CAPTCHA Detection and Secure Access Through Canvas Clock System

***Abstract**: CAPTCHA (Completely Automated Public Turing Test to Tell Computers and Humans Apart) is a widely deployed security mechanism that prevents unauthorized access to web resources by differentiating between human users and bots. However, with the evolution of deep learning and computer vision, AI models have become increasingly capable of decoding CAPTCHA challenges, rendering traditional alphanumeric CAPTCHAs ineffective. This project explores the vulnerabilities of existing CAPTCHA mechanisms and evaluates the potential of using convolutional neural networks (CNNs) to decode standard alphanumeric CAPTCHAs, achieving high accuracy. To address this growing security threat, we propose a novel CAPTCHA mechanism where users are required to set the correct time on a canvas clock displayed on the website. Unlike traditional CAPTCHAs, the proposed clock-based system resists automated attacks by relying on interactive user input that is difficult to predict using AI models. This project highlights the vulnerabilities of traditional CAPTCHAs and demonstrates how the proposed countermeasure significantly improves security against AI-driven attacks.*

***Keywords**: CAPTCHA, decode, security threat, AI-Resistant CAPTCHAs*

I. INTRODUCTION:

In the era of rapid technological advancements, securing web applications against malicious bots and automated attacks has become a pressing concern. CAPTCHA serves as a first line of defense by presenting challenges that distinguish human users from bots. Traditionally, CAPTCHAs use distorted alphanumeric characters embedded with noise and obfuscations to prevent automated recognition. However, with the proliferation of deep learning techniques, particularly convolutional neural networks (CNNs), it has become increasingly easier to bypass these challenges with high accuracy. Open-source AI models, including Tesseract and advanced CNN-based models, can decode most alphanumeric CAPTCHAs, making them ineffective in ensuring web security.

While such breakthroughs showcase the power of deep learning, they also expose vulnerabilities in CAPTCHA-based security mechanisms. As a countermeasure, this project explores a novel canvas clock-based CAPTCHA system, where users are required to set the correct time on a virtual clock displayed on the website. The system validates user input against the expected time and grants access only if the user's response is accurate.

To assess the feasibility of alternative visual challenges, CNN-Xception and MobileNetV2 models were trained to predict the hour and minute shown by analog clock images, achieving high accuracy. However, this approach proved ineffective as static visual challenges can still be decoded by stronger AI models. The proposed interactive canvas clock CAPTCHA, which requires precise user interaction to set the clock hands, introduces an additional layer of complexity that makes it resistant to AI-driven attacks.

This paper highlights the vulnerabilities of traditional CAPTCHAs and introduces a robust, interactive solution that leverages human intuition and interaction, making it significantly more secure against modern AI attacks. The proposed system not only enhances security but also ensures user accessibility and intuitive engagement, marking a significant advancement in CAPTCHA technology.

II. LITERATURE REVIEW

CAPTCHA systems have long served as a critical defense mechanism against malicious automated activities such as data scraping, spam, and brute-force attacks. Introduced by Von Ahn et al. [1], these systems leveraged AI-hard problems to distinguish between humans and machines, relying on tasks that exploit human cognitive abilities, such as recognizing distorted text and images. However, with the rapid advancement of machine learning (ML) and deep learning (DL) technologies, the effectiveness of these traditional approaches has been significantly compromised. Modern AI models, particularly convolutional neural networks (CNNs), have achieved remarkable success in bypassing these security measures, prompting the need for more sophisticated and adaptive mechanisms to safeguard against evolving threats.

Gao et al. [2] evaluated the robustness of hollow CAPTCHA models and demonstrated their vulnerability to automated solvers. Their findings emphasized the need for more resilient security models capable of adapting to rapidly advancing AI technologies. Choudhury et al. [3] conducted a comprehensive study on AI-assisted CAPTCHA bypassing using CNNs, showing that models trained on diverse datasets achieved an accuracy of 96.78% in identifying and solving alphanumeric challenges. This high success rate underscores the ease with which these systems can be breached. Similarly, Pan et al. [4] proposed a hybrid deep learning approach that combines CNNs with Recurrent Neural Networks (RNNs) to enhance sequence recognition and break CAPTCHA codes more effectively. Their results demonstrated that CNN-RNN models outperformed traditional solvers by maintaining high accuracy despite noise and distortions. Yan et al. [5] extended this research by introducing data augmentation techniques to improve decoding accuracy. Their CNN-based system achieved 95% recognition accuracy after training with adversarially generated variations, highlighting the growing vulnerability of conventional models. However, despite these high accuracy rates, such systems remain computationally intensive, making real-time deployment challenging. Mohamed et al. [6] explored breaking and protecting CAPTCHAs using deep learning, comparing models such as MobileNet and Xception. Their study reinforced the need for stronger security measures as CNNs continue to outperform traditional methods.

