International Journal of Environmental Sciences
ISSN: 2229-7359
Vol. 11 No. 16s,2025
https://theaspd.com/index.php

Passive Captcha: Ai Driven Bot Detection For Seamless User Experience

Chirag Mohitkar[1], Aditya Kharat[2], Nupur Nashirkar[3], Tilakkumar Pardeshi[4], Dr. Prajwal S. Gaikwad[5]
[1,2,3,4]Student, Department of Computer Engineering, AISSMS IOIT, Pune, India chiragmohitkar@gmail.com, adityakharat7028@gmail.com, nashirkarnupur65@gmail.com, tilak755@gmail.com
[5]Assistant Professor, Department of Computer Engineering, AISSMS IOIT, Pune, India prajwal.gaikwad@aissmsioit.org

Abstract
Traditional CAPTCHA approaches are becoming more susceptible to automated solution techniques, for which reason sophisticated and adaptive security techniques must be formulated. In this document, we present a behavior- based CAPTCHA improvement framework based on machine learning-assisted analysis of real-time user behavior. In contrast to depending on static challenges, our strategy records and assesses behavioral biometrics in the form of keystroke dynamics and mouse movement patterns in order to distinguish humans from bots.The Keystroke Detection Module regularly identifies characteristics such as dwell time, inter-key delay, and typing rhythm using a trained Random Forest classifier to detect bot-like typing behavior. At the same time, the Mouse Movement Detection Module scrutinizes trajectory characteristics such as speed, curvature, jitter, and direction changes to detect automated patterns, e.g., linear or grid movement. A majority voting system is used to make robust classification by combining multiple trajectory judgments.Both modules are combined into a real-time detection system that includes GUI support and a Flask REST API, allowing multi-modal analysis through the combination of mouse and keystroke inputs. Classification models are exportable in ONNX format to facilitate portability across platforms. To extensively verify system resilience, Selenium-based automation simulates bot behavior, including artificial typing and mouse movements. Test results indicate high precision in real-time bot detection with a seamless user experience and strong security. This research enhances CAPTCHA systems by replacing challenge-response modes with adaptive behavior-based authentication.

Index Terms: *User Behavior Analysis, Deep Learning, Human-Bot Differentiation, Keystroke Dynamics.*

INTRODUCTION

CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) systems have long served as a frontline defense against automated access to web services. By presenting challenges that are easy for humans but difficult for machines, traditional CAPTCHA systems aimed to prevent bot activity such as spamming, credential stuffing, and scraping. However, recent advances in automation tools and machine learning have enabled bots to increasingly bypass these systems by mimicking human-like behavior with high precision.

This growing vulnerability has exposed significant limitations in static CAPTCHA challenges, prompting a shift toward behavior-based verification. Unlike traditional CAPTCHAs that rely on solving puzzles or identifying images, behavior-based methods analyze the natural patterns of human interaction—such as typing rhythms and mouse trajectories—to distinguish legitimate users from bots.

In this study, we propose a dynamic, behavior-driven alternative to traditional CAPTCHA systems. Our approach focuses on two key biometric modalities: keystroke dynamics and mouse movement patterns. By analyzing features like dwell time, inter-key delay, trajectory curvature, and pointer speed, our system classifies users using a Random Forest model, selected for its interpretability and efficiency in real-time applications.To ensure real-world applica- bility, we developed a real-time GUI for live detection and a Flask-based REST API for seamless integration with web services. The trained models are exportable in ONNX format, enabling deployment across various platforms. Additionally, we employ Selenium-based automation to simulate bot interactions, allowing us to rigorously test the system's resilience against sophisticated scripted behaviors.

Our work contributes to the growing field of intelligent bot detection by offering a non-intrusive, adaptive verification method that enhances user experience without compromising security. This paper outlines the system design, implementation, and experimental evaluation of our approach, demonstrating its potential as a robust alternative to conventional CAPTCHA mechanisms.

