Advances in Nonlinear Variational Inequalities
ISSN: 1092-910X
Vol 28 No. 2s (2025)

A Review on New Approaches to CAPTCHA for Enhancing Security and Usability

[1]Mohammad Umar,[2] Dr. Manju Papreja
[1]Research Scholar (Computer Science)
Department of Computer Science and Engineering
Shri Venkateswara University, Gajraula, UP, India
Email: mohammadumarbpl@gmail.com
[2]Research Guide (Computer Science)
Department of Computer Science and Engineering,
Shri Venkateswara University, Gajraula, UP, India
Email: manju.papreja@gmail.com

Article History:

Received: 07-01-2025

Revised: 19-02-2025

Accepted: 25-02-2025

Abstract: CAPTCHA systems, or Completely Automated Public Turing test to tell Computers and Humans Apart, are well-known as automated programs used to filter out real human users from bots. Unfortunately, ordinary CAPTCHAs, including the text-based ones and the image recognition challenges, are becoming easier for sophisticated machine learning systems to crack and more annoying for users to complete. This paper applies new methods of CAPTCHA security customization by focusing on improvement of usability. Paper analyzes emerging methods such as behavioral biometrics, game-based CAPTCHAs, and AI-driven adaptive CAPTCHAs. In addition, it examines the effectiveness of these methods in counteracting different types of automated attacks and their impacts on user experience. The paper ends by offering some thoughts about the future of CAPTCHA technology, arguing that research should aim at a combination of security and usability for users. So, the intension of the paper is to examine the new approaches and compare them with each other and what should be the impact on the security system. There are so many tricks or hacks through which security can be breached. So, for that reason an ideal system is required to maintain the security.

Keywords: CAPTCHA, AI Driven, Game, Biometric, Web Security, Turing Test, Authentication.

1. INTRODUCTION

For more than 20 years CAPTCHA systems have been a vital component of web security preventing automated bots from gaining access to online services. Presenting a problem that is simple for people to solve but challenging for computers is the main objective of CAPTCHA. Audio challenges image classification and distorted text recognition are examples of traditional CAPTCHA systems that have proven successful in the past. But due to the development of advanced machine learning algorithms automated bots are increasingly evading these systems. Furthermore users frequently become frustrated by traditional CAPTCHAs because of their intricacy and lack of accessibility especially for those who are visually or auditorily impaired [1]. However as technology develops more complex machine learning algorithms and automated attacks are able to compromise traditional CAPTCHA systems which range from image-based challenges to distorted text recognition. The intricacy inaccessibility and subpar user experience of these systems however frequently irritate users casting doubt on their long-term sustainability. Many traditional CAPTCHA designs are no longer relevant due to the quick advancements in machine learning and artificial intelligence (AI). Text-based and image-based CAPTCHAs can now be solved by bots with alarming

accuracy thanks to deep learning models and advanced optical character recognition (OCR). Furthermore traditional CAPTCHAs frequently create barriers to accessibility by excluding users with disabilities such as those who have visual or auditory impairments. Innovative CAPTCHA solutions that prioritize inclusivity and usability while simultaneously enhancing security are becoming increasingly necessary as a result of these issues.

