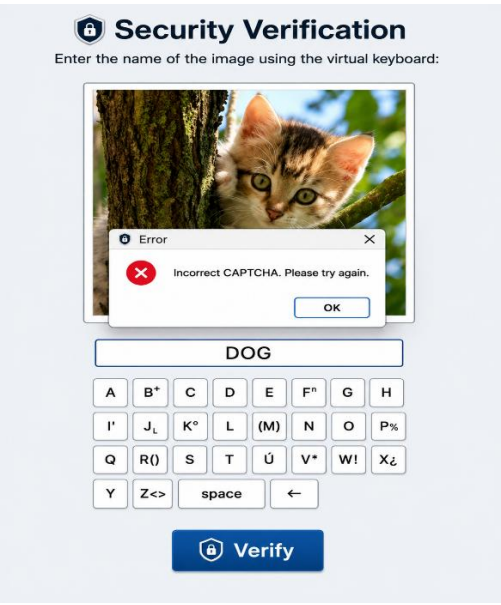

Figure 5. Incorrect CAPTCHA

f. Access granted

Upon successful validation of the CAPTCHA input, the user is granted access to the intended functionality, which could include logging into a secure system or completing specific tasks within the authenticated environment [23]. This validation step ensures that the user is verified as human and not an automated bot, thereby maintaining the security of the system. Access to the desired functionality is contingent upon accurate completion of the CAPTCHA challenge, affirming the user's legitimacy and permitting interaction with the secure platform or services.

4. RESULTS AND DISCUSSION

This section presents an assessment of the proposed graphical CAPTCHA system based on different criteria and examines the outcomes. One of the system's main assets is its ability to accurately identify and reject bots, resulting in high efficiency. Hence, we carried out a comprehensive study with a sample size of more than 200 users to assess the effectiveness of the suggested CAPTCHA in real-life scenarios. Through the examination of user feedback and data gathered in this study, we evaluated the efficiency of the CAPTCHA by considering factors such as accuracy, readability, and resistance against OCR bots.

Readability: systems readability is the ease in identifying the image, user feedback regarding how easy it was to solve the presented CAPTCHA challenges was evaluated as users rated the CAPTCHA's on a scale from 1 (very easy) to 5 (very difficult). The analysis showed positive results, with 47% of users rating the CAPTCHAs as a 1 (indicating very easy), 24% rating them as a 2, and 21% rating them as a 3 (neutral) as shown in Figure 6.

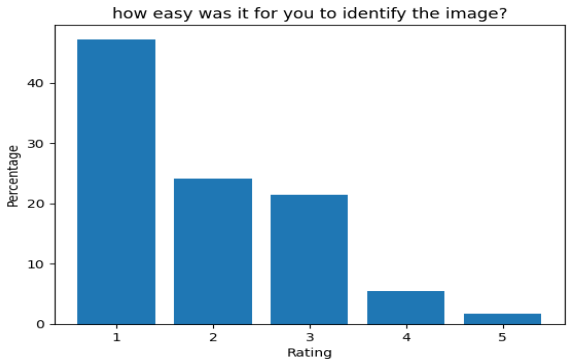

Figure 6. User responses for ease of object/element identification

Accuracy: the accuracy of the graphical CAPTCHA system is measured by users' ability to correctly identify objects within the images as shown in Figure 7. User feedback revealing an 86.3% ease of use rate demonstrates the system's effectiveness in verifying users and thwarting bots. This high rate of user acceptance reflects the system's success in providing secure and user-friendly authentication. The graphical challenges presented are sufficiently clear and interpretable, ensuring reliable identification and validation of legitimate users while deterring automated bots.

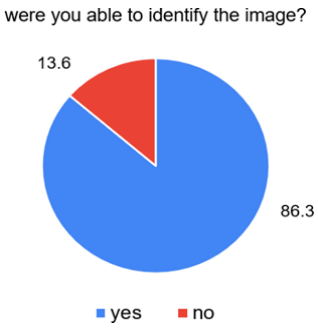

Figure 7. Systems accuracy

Resistance against OCR bots: graphical CAPTCHA images were tested against OCR bots like EditPad [15], Astica AI [16], and image recognize [17], showing strong resistance to OCR attacks. Bots couldn't decipher the CAPTCHA objects due to complex graphical elements and dynamic challenges like distortion and rotation. This approach enhances authentication system security against automated threats.