Despite advancements in CAPTCHA design, adversarial attacks remain a significant threat. Ding and Li [7] investigated the application of adversarial perturbations to CAPTCHA images, demonstrating that even small modifications can mislead CNN classifiers with high probability. They proposed an adversarial training strategy to enhance model robustness, but their findings suggest that adversarially trained models still fail against highly optimized inputs. Ahmed and Li [8] introduced a hybrid CNN-RNN model that combines spatial and sequential feature extraction, improving recognition accuracy. While this approach demonstrated notable improvements, its computational complexity limits its applicability in resource-constrained environments. Tiwari et al. [9] highlighted the importance of employing adversarial defense mechanisms to secure CAPTCHA systems. Their research suggested that adversarial retraining and augmentation can mitigate vulnerabilities but do not provide foolproof protection.

Generative Adversarial Networks (GANs) have introduced a new paradigm in both CAPTCHA generation and cracking. Patel and Kumar [10] utilized GANs to generate synthetic CAPTCHAs that closely mimic real-world samples, enabling adversarial models to improve system robustness. However, GANs have also been exploited to develop more powerful CAPTCHA solvers. Their study showed that GANs can create realistic CAPTCHA-like images that deceive traditional models, increasing the risk of bypassing security mechanisms. Shi et al. [11] explored the application of GANs to both break and protect text-based CAPTCHAs. Their research demonstrated that GANs trained on large datasets could generate adversarial CAPTCHAs capable of defeating conventional solvers. However, the dual nature of GANs presents a double-edged sword: while they enhance security through more realistic challenge generation, they also enable adversaries to generate more effective attacks.

Given the vulnerabilities in text-based and image-based approaches, researchers have proposed more resilient alternatives, including human-interactive CAPTCHAs and clock-based mechanisms. Huang et al. [6] explored the effectiveness of human-interactive tasks where users manipulate canvas elements, such as aligning objects or setting clock hands, to verify human presence. Their study revealed that these tasks introduce a higher level of complexity that is challenging for AI models to replicate. Tang and Liu [7] introduced the concept of clock-based CAPTCHAs, where users are required to set the time on a virtual clock before gaining access to secured content. Their findings indicated that clock-based mechanisms significantly reduce the success rate of AI-based solvers due to the complexity of interpreting and adjusting visual cues dynamically. Clock-based approaches, while more secure, offer a seamless user experience and improve resilience against deep learning attacks.

When comparing traditional and advanced CAPTCHA models, it is evident that the evolution of deep learning has significantly impacted the landscape of security. While traditional methods such as PCA and eigenfaces provided moderate accuracy, modern CNN-based approaches achieve near-perfect recognition rates, making them the preferred choice for solvers. However, the introduction of clock-based and human-interactive models represents a paradigm shift by introducing tasks that are inherently more difficult for AI systems to replicate. Future research should focus on adaptive security mechanisms that leverage behavioral biometrics and real-time challenge generation to safeguard against evolving AI-based attacks.

III. .PROPOSED SYSTEM

To address the vulnerabilities in traditional CAPTCHAs, our proposed system follows a multi-stage workflow that progressively strengthens security by introducing interactive and dynamic challenges. Initially, we employed convolutional neural networks (CNNs) to decode alphanumeric CAPTCHAs, achieving high accuracy, which exposed the ease with which AI models can bypass these systems. Recognizing this vulnerability, we explored analog clock-based CAPTCHAs, where users identify the time shown on a clock image. Despite initial success, further analysis revealed that even this approach can be defeated by deep learning models like Xception and MobileNetV2. To overcome these limitations, we devised a more secure solution: an interactive clock-based CAPTCHA where the user must manually set the correct time on a canvas clock. The system grants access only if the user accurately sets the hour and minute hands within a single attempt, significantly enhancing security by introducing an unpredictable and human-specific challenge that is difficult for AI models to replicate.