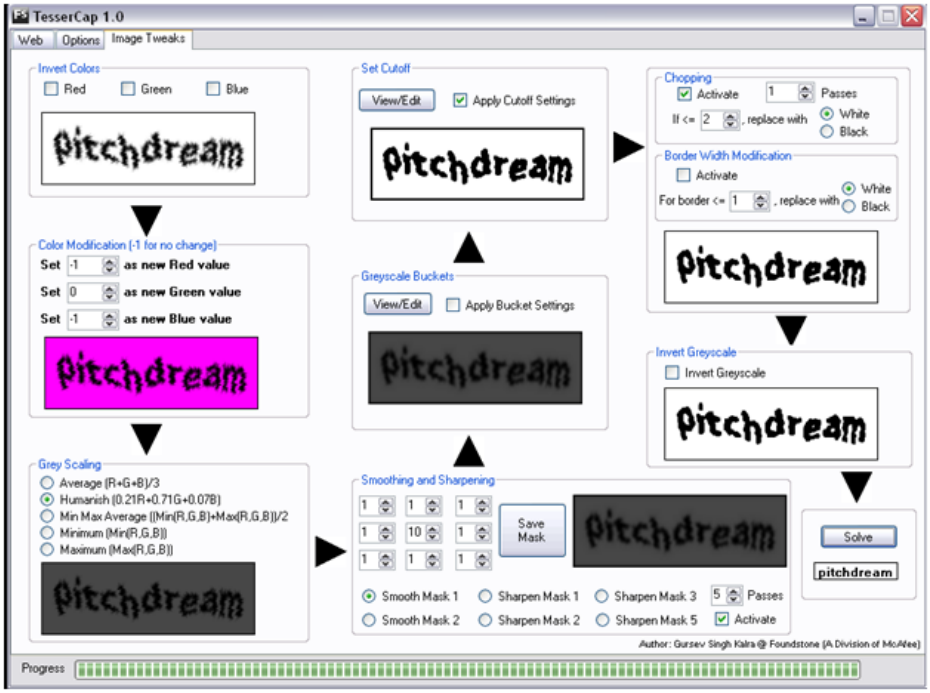

Figure 1: Extraction of CAPTCHA using OCR [2]

Fig. 1 shows how a CAPTCHA can be solved using OCR by applying some filter or preprocessing approaches. This study examines new developments and trends in CAPTCHA design emphasizing tactics that overcome the drawbacks of conventional systems. We look at innovative methods like behavioral biometrics which take advantage of distinctive human interaction patterns like mouse movements and keystroke dynamics game-based CAPTCHAs which use interactive challenges and puzzles to draw users in and discourage bots and AI-driven adaptive CAPTCHAs which change their type and difficulty in real time according to user behavior. By balancing strong security with a smooth user experience these strategies hope to keep CAPTCHA systems functional in the face of increasingly complex cyber threats [3]. In order to give a thorough grasp of the future of CAPTCHA systems this paper reviews the advantages and disadvantages of these novel techniques. We assess how well they work to reduce automated attacks increase accessibility for a range of user demographics and improve usability. In the end this study emphasizes how crucial it is to innovate CAPTCHA design stressing the need for inclusive user-friendly and secure solutions. As the digital world keeps changing creating next-generation CAPTCHA systems will be essential to protecting online platforms and guaranteeing that every user has a good experience.

2. APPROACHES TO CAPTCHA DESIGN

The most popular type of CAPTCHA is text-based which requires users to identify and enter distorted text. It is based on the idea that people can easily decode distorted characters while computers have trouble. However technological advancements in machine learning and optical character recognition (OCR) have greatly diminished their efficacy. Bursztein et al. [4] have shown that machine learning algorithms are capable of solving text-based

CAPTCHAs with high accuracy rendering them more susceptible to automated attacks. CAPTCHAs based on images ask users to choose which of a collection of images best fit a predetermined criterion (e. g. G. more resilient to OCR-based attacks such as select all images with cars) but they are still vulnerable to machine learning algorithms especially convolutional neural networks (CNNs) that have been trained on sizable datasets of labeled images [5]. Tam et al. [6] elaborated that furthermore users with visual impairments may find image-based CAPTCHAs difficult to use because they frequently rely on visual cues. As a substitute for visually impaired users audio CAPTCHAs ask users to transcribe distorted audio clips. But even for users without hearing loss these CAPTCHAs can be challenging to understand and new developments in speech recognition technology have made it possible for automated bots to solve them more accurately. Traditional CAPTCHA systems main drawbacks are their susceptibility to machine learning attacks their poor usability which causes users to become frustrated and give up and their inaccessibility to users with visual or auditory impairments which prevents a sizable section of the population from using online services.

