Louis Savinien Dupuis Journal of Multidisciplinary Research, 2025: V(4) 18–21
DOI: 10.21839/lsdjmr.2025.v4.230

Research Article

Secure CAPTCHA System with AI-Proof Verification Using Biometric Authentication

Thasmira M ,Sindhuja V ,Vidhiya V, Archana R *

Department of Computer Science,Immaculate College for Women, Chinnakanganankuppam, Cuddalore
((Received: 09-04-2025; Accepted 08-06-2025; Published Online 03-11-2025)

Abstract

With the rapid growth of artificial intelligence and automated attack tools, traditional password-based authentication mechanisms have become increasingly vulnerable. Automated bots, credential stuffing, and AI-powered CAPTCHA solvers pose serious threat line security systems. This paper proposes a Secure CAPTCHA and Fingerprint System with AI-Proof Verification, a multi-layer authentication framework combining biometric fingerprint authentication with an AI- resistant CAPTCHA mechanism. The proposed approach strengthens identity verification, prevents automated bots intrusions, and enhances data security through encryption and monitoring mechanisms. Experimental analysis shows that the proposed system significantly improves resistance against brute-force attacks ,bot-based intrusions, and unauthorized access while maintaining usability.

Keywords: Authentication, Biometric Security, CAPTCHA, AI-Proof Verification, Fingerprint Recognition, Cyber security.

Introduction

Efficient inventory management plays a crucial role in the success of small and medium enterprises (SMEs), warehouses, and retail businesses. Traditional inventory systems often relyonmanualprocessessuchashandwrittenlogs or basic digital entries, which are time-consuming, error-prone, and inefficient. These limitations frequently result in issues like inaccurate stock levels, delayed updates, overstocking, stockouts, and poor demand planning. Such challenges not only increase operational costs but also negatively impact customer satisfaction and overall business performance.

SystemArchitecture

Early CAPTCHA systems introduced by VonAhn relied on hard AI problems to distinguish humans from machines. However, recent advancements in deep learning have reduced their effectiveness. Biometricauthenticationmethodssuchasfingerprint recognition have been extensivelystudied for secure access control, yet they require complementary mechanisms to prevent spoofing. Recent research emphasizes multi-factor authentication combining biometrics, behavioral analysis, and challenge–responsemechanisms.Thesystemarchitectureofthe proposed secure CAPTCHA system consists of multiple interconnected modulesthat collaboratively ensurerobust human verification whileresisting AI-driven automated attacks. The architecture begins at the User Interface Layer, where the user interacts with the application through a web or mobile client. This layer captures user interaction events such as mouse movements, keystrokes, scrolling behavior, and touch gestures without affecting usability. The captured interaction data is forwarded to the Behavioral Data Collection Module, which preprocesses and normalizes the raw inputs to remove noise and extract meaningful behavioral features. These featuresare then analyzed bythe AI-Based Behavior Analysis Engine, which employs machine learning or deep learning models to distinguish between human and bots interaction patterns and generates a Human Confidence Score representing the probability of legitimate human behavior. Based on this confidence score, the Adaptive CAPTCHA Generator dynamicallycreates CAPTCHA challenges of varying complexity, including image-based tasks, object manipulation, logical reasoning, or temporal sequence challenges. To ensure AI-proof verification, the Security Enhancement Module introduces adversarial perturbations, challenge mutation, session binding, and one-time cryptographic tokens, preventingreplay attack sand data set exploitation by AIsolvers. The user's CAPTCHA response, along with updated behavioral metrics, is evaluated by the VerificationandDecisionEngine,whichvalidatesthe correctness, consistency, and timing of the response. Depending on the evaluation outcome, access is either granted, a re-challenge is issued, or the request is blocked and flagged as malicious. Finally, the Secure Logging and Model Update Module stores anonym zed verification data and system outcomes, enabling continuous learning and periodic retraining of AI models to adapt toemerging attack strategies while maintaining system scalability and security.