LITERATURE SURVEY

Moradi and Morteza (2024) discussed the evolution of CAPTCHA system design, emphasizing the dilemma of ensuring security while maintaining user accessibility. Their work illustrates how deep learning, especially CNNs, has revealed weaknesses in conventional image-based CAPTCHAs. With the capacity to handle large datasets, these models can now easily overcome most existing CAPTCHA challenges. To counter automated attacks, the authors propose introducing more sophisticated and adaptive CAPTCHA mechanisms. They also emphasize the importance of having a system that is highly secure yet provides an easy user experience, promoting the implementation of behavioral biometrics and adaptive verification methods. This research provides insightful findings on how CAPTCHA systems can be made stronger against future threats.[1]

In 2024, Cheng Zhijun proposed the Reinforced Perturbation Generation (RPG) model, which utilizes reinforcement learning to generate text-based CAPTCHAs that are secure yet user-friendly. RPG manipulates CAPTCHA text so that it becomes challenging for computer programs to understand but remains readily legible by humans. Experimental results show that RPG successfully resists conventional computerized attacks with a great increase in CAPTCHA security. By achieving a balance between machine-based attack security and providing a seamless user experience, this approach is a milestone in CAPTCHA technology.[2]

Sharma, Sahil, and Dhawan Singh, in their research work of 2024, offer a critical analysis of how CAPTCHA systems have evolved, tracking their journey through the ages and analyzing how they have learned to counter the emerging security risks. They provide a detailed look at the different types that have emerged, such as dynamic CAPTCHAs, text-based ones, image-based systems, and even audio-based solutions. Each of these variants offers its own unique way of distinguishing humans from bots, reflecting the ongoing battle between security needs and technological advancement. They provide an overview of relay approaches and their shortcomings, providing the transformative potential of machine learning to increase web security. The paper highlights the need for future studies to break away from the current limitations inherent in deep learning approaches applied in CAPTCHA systems. The study provides valuable details on how machine learning can shape the future CAPTCHA design, providing avenues for enhanced security while, at the same time, overcoming existing limitations.[3]

The authors Iyapparaja, M., Isvarya Karunanithi, and Sahana Bhat (2024) demonstrate that keystroke dynamics, combined with Mahalanobis distance and machine learning algorithms such as Isolation Forest, can achieve a 90 accuracy rate, offering a secure and convenient authentication method suitable for applications in banking, e-commerce, and access control systems [4]

Yusuf, Mukhtar Opeyemi, Divya Srivastava, and Riti Kushwaha (2023) introduce a Self-Supervised Multiview CAPTCHA Recognition Model (SS-MCR) that utilizes contrastive learning to improve text-CAPTCHA recognition with limited labeled data. The model outperforms traditional methods by enhancing CAPTCHA security while minimizing the reliance on large labeled datasets. This innovative approach provides a more efficient solution to CAPTCHA recognition, addressing challenges in security and data labeling.[5]

The authors Herna ́ndez-Castro, Carlos, David F. Barrero, and Maria Dolores R-Moreno (2023) find inherent design weaknesses in CaptchaStar and conduct an in-depth analysis with the BASECASS approach, including machine learning methods. Their findings show an attack bypassing CaptchaStar with a nearly 100 percent success rate, thus pointing to critical weaknesses in its design and highlighting the necessity of CAPTCHA security enhancements.[6]

Ma, Wenshuo (2023) introduces Momentum Integrated Gradients (MIG), a novel attack method that generates transferable adversarial examples for both Vision Transformers (ViTs) and Convolutional Neural Networks (CNNs). The method demonstrates superior performance and transferability, offering an effective approach to attack deep learning models across different architectures.[7]

Wang, Ping (2023) provides a comprehensive investigation of text-based CAPTCHA attacks, presenting a new taxonomy of CAPTCHA schemes and a unified attack framework. The study evaluates 20 CAPTCHA schemes for accuracy and efficiency, providing valuable insights into their robustness. Additionally, the author provides an open-access dataset with 22 CAPTCHA sample sets to support further research in CAPTCHA security.[8]