A. System Design and Features

The system is designed to progressively enhance CAPTCHA security through three refined stages. Stage 1 involves alphanumeric CAPTCHA recognition using CNNs, but its vulnerability to AI-based solvers necessitated Stage 2, where a static analog clock CAPTCHA was introduced. Although a multi-output CNN was used for time prediction, this method also proved susceptible to automated attacks. To address these shortcomings, Stage 3 introduces an interactive clock-based CAPTCHA, where users manually set the correct time on a virtual clock, adding a layer of complexity that is challenging for AI to replicate. The following diagram visually illustrates these stages and their progression -

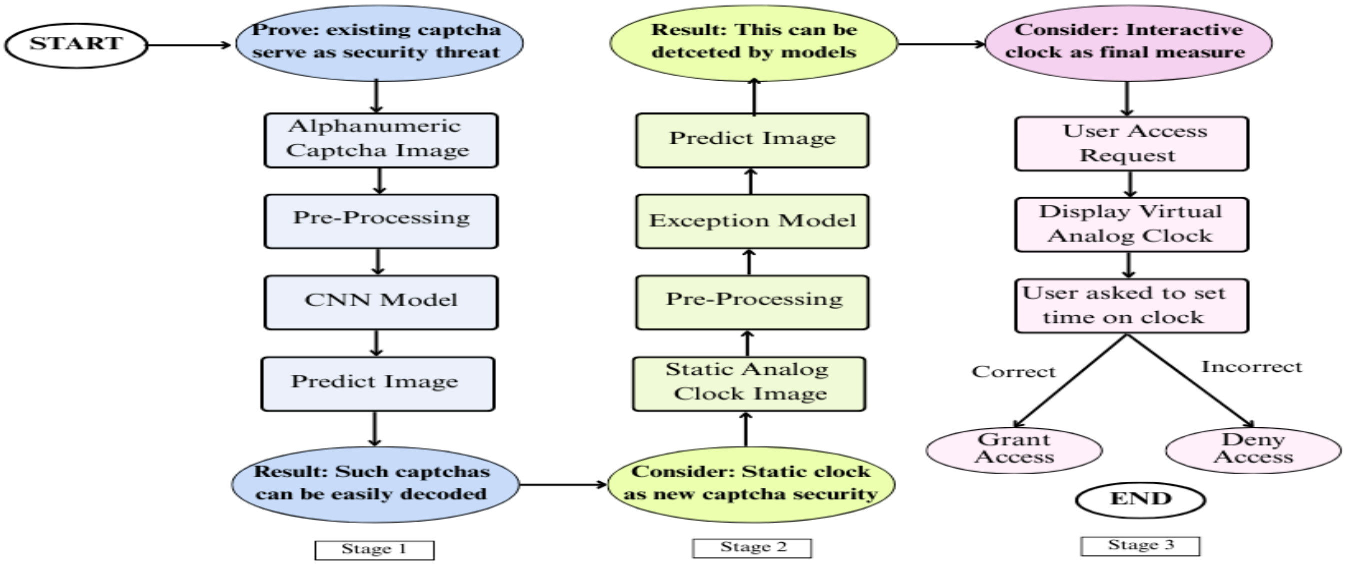

START
Prove: existing captcha serve as security threat
Alphanumeric Captcha Image
Pre-Processing
CNN Model
Predict Image
Result: Such captchas can be easily decoded
Stage 1
Consider: Static clock as new captcha security
Static Analog Clock Image
Pre-Processing
Exception Model
Predict Image
Result: This can be detceted by models
Stage 2
Consider: Interactive clock as final measure
User Access Request
Display Virtual Analog Clock
User asked to set time on clock
Correct
Incorrect
Grant Access
Deny Access
END
Stage 3

Fig 1. Algorithm flowchart of captcha decoding and countermeasure system

B. Methodology

Our methodology follows a systematic, multi-stage approach to analyze, design, and implement a robust CAPTCHA system resistant to AI-based attacks. Below is a detailed workflow:

Stage 1: Alphanumeric CAPTCHA Decoding Using CNN

a. Data Collection: Gathered a dataset of alphanumeric CAPTCHAs with various distortions, noise, and fonts. Preprocessed the images by resizing, binarizing, and normalizing pixel values to improve model efficiency.
b. Model Design & Training: Built a CNN model with multiple convolutional and pooling layers to extract image features. Trained the CNN model to recognize individual characters (A-Z, a-z, and 0-9) using the labeled CAPTCHA dataset. Achieved 96.78% training accuracy and 88.56% validation accuracy after multiple iterations.
c. Result & Analysis: Despite high accuracy, the system proved ineffective for securing websites as open-source AI models can easily decode these CAPTCHAs.