A. Behavioral Biometrics CAPTCHAs

CAPTCHAs that use behavioral biometrics use distinct human behavioral patterns like mouse motions keystroke patterns and touchscreen interactions to distinguish between people and automated programs. By analyzing user behavior on their devices these systems build a profile of human behavior that is hard for bots to imitate. Instead of using conventional visual or textual challenges behavioral biometric CAPTCHAs analyze distinct patterns in user behavior to differentiate humans from bots. Keystroke dynamics mouse movement trajectories touchscreen gestures scroll behavior and response timing are examples of subtle unconscious user interactions that these systems track and assess. Because human motor patterns and decision-making processes are unique and complex behavioral biometrics are intrinsically challenging for bots to imitate in contrast to static CAPTCHAs that can be circumvented through image recognition or OCR techniques. Usually functioning in the background these CAPTCHAs provide a smooth user experience while consistently verifying identity through consistent behavior. This makes them extremely effective against automated attacks and credential stuffing without interfering with user workflow [7].

a. *Mouse Movement Analysis*

Analysis of mouse movements CAPTCHAs monitor the direction and velocity of a users mouse clicks while they navigate a website. When it comes to mouse movement humans are more unpredictable and erratic than bots which typically take straight-line routes. These patterns allow behavioral biometric CAPTCHAs to differentiate between humans and bots [8]. CAPTCHAs based on mouse movement analysis use the distinct non-linear patterns of human cursor movements to differentiate between automated bots and actual users. While humans naturally move in irregular adaptive ways these systems monitor parameters like speed acceleration curvature hesitation and click behavior. In contrast bots typically move in straight lines or at a constant speed. Active versions require users to make specific gestures like tracing paths drawing shapes or dragging sliders whereas passive implementations like Google's reCAPTCHA v3 use background movement analysis to assign risk scores. This methods primary benefit is a smooth user experience with little friction which makes it more difficult for bots to imitate natural behavior. There are obstacles though like the growing complexity of AI-driven bots that can mimic human-like cursor movements and accessibility concerns for users with motor impairments. Mouse-based CAPTCHAs are widely used in

security applications such as automated bot prevention in online services and fraud detection in financial systems despite these drawbacks.

b. Keystroke Dynamics

CAPTCHAs examine the rhythm and timing of a user keystrokes while they type. Every person has a distinctive typing style that can be used to confirm who they are. Conversely bots are easier to identify because they usually type with consistent and uniform timing [9].

c. *Touchscreen Interactions*

As mobile devices become more and more common touchscreen interaction analysis has emerged as a promising field for CAPTCHA design. These systems examine how users move their fingers across touchscreens taking note of their pressure speed and angle. There is a trustworthy way to differentiate between human and bot touch interactions because human touch interactions are more unpredictable and varied [10]. When it comes to behavioral biometrics CAPTCHAs (keystroke dynamics) analyze a user typing patterns in order to verify their identity and differentiate between humans and bots. This method records and assesses specific characteristics like the length of time spent on keystrokes (dwell time) the interval between keystrokes (flight time) typing rhythm speed error rate and consistency. Because every person has a distinct typing signature that is influenced by cognitive physiological and motor characteristics automated scripts and malevolent actors find it challenging to imitate. Keystroke dynamics are employed in CAPTCHA systems to silently monitor and verify user behavior in the background while they complete text input tasks like form filling or password entry rather than to provide overt challenges. Modern machine learning models are used to identify typical typing patterns and highlight any deviations that might point to bot activity. Due to its resistance to impersonation replay and automation attacks this technique improves security while also improving usability by avoiding invasive verification procedures.

B. Game-based CAPTCHAS

Game-based CAPTCHAs ask users to demonstrate their humanity by solving a straightforward game or puzzle. These CAPTCHAs are meant to make the user experience more interesting and fun while making it harder for bots to solve. Using basic games game-based CAPTCHAs are interactive human verification systems that take advantage of people's innate problem-solving coordination and perceptual skills to differentiate between humans and automated bots. These CAPTCHAs challenge users to play quick simple games like matching pairs dragging objects to predetermined spots or guiding a character through a simple obstacle in place of more conventional distorted text or image recognition tasks. Because these tasks require cognitive reasoning spatial awareness and motor control they are meant to be simple and even enjoyable for humans but challenging for bots. Because game-based CAPTCHAs frequently include randomness real-time response and visual feedback it is challenging for automated programs to create broadly applicable strategies to get around them. They also enhance user experience by lowering the annoyance that traditional CAPTCHAs are known to cause all the while preserving strong defenses against bot-based attacks. Additionally their design provides opportunities for gamified user engagement ongoing security evaluation through behavioral interaction and accessibility enhancements.