Authors Sinha, Soumen, and Mohammed Imaz Surve (2023) achieved 94.67 percent accuracy in alphanumeric CAPTCHA breaking on a 200,000-sample dataset. The approach showed more robust recognition and performance compared to traditional deep learning methods and thus indicates exceptional progress in the field of CAPTCHA- breaking methods.[9]

Nuwan Kaluarachchi and Sevvandi Kandanaarachchi (2023) integrate novel features based on key distances with traditional flight times, achieving over 99 percent accuracy and less than 10 percent equal error rates across desktop, mobile, and tablet devices. Their approach surpasses existing keystroke dynamics methods, offering enhanced performance and versatility across different platforms.[10]

Zhao, Ruijie (2023) utilizing masked autoencoders (MAE) with ViT encoder and semi-supervised learning, significantly outperforms existing methods and achieves high efficiency, solving CAPTCHAs in 25 ms on a CPU and 9 ms on a GPU while effectively breaking complex CAPTCHA schemes with minimal labeled data.[11]

Authors Gajani, Yuvraj K., Shivam Bhardwaj, and M. Thenmozhi (2023) used Neural Style Transfer with VGG-16 to create visually challenging CAPTCHAs that enhance security by preventing automated bot attacks. Their experimental validation shows the effectiveness of the approach, with metrics such as MSE: 12934.04, RMSE: 113.72, and PSNR: 7.013, demonstrating resilience against similarity-based attacks.[12]

Chen, Jun (2023) separates style from structure by using a style transfer network to convert complex handwritten CAPTCHAs into simple print-friendly ones. The method has more accurate breaking than those introduced at NDSS'16, CCS'18, and "Science" 2017, as reflected by the experiment results on eBay, Google, and reCAPTCHA CAPTCHAs.[13]

Tariq, N.O.S. H. I.N.A. (2023) evaluates the usability, robustness, and weaknesses of various CAPTCHA types. The study summarizes common attack methods and compares the differences between CAPTCHA systems and their vulnerabilities. Highlights the challenges of securing CAPTCHAs against evolving automated threats and provides a comprehensive analysis of the effectiveness of different CAPTCHA approaches. Through an identification of current gaps and suggestion of new areas for future study, this research helps develop the field. This work contributes to the advancement of the field by identifying gaps and proposing areas for further investigation [14].

In 2023, scientists Dinh, Nghia, Kiet Tran-Trung, and Vinh Truong Hoang proposed a novel method of bolstering the security of conventional CAPTCHAs. By incorporating invisible noise with adversarial examples using a process known as Neural Style Transfer, they created a more robust CAPTCHA system. This process considerably raises the bar for deep learning models to defeat CAPTCHAs, introducing an additional level of security against increasingly sophisticated automated attacks. Consequently, the system is more efficient at identifying and inhibiting bot behavior while having robust security protocols.[15]

In a 2023 paper, Trong, Nghia Dinh, Thien Ho Huong and Vinh Truong Hoang explored further the new ways of enhancing CAPTCHA security using state-of-the-art methods such as adversarial samples and neural style transfer. The method, through the integration of text-based, image-based, and cognitive hurdles, renders CAPTCHAs extremely difficult for automated systems to bypass without compromising user convenience. The paper offers illustrations of how deep learning and cognitive principles can be used to strengthen bot identification without compromising user experience. The authors have indicated that their method may potentially result in future CAPTCHA systems that are more resilient and adaptable.[16]

Momentum Integrated Gradients (MIG), which was proposed as an attack method by Wenshuo Ma in 2023, is crafted to produce adversarial examples that are universally usable across various neural network architectures such as Convolutional Neural Networks (CNNs) and Vision Transformers (ViTs). The integration of momentum-based accumulation with integrated gradients in MIG makes it very efficient in transferring adversarial situations between models. Large-scale testing reveals that this method performs better than conventional methods in many scenarios and is thus a better strategy for testing and undermining neural network robustness.[17]

