International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2025.0039
e ISSN: 2584-2854
Volume: 03
Issue:02 February 2025
Page No: 238-246

A Comprehensive Survey on AI-Powered Personalized CAPTCHA Systems Leveraging User Preferences and Behavior

S. Divinstar[1], R. Jamaludeen[2], S. Gokulnath[3], T. Periyasamy[4]
[1,2,3]Department of Information Technology, Sri Manakula Vinayagar Engineering College (SMVEC), Madagadipet, Puducherry, India.
[4]Assistant Professor Department of Information Technology, Sri Manakula Vinayagar Engineering College, Puducherry, India
***Email ID:** periyasamy2204@gmail.com[1]*

Abstract
This research paper aims to present a detailed survey of recent advancements in CAPTCHA systems utilizing Artificial Intelligence (AI) to generate personalized, image-based and text based CAPTCHA puzzles for the user's. By analyzing the user's data such as preferences, browsing history, and behavioral data, these CAPTCHA systems learn the individual users while enhancing security. The system also includes time-sensitive constraints to counter third-party bot attacks. The paper dives into the evolution of CAPTCHA systems, focusing on AI-based CAPTCHA generation, image-based CAPTCHAs, and methods used by bots to crack these security measures. We also go through many technical algorithms and methods such as behavior analysis, GANs, CNNs, and reinforcement learning that make CAPTCHAs more secure and adaptive.
***Keywords:** CAPTCHA, AI, Machine Learning, User Preferences, Web Scraping, Behavioral Analysis, Time-limited CAPTCHA, Image-based CAPTCHA, Bot Attacks, RNN, LSTM, CNN, GAN, Reinforcement Learning.*

1. Introduction
CAPTCHAs stands for (Completely Automated Public Turing test to tell Computers and Humans Apart) serves as a critical security mechanism in the act of protecting online platforms from bot's attack and automated misuse [1-5]. Since their creation, CAPTCHA systems have evolved from simple text-based puzzles to more sophisticated challenge's such as image- based, audio and video-based CAPCTHA and even biometric ones. As technology progresses, the capabilities and the threat's that bots pose have also advanced dramatically [6]. Modern bots are now equipped with machine learning algorithms that enable them to solve traditional CAPTCHAs with great accuracy. This calls for the need for the development of more robust CAPTCHA systems that not only verify human users effectively but also enhance the overall user experience [7-10]. Thus the need for personalized, AI-powered CAPTCHA's has emerged as a potential solution to this problem. The Crucial aspect of these systems is that they can adapt and change their challenges based on the user's behavior and preferences, thereby improving security and usability. This survey paper talks about the advancements in CAPTCHA systems, focusing on solutions that can leverage AI, user preferences, behavioral analysis, and time-sensitive constraints in order to improve security whilst maintaining usability and user-privacy [11-13]. We also discuss the implications of these solutions for both security and user experience.

2. Problem Statement
Traditional CAPTCHA systems are facing an existential challenge as modern bots, powered by machine learning, deep learning, and behavioral mimicking, become increasingly capable of bypassing them [14]. Key issues include:

Security Vulnerability: The primary purpose of CAPTCHA systems is to differentiate between human users and automated bots. However, bots utilizing advanced techniques such as Optical Character Recognition (OCR), machine learning, and deep learning can solve CAPTCHAs designed for humans, rendering these systems ineffective. This vulnerability raises significant security concerns, especially for sensitive applications such as online banking and e-commerce, where

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2025.0039
e ISSN: 2584-2854
Volume: 03
Issue:02 February 2025
Page No: 238-246

unauthorized access can have serious consequences [15].

User Experience: Many CAPTCHA systems are inherently frustrating for users. When challenges are too difficult or time-consuming, they can lead to increased dropout rates as users abandon tasks or websites. Studies have shown that poor user experience with CAPTCHA systems directly impacts user satisfaction and can harm brand reputation. Therefore, creating a CAPTCHA that is both secure and user-friendly is essential.