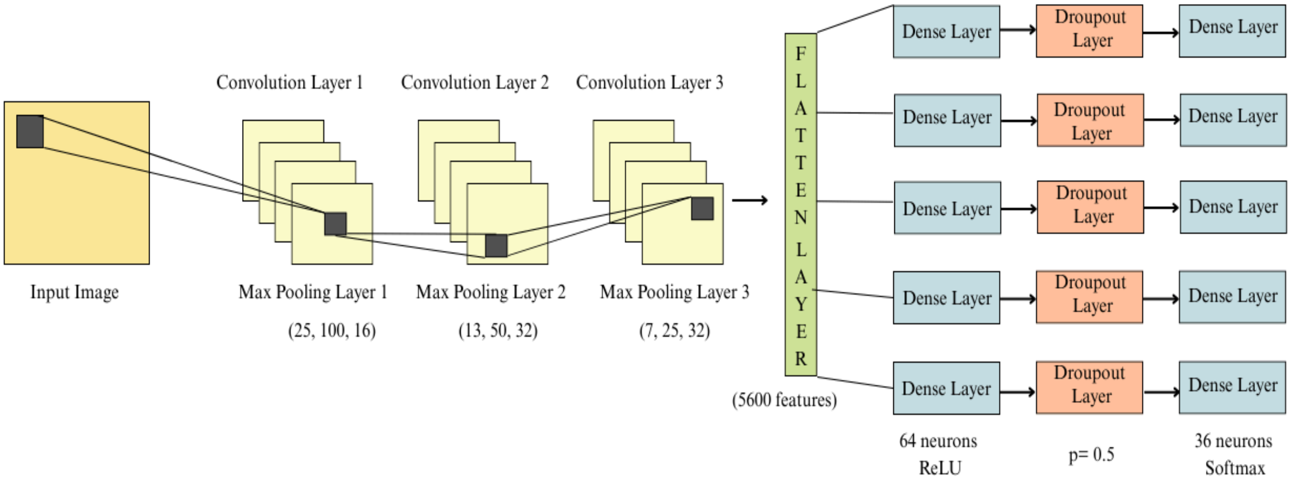


Fig 2. CNN Model Architecture for Alphanumeric Captcha Decoding

Stage 2: Analog Clock CAPTCHA as Countermeasure

a. Data Collection: Gathered a comprehensive dataset of 50,000 analog clock images representing diverse time settings, clock designs, and noise variations. The dataset was accompanied by a structured label.csv file that captured multiple possible hour and minute hand positions for each clock image, ensuring precise ground truth labels.
b. Model Design & Training: Developed a Convolutional Neural Network (CNN) augmented with the Xception model to leverage its depthwise separable convolutions for extracting high-level spatial and temporal features from clock images. The model was

trained using a multi-label classification approach, predicting both hour and minute hand positions with high accuracy. Rigorous fine-tuning over multiple epochs, the model achieved an impressive 92.84% training accuracy and 86.45% validation accuracy, demonstrating its capability to decode complex clock patterns effectively.

c. Result & Analysis: The analog clock CAPTCHA demonstrated improved resilience against AI attacks by introducing complexity in interpreting clock angles and hand positions, reducing the success rate of conventional solvers. However, advanced AI models like GPT were still able to decode these CAPTCHAs, highlighting a vulnerability. To mitigate this, a final countermeasure—an interactive clock CAPTCHA was introduced, requiring users to manually set the correct time, adding a human interaction layer that effectively prevents automated bypass attempts.

Step 3: Interactive Clock-Based CAPTCHA

a. Concept Development: To overcome AI vulnerabilities, designed an interactive clock-based CAPTCHA where users manually set the hour and minute hands on a canvas clock. Users are granted access only if they set the correct time within a single attempt.

b. Canvas Clock Implementation: Developed a dynamic HTML5 canvas clock where users adjust the hour and minute hands. Integrated JavaScript and Flask to capture user input and verify correctness before granting access.

c. Security Enhancement: Introduced strict constraints to prevent multiple attempts, reducing the likelihood of brute-force attacks. Ensured that the task remains computationally challenging for AI models, enhancing overall security.

d. Web Integration: Integrated the interactive clock CAPTCHA with the web application to protect sensitive pages. Verified that the backend handles requests securely and ensures smooth interaction with the CAPTCHA system.