In 2023, Wang Wenhai employed deformable convolution to enhance adaptive spatial aggregation, yielding state- of-the-art performance on benchmark datasets such as ImageNet, COCO, and ADE20K. The approach achieved new records with 65.4 mAP on the test-dev of COCO and 62.9 mIoU on ADE20K, which demonstrated its efficiency in enhancing object detection and segmentation tasks. The performance outshines that of top Convolutional Neural Networks (CNNs) and Vision Transformers (ViTs), thereby confirming the effectiveness of deformable convolution in improving spatial feature aggregation. The study demonstrates the ability of the method in pushing the boundaries of tasks with object detection and segmentation. The study adds to the current progress in computer vision by offering enhanced accuracy and efficiency in these complicated datasets.[18]

Zhenao Wei, Pujana Paliyawan, and Ruck Thawonmas concentrated on enhancing AI players in the lottery card matching game in their 2022 study. They created a linear model that improved deep-feature similarities by utilizing previously gathered data from human gamers. Their results demonstrate that although this approach aids in bridging the gap between human and machine perception of pictures, optimal results still require a specific quantity of human- like similarity data. The study emphasizes how crucial it is to combine human knowledge with machine learning to achieve more accurate results. 2[19]

Qiu, Jucheng, and Xiaoyu Wu (2021) proposed a multi-task learning method using a convolutional neural network for end to-end CAPTCHA recognition, combined with an active learning strategy to select the most representative samples demonstrating that this approach significantly improves accuracy compared to random sample selection and enhances the efficiency of training with fewer samples.[20]

DESIGN METHODOLOGY

A. *Overview*

Our system differentiates humans from bots by analyzing real-time behavioral data from keystroke dynamics and mouse movements. Features such as typing rhythm, key press durations, cursor speed, and movement patterns are extracted and preprocessed to capture meaningful interaction characteristics.

For classification, we apply machine learning models tailored to each data type, using optimized algorithms to enhance detection accuracy. The system combines results from keystroke and mouse analysis for more reliable identification.

Detection is enabled through a real-time GUI and a REST API for easy integration with web platforms. Models are exported in a cross-platform format to support diverse deployment environments. Selenium-based automation is employed to simulate bot interactions and evaluate system robustness.

We measure performance using standard metrics to ensure a balance between security and user experience. Future enhancements aim to incorporate real-time visualization and adaptive thresholding for improved, seamless verification.

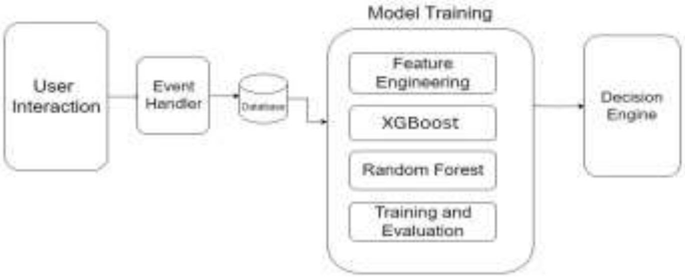

Fig. 1. System Architecture

B. *Data Acquisition*

Behavioral data is collected from users interacting with web interfaces, focusing on two primary modalities:

keystrokes and mouse movements. Keystroke data includes key press and release events along with timing information such as dwell time and inter-key intervals. Mouse data captures cursor positions over time, movement trajectories, speeds, and click events.

To gather realistic human interaction patterns, data is recorded during typical user sessions in a controlled environment. Additionally, automated bot interactions are simulated using Selenium scripts, which generate synthetic keystrokes and mouse movements to mimic various automated attack scenarios.

All collected raw data is logged and securely stored for preprocessing and feature extraction. This comprehensive dataset ensures that the model is trained and tested on a diverse range of behaviors, enabling effective differentiation between humans and bots.