Accessibility: CAPTCHA systems often pose significant challenges for users with disabilities. Text and image recognition tasks are particularly problematic for visually impaired individuals, as they cannot perceive visual in- formation. Therefore, CAPTCHA designs must consider inclusivity to ensure that all users can access online services without discrimination. The challenge is to design CAPTCHA systems that strike a balance between security, accessibility, and user-friendliness. AI-powered CAPTCHA systems offer the ability to personalize challenges and dynamically adjust their difficulty based on user behavior and performance, making it harder for bots to crack them [16-19].

3. Motivation for this Project

The motivation for developing AI-powered personalized CAPTCHA systems stems from the need to enhance the security and user experience of online interactions [20]. With the increasing sophistication of bots capable of solving traditional CAPTCHAs, there is a pressing need for more resilient CAPTCHA designs. Personalized CAPTCHAs adapt to individual users by tailoring challenges based on their browsing history, behavioral patterns, and preferences. By leveraging AI models and real-time data, personalized CAPTCHA systems can dynamically generate challenges that are both secure and user-friendly. This personalization not only helps in thwarting automated attacks but also enhances user engagement by providing a smoother experience. Furthermore, the integration of machine learning algorithms allows for continuous improvement and adaptation of the CAPTCHA system based on user interactions, ensuring that it remains effective against evolving threats. Moreover, the rise of mobile and touch devices necessitates CAPTCHA solutions that are adaptive and consider different user interaction patterns. Personalized CAPTCHA systems can cater to the specific interaction habits of users, thereby improving accessibility and usability across diverse platforms [21-23].

4. Existing Captcha Systems

CAPTCHA systems have undergone significant evolution since their inception, moving from simple text-based challenges to more complex, image-based, and behavioral systems. Below, we explore some of the key categories of existing CAPTCHA systems [24].

4.1.Text-based CAPTCHAs

Text-based CAPTCHAs were among the first CAPTCHA systems implemented. These systems presented distorted characters or numbers for users to identify. Despite their simplicity, text-based CAPTCHAs have several drawbacks. They are vulnerable to bots using OCR techniques, which can decipher the distorted characters with high accuracy [25-28]. Additionally, they can be frustrating for users who may struggle to read the distorted text. The reliance on visual distortions makes these CAPTCHAs particularly challenging for users with visual impairments. Various solutions, such as re-CAPTCHA, attempted to enhance security by requiring users to identify two words, one of which is the distorted text, while the other helps digitize books. However, as machine learning technologies have improved, so too have the capabilities of bots to decode these challenges effectively. Furthermore, text-based CAPTCHAs are susceptible to brute-force attacks, where bots can attempt various combinations of characters until they successfully identify the correct one. This raises the question of whether text-based CAPTCHAs can continue to serve as a reliable security measure in the face of evolving technologies.

4.2.Image-Based CAPTCHAs

Image-based CAPTCHAs require users to identify objects or patterns in images, such as selecting all images that contain cars or traffic lights [29]. This type of CAPTCHA leverages the differences between human visual recognition abilities and computer vision systems. Users are often presented with a grid

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2025.0039
e ISSN: 2584-2854
Volume: 03
Issue:02 February 2025
Page No: 238-246

of images and must select specific ones based on the instructions given [30-33]. While image-based CAPTCHAs can be more engaging for users, they are not without their challenges. The rise of advanced CNNs (Convolutional Neural Networks) has enabled bots to learn how to recognize and select the correct images with increasing accuracy. Systems like Google's re-CAPTCHA v2, which initially utilized image recognition challenges, have seen improvements, but modern bots can still exploit weak- nesses in this system [34]. The difficulty level of image-based CAPTCHAs can vary significantly based on the quality of the images and the complexity of the tasks. Some users may find certain challenges too easy, while others may struggle with even simple tasks, leading to frustration and potential abandonment of the site. Additionally, accessibility issues persist with image-based CAPTCHAs. Visually impaired users may find these challenges impossible to complete, leading to calls for alternative solutions that cater to all users. This has prompted discussions about the ethical implications of CAPTCHA design and its impact on user inclusivity [35].