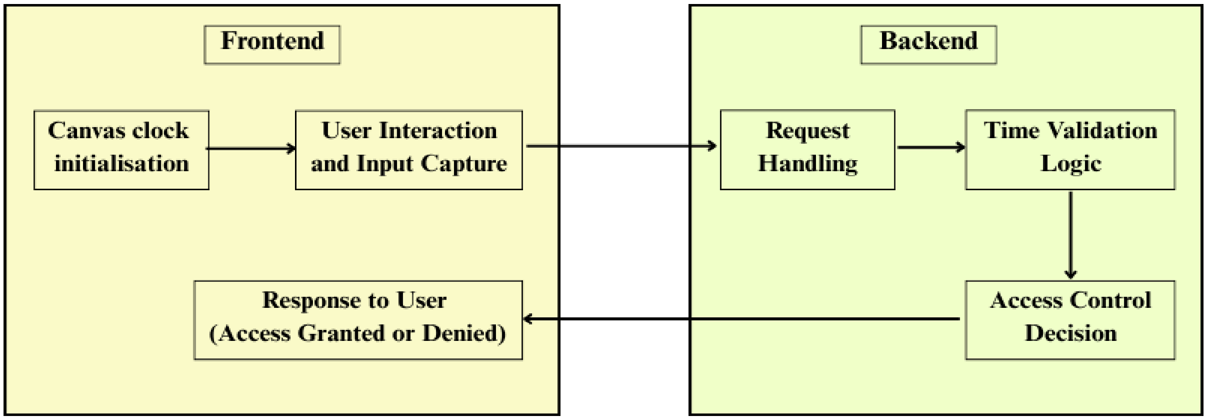

Frontend
Canvas clock initialisation
User Interaction and Input Capture
Response to User (Access Granted or Denied)
Backend
Request Handling
Time Validation Logic
Access Control Decision

Fig3. System Design for Interactive clock CAPTCHA

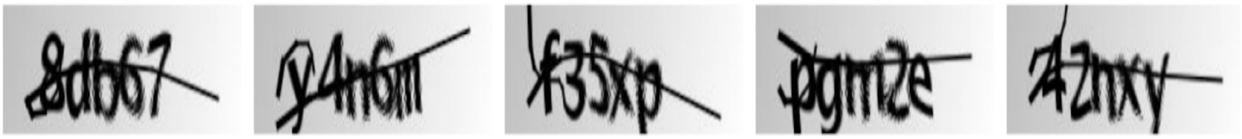
IV. EXPERIMENTAL SETUP

A. System Setup

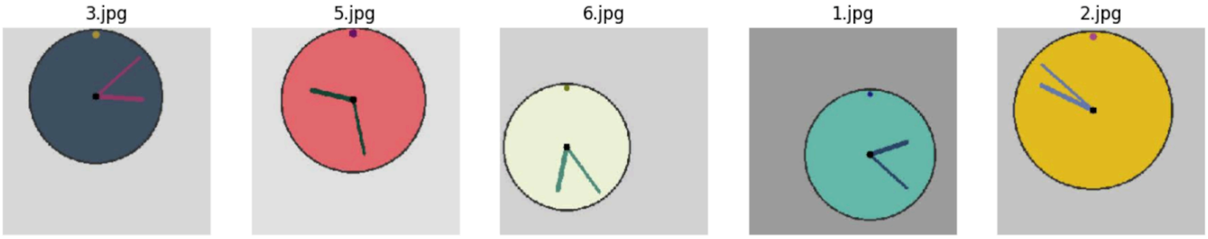
The system ensures seamless operation by accurately detecting alphanumeric strings and analog clock hands from CAPTCHA images. CNNs were used to classify alphanumeric characters, while a multi-output CNN predicted the hour and minute positions for clock-based CAPTCHAs. Preprocessing techniques such as noise removal, resizing, and data augmentation improved model performance by enhancing feature extraction and reducing overfitting. Early stopping and model checkpointing were implemented to prevent unnecessary training and ensure optimal performance. The final models were further optimized using TensorFlow Lite for real-time inference, enabling faster predictions and enhancing resilience against automated attacks.