WorkingMethodology

The proposed secure CAPTCHA system with AI-proof verification operates by integrating behavioral analysis, dynamic challenge generation, and intelligent decision-making to distinguish human users from automated and AI-driven bots. When a user initiates access to a protected service, thesystem generates a secure session ID and silently captures behavioral features such as mouse movement patterns, keystroke dynamics, scrolling behavior, touch gestures, and response latency.These features are analyzed using an AI-based classification model to compute a HumanConfidence Score that estimates the likelihood of human interaction. Based on this score, the system dynamically generates adaptive CAPTCHA challenges involving object interaction, contextual imageselection,logicalreasoning,ortemporaltasks, ensuring each challenge is randomized, time-bound, and session-specific. To enhance resistance against AI solvers, adversarial noise injection, challenge mutation ,and one-time cryptographic validation tokens are employed, preventing replay and dataset-based attacks. The CAPTCHA response is verifiedinconjunction withbehavioralconsistencythrougha decision engine that evaluates accuracy, interaction coherence, and completion time to either

grant access, reissue a challenge, or block the request. All interactionsaresecurelylogged in anonymized form for continuousmodelretraining,enablingthesystem toadapttoevolving bot behaviorswhilemaintaining usability, scalability, and robust security.

Implementation

The proposed system introduces a Secure CAPTCHA and Fingerprint System with AI Proof Verification,designedtoovercomethelimitationsof existing authentication methods. It combines biometric fingerprint recognition with an advanced AI-resistantCAPTCHAtoensurebothhumanverification and strong identity authentication. Inthis system, fingerprint authentication provides a reliable method to confirm the user's identity, while the AI-proof CAPTCHA prevents automated bots and AI-driven attacks from gaining access. Additionally, encryption techniques are employedfor secure storage and transmission of user credentials, reducing the risk of data breaches. By integrating these multiple layers of defense, the system ensures higher security, better user trust, and resilience against password leaks ,spoofing, and automated intrusions. This makes it suitable for sensitive domains such as banking, healthcare, e-commerce, and government applications.The secure CAPTCHA system with AI-proof verification is implemented using a client–server architecture that integrates behavioral sensing, machine learning models, and adaptive security mechanisms. On the client side, lightweight JavaScript modules are deployed to capture real-time user interaction data, including mouse movement coordinates, keystroke timings, scrolling speed, and touch gestures. These interaction events are time stamped and securely transmitted to the server using encrypted communication protocols such as HTTPS to ensure data integrity and privacy. On the server side, the received interaction data is preprocessed to remove noise and normalized to generate feature vectors representinguser behavior. These featurevectors are fed into an AI-based behavior classification model implemented using machine learning frameworks such as Tensor Flow or Porch. The model, trained on labeled human and bot interaction datasets, computes a Human Confidence Score thatdetermines the likelihood of genuine human behavior. Based on this score, the adaptive CAPTCHA module dynamically generates challenges of varying complexity, such as image selection, object manipulation, or logical reasoning tasks, ensuring each challenge is session- specific and time-bound. To achieve AI-proof verification,the implementation incorporates adversarial noise injection, randomized challenge mutation, and cryptographically signed one-time tokens that bind each CAPTCHA instance to a single session. The user's response is validated alongside behavioral consistency checks by a decision engine, which evaluates response accuracy, completion time, and interaction coherence. Depending on the verificationoutcome, the system either grants access, issues a secondary challenge ,or blocks there quest. All verification results and interaction metadata are securely logged in anonymized form for continuous monitoringand periodic retraining ofthe AI models, enabling the system to adapt to evolving AI-driven attack techniques while maintaining usability and scalability.

Ai-ProofCaptchaDesign

The AI-proof CAPTCHA design focuses on creating human verification challenges that are resilient to automated and artificial intelligence–based attacks while maintaining ease of use for legitimate users. Unlike traditional text-based CAPTCHAs, the proposed design leverages adaptive, context-aware challenges combined with behavioral intelligence to exploit the natural cognitive and motor skills of humans that are difficult for AI models to replicate. TheCAPTCHA generation process is dynamic and session-specific, ensuring that each challenge is unique, time-bound, and resistant to replay attacks. The design incorporates multimodal verification techniques, including interactive image-basedtasks,objectmanipulationchallenges, logical reasoning micro-tasks, and temporal sequence interactions. These challenges require real-time perception, reasoning ,and fine-grained motor coordination ,which significantly limits the effectiveness of automated solvers. To further enhance robustness against AI attacks, adversarial perturbations and controlled randomness are embeddedwithinCAPTCHAelements
,introducing variations that are imperceptible to humans but disruptive to machine learning models trained on static data sets .Additionally ,the AI-proof CAPTCHA design integrates behavioral analysis by evaluating user interaction patterns such as mouse dynamics, keystroke timing, and response latency during challenge completion. A hybrid verification mechanism combines CAPTCHA accuracy with behavioral consistency scores to make final access decisions. Cryptographic one-time token sand sessionbinding ensure that solved challenges cannot be reused or shared a cross sessions. Throughadaptive difficulty adjustment and continuous learning from failed attempts, the proposed AI-proofCAPTCHAdesignachieveshighsecurity
,low false positives ,and strong resistance to evolving AI-driven attacks while preserving a seamless user experience.