C. ***Model Training and Testing***

The model training and testing process involves transforming raw interaction data into meaningful behavioral features. Key features extracted include session time, total keystrokes, mouse movement distance, number of clicks, click rate, idle time, and movement speed—each crucial for distinguishing human behavior from automated bot patterns.

The dataset is split into an 80:20 ratio for training and testing to evaluate model performance on unseen data. Cross-validation is applied to further assess model stability and prevent overfitting, thereby enhancing generalization across diverse user behaviors. Feature scaling is performed to normalize input values, improving model stability and convergence.

For keystroke data, classifiers such as Random Forest and XGBoost are trained with hyperparameter tuning to optimize performance. Mouse movement data is analyzed using a range of machine learning algorithms to capture subtle behavioral nuances. Model evaluation employs metrics including accuracy, precision, recall, and F1-score, aiming for reliable bot detection while minimizing false positives.

D. ***Algorithms Applied***

Our system employs a range of machine learning algorithms designed to effectively analyze behavioral biometric data for distinguishing humans from bots.

Keystroke Analysis: We utilize Random Forest and XGBoost classifiers due to their strong ability to model complex interactions among features like dwell time and inter-key delays. These algorithms are well-suited for handling high-dimensional data and provide robust predictions. Hyperparameter tuning is performed to optimize model performance, ensuring both accuracy and generalization across varied typing patterns.

Mouse Movement Analysis: To capture the diverse and subtle nature of mouse dynamics, we apply several classification algorithms, including Logistic Regression, Random Forest, Gradient Boosting, AdaBoost, Gaussian Naive Bayes, K-Nearest Neighbors (KNN), and Support Vector Machines (SVM). Each algorithm contributes unique strengths — for instance, Logistic Regression offers interpretability, while ensemble methods like Gradient Boosting and AdaBoost enhance predictive power by combining multiple weak learners. SVM excels at handling non-linear decision boundaries, which are common in behavioral data.

By employing this broad set of algorithms, the system can analyze multiple facets of user behavior from different perspectives, enhancing its robustness and accuracy in detecting automated interactions. The ensemble approach also helps reduce errors from any single classifier, resulting in more reliable and consistent bot detection.

OBSERVATIONS AND RESULTS

The experimental evaluation of our system demonstrated strong performance in distinguishing human users from bots through behavioral analysis. Keystroke-based models, particularly Random Forest and XGBoost with tuned hyperparameters, showed high accuracy in capturing subtle variations in typing rhythm, dwell time, and inter-key delays. These models consistently achieved strong precision and recall, indicating reliable detection of automated typing patterns while minimizing false positives.

Mouse movement classifiers, leveraging a diverse set of algorithms, effectively identified non-human cursor behaviors such as linear trajectories and repetitive grid patterns commonly exhibited by bots. Ensemble methods like Gradient Boosting and AdaBoost provided robust classification performance, while SVM and K-Nearest

Neighbors contributed valuable insights by detecting non-linear and neighborhood-based patterns in movement data. Integration of keystroke and mouse movement analysis via the combined detection framework resulted in im- proved overall accuracy and confidence scores. This multi-modal approach enhanced resilience against sophisticated automated attacks that mimic human behavior in one modality but not the other.

Testing with Selenium-driven bot simulations validated the system's robustness, revealing that automated interactions could be detected reliably despite attempts to mimic human input timing and movement variability. Performance metrics such as accuracy, precision, recall, and F1-score consistently indicated a balance between strong bot detection and low disruption to genuine users.

These results highlight the potential of behavior-based, machine learning-driven CAPTCHA alternatives to provide seamless user verification without traditional challenge-response interruptions.