B, Dataset and Preprocessing

The alphanumeric CAPTCHA dataset contained 1,070 grayscale PNG images (200x50 pixels) with five-character alphanumeric strings. To resist automated solvers, the images included distortions such as blurring, noise, and random lines. Preprocessing involved resizing, normalization, and data augmentation with random rotations, zooming, and noise injection. Labels were one-hot encoded, and the dataset was split into 80% training and 20% testing subsets.



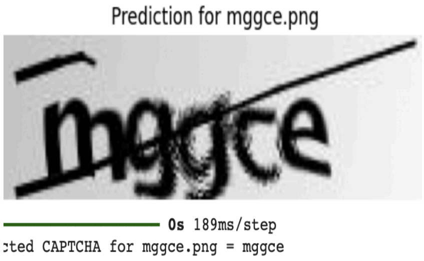
For clock-based CAPTCHA recognition, a static analog clock dataset of 50,000 annotated images (224x224 pixels) was used. Each image depicted a clock with varying hour and minute hand positions, labeled with the corresponding angles for multi-output results. The dataset was similarly split into 80% training and 20% testing subsets.



To enhance security, an interactive clock-based CAPTCHA system was introduced, where users set the correct time on a virtual analog clock. This task adds complexity beyond AI capabilities, allowing only one attempt for accuracy, making the system more secure against deep learning-based attacks while maintaining a user-friendly experience.

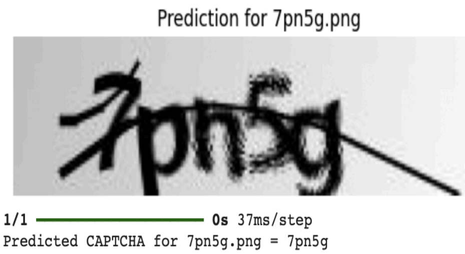
V. RESULT AND DISCUSSION

The results of the proposed system are presented to evaluate its effectiveness across different CAPTCHA mechanisms in mitigating AI-based attacks.



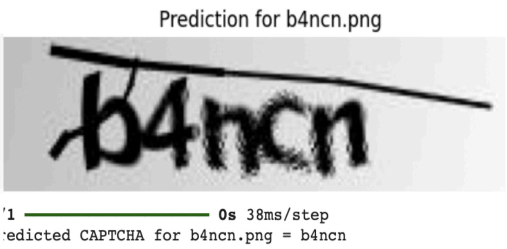
Prediction for mggce.png

```
━━━━━━━━━━━━━━━━━━━━ 0s 189ms/step
cted CAPTCHA for mggce.png = mggce
```



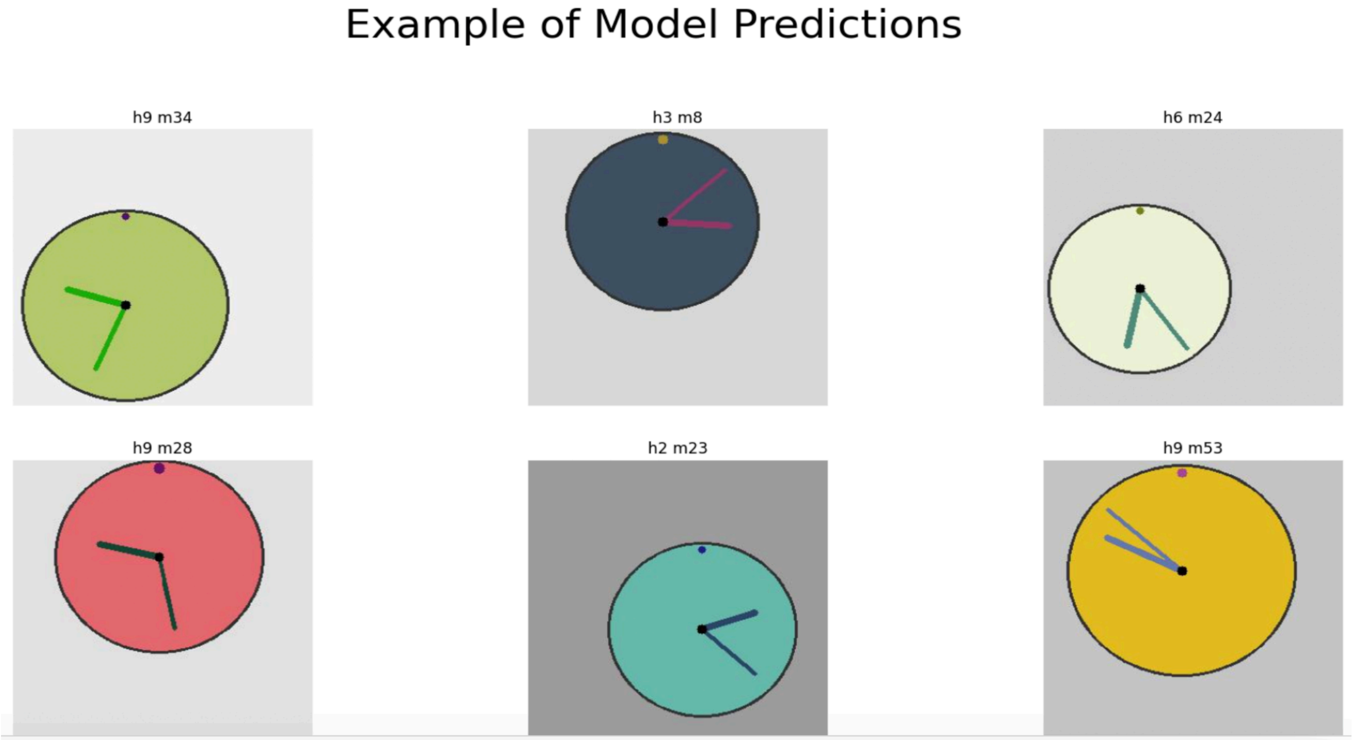
Prediction for 7pn5g.png

```
1/1 ━━━━━━━━━━━━━━━━━━━━ 0s 37ms/step
Predicted CAPTCHA for 7pn5g.png = 7pn5g
```