a. Puzzle CAPTCHAs

Puzzle CAPTCHAs ask users to complete a basic puzzle like putting pieces in the right order or finishing a pattern. Humans can easily solve these CAPTCHAs but bots find them difficult especially when the puzzles require spatial or visual reasoning [11]. As a sort of human

verification mechanism puzzle CAPTCHAs require users to perform visually intuitive and cognitively stimulating tasks like putting together jigsaw pieces reorienting distorted images or sliding objects into designated slots in order to demonstrate their humanity. Bots and automated programs find it challenging to replicate the human brains superior visual perception spatial reasoning and fine motor control which these CAPTCHAs take advantage of. Usually created with dynamic HTML5 or JavaScript interfaces puzzle CAPTCHAs are made to be solved with straightforward click-or drag-and-drop actions. However they incorporate variation and randomization to avoid predictable bot responses. Analyzing user interaction behavior including speed fluidity and response patterns in addition to the accuracy of the solution improves security by enabling systems to identify questionable activity. In contrast to text-based challenges puzzle CAPTCHAs are easier to use and frequently accessible while still offering robust protection against automated attacks and brute-force bypass attempts.

b. Interactive Game CAPTCHAs

Users must finish a brief interactive game as part of CAPTCHAs to demonstrate their humanity. These entertaining and captivating games are made to entice players to finish the CAPTCHA without becoming frustrated. Simple platformer games memory games and reaction-time tests are a few examples [12]. An enhanced method of human verification interactive game CAPTCHAs immerse users in dynamic real-time mini-games that are hard for bots to imitate and are intended to take advantage of human cognitive and motor abilities including pattern recognition timing spatial awareness and problem-solving. Users must complete these CAPTCHAs usually in a brief amount of time by guiding an object through a maze catching falling objects or avoiding obstacles. CAPTCHAs in interactive games as opposed to passive verification techniques actively evaluate the user's capacity to react to stimuli make choices under pressure and display natural behaviors like hesitation error correction and fluctuating reaction times. To further differentiate humans from automated agents they also gather and examine user interaction data including movement paths click timing and gesture dynamics. These CAPTCHAs enhance user experience while providing strong defense against script automation replay strategies and machine learning-based attacks by fusing security and entertainment. Because of their complexity and adaptability they work particularly well in contemporary cybersecurity applications where conventional CAPTCHAs might not work.

C. AI-Driven Adaptive CAPTCHAs

Machine learning algorithms are used by AI-driven adaptive CAPTCHAs to dynamically change the CAPTCHAs type and difficulty in response to user behavior. These systems modify the CAPTCHA challenge to make it safe and easy to use by analyzing user interactions in real-time. CAPTCHAs with adaptive difficulty modify the challenges level of difficulty in response to the user's performance. A more difficult CAPTCHA might be shown by the system to make sure the user is not a bot for instance if they successfully complete a simple one. The system might on the other hand offer a less complicated task to a user who finds a CAPTCHA difficult in order to prevent frustration [13]. To customize the CAPTCHA challenge context-aware CAPTCHAs make use of contextual data including the user's location device and browsing history. For instance a user visiting a website from a device they trust might be shown a simpler CAPTCHA whereas a user visiting the site from a device they are unfamiliar with might be shown a more difficult CAPTCHA [14]. Using machine learning algorithms AI-driven adaptive CAPTCHAs are a clever context-aware development

of conventional CAPTCHA systems that dynamically modify the challenges type and difficulty in response to real-time evaluations of user behavior and risk level. To determine whether an interaction is automated or human these systems continuously examine a variety of signals such as device information browsing habits geolocation mouse movements keystroke dynamics and past user data. This assessment determines how the CAPTCHA changes either by making the challenge more difficult for suspicious activity or by making it easier for authorized users to complete sometimes letting trusted users get through with no apparent difficulty at all. These CAPTCHAs AI engine is trained to use behavioral biometrics and pattern recognition to identify anomalies mimicry or scripted interactions enhancing security while reducing friction. A more seamless and customized user experience is made possible by this adaptive strategy which also lowers false positives and fortifies defenses against emerging threats like adversarial AI tactics CAPTCHA farms and botnets.