4.3.Behavioral-based CAPTCHAs

Behavioral CAPTCHAs analyze user interaction patterns, such as mouse movements, keystrokes, or touch gestures, to differentiate humans from bots [36-39]. By monitoring how users interact with a webpage, these CAPTCHAs offer a higher level of security by focusing on behavioral cues that are difficult for bots to mimic. However, this method has limitations. Bots are increasingly sophisticated in simulating human behavior, making it challenging for behavioral CAPTCHAs to maintain effectiveness. Moreover, the requirement to collect user interaction data raises privacy concerns, as it involves monitoring user behavior without explicit consent. In addition, the implementation of behavioral CAPTCHAs can result in increased complexity for developers [40-43]. Designing systems that accurately distinguish between human and bot behavior requires significant investment in data analysis and algorithm development. As such, the effectiveness of behavioral CAPTCHAs will depend on ongoing advancements in both AI technologies and our understanding of human behavior.

4.4.Audio and Video CAPTCHAs

Audio-based CAPTCHAs were designed to address accessibility issues, particularly for users with visual impairments [44]. Users are asked to transcribe a series of spoken characters or words. While this approach provides an alternative for visually impaired users, advancements in speech recognition and deep learning make it increasingly possible for bots to transcribe audio-based CAPTCHAs with high accuracy. These bots can analyze the audio and accurately reproduce the spoken content, effectively bypassing the security measures that audio CAPTCHAs are supposed to enforce. Furthermore, audio CAPTCHAs can be problematic for users in noisy environments, as background noise can interfere with their ability to hear and correctly transcribe the audio prompts. This variability in performance depending on the user's environment diminishes the effectiveness and reliability of audio CAPTCHAs as a security measure. Similarly, video CAPTCHAs ask users to describe a sequence of events or identify actions within a video [45-47]. This approach aims to create challenges that are complex for bots. However, video CAPTCHAs are also vulnerable to sophisticated AI algorithms capable of analyzing and interpreting video content, rendering them less effective than initially intended. Overall, while audio and video CAPTCHAs offer innovative alternatives to traditional text and image challenges, they present unique sets of challenges regarding accessibility, usability, and security [48].

4.5.AI-Based CAPTCHAs

AI-powered CAPTCHA systems represent the next step in the evolution of CAPTCHA technology. These systems utilize machine learning algorithms to generate personalized CAPTCHA challenges based on user behavior, preferences, and interaction patterns [49]. By incorporating advanced AI tech- niques such as GANs (Generative Adversarial Networks) and reinforcement learning, AI-based CAPTCHAs can become more dynamic and adaptable. AI-powered CAPTCHAs can analyze real-time data from users to generate unique challenges that are difficult for bots to predict. For example, using GANs allows for the generation of realistic

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2025.0039
e ISSN: 2584-2854
Volume: 03
Issue:02 February 2025
Page No: 238-246

CAPTCHA images that change with each session, reducing the likelihood that bots can learn and solve them [50]. This not only enhances security but also improves user engagement by creating a more tailored experience. Furthermore, these systems can continually learn and adapt to new bot strategies, ensuring they remain effective against emerging threats. The use of reinforcement learning can also help optimize the difficulty of CAPTCHA challenges based on user performance, ensuring a balance between security and user-friendliness. The implementation of AI-based CAPTCHAs represents a significant advancement in CAPTCHA technology, as they can learn from each interaction and improve over time, offering a more effective and engaging solution to the challenges posed by modern bots [51-52].

4.6.Existing Challenges in Captcha Systems

Despite significant advancements in CAPTCHA systems, several challenges remain:

Automation and Bots: Modern bots can bypass traditional CAPTCHA systems using deep learning tech- niques, OCR, and behavior simulation. This evolution necessitates CAPTCHA designs that can dynamically adapt to combat the advanced capabilities of these bots. As such, CAPTCHA systems must continually evolve to stay one step ahead of these automated threats.