To assess the model's efficiency, we use the following performance metrics:

To assess the overall performance of a classification model by measuring how many predictions it got right compared to the total number of predictions

$$\text{Accuracy} = \frac{\text{Correct Predictions}}{\text{Total Predictions}}$$

To measure how many of the predicted positive instances are actually positive.

$$\text{Precision} = \frac{TP}{TP + FP}$$

To measure how well the model captures all relevant instances.

$$\text{Recall} = \frac{TP}{TP + FN}$$

F1-Score: Harmonic mean of Precision and Recall, ensuring a balanced measure.

$$F1 = 2 \times \frac{\text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}}$$

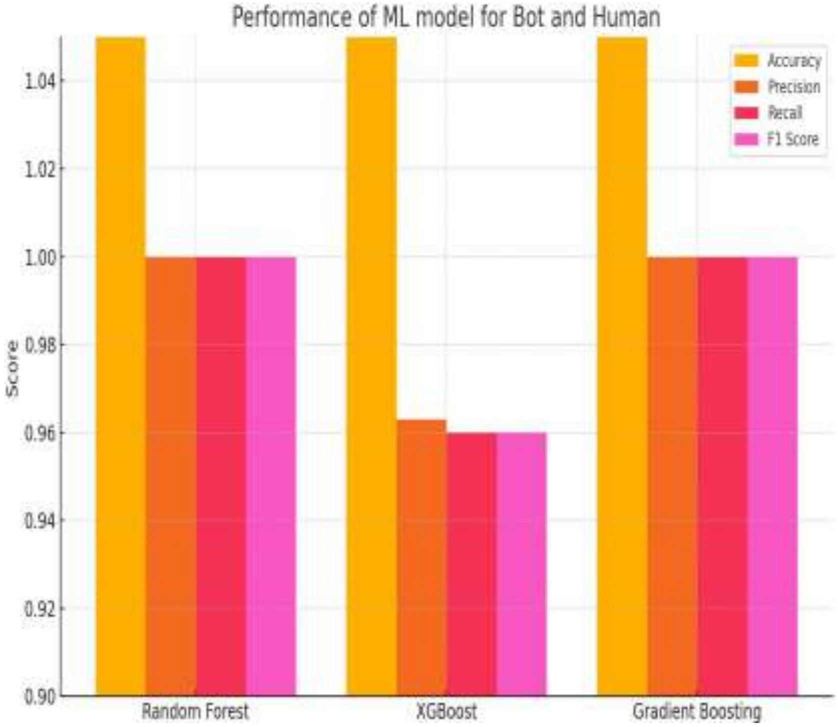

Fig. 2. Comparison of ML Models

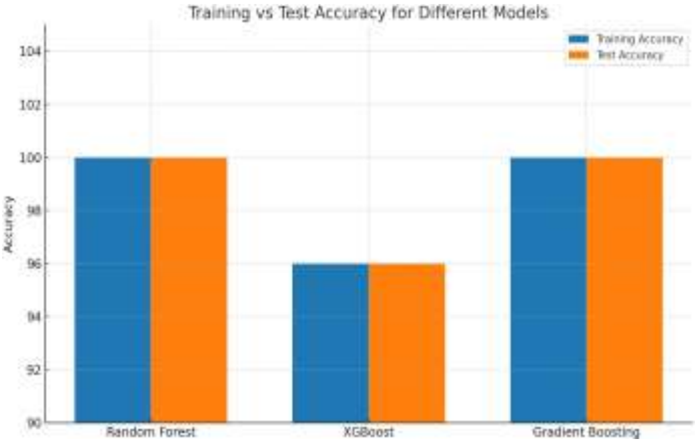

Fig. 3. Training Vs. Test Accuracy Comparison

ML Model	Accuracy	Precision	Recall	f1score
Random Forest	100	1.00	1.00	1.00
XGBoost	96	0.9629	0.9600	0.9599
Gradient Boost- ing	100	1.00	1.00	1.00

TABLE I PERFORMANCE OF ML MODELS FOR BOT AND HUMAN

Observations:

- This work describes an effective methodology in separating human users from robots by monitoring their behaviors and utilizing machine learning strategies.
- Utilizing Support Vector Machines and Random Forest, the system optimizes the handling of keystroke patterns, mouse trace dynamics, click actions, and session durations to further develop CAPTCHA approaches. Inclusion of real-time data sampling and session tracking enables greater responsiveness from the model for bot identification at a minimal loss to human users.
- In addition, feature engineering and normalization of data enhance stability in classification, making way for an intelligent, CAPTCHA-free authentication experience without lowering security levels.
- Despite these innovations, adaptive bot behavior, adversarial attacks, and platform-specific differences are avenues of future research. Additional advancements may include integration of reinforcement learning, optimization of deep learning architectures, and multi-model behavioral analysis for better accuracy and robustness.
- By creating an unobtrusive but secure CAPTCHA substitute, this research is a contribution to future-generation AI-based authentication frameworks, with uses in web security, fraud detection, and user experience enhance- ment.

ML Model	Training Accuracy (%)	Test Accuracy (%)
Random Forest	100	100
XGBoost	96	96
Gradient Boosting	100	100

TABLE II TRAINING VS. TEST ACCURACY FOR DIFFERENT MODELS

CONCLUSION

This study successfully demonstrates that behavioral biometrics combined with machine learning can effectively distinguish human users from automated bots, enhancing CAPTCHA security while maintaining user convenience. By analyzing keystroke and mouse movement patterns, the system provides a robust, adaptive alternative to traditional CAPTCHA methods, reducing user friction without compromising protection against automated attacks. The integration of real-time monitoring and comprehensive feature processing contributes to a stable and accurate classification framework. Although challenges remain—such as evolving bot tactics and platform variability—this
approach lays a strong foundation for future work aimed at creating seamless, non-intrusive verification systems. Future research will focus on incorporating advanced learning techniques and expanding behavioral modalities to further improve detection accuracy and resilience. Overall, this work advances the development of intelligent, user-friendly authentication solutions that align with the growing need for secure yet effortless online experiences.

ACKNOWLEDGMENT

The success and outcome of this report demanded a great deal of direction. We are thankful to our guide, Mrs. Prajwal S. Gaikwad, for her experience and support. We appreciate her for her insight and information, which were extremely useful throughout the course of the study. We would like to thank Dr. S.N. Zaware, Head of the Computer Engineering Department, AISSMS Institute of Information Technology, for her assistance. We would also like to thank our Principal Dr. P.B. Mane for his energetic and helpful advice during the project, as well as for providing the essential facilities that enabled us to complete our dissertation work.

REFERENCES

[1] Moradi, M., Moradi, M., Palazzo, S., Rundo, F. and Spampinato, C.,2024. Image CAPTCHAs: When Deep Learning Breaks the Mold. IEEE Access.

[2] Cheng, Z., Wu, Z., Yang, Z., Yang, Z., Li, X. and Liu, W., 2024, May. Reinforced Perturbation Generation for Adversarial Text-based CAPTCHA. In 2024 27th International Conference on Computer Supported Cooperative Work in Design (CSCWD) (pp. 2746-2751). IEEE.

[3] Sharma, S. and Singh, D., 2024, March. CAPTCHA in Web Security and DeepCaptcha Configuration based on Machine learning. In 2024 3rd International Conference for Innovation in Technology (INOCON) (pp. 1-6). IEEE

[4] Iyapparaja, M., Karunanithi, I. and Bhat, S., 2024, February. Enhancing User Authentication through Keystroke Dynamics Analysis using Isolation Forest algorithm. In 2024 Second International Conference on Emerging Trends in Information Technology and Engineering (ICETITE) (pp. 1-5). IEEE.

[5] Yusuf, M.O., Srivastava, D. and Kushwaha, R., 2023, December. Exploring selfsupervised learning in Multiview captcha recognition. In 2023 IEEE 20th India Council International Conference (INDICON) (pp. 1106-1111). IEEE.

