RESEARCH PAPER

# An Intelligent Adaptive CAPTCHA Mechanism Using OCR and CNN for Secure Pharmaceutical Information Systems

**Dr. Resmi G Nair[1], Dr Sangeetha Shibu[2], Mr Jinu Raj R[3], Mrs Divya GS[4], Mrs Jincy Jesudasan[5]**

[1]Dean Academics & HOD of Department of Artificial Intelligence and Data Science, Holy Grace Academy of Engineering. Kuruvilassery, Mala, Kerala. reshmignair82@gmail.com

[2]Professor & HOD, Dept of Computer Science and Engineering, Rajadhani Institute of Engineering and Technology, Kerala. Email: sangeethas@rietedu.in

[3]Assistant Professor, Dept of Computer Science and Engineering, Rajadhani Institute of Engineering and Technology, Kerala. Email: jinurajr@rietedu.in

[4]Assistant Professor, Dept of Computer Science and Engineering, Rajadhani Institute of Engineering and Technology, Kerala. Email: divyags@rietedu.in

[5]Assistant Professor, Dept of Computer Science and Engineering, Rajadhani Institute of Engineering and Technology, Kerala. Email: jincyjesudasan@rietedu.in

**Abstract**

In modern pharmaceutical information systems, ensuring secure access to sensitive drug-related data and digital healthcare platforms has become increasingly important due to the growing threat of automated bot attacks and unauthorized access. Traditional CAPTCHA mechanisms provide a basic level of protection; however, they often compromise usability and accessibility, particularly for users accessing pharmaceutical databases and healthcare portals. This study proposes an intelligent adaptive CAPTCHA mechanism that integrates Optical Character Recognition (OCR) and Convolutional Neural Networks (CNNs) to enhance authentication and security in pharmaceutical information systems. The proposed system employs machine learning techniques and real-time behavioral analysis to dynamically adjust CAPTCHA difficulty based on user interaction patterns and response times. By continuously monitoring user behavior, the system intelligently generates personalized challenges that improve usability for legitimate users while effectively identifying automated bots. The framework incorporates multimodal CAPTCHA formats, including text and image-based challenges, improving accessibility and adaptability across diverse user groups. Additionally, the adaptive design increases resistance to automated bot training and improves overall system robustness. Experimental results demonstrate that the proposed approach achieves higher detection accuracy, reduced false-positive rates, and improved user experience compared to traditional CAPTCHA systems. The intelligent adaptive CAPTCHA mechanism provides a secure and user-friendly solution for protecting pharmaceutical data platforms, drug information systems, and digital healthcare applications from malicious automated access.

**Keywords :** Self-Adaptive CAPTCHA, Machine Learning, Bot Detection, OCR, CNN, Accessibility, Cybersecurity, User Experience, Multi-Modal Challenges

**How to cite this article:** Nair RG, Shibu S, Raj JR, Divya GS, Jesudasan J. An Intelligent Adaptive CAPTCHA Mechanism Using OCR and CNN for Secure Pharmaceutical Information Systems. Int J Drug Deliv Technol. 2026;16(11s): 429-438. DOI: 10.25258/ijddt.16.11s.43

## 1. Introduction

The unprecedented growth of digital services, e-commerce platforms, and online communication channels has revolutionized modern life, offering convenience and accessibility like never before. However, this rapid digitization has simultaneously opened the floodgates to a range of sophisticated cyber threats. Among these, automated bots pose one of the most insidious and rapidly evolving challenges. These bots are frequently employed for malicious activities such as scraping proprietary content, launching brute-force attacks, committing online fraud, impersonating legitimate users, and flooding systems with spam. As a result, distinguishing human users from bots has become a critical necessity for maintaining security, integrity, and trust in digital ecosystems.

This challenge is particularly significant in pharmaceutical information systems and digital healthcare platforms, where sensitive data such as drug formulations, clinical research records, patient prescriptions, and supply-chain information are stored and accessed through online portals. Unauthorized automated access to these systems may lead to data breaches, manipulation of drug information, intellectual property theft, or disruption of pharmaceutical supply chains. Consequently, ensuring secure authentication

mechanisms in pharmaceutical databases and healthcare platforms has become a critical requirement for safeguarding public health infrastructure.

CAPTCHA systems—Completely Automated Public Turing tests to tell Computers and Humans Apart—were initially developed as a robust solution to combat such threats. These systems typically challenge users with tasks that are presumed to be easy for humans but difficult for automated scripts, such as identifying distorted characters, recognizing objects in images, or solving basic logic puzzles. Traditional CAPTCHA systems have served as gatekeepers for years, offering a layer of protection against unauthorized or malicious bot access. In pharmaceutical platforms, CAPTCHAs are often deployed to secure drug information portals, clinical research databases, and e-prescription systems, preventing automated misuse.

Yet, despite their long-standing role, conventional CAPTCHA models are increasingly losing their effectiveness. With the emergence of deep learning, Optical Character Recognition (OCR), and generative AI technologies, modern bots can now mimic human behavior and solve CAPTCHA puzzles with high accuracy. Pre-trained models can be fine-tuned to recognize common CAPTCHA formats, and even behavioral CAPTCHA systems have been reverse-engineered by attackers using reinforcement learning techniques. In essence, what was once a reliable security measure is now a predictable and sometimes even vulnerable component of web applications, including those used in healthcare and pharmaceutical sectors.