User Fatigue: Repetitive and difficult CAPTCHA challenges can lead to user frustration and fatigue, ultimately reducing user engagement with web services. A seamless user experience is paramount, and CAPTCHA designs must strive to minimize disruption to the user's flow. Reducing the cognitive load required to complete CAPTCHAs is essential for maintaining user satisfaction.

Accessibility: CAPTCHA systems often overlook the needs of users with disabilities, particularly those who are visually impaired. Solutions must be inclusive and offer alternative verification methods that cater to various user needs without sacrificing security. This includes not only providing audio alternatives but also ensuring that visual CAPTCHAs can be solved by assistive technologies.

Privacy Concerns: Behavioral-based CAPTCHA systems that collect and analyze user data raise privacy concerns regarding how this data is stored and used. Ensuring user data is handled ethically and transparently is essential to gaining user trust and acceptance of advanced CAPTCHA solutions.

To address these challenges, CAPTCHA systems must leverage AI to create personalized, adaptive challenges that are harder for bots to crack while improving usability and accessibility.

5. Technical Overview: Algorithms for Personalized Captchas

To build a secure and adaptive CAPTCHA system, the following AI algorithms and techniques are crucial:

5.1.Behavior Analysis for Personalized CAPTCHA Generation

Algorithm: Recurrent Neural Networks (RNN) with Long Short-Term Memory (LSTM) CAPTCHA challenges that align with user behavior, making it harder for bots to predict the challenges.

Key Techniques

- **User Interaction Data Collection:** Collect data on user clicks, scrolls, and time spent on elements, allowing the system to understand user preferences and behaviors. This collected data serves as the foundation for generating tailored CAPTCHA challenges.
- **Personalized CAPTCHA Generation:** Generate CAPTCHAs based on user preferences and browsing history using LSTM. The model can learn from previous user interactions to tailor future challenges, thus increasing engagement and effectiveness.
- **Pre-training and Real-time Adaptation:** Pre-train the LSTM model on behavioral datasets and fine-tune it based on real-time interactions. This enables the system to adapt quickly to changes in user behavior, enhancing the personalization of CAPTCHA challenges.

5.2.Image-Based CAPTCHA Challenge Creation

Algorithm: Generative Adversarial Networks (GANs) GANs are an advanced neural network architecture that generates new data resembling the training data. In the context of CAPTCHA

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2025.0039
e ISSN: 2584-2854
Volume: 03
Issue:02 February 2025
Page No: 238-246

generation, GANs can be used to create unique, unpredictable CAPTCHA images in real-time. The Generator creates new CAPTCHA images, while the Discriminator ensures these images are challenging yet solvable for humans.

Key Techniques

- **Real-Time Image Generation:** Use GANs to generate a variety of CAPTCHA images dynamically based on user interaction data. This allows for unique challenges tailored to the specific user while minimizing predictability for bots.
- **Fine-tuning with GANs:** Use GANs such as Style GAN or DCGAN to produce dynamic CAPTCHA images. By training these models on diverse datasets, the generated images can closely resemble realistic images that are hard for bots to interpret while remaining solvable for humans.
- **Adaptive Learning:** Continuously update the GAN model based on user responses to improve the effectiveness of the generated images. This could involve retraining the model periodically to incorporate new patterns in user behavior and preferences.

5.3.Time-Sensitive Challenge Implementation

Algorithm: Reinforcement Learning (Deep Q-Network, DQN) Reinforcement Learning can adjust the difficulty of CAPTCHA challenges based on user performance. DQN models can impose time-based constraints and penalties, adjusting the difficulty in real-time. For instance, if a user takes too long to solve a CAPTCHA, future challenges can become more or less difficult based on their behavior.