3. PERFORMANCE EVALUATION

Probability statistics pattern recognition machine learning cryptography and computational complexity are all involved in the mathematics underlying CAPTCHA (Completely Automated Public Turing test to Tell Computers and Humans Apart) systems. The fundamental mathematical ideas at play are broken down here.

A. Probability and Statistics

CAPTCHA systems frequently examine user behavior (e. g. A. Probabilistic models are used in behavioral biometrics (CAPTCHAs).

a. Bayesian Inference

A statistical technique called Bayesian inference adjusts a hypothesiss probability in response to new information. This is the hypothesis for behavioral CAPTCHAs.

“This user is human” vs. “This user is a bot.”

Suppose you watch how a user moves their mouse or how they time their keystrokes. This is how you update your beliefs,

$$P(Human|Behavior) = \frac{P(Human|Behavior).P(Human)}{P(Behavior)} \quad (1)$$

$P(Human)$ is the probability that user is a human, $P(Behavior)$ is total probability where behavior has been observed, $P(Human|Behavior)$ is the probability of observed baviour where user is human. When more behavioral information is gathered throughout the interaction CAPTCHA systems can use Bayesian models to dynamically update the confidence score that a user is human.

b. Gaussian Distributions

When it comes to things like mouse trajectory smoothness dwell time (the amount of time a key is pressed) and typing speed humans are naturally variable. The normal (Gaussian) distributions can frequently be used to model these behaviors.

$$f(x) = \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{(x-\mu)^2}{2\sigma^2}} \quad (2)$$

Where, x is the observed behavioral metric, μ is the mean and σ is the standard deviation. Because of this the system is able to simulate normal human behavior anything that deviates from this distribution is signaled as suspicious (probably a bot).

c. ***Thresholding (Decision Making)***

When it comes to CAPTCHA decision-making thresholding is the process of determining whether a users input is human or bot-generated by calculating a similarity or confidence score. Once the user's response (e. g. A. text input picture selection) the system evaluates it against a reference or anticipated value up to the upper limit. T.

$$Decision = \begin{cases} Human, & if\ S \geq T \\ Bot, & ifS < T \end{cases} \quad (3)$$

Where S stands for the confidence level or similarity score. If the score is at or above the cutoff, T the input is rejected as being bot-like otherwise it is accepted as probably human. False positives (bots passing) and false negatives (humans rejected) are balanced by the threshold.

B. Security Metrics

A CAPTCHA systems performance is measured by assessing how well it strikes a balance between security (inhibiting bots) and usability (avoiding user annoyance). The main indicators and techniques that you can employ are as follows:

a. Bot Detection Rate (True Positive Rate)

A CAPTCHA systems ability to recognize and prevent automated bot interactions is gauged by its Bot Detection Rate also referred to as the True Positive Rate (TPR). It shows the percentage of real bots that the CAPTCHA mechanism correctly identifies and blocks access to. Since most bots are effectively stopped a high TPR denotes strong security. This formula can be used to determine the Bot Detection Rate.

$$True\ Positive\ Rate = \frac{True\ Positive}{True\ Positive + False\ Negative} \quad (4)$$

Where False Negative is bots that were inadvertently let through as if they were human and True Positive is the number of bots that were correctly identified.

b. ***False Negative Rate***

The fraction of bots that a CAPTCHA system misses and let's passes as real users is known as the False Negative Rate or FNR. It indicates a flaw in the security of the CAPTCHA because a high FNR indicates that more bots are getting past the security measures. The more effectively the system prevents automated abuse the lower the FNR. The following formula can be used to determine the False Negative Rate.

$$False\ Negative\ Rate = \frac{False\ Negative}{False\ Positive + False\ Negative} \quad (5)$$

Where bots that get past the CAPTCHA are known as False Negatives (FN) and bots that are correctly detected and blocked are known as True Positives (TP).

c. Resistance to Known Attacks

A CAPTCHA systems resistance to known attacks is its capacity to resist automated methods that attackers frequently employ to get around verification. These include text-based CAPTCHAs that use optical character recognition (OCR) audio CAPTCHAs that use audio processing script-based bots that use Selenium and machine learning algorithms that are trained to solve visual puzzles. Even when these attacks are made a system with high resistance keeps its accuracy and efficacy. This metric can be quantitatively expressed as follows though there isn't a single universal formula for it.

$$Attack\ Success\ Rate = \frac{Successful\ Bypass\ Attempts}{Total\ Attack\ Attempts} \quad (6)$$

A lower attack success rate denotes greater resistance making it more difficult for bots to use well-known techniques to get past the CAPTCHA.