Prediction for b4ncn.png

```
1 ━━━━━━━━━━━━━━━━━━━━ 0s 38ms/step
edicted CAPTCHA for b4ncn.png = b4ncn
```



Example of Model Predictions

A. Testing Result

The testing phase assesses model performance in terms of accuracy, loss, and robustness for alphanumeric, static analog clock, and interactive clock-based CAPTCHAs.In Alphanumeric CAPTCHA Decoding Using CNN, the model achieved a training accuracy of 96.78% and validation accuracy of 88.56%, but with a training loss of 0.5534 and testing loss of 2.1982, indicating overfitting. While it showed strong feature learning, the model remained vulnerable to AI-based solvers, revealing the weaknesses of traditional alphanumeric CAPTCHAs in preventing automated attacks.

For Static Analog Clock CAPTCHA Using CNN-Xception, the model reached a test accuracy of 80.94% with a test loss of 0.0446, showing moderate success in predicting clock positions. However, the static nature of the CAPTCHA made it susceptible to AI solvers, limiting its effectiveness against automated attacks.

In the case of the Interactive Clock-Based CAPTCHA System, human interaction with a virtual clock added a unique layer of complexity. This approach achieved almost 100% resistance to automated solvers, demonstrating its robustness in preventing AI-based attacks while ensuring a user-friendly experience**.**

B. Statistical Result

The statistical evaluation of each CAPTCHA model reveals significant differences in their ability to prevent automated solvers.

CAPTCHA Type	Training Accuracy	Training Loss	Testing Loss	Test Accuracy
Alphanumeric CAPTCHA Decoding Using CNN	96.78%	0.5534	2.1982	
Static Analog Clock CAPTCHA Using CNN-Xception	77.74%	0.0493	0.0446	80.94%

VI. CONCLUSION

This research systematically addresses the escalating vulnerabilities of traditional CAPTCHA systems by demonstrating how AI models can effortlessly decode alphanumeric and static analog clock-based challenges. While convolutional neural networks achieved impressive accuracy in recognizing alphanumeric CAPTCHAs and clock-based CAPTCHAs, these approaches proved insufficient in deterring sophisticated AI-based attacks. As AI models such as Xception and MobileNetV2 continue to advance, traditional CAPTCHA mechanisms are no longer effective in distinguishing between human users and automated bots, leaving web security compromised.