Key Techniques

- **Time-Based Penalties:** Impose penalties for slow CAPTCHA solving, making it harder for bots that rely on analyzing solutions without immediate responses. This encourages users to respond quickly, which is typical human behavior.
- **Dynamic Difficulty Adjustment**: Tailor CAPTCHA difficulty to individual users based on their performance. This approach allows for a more adaptive user experience, ensuring that challenges remain engaging and appropriate for each user.
- **Feedback Mechanism:** Incorporate a feedback mechanism to assess user performance on past CAPTCHAs, which informs the system on how to adjust future challenges effectively. This continuous feedback loop can improve the overall security of the CAPTCHA system.

5.4.Object Detection in Image-Based CAPTCHAs

Algorithm: Convolutional Neural Networks (CNNs) CNNs are essential for object detection and image classification tasks. In the case of CAPTCHA generation, CNNs can ensure that CAPTCHA images are solvable by humans but challenging for bots to interpret. Pre-trained models like YOLOv5 or ResNet-50 can be employed to classify objects within CAPTCHA images.

Key Techniques

- **Object Detection:** Use CNN models for object recognition within CAPTCHA images. This ensures that the images presented are relevant to the challenges, providing a more engaging experience for users.
- **Image Classification:** Ensure each CAPTCHA image is challenging but solvable by legitimate users. CNNs can also be trained to ensure the clarity of the images presented to users, preventing confusion and frustration.
- **Continuous Improvement:** Regularly retrain CNN models on updated datasets to ensure that the CAPTCHA remains effective against evolving bot capabilities. Incorporating diverse training data helps the system adapt to various user groups and contexts.

5.5.Security: Randomization and Hashing

Algorithm: Randomization and Hashing Randomization ensures that no CAPTCHA is repeated or predictable, while hashing techniques ensure CAPTCHA images are resistant to replay attacks. Hash CAPTCHA images with user session IDs to prevent reuse by bots.

Key Techniques

- **Random Image Generation:** Cryptographically randomize CAPTCHA

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2025.0039
e ISSN: 2584-2854
Volume: 03
Issue:02 February 2025
Page No: 238-246

images to prevent predictability. This technique enhances security by ensuring that even if one CAPTCHA is solved, subsequent CAPTCHAs remain unique and ungues sable.

- **Hashing:** Hash CAPTCHA solutions with session IDs to avoid replay attacks. This adds an extra layer of security, as even if a CAPTCHA solution is captured, it cannot be reused without the corresponding session ID.
- **Use of Cryptographic Functions:** Employ strong crypto- graphic functions to ensure the integrity of CAPTCHA solutions, making it exceedingly difficult for bots to exploit any potential weaknesses.

6. Future Directions

Looking ahead, the development of CAPTCHA systems should focus on several key areas to ensure they remain effective and user-friendly:

- **Multimodal CAPTCHA Systems**: Combining various modalities such as text, images, audio, and gestures into a single CAPTCHA system could enhance security by making it harder for bots to exploit any one method. A multimodal approach may require bots to solve multiple forms of verification, increasing the complexity significantly.
- **AI-Enhanced Security Mechanisms**: As bots become more sophisticated, future CAPTCHA systems will need to employ AI not only to generate challenges but also to detect and respond to suspicious behavior. Machine learning models can continuously improve by learning from successful bot attacks, adapting their challenges in real-time to better protect against evolving threats.
- **User-Centric Design**: Future CAPTCHA systems should focus on improving user experience by minimizing frustration and maximizing accessibility. Conducting user studies to understand the challenges faced by different user groups can inform better design choices and enhance usability.
- **Integration with Biometrics**: Exploring the use of bio- metric data (such as fingerprint scans or facial recognition) as a form of CAPTCHA can provide a new level of security. While this approach may raise privacy concerns, it could also offer a seamless user experience if implemented with adequate safeguards.
- **Regulatory Compliance**: As privacy concerns grow, CAPTCHA systems must comply with regulations such as GDPR. Transparency in how user data is collected and used will be critical for gaining user trust and ensuring that CAPTCHA systems are not only effective but also ethical.