Figure 8 shows AI-based image analysis interface showing object detection, image captioning, and confidence scores for recognized objects, demonstrating automated scene understanding. Figure 9 presents the object detection output generated by the recognition model, where multiple objects within a crowded scene are

identified and highlighted using bounding boxes. The detected objects are listed alongside their corresponding confidence scores, demonstrating the system's capability to accurately recognize and classify visual entities. These recognized object labels serve as candidate inputs for the CAPTCHA validation process. Figure 10 shows customized virtual keyboard with randomized characters and special symbols, designed to enhance CAPTCHA security against automated attacks.

Figure 8. Image test against OCR bots

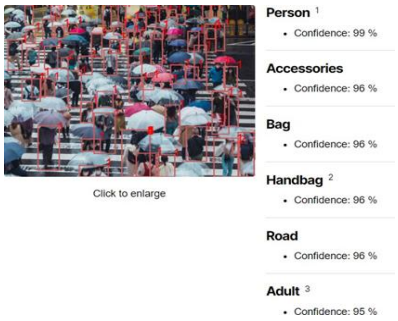

Figure 9. Online OCR bot test at image recognizer

Figure 10. Online OCR bot test at editpad

5. CONCLUSION

The increasing sophistication of OCR bots poses a heightened risk of automated attacks, underscoring the need for robust defenses against these evolving threats. Conventional CAPTCHA systems have proven vulnerable to OCR techniques, rendering text-based schemes ineffective. In response, our proposed graphical CAPTCHA authentication system introduces a novel approach to enhance security. Our system leverages graphical images of everyday objects, such as bottles, tables, and cards, integrated with a customized virtual keyboard to create engaging challenges that are difficult for bots to decipher. By utilizing graphical elements and user-friendly interfaces, we strike a balance between security and usability. During testing, our system demonstrated strong human performance, with over 87% success in user authentication, highlighting its effectiveness in verifying legitimate users. Additionally, our approach exhibited significant resistance to OCR-based attacks, with advanced bots achieving less than optimal accuracy in solving our CAPTCHAs. Overall, our graphical CAPTCHA authentication system represents an innovative step towards improving website security and usability. By integrating engaging graphics and customized interactions, we aim to provide a secure authentication process that is user-friendly while effectively thwarting automated threats, thus enhancing the overall cybersecurity posture of web-based services.

FUNDING INFORMATION

Authors state no funding involved.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Jyoti B Deone	✓	✓			✓	✓		✓	✓	✓		✓	✓	
Jyoti Kundale	✓	✓	✓		✓	✓	✓		✓	✓				
Sumedha Bhagwat	✓	✓		✓	✓	✓			✓	✓	✓			

C : **C**onceptualization
M : **M**ethodology
So : **So**ftware
Va : **Va**lidation
Fo : **Fo**rmal analysis
I : **I**nvestigation
R : **R**esources
D : **D**ata Curation
O : Writing - **O**riginal Draft
E : Writing - Review & **E**diting
Vi : **Vi**sualization
Su : **Su**pervision
P : **P**roject administration
Fu : **Fu**nding acquisition

CONFLICT OF INTEREST STATEMENT

The authors declare that there is no conflict of interest regarding the publication of this paper.

DATA AVAILABILITY

The data that support the findings of this study are available from the corresponding author upon reasonable request. The datasets generated and analyzed during the current study consist of experimental results obtained from user evaluations and OCR testing of the proposed graphical CAPTCHA authentication system. No publicly available dataset was used in this research.

REFERENCES

[1] Y. Raut, S. Pote, H. Boricha, and P. Gunjgur, "A Robust Captcha Scheme for Web Security," in *2022 6th International Conference on Computing, Communication, Control and Automation (ICCUBEA)*, Aug. 2022, pp. 1–6, doi: 10.1109/ICCUBEA54992.2022.10011113.

[2] M. Umar, "A Review on Evolution of various CAPTCHA in the field of Web Security," *International Journal for Research in Applied Science and Engineering Technology*, vol. 10, no. 2, pp. 72–78, Feb. 2022, doi: 10.22214/ijraset.2022.40190.

[3] A. Dionysiou and E. Athanasopoulos, "SoK: Machine vs. machine – A systematic classification of automated machine learning-based CAPTCHA solvers," *Computers and Security*, vol. 97, pp. 1-14, Oct. 2020, doi: 10.1016/j.cose.2020.101947.