*C. **USABILITY METRICS***

The ease and effectiveness with which authorized human users can interact with and successfully complete the CAPTCHA without experiencing frustration or failure is measured by usability metrics for CAPTCHA systems. These metrics make sure that although the system is safe from bots actual users won't be hindered by it. These are important usability metrics.

*a. **Human Success Rate (True Negative Rate)***

The True Negative Rate (TNR) sometimes referred to as the Human Success Rate gauges how well a CAPTCHA system enables valid human users to pass without being mistakenly identified as bots. It shows how usable the system is a higher rate means that the majority of legitimate users are recognized and not blocked. This is necessary to guarantee that security precautions don't impair user experience. The following is the formula to determine the Human Success Rate.

$$True\ Negative\ Rate = \frac{True\ Negative}{True\ Positive + False\ Negative} \quad (7)$$

In this case False Positive (FP) is actual users who are mistakenly blocked by the CAPTCHA while True Negative (TN) is actual users who are correctly permitted to pass.

*b. **False Positive Rate (FPR)***

The percentage of valid human users who are mistakenly identified as bots and prevented access by the CAPTCHA system is known as the False Positive Rate or FPR. Poor usability is indicated by a high FPR because it irritates users and may drive away real users. In order to maintain security and guarantee a seamless user experience this rate should ideally be as low as feasible. This is the formula used to determine the False Positive Rate.

$$False\ Positive\ Rate =$$

$$\frac{False\ Positive}{True\ Negative + False\ Positive} \quad (8)$$

Where real users who are incorrectly blocked are known as False Positives (FP) and real users who are correctly allowed through are known as True Negatives (TN).

c. ***Average Solve Time***

Average Solve Time gauges how long it typically takes users to finish a CAPTCHA task indicating how fast and simple it is to solve. Shorter solve times typically indicate a more user-friendly experience while longer times might imply the CAPTCHA is too complex or confusing. This is a crucial usability metric. Excessive solve times may cause users to become frustrated and abandon more frequently. The following formula can be used to determine Average Solve Time.

$$Average\ Solve\ Time = \frac{\sum Solve\ Times\ of\ All\ Users}{Number\ of\ Users} \quad (9)$$

This metric makes sure CAPTCHAs don't take too long for real users which aid developers in striking a balance between security and accessibility.

d. ***Abandonment Rate***

The Abandonment Rate quantifies the proportion of users who abandon a process after seeing a CAPTCHA frequently as a result of frustration difficulty or confusion. It is an important usability metric that shows how much the CAPTCHA detracts from conversion rates and user experience. If the CAPTCHA is too difficult or invasive users may give up before finishing their intended action as indicated by a high abandonment rate. This is the formula used to determine the abandonment rate.

$$Abandonment\ Rate = \frac{Users\ Who\ Quit\ After\ CAPTCHA}{Total\ Users\ Presented\ with\ CAPTCHA} \quad (10)$$

e. ***User Satisfaction (Qualitative)***

A subjective usability metric called User Satisfaction (Qualitative) gauges how users feel about using a CAPTCHA system. It is usually obtained through surveys interviews or feedback forms and represents opinions about straightforwardness ease fairness or frustration. Rating scales can be used to quantify it even though there isn't a precise numerical formula for it. A. summarized using an average score (1 to 5 or 1 to 10). For calculating average user satisfaction the following is an example formula.

$$Average\ Satisfaction\ Score = \frac{\sum User\ Ratings}{Number\ of\ Respondents} \quad (11)$$

This metric guides CAPTCHA system improvements based on actual user experience by identifying design flaws or usability issues that may not be captured by purely quantitative data.