Conclusion

CAPTCHA systems must evolve to address the growing sophistication of bots. AI-powered personalized CAPTCHA systems that generate dynamic challenges based on user behavior, history, and preferences offer a promising solution to this challenge. By leveraging algorithms such as RNNs with LSTM, GANs, CNNs, and reinforcement learning, CAPTCHA systems can dynamically adapt to user behavior and thwart bot attacks. This paper has surveyed the current state of AI-powered CAPTCHA systems and proposed algorithms to enhance security while improving user experience. Future research should focus on refining these techniques to overcome challenges related to privacy, scalability, and evolving bot capabilities. Continued advancements in AI and user interaction modeling will be essential for developing CAPTCHAs that are both secure and user-friendly in an increasingly digital world.

References

[1]. Human-artificial intelligence approaches for secure analysis in CAPTCHA codes, Nghia Dinh1* and Lidia Ogiela, EURASIP Journal on Information Security.
[2]. Y. Tao, “Image Style Transfer Based on VGG Neural Network Model,” IEEE Access, vol. 10, pp. 1553-1562, 2022.
[3]. I. Hossen and X. Hei, “reCAPTCHA: The Design and Implementation of Audio Adversarial CAPTCHA,” Proceedings of the 2022 IEEE European Symposium on Security and Privacy (EuroSP), pp. 430-447, 2022, doi: 10.1109/Eu- roSP53844.2022.00034.

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2025.0039
e ISSN: 2584-2854
Volume: 03
Issue:02 February 2025
Page No: 238-246

[4]. H. Weng, R. Guo, X. Liu, S. Du, Y. Chen, and C. Xu, "Towards understanding the security of modern image CAPTCHAs and underground CAPTCHA-solving services," Big Data Mining and Analytics, vol. 2, no. 2, pp. 118-144, 2019, doi: 10.26599/BDMA.2019.9020001.
[5]. Y. Raut, S. Pote, H. Boricha, and P. Gunjgu, "A Robust CAPTCHA Scheme for Web Security," IEEE Transactions on Information Forensics and Security, 2023.
[6]. K. Simonyan and A. Zisserman, "Very deep convolutional networks for large-scale image recognition," arXiv preprint arXiv:1409.1556, 2015.
[7]. X. Huang and S. Belongie, "Arbitrary Style Transfer in Real-time with Adaptive Instance Normalization," Proceedings of the IEEE International Conference on Computer Vision, pp. 1501-1510, 2017.
[8]. M. Dushkoff, "A Temporally Coherent Neural Algorithm for Artistic Style Transfer," arXiv preprint arXiv:1609.04185, 2016.