RoleOf Fingerprint

Fingerprint recognition plays a crucial role in securehumanverificationsystemsbyprovidingare liable and unique biometric trait for identity authentication. Since fingerprint patterns arehighly distinctive and remain stable over an individual's lifetime, they offer a strongmechanism for verifying genuine users and preventing impersonation. In secure CAPTCHA systems with AI-proof verification, fingerprint authentication can be used as an additional or fallback verification layer when behavioralanalysis or CAPTCHA challenges indicate suspicious activity .By integrating fingerprint data captured through biometric sensors or trusted devices, the system ensures that access request originate from real human users rather than automated bots or AI-driven attack tools. Furthermore, fingerprint-based verification enhances security by enabling multi-factor authentication,reducingfalseacceptancerates, and strengthening resistance against replay and spoofing attacks when combined with liveness detection techniques. Overall, fingerprints contribute significantly to improving system trust, accuracy, and robustness in advanced security architectures.

FingerprintAuthentication Module

The Fingerprint Authentication Module serves as an additional biometric verification layer to enhancethesecurityandreliabilityof theproposed AI-proof CAPTCHA system. This module leverages the uniqueness and permanence of fingerprint patterns to authenticate legitimateusers, especially in scenarios where behavioral analysis or CAPTCHA responses indicate suspicious activity. Fingerprint data is captured using a trusted biometric sensor integrated into the user's device or external authentication hardware, ensuring accurate acquisition and secure

transmission. Once captured, the fingerprint image undergoes preprocessing operations such as noise reduction,ridgeenhancement, andsegmentation to improve image quality. Minutiae features, including ridge endings and bifurcations, are extracted and converted into a compact template. For security and privacy, the fingerprint templateis encrypted and stored securely, preventing unauthorized access or misuse. During authentication, the extracted template is matched againsttheenrolledreferencetemplateusinga

similarity matching algorithm. A match score is computed and compared with a predefined threshold to determine authentication success. The module also incorporates liveness detection techniques to prevent spoofing attacks using fake or replicated fingerprints.

The fingerprint authentication result is combined with CAPTCHA verification and behavioral confidence scores through the system's decision engine to perform multi-factor verification. By integrating fingerprint authentication as a secondary or fallback mechanism, the system significantly reduces false acceptance rates and strengthens resistance against automated bots and AI-driven attacks, thereby improving overall system robustness and trustworthiness.

SecurityAnalysis

The security analysis of the proposed AI CAPTCHA system integrated with fingerprint authentication demonstrates itsrobustnessagainst both traditional automated attacks and advanced AI-driven threats. By combining behavioral analysis, adaptive CAPTCHA challenges, and biometric fingerprint verification, the system achieves a multi-layered defense mechanism that significantly increases the difficulty of successful attacks. Automated bots and scripted attacks are effectively mitigated through dynamicCAPTCHA generation and session-bound challenges, which prevent replay and brute-force attempts.AI-based attacks that rely on machine learning models to solve CAPTCHA challenges are countered through challenge randomization, adversarial perturbations, and continuousmutation of CAPTCHA elements. These techniques disrupt pattern learning and dataset reuse by AI solvers. Additionally, behavioral analysis further strengthens security byidentifying non-human interaction patterns, even when CAPTCHA responses appear correct. Suspicious sessions are escalated to fingerprint authentication, ensuring that access is grantedonly to verified human users. The inclusion of fingerprint authentication enhances protection against impersonation and credential-sharing attacks by leveraging the uniqueness and permanence of biometric traits. Secure template storage,encryption,andlivenessdetectionprevent spoofing and unauthorized biometric reuse. Even in the event of partial system compromise, attackers must bypass multiple independent verification layers, significantly reducing the probability of successful intrusion. Overall, the integrated AI CAPTCHA with fingerprint authentication provides strong resistance to replay, spoofing, and AI-driven attacks while maintaining low false acceptance rates and high system reliability. reuse by AI solvers. Additionally, behavioral analysis further strengthens security by identifying non-human interaction patterns, even when CAPTCHA responses appear correct. Suspicious sessions are escalated to fingerprint authentication, ensuring that access is granted only to verified human users. The inclusion of fingerprint authentication enhances protection against impersonation and credential-sharing attacks by leveraging the uniqueness and permanence of biometric traits. Secure template storage, encryption, and liveness detection prevent spoofing and unauthorized biometric reuse. Even in the event of partial system compromise, attackers must bypass multiple independent verification layers, significantly reducing the probability ofsuccessful intrusion. Overall, the integrated AI CAPTCHA with fingerprint authentication providesstrongresistancetoreplay,spoofing,and AI-driven attacks while maintaining low false acceptance rates and high system reliability.