4. CONCLUSION & FUTURE SCOPE

To sum up behavioral biometric CAPTCHAs present a viable method for detecting bots by examining distinctive human behavior patterns like mouse movement touchscreen interactions and typing speed. Due to their lack of dependence on conventional techniques like puzzles or distorted text these systems improve security while reducing user friction. There are still issues though mainly with regard to privacy issues the possibility of sophisticated attacks that circumvent behavioral patterns and the requirement for cross-platform accuracy. The future of behavioral biometrics in CAPTCHA systems will focus on enhancing the robustness and adaptability of detection algorithms incorporating machine learning models to more accurately identify and authenticate users and protecting privacy through encrypted or decentralized data handling methods. Further enhancing the security and dependability of CAPTCHAs is the investigation of multi-modal biometrics that integrate behavior with additional identification factors.

References:

[1] Kumar, "Emerging trends in CAPTCHA design: A review of novel approaches for strengthening security and enhancing usability," Unpublished manuscript, 2023.
[2] Dayanand, W. J. a. K. J. (2023). Machine Learning-Based CAPTCHA defenses for mobile and IoT devices. ijaec.rpress.co.in. https://doi.org/10.8845/4w94jk96
[3] Brand, I. (2024, July 5). Assessing the future of CAPTCHA in cyber defense. Indonesia Brand. https://www.indonesiabrand.co.id/blog/assessing-the-future-of-captcha-in-cyber-defense/?utm_source=chatgpt.com
[4] Bursztein, E., Bethard, S., Fabry, C., Mitchell, J. C., & Jurafsky, D. (2011). How good are humans at solving CAPTCHAs? A large scale evaluation. "IEEE Symposium on Security and Privacy", 399-413.
[5] Goodfellow, I. J., Bulatov, Y., Ibarz, J., Arnoud, S., & Shet, V. (2014). Multi-digit number recognition from street view imagery using deep convolutional neural networks. "arXiv preprint arXiv:1312.6082".
[6] Tam, J., Simsa, J., Hyde, S., & von Ahn, L. (2008). Breaking audio CAPTCHAs. "Advances in Neural Information Processing Systems", 1625-1632.
[7] Acién, A., Morales, A., Fierrez, J., Vera-Rodríguez, R., & Delgado-Mohatar, Ó. (2021). BeCAPTCHA: Behavioral bot detection using touchscreen and mobile sensors benchmarked on HuMIdb. *Engineering Applications of Artificial Intelligence, 98*, 104058. https://doi.org/10.1016/j.engappai.2020.104058
[8] Bailey, K. O., Okolica, J. S., & Peterson, G. L. (2014). User identification and authentication using multi-modal behavioral biometrics. "Computers & Security", 43, 77-89.
[9] Monrose, F., & Rubin, A. D. (2000). Keystroke dynamics as a biometric for authentication. "Future Generation Computer Systems", 16(4), 351-359.
[10] Frank, M., Biedert, R., Ma, E., Martinovic, I., & Song, D. (2013). Touchalytics: On the applicability of touchscreen input as a behavioral biometric for continuous authentication. "IEEE Transactions on Information Forensics and Security", 8(1), 136-148.

[11] Gao, H., Wang, W., Qi, J., Wang, X., Liu, X., & Yan, J. (2016). The robustness of hollow CAPTCHAs. "Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security", 1070-1081.

[12] Bursztein, E., Martin, M., & Mitchell, J. C. (2014). Text-based CAPTCHA strengths and weaknesses. "ACM Transactions on Information and System Security (TISSEC)", 16(1), 1-32.

[13] Chellapilla, K., Larson, K., Simard, P. Y., & Czerwinski, M. (2005). Designing human friendly human interaction proofs (HIPs). "Proceedings of the SIGCHI Conference on Human Factors in Computing Systems", 711-720.

[14] Zhu, B. B., Yan, J., Li, Q., Yang, C., Liu, J., Xu, N., ... & Wang, Z. (2010). Attacks and design of image recognition CAPTCHAs. "Proceedings of the 17th ACM Conference on Computer and Communications Security", 187-200.