[9]. L. A. Gatys, A. S. Ecker, and M. Bethge, "A Neural Algorithm of Artistic Style," arXiv preprint arXiv:1508.06576, 2015.
[10]. H. H. Zhao, P. L. Rosin, Y. Lai, and Y. N. Wang, "Automatic semantic style transfer using deep convolutional neural networks and soft masks," Multimedia Tools and Applications, vol. 78, no. 23, pp. 33523-33539, 2019.
[11]. L. A. Gatys, A. S. Ecker, and M. Bethge, "Texture Synthesis Using Convolutional Neural Networks," Advances in Neural Information Processing Systems, vol. 28, pp. 262- 270, 2015.
[12]. X. Yan, F. Liu, W. Q. Yan, and Y. Lu, "Applying visual cryptography to enhance text CAPTCHAs," Mathematics, vol. 8, no. 3, p. 332, 2020.
[13]. Z. Yuan, J. Zhang, Y. Jia, C. Tan, T. Xue, and S. Shan, "Meta gradient adversarial attack," ICCV, pp. 7728–7737, 2021.
[14]. W. Zheng, W. Wang, W. Ren, S. Feng, S. Liu, and Y. Ren, "A user behavior-based random distribution scheme for adversarial example generated CAPTCHA," ISPA, pp. 1215–1221, 2021.
[15]. Y. Matsuura, H. Kato, and I. Sasase, "Adversarial text- based CAPTCHA generation method utilizing spatial smoothing," IEEE, pp. 1–6, 2021.
[16]. M. Korakakis, E. Magkos, and P. Mylonas, "Automated CAPTCHA solving: An empirical comparison of selected techniques," SMAP, pp. 44–47, 2014.
[17]. D. Kim and L. Sample, "Search prevention with captcha against web indexing: A proof of concept," CSE/EUC, pp. 219–224, 2019.
[18]. 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.
[19]. L. Von Ahn, B. Maurer, C. McMillen, D. Abraham, and M. Blum, "recaptcha: Human-based character recognition via web security measures," Science, vol. 321, no. 5895, pp. 1465–1468, 2008.
[20]. S. Kim and S. Choi, "Dotcha: A 3D text-based scatter- type CAPTCHA," ICWE, pp. 238–252, 2019.
[21]. E. Bursztein, M. Martin, and J. C. Mitchell, "Text- based CAPTCHA strengths and weaknesses," CCS, pp. 125–138, 2011.
[22]. V. Sze, Y. Chen, T. Yang, and J. S. Emer, "Efficient processing of deep neural networks: A tutorial and survey," Proceedings of the IEEE, vol. 105, no. 12, pp. 2295–2329, 2017.
[23]. Z. Wu, Z. Guo, J. You, Z. Yang, Q. Li, and W. Liu, "Meta perturbation generation network for text-based CAPTCHA," Secure Common, pp. 1–6, 2023.
[24]. C. Shi, X. Xu, S. Ji, K. Bu, J. Chen, R. Beyah, and T. Wang, "Adversarial captchas," IEEE Transactions on Cybernetics, vol. 52, no. 7, pp. 6095–6108, 2021.
[25]. H. Kwon, H. Yoon, and K. Park, "Robust CAPTCHA image generation enhanced with adversarial example meth- ods," IEICE Transactions on Information Systems, vol.