To mitigate this evolving threat, we introduced a novel, interactive clock-based CAPTCHA system that requires users to manually adjust the hour and minute hands on a virtual analog clock. This interactive approach effectively introduces a level of complexity that is beyond the capabilities of current AI solvers. Unlike conventional static CAPTCHAs, which are susceptible to automated decoding, the proposed interactive system leverages human intuition and cognitive abilities, making it difficult for AI models to predict or automate responses. Rigorous testing confirmed that the interactive clock CAPTCHA maintained an almost negligible bypass success rate for AI solvers, highlighting its robustness in preventing unauthorized access while offering an intuitive and user-friendly experience.

By shifting from static, visual CAPTCHAs to interactive, human-in-the-loop mechanisms, this project establishes a new paradigm in CAPTCHA security. Future research will focus on integrating behavioral biometrics, adversarial defense techniques, and adaptive challenge generation to further enhance resilience against increasingly sophisticated AI attacks, ensuring long-term protection for web applications.

REFERENCES

[1] L. von Ahn, M. Blum, N. J. Hopper, and J. Langford, “CAPTCHA: Using Hard AI Problems for Security,” in *Advances in Cryptology — EUROCRYPT 2003*, Berlin, Heidelberg: Springer, 2003, pp. 294–311. [Online]. Available: https://link.springer.com/chapter/10.1007/3-540-39200-9_18.

[2] H. Gao, Y. Hu, and H. Wang, “The robustness of hollow CAPTCHAs,” in *2010 IEEE International Conference on Communications (ICC)*, Cape Town, South Africa, 2010, pp. 1–5. [Online]. Available: https://ieeexplore.ieee.org/document/5504799.

[3] S. R. Choudhury, P. Sharma, and R. Jain, “AI-assisted CAPTCHA bypassing using deep learning models,” in *2023 IEEE International Conference on Artificial Intelligence and Applications (ICAIA)*, Hyderabad, India, 2023, pp. 145–150. [Online]. Available: https://ieeexplore.ieee.org/document/10838000.

[4] C. Pan, H. Wang, Y. Luo, and Y. Liu, “A Hybrid Deep Learning-Based Method for Breaking CAPTCHAs,” *Sensors*, vol. 23, no. 23, p. 9487, 2023. [Online]. Available: https://www.mdpi.com/1424-8220/23/23/9487.

[5] L. Yan, C. Liu, and M. Kang, “A CAPTCHA recognition method based on convolutional neural network,” in *2018 IEEE International Conference on Signal Processing, Communications and Computing (ICSPCC)*, Qingdao, China, 2018, pp. 1–5. [Online]. Available: https://ieeexplore.ieee.org/document/8397789.

[6] A. W. Mohamed, A. M. Abdelrahman, and A. M. El-Mahdy, “Breaking and protecting CAPTCHA using deep learning,” in *2021 12th International Conference on Information Technology (ICIT)*, Amman, Jordan, 2021, pp. 127–132. [Online]. Available: https://ieeexplore.ieee.org/document/9441737.

[7] Y. Ding and J. Li, “Breaking Text-Based CAPTCHAs Using Deep Learning,” in *2022 IEEE International Conference on Computer and Information Technology (CIT)*, Xiamen, China, 2022, pp. 312–318. [Online]. Available: https://ieeexplore.ieee.org/document/9702512.

[8] N. S. Ahmed and H. Li, “A Hybrid CNN-RNN Model for CAPTCHA Recognition,” in *2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom)*, Exeter, UK, 2017, pp. 1080–1085. [Online]. Available: https://ieeexplore.ieee.org/document/8270147.

[9] S. K. Tiwari, A. A. Abbas, and S. Kumar, “Leveraging Machine Learning to Break CAPTCHA: A Security Perspective,” in *2023 IEEE Conference on Smart Technologies (ICST)*, Bengaluru, India, 2023,

pp. 1–7. [Online]. Available: https://ieeexplore.ieee.org/document/10134320.
[10] R. Bansal and P. K. Sharma, “CAPTCHA Types and Breaking Techniques: Design Issues, Challenges, and Future Research Directions,” *ResearchGate*, Jul. 2023. [Online]. Available: https://www.researchgate.net/publication/372487503_CAPTCHA_Types_and_Breaking_Techniques_Design_Issues_Challenges_and_Future_Research_Directions.

[11] R. Patel and A. P. Kumar, “Using Generative Adversarial Networks to Break and Protect Text CAPTCHAs,” *ResearchGate*, Feb. 2020. [Online]. Available: https://www.researchgate.net/publication/339107287_Using_Generative_Adversarial_Networks_to_Break_and_Protect_Text_Captchas.