[6] Hern´andez-Castro, C., Barrero, D.F. and R-Moreno, M.D., 2023. Breaking CaptchaStar using the BASECASS methodology. ACM Transactions on Internet Technology, 23(1), pp.1-12.

[7] Ma, W., Li, Y., Jia, X. and Xu, W., 2023. Transferable adversarial attack for both vision transformers and convolutional networks via momentum integrated gradients. In Proceedings of the IEEE/CVF International Conference on Computer Vision (pp. 4630-4639).

[8] Wang, P., Gao, H., Guo, X., Xiao, C., Qi, F. and Yan, Z., 2023. An experimental investigation of text-based captcha attacks and their robustness. ACM Computing Surveys, 55(9), pp.1-38.

[9] Sinha, S. and Surve, M.I., 2023, September. CAPTCHA Recognition And Analysis Using Custom Based CNN Model-Capsecure. In 2023 International Conference on Emerging Techniques in Computational Intelligence (ICETCI) (pp. 244-250). IEEE.

[10] Nuwan Kaluarachchi, S.K., 2023. DEFT: A new distance-based feature set for keystroke dynamics.

[11] Zhao, R., Deng, X., Wang, Y., Yan, Z., Han, Z., Chen, L., Xue, Z. and Wang, Y., 2023, May. GeeSolver: A generic, efficient, and effortless solver with selfsupervised learning for breaking text captchas. In 2023 IEEE Symposium on Security and Privacy (SP) (pp. 1649-1666). IEEE

[12] Gajani, Y.K., Bhardwaj, S. and Thenmozhi, M., 2023, April. Guarding Against Bots with Art: NST-based Deep Learning Approach for CAPTCHA Verification. In 2023 International Conference on Recent Advances in Electrical, Electronics, Ubiquitous Communication, and Computational Intelligence (RAEEUCCI) (pp.1-5). IEEE.

[13] Chen, J., Luo, X., Zhu, L., Zhang, Q. and Gan, Y., 2023. Handwritten CAPTCHA recognizer: a text CAPTCHA breaking method based on style transfer network. Multimedia Tools and Applications, 82(9), pp.13025-13043.

[14] Tariq, N.O.S.H.I.N.A., Khan, F.A., Moqurrab, S.A. and Srivastava, G., 2023. CAPTCHA Types and Breaking Techniques: Design

Issues, Challenges, and Future Research Directions. arXiv preprint arXiv:2307.10239.

[15] Dinh, N., Tran-Trung, K. and Hoang, V.T., 2023. Augment CAPTCHA Security Using Adversarial Examples With Neural Style Transfer. IEEE Access.

[16] Trong, N.D., Huong, T.H. and Hoang, V.T., 2023. New cognitive deep-learning CAPTCHA. Sensors, 23(4), p.2338.

[17] Ma, W., Li, Y., Jia, X. and Xu, W., 2023. Transferable adversarial attack for both vision transformers and convolutional networks via momentum integrated gradients. In Proceedings of the IEEE/CVF International Conference on Computer Vision (pp. 4630-4639).

[18] Wang, W., Dai, J., Chen, Z., Huang, Z., Li, Z., Zhu, X., Hu, X., Lu, T., Lu, L., Li, H. and Wang, X., 2023. Internimage: Exploring large-scale vision foundation models with deformable convolutions. In Proceedings of the IEEE/CVF conference on computer vision and pattern recognition (pp. 14408-14419).

[19] Wei, Z., Paliyawan, P. and Thawonmas, R., 2022. Improving Deep-Feature Image Similarity Calculation: A Case Study on an Ukiyo-e Card Matching Game Lottery. IEEE Access, 10, pp.44608-44616.

[20] Qiu, J. and Wu, X., 2021, December. Captcha Recognition based on Multitask Convolutional Neural Network and Active Learning. In 2021 IEEE Fourth International Conference on Artificial Intelligence and Knowledge Engineering (AIKE) (pp. 108-112). IEEE.