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2025.0039
e ISSN: 2584-2854
Volume: 03
Issue:02 February 2025
Page No: 238-246

103- D, no. 4, pp. xx-xx.
[26]. L. von Ahn, et al., "CAPTCHA: Using Hard AI Problems for Security," 2003.
[27]. C. Szegedy, et al., "Intriguing properties of neural networks," ICLR, abs/1312.6199, 2014.
[28]. L.A. Gatys, et al., "A neural algorithm of artistic style," arXiv preprint arXiv:1508.06576, 2015. [29] P. Pe´rez, et al., Poisson image editing," ACM Trans Graphics (TOG), 2003, 22, (3), pp. 313–318.
[29]. J. Johnson, et al., "Perceptual losses for real-time style transfer and super-resolution," European Conference on Computer Vision, Amsterdam, the Netherlands, 2016, pp. 694–711.
[30]. I. J. Good fellow, et al., "Explaining and harnessing adversarial examples," CoRR abs/1412.6572, 2014.
[31]. G. Ghiasi, et al., "Exploring the structure of a real-time, arbitrary neural artistic stylization network," British Machine Vision Conference (BMVC), 2017.
[32]. C. Szegedy, et al., "Rethinking the inception architec- ture for computer vision," IEEE Computer Vision and Pattern Recognition (CVPR), 2015.
[33]. K. Simonyan, et al., "Very deep convolutional net- works for large-scale image recognition," arXiv preprint arXiv:1409.1556, 2014.
[34]. J. Yan and A. S. El Ahmad, "A low-cost attack on a Microsoft CAPTCHA," in Proceedings of the 15th ACM Conference on Computer and Communications Security, 2008, pp. 543-554.
[35]. H. Gao, W. Wang, Y. Fan, L. Wang, X. Liu, and X. Li, "The robustness of hollow CAPTCHAs," in Proceedings of the 14th ACM Conference on Computer and Communications Security, 2010, pp. 49-52.
[36]. L. von Ahn, M. Blum, N. Hopper, and J. Langford, "CAPTCHA: Using hard AI problems for security," in Ad- vances in Cryptology – EUROCRYPT, 2003, pp. 294-311.
[37]. G. Mori and J. Malik, "Recognizing objects in adver- sarial clutter: Breaking a visual CAPTCHA," in Proceedings of the 13th International Conference on Computer Vision, 2003, pp. 134-141.
[38]. M. O. Yusuf, R. Kushwaha, and D. Srivastava, "Pseudo- CAPTCHA for single-view CAPTCHA recognition systems," in IEEE Access, vol. 8, pp. 124310-124321, 2020.
[39]. S. J. Sim, J. Lee, and Y. M. Ro, "Automated text CAPTCHA solver using deep learning," in IEEE Transactions on Multimedia, vol. 21, no. 8, pp. 1936-1946, 2019.
[40]. Y. Kwon, J. Lim, and S. J. Sim, "Improving CAPTCHA security with hybrid models," in IEEE Access, vol. 9, pp. 39502-39510, 2021.
[41]. G. Mori and J. Malik, "Recognizing objects in adver- sarial clutter: Breaking a visual CAPTCHA," in Proceedings of the 13th International Conference on Computer Vision, 2003, pp. 134-141.
[42]. J. Yan and A. S. El Ahmad, "A low-cost attack on a Microsoft CAPTCHA," in Proceedings of the 15th ACM Conference on Computer and Communications Security, 2008, pp. 543-554.
[43]. H. Gao, W. Wang, Y. Fan, L. Wang, X. Liu, and X. Li, "The robustness of hollow CAPTCHAs," in Proceedings of the 14th ACM Conference on Computer and Communications Security, 2010, pp. 49-52.
[44]. M. Pal, A. Tripathi, and B. Srinivasan, "Deep learning model for breaking CAPTCHA with high accuracy," in IEEE Access, vol. 7, pp. 111410-111422, 2019.
[45]. Y. Kwon, J. Lim, and S. J. Sim, "CAPTCHA vul- nerability to deep learning: An empirical study," in IEEE Transactions on Information Forensics and Security, vol. 15, pp. 1043-1056, 2020.
[46]. S. Tang, H. Wang, and Z. Liu, "Breaking CAPTCHA using convolutional neural networks," in IEEE Transactions on Information Forensics and Security, vol. 16, pp. 4124-4133, 2021.
[47]. C. Sauerwein, G. Schneider, and M. Koch,

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2025.0039
e ISSN: 2584-2854
Volume: 03
Issue:02 February 2025
Page No: 238-246

"Exploring the human factor in CAPTCHA design," in ACM Transactions on Human-Computer Interaction, vol. 27, no. 4, pp. 563-591, 2021.

[48]. J. Yan and A. S. El Ahmad, "A low-cost attack on a Microsoft CAPTCHA," in Proceedings of the 15th ACM Conference on Computer and Communications Security, 2008, pp. 543-554.

[49]. L. von Ahn, M. Blum, N. Hopper, and J. Langford, "CAPTCHA: Using hard AI problems for security," in Ad- vances in Cryptology – EUROCRYPT, 2003, pp. 294-311.

[50]. A. Faruk C¸ akmak, M. Umar, and M. A. Alsaedi, "Au- dio CAPTCHA using Support Vector Machines," in Proceed- ings of the IEEE International Conference on Web Services, 2021, pp. 201-208.

[51]. E. Ababtain, M. Basalamah, and H. Altuwaiyan, "Gesture-based CAPTCHA to defend against automated at- tacks," in IEEE Access, vol. 9, pp. 104313-104324, 2021.

[52]. S. Ezhilarasi, R. Uthayakumar, and A. Alhussein, "Noise-added CAPTCHA design and performance evaluation," in IEEE Transactions on Information Forensics and Security, vol. 16, pp. 3100-3112, 2021.