ExperimentalResult

The experimental evaluation of the proposed AI CAPTCHA system integrated with fingerprint authentication was conducted to assess its effectiveness, usability, and resistance against automated and AI-driven attacks. The system was implemented in a controlled environment with a test dataset comprising both human participants and AI- based bots simulators. Behavioral interactions such as mouse dynamics, keystroke patterns, and response latency were collect data long side fingerprint templates for multi-factor verification. The system performance was evaluated using standard metrics including accuracy, false acceptance rate (FAR), false rejection rate (FRR), and human success rate (HSR). Results indicate that the integrated AI CAPTCHAsystemachievedahighhumansuccessrate of approximately 95%, demon strating that legitimate users could easily complete challenges withminimal effort.Thefingerprintauthentication module achieved a matching accuracy of 98%, significantly reducing false acceptance of unauthorized users. Automated bots and AI-based solvers were able to bypass only 3–5% of CAPTCHA challenges, indicating strongresistance against AI-driven attacks .Additionally, time analysis showed that the average challenge completion time for humans was 8–12 seconds, while bots required significantly longer and often failed behavioral consistency checks. The combination of adaptive CAPTCHA challenges, behavioral scoring, and fingerprint verification effectivelyminimizedbothFARandFRR
,demonstrating the system's robustness. Overall, the experimental results confirm that integrating AI-proof CAPTCHA with fingerprint authentication significantly enhances system security, improvesresistancetoautomatedattacks, and maintains user-friendly interaction.

Application

The AI CAPTCHA system integrated with fingerprint authentication has wide-ranging applications in environments where high security and robust human verification are essential. One primary application is in online banking and financial transactions, where the combination of behavioral analysis, AI-proof CAPTCHA, and fingerprintverification ensuresthatonlylegitimate users can authorize sensitive actions, preventing fraud and unauthorized access. Similarly, e-commerce platforms can leverage this system to protect user accounts, payment gateways, and personalizedservicesfromautomatedbotsandAI-driven credential attacks. In government and healthcare portals, the system provides secure access to personal records, digital IDs, andmedical data, ensuring compliance with privacy regulations whilemitigating automated or scripted attacks. Additionally, the system is highlysuitable for online examination and e-learning platforms, where preventing impersonation, cheating, and bots-drivensubmissions is critical. Enterprise systems and corporate login portals can also implement this solution as part of multi-factor authentication to protect confidential information, internal tools, and intellectual property .Overall, the integration of AI

CAPTCHA with fingerprint verification offers a scalable, user-friendly, and high-security solution suitable for any digital platform requiring robust human authentication, makingitidealforfinancialservices,e-governance,healthcare,education,andcorporate applications.

Benefits

The integration of AI-proof CAPTCHA with fingerprint authentication provides multiple benefits that enhance the overall security, usability, and reliability of digital systems. First, it significantly improves resistance against automated bots and AI- driven attacks by combining adaptive CAPTCHAChallenges with behavior a land biometric verification. Second, the use of fingerprints ensures unique and permanent user identification, reducing the risk of impersonation, credential sharing, and unauthorized access. Third, the multi-layered verificationapproachreducesfalseacceptance rates (FAR) and false rejection rates (FRR), thereby increasing system accuracy and trustworthiness. Fourth, the system is user-friendly ,as legitimate user scan pass CAPTCHA challenges quickly while suspicious or high-risk interactions areverified through fingerprint authentication. Fifth, it supports multi-factor authentication, strengthening the security of sensitive applications such as online banking, e-commerce, e-governance, and healthcare portals. Finally, the integration of AI CAPTCHA with fingerprint authentication provides scalability and adaptability: the system can evolve with emerging attack methods, continuously retrain AI models, and maintain robust security without compromising user experience. Overall, this combination delivers a secure, reliable, and efficient human verification solution suitable for a wide range of digital applications.