[4] A. Thakur, Bhavishya, and P. Singh, "A Novel Deep Learning Based Fully Automated Framework for Captcha Security Vulnerability Checking," in *Lecture Notes in Networks and Systems*, vol. 791, 2024, pp. 431–443, doi: 10.1007/978-981-99-6755-1_33.

[5] R. Cheng *et al.*, "MetaFL: Privacy-preserving User Authentication in Virtual Reality with Federated Learning," in *SenSys 2024 - Proceedings of the 2024 ACM Conference on Embedded Networked Sensor Systems*, Nov. 2024, pp. 54–67, doi: 10.1145/3666025.3699322.

[6] Y. Zhang, H. Gao, G. Pei, S. Luo, G. Chang, and N. Cheng, "A survey of research on CAPTCHA designing and breaking techniques," in *Proceedings - 2019 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)*, Aug. 2019, pp. 75–84, doi: 10.1109/TrustCom/BigDataSE.2019.00020.

[7] Y. Zi, H. Gao, Z. Cheng, and Y. Liu, "An End-to-End Attack on Text CAPTCHAs," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 753–766, 2020, doi: 10.1109/TIFS.2019.2928622.

[8] D. Kumar, R. Singh, and S. S. Bamber, "Your CAPTCHA Recognition Method Based on DEEP Learning Using MSER Descriptor," *Computers, Materials & Continua*, vol. 72, no. 2, pp. 2981–2996, 2022, doi: 10.32604/cmc.2022.024221.

[9] C. Adams, *One-Time Password*. Springer, 2005, doi: 10.1007/978-1-4419-5906-5_785.

[10] A. A. Süzen, "UNI-CAPTCHA: A Novel Robust and Dynamic User-Non-Interaction CAPTCHA Model Based on Hybrid biLSTM+Softmax," *Journal of Information Security and Applications*, vol. 63, Dec. 2021, doi: 10.1016/j.jisa.2021.103036.

[11] M. Tang, H. Gao, Y. Zhang, Y. Liu, P. Zhang, and P. Wang, "Research on Deep Learning Techniques in Breaking Text-Based Captchas and Designing Image-Based Captcha," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 10, pp. 2522–2537, Oct. 2018, doi: 10.1109/TIFS.2018.2821096.

[12] L. A. Alreshoodi and S. A. Alsuhibany, "A Proposed Methodology for Detecting Human Attacks on Text-based CAPTCHAs," *International Journal of Engineering Research and Technology*, vol. 13, no. 4, pp. 625–630, Apr. 2020, doi: 10.37624/ijert/13.4.2020.625-630.

[13] H. S. Lallie *et al.*, "Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic," Computers and Security, vol. 105, p. 102248, Jun. 2021, doi: 10.1016/j.cose.2021.102248.

[14] I. Akrout, A. Feriani, and M. Akrout, "Hacking Google reCAPTCHA v3 using Reinforcement Learning," *arXiv*, 2019, doi: 10.48550/arXiv.1903.01003.

[15] X. Xu, L. Liu, and B. Li, "A survey of CAPTCHA technologies to distinguish between human and computer," *Neurocomputing*, vol. 408, pp. 292–307, Sep. 2020, doi: 10.1016/j.neucom.2019.08.109.

[16] A. Acien, A. Morales, J. Fierrez, and R. Vera-Rodriguez, "BeCAPTCHA-Mouse: Synthetic mouse trajectories and improved bot detection," *Pattern Recognition*, vol. 127, Jul. 2022, doi: 10.1016/j.patcog.2022.108643.

[17] S. Hosseini, A. E. Nezhad, and H. Seilani, "Botnet detection using negative selection algorithm, convolution neural network and classification methods," *Evolving Systems*, vol. 13, no. 1, pp. 101–115, Feb. 2022, doi: 10.1007/s12530-020-09362-1.
[18] Z. Veličković and Z. Milivojević, "Web Applications Protection from Automated Attacks by the reCAPTCHA API," *Journal of Mechatronics, Automation and Identification Technology*, vol. 5, no. 2, pp. 7–11, 2020.
[19] S. Tian and T. Xiong, "A Generic Solver Combining Unsupervised Learning and Representation Learning for Breaking Text-Based Captchas," in *The Web Conference 2020 - Proceedings of the World Wide Web Conference (WWW)*, Apr. 2020, pp. 860–871, doi: 10.1145/3366423.3380166.
[20] D. Hitaj, B. Hitaj, S. Jajodia, and L. V. Mancini, "Capture the Bot: Using Adversarial Examples to Improve CAPTCHA Robustness to Bot Attacks," *IEEE Intelligent Systems*, vol. 36, no. 5, pp. 104–112, Sep. 2021, doi: 10.1109/MIS.2020.3036156.
[21] A. O. Adesina, P. S. Ayobioloja, I. C. Obagbuwa, T. J. Odule, A. A. Afolorunso, and S. A. Ajagbe, "An Improved Text-Based and Image-Based CAPTCHA Based on Solving and Response Time," *Computers, Materials & Continua*, vol. 74, no. 2, pp. 2661-2675, 2022, doi: 10.32604/cmc.2023.031245.
[22] Q.-q. Wu, J.-j. Lang, S.-j. Wei, M.-l. Ren, and E. Seidel, "A novel construction of correlation-based image CAPTCHA with random walk," *Advances in Intelligent Systems and Computing*, vol. 670, 2019, pp. 339–346, doi: 10.1007/978-981-10-8971-8_31.
[23] N. D. Trong, T. H. Huong, and V. T. Hoang, "New Cognitive Deep-Learning CAPTCHA," *Sensors*, vol. 23, no. 4, 2023, doi: 10.3390/s23042338.
[24] N. Dinh and L. Ogiela, "Human-artificial intelligence approaches for secure analysis in CAPTCHA codes," *EURASIP Journal on Information Security*, vol. 2022, 2022, doi: 10.1186/s13635-022-00134-9.
[25] A. Bera, D. Bhattacharjee, and H. P.H. Shum, "Two-stage human verification using HandCAPTCHA and anti-spoofed finger biometrics with feature selection," *Expert Systems with Applications*, vol. 171, 2021, doi: 10.1016/j.eswa.2021.114583.

BIOGRAPHIES OF AUTHORS

Jyoti B Deone is currently working as an Assistant Professor at the Ramrao Adik Institute of Technology, School of Engineering, DY Patil Deemed to be University, Nerul, Navi Mumbai, Maharashtra, India. She is completed her doctorate in Computer Engineering at Dr. Babasaheb Ambedkar Marathwada University, Chhatrapati Sambhajinagar (Aurangabad), in 2025. She has a total of 16 years of teaching and research experience. She has published more than 20 research papers in Scopus-indexed international journals and conferences. Additionally, she has published 3 patents and copyright under her name. Her area of specialization is data science and machine learning. She has been a reviewer to reputed international conferences and journals. She is a member of the professional body ISTE. She can be contacted at email: jyoti.deone@dypatil.edu.

Dr. Jyoti Kundale is currently serving as an Assistant Professor in the Department of Information Technology at Ramrao Adik Institute of Technology (RAIT), School of Engineering, D Y Patil Deemed to be University, Nerul, Navi Mumbai, Maharashtra, India. She has 16 years of teaching and professional experience in the field of computer science and information technology. She obtained her Ph.D. from the University of Mumbai in 2023. Her academic contributions include the publication of 6 research papers in Scopus-indexed journals and more than 25 papers in international conferences. She has also been granted 4 patents and copyrights to her credit. Her research interests include machine learning, big data analytics, deep learning, computer vision, and pattern recognition. She has served as a reviewer for reputed international journals and conferences and has also chaired technical sessions at several prestigious international conferences. She has successfully received one Faculty Development Program (FDP) grant and is currently guiding two Ph.D. research scholars. She is an active member of the professional bodies Association for Computing Machinery (ACM) and Indian Society for Technical Education (ISTE). She can be contacted at email: jyoti.kundale@dypatil.edu.

Sumedha Bhagwat received her PG and Ph.D. degree in Computer Engineering from the Ramrao Adik Institute of Technology (RAIT), Mumbai University. She served in various roles in teaching since 2014. She has been Assistant Professor at RAIT since 2014, where she has been dedicated teaching and mentoring students in various aspects of computer science and engineering. She has authored journal publications and presented research at 15 conferences. She has been filed one patent and holds two copyrights and two book chapters. Additionally, she has successfully handled one consultancy project. Her research interests lie in the fields of image processing and computer vision. She can be contacted at email: sumedha.bhagwat@dypatil.edu.