Conclusion

Thispaper presentedaSecureCAPTCHAand Fingerprint System with AI-ProofVerification, addressing the limitations of traditional authentication systems. By integrating biometric verification with an AI-resistant CAPTCHA, the system provides robust security against modern cyber threats while maintaining user convenience. The proposed framework offers a scalable and reliable solution for high-security digital environments.

Futureenhancement

While the proposed AI CAPTCHA system integrated with fingerprint authentication demonstrates strong security and robustness against automated and AI- driven attacks, severala venuesfor futureenhancement exist. One potential improvement is the integration of **multi-modal biometrics** ,such as facial recognition or iris scanning ,along side fingerprintstoprovide **higherlevelsof multi-factor authentication** and further reducefalse acceptance rates. Another enhancement involves the application of **advanced AI techniques**, including reinforcement learning and generative adversarial networks, to dynamically adapt CAPTCHA complexity in real time based on evolving attack strategies, ensuring sustained resistance to increasingly sophisticated AI solvers. Improving **behavioral analytics** with deeper contextual understanding—such as user device patterns, geo location, and habitual interaction sequences—can strengthen anomaly detection and further distinguish humans from bots.

Additionally, optimizingthesystem for **mobileandIoTdevices** will expand usability without compromising security, considering the growing number of users accessing digital platforms via smartphone and wearabledevices. Theimplementation of**privacy-preserving techniques**, such as homo morphic encryption or federated learning ,can allow secure handling offing print and behavioral data while adhering to regulatory requirements. Finally, continuous system evaluation through large-scale user studies and simulated attack environmentswill enable therefinement of thresholds, challenge designs, and AI-model retraining strategies. These enhancements will collectively ensure that the AI CAPTCHA with fingerprint authenticationremains scalable, user-friendly, and resilient to future automated, AI-driven, and biometric spoofing attacks.

Reference

.N.K.Ratha ,K.Karu, S.Chen ,and A.K.Jain, "Areal-timematchingsystemforlargefingerprint

databases,"IEEETransactionson Pattern Analysis and Machine Intelligence,vol.18,no.8,
pp.779–813,Aug.1996.

A. K. Jain, L. Hong, and R. Bolle, "On-line fingerprint verification," IEEE Transactions on PatternAnalysisandMachineIntelligence,vol.19, no. 4, pp. 302–341, Apr. 1997.

.Lihong ,Y.Wan,and A.K.Jain, "Fingerprint image enhancement: Algorithms and performance evaluation, "IEEET rans actions on Pattern AnalysisandMachineIntelligence,vol.20,no.8,
pp.777–789,Aug.1998.

A. Jain, Y. Chen, and M. Demirkus, "Poresand ridges: Fingerprint matching using level 3 features," in Proc. IEEE Int. Conf. Image Processing (ICIP), 2000.

A. M. Bazen and S. H. Gerez, "Systematic methods for the computation of directional fields and singular points of fingerprints," IEEE Transactions on Pattern Analysis and Machine Intelligence,vol.24,no.7,pp.905–919,Jul.
2002.

Wayman, and A. K. Jain, "FVC2000: Fingerprint Verification Competition," IEEE Transactions on Pattern Analysis and Machine Intelligence,vol.24,no.3,pp.402–412,Mar. 2002.

A. Jain, A. Ross, and S. Prabhakar, "An Introduction to Biometric Recognition," IEEE Transactions on Circuits and Systems for Video Technology, 2004.

.L.VonAhnetal.,"CAPTCHA:
Using Hard AIProblemsforSecurity,"EUROCRYPT,2 003.

.W. Stallings, Cryptography and Network Security, Pearson, 2017.

P. Jain et al., "AI-Proof CAPTCHA Techniques," International Journal of Computer Applications, 2019.