Additionally, a significant usability gap persists in existing CAPTCHA implementations. These systems often operate under the assumption that all users possess similar capabilities, failing to consider those with disabilities, cognitive impairments, or differing technological proficiency. For individuals with visual impairments, dyslexia, motor disorders, or non-native language barriers, completing a CAPTCHA can become not only frustrating but also exclusionary. This lack of inclusivity undermines user experience and can lead to reduced engagement, abandoned sessions, or even digital inaccessibility for large segments of users accessing healthcare services or pharmaceutical portals.

In response to these multifaceted issues, this paper presents an intelligent self-adaptive CAPTCHA mechanism designed for secure pharmaceutical information systems. The proposed system dynamically tailors challenge complexity and content based on real-time user behavior analysis. Instead of deploying static, one-size-fits-all challenges, the system continuously monitors interaction patterns—such as typing cadence, mouse pointer speed, click delay, and historical attempt accuracy—to estimate the user's authenticity and adjust the CAPTCHA accordingly. This ensures that legitimate users, including healthcare professionals and researchers accessing pharmaceutical platforms, are presented with appropriately challenging and accessible puzzles while increasing the difficulty threshold for suspected bot activities.

The system specifically incorporates text-based and image-based CAPTCHA challenges powered by Optical Character Recognition (OCR) and Convolutional Neural Networks (CNNs). OCR models are used to generate and validate distorted pharmaceutical-related text patterns, while CNN-based models support image recognition tasks for identifying medical objects, symbols, or contextual image patterns. These machine learning components operate within a modular and scalable architecture designed to enhance the security of drug information systems, pharmaceutical research portals, and healthcare data platforms.

A key innovation of this architecture is its real-time adaptive feedback mechanism, where the system continuously collects user interaction data, refines its difficulty model, and dynamically modifies CAPTCHA challenges based on behavioral patterns. This adaptive capability improves bot-detection accuracy and enhances resilience against evolving AI-driven bot attacks targeting pharmaceutical systems.

Furthermore, the proposed system emphasizes accessibility, inclusivity, and personalized interaction, ensuring that legitimate users—such as pharmacists, researchers, clinicians, and healthcare administrators—can access digital pharmaceutical platforms without unnecessary cognitive or usability barriers. By integrating adaptive logic with intelligent machine learning techniques, the framework enhances both security and usability, addressing critical challenges in modern pharmaceutical information systems.

This research presents the complete design and implementation of the adaptive CAPTCHA framework, including data acquisition, behavioral analysis, machine learning model integration, challenge generation, response validation, and feedback-based adaptation. The study also examines practical deployment considerations such as system scalability, response latency, cross-device compatibility, and privacy protection in pharmaceutical environments.

Ultimately, this work aims to contribute a secure, intelligent, and adaptive authentication mechanism capable of protecting pharmaceutical information systems from sophisticated automated threats, while maintaining accessibility and usability for diverse user groups in digital healthcare ecosystems.

## 2. Literature Survey

Over the past decades, CAPTCHA systems have undergone significant evolution to counter the growing sophistication of automated bots. Traditional CAPTCHA mechanisms, such as text-based CAPTCHAs, require users to recognize and transcribe distorted characters. While effective in the past, these systems have become increasingly vulnerable due to advances in Optical Character Recognition (OCR) techniques and machine learning-based attacks.

Alternative approaches, such as image-based CAPTCHAs, challenge users to identify objects or patterns within images. Though visually engaging, they often lack accessibility for users with visual impairments and can be bypassed by deep learning models capable of image classification. Audio CAPTCHAs attempt to address accessibility issues by providing auditory challenges; however, speech recognition technologies and noise removal algorithms have made them susceptible to automated attacks.

More advanced CAPTCHA systems, including re CAPTCHA v2 and v3, leverage behavioural analysis and risk assessment to differentiate users from bots. These approaches utilize passive detection techniques to analyse user interactions, minimizing the friction associated with solving explicit challenges. Nevertheless, these methods often raise privacy concerns and may not guarantee complete security against sophisticated bots that mimic human behaviour.

Despite the diversity of CAPTCHA mechanisms, the persistent challenge lies in balancing security with usability and accessibility. Most existing solutions either fail to adapt to evolving threats or neglect inclusivity for users with disabilities. This paper addresses this gap by introducing a self-adaptive CAPTCHA system capable of dynamically adjusting difficulty and challenge types based on real-time user interactions and behavioral data, thus offering a more resilient and inclusive approach to online security.

Recent advancements in CAPTCHA systems have introduced innovative models that aim to improve both security against AI-based attacks and user accessibility. One such model uses **neural style transfer** to generate stylized images that confuse deep learning models while still being easily recognizable by humans. This approach leverages statistical metrics like Jensen-Shannon divergence to evaluate its effectiveness and supports extensions into multimodal and accessible CAPTCHA designs.

Another model enhances security by generating CAPTCHAs from **random collages of segmented objects**. By varying occlusions, scales, and layers, the model creates complex visual challenges that are difficult for object detection algorithms to solve. At the same time, humans can still recognize the objects due to semantic familiarity, and future extensions may incorporate tagging and natural language questions for more cognitive depth.

A **gamified CAPTCHA system** uses an interactive drag-and-drop interface where users must match images with appropriate targets. This type of cognitive engagement prevents bot interaction and makes the CAPTCHA experience more enjoyable. It is also optimized for low-resource environments and can be scaled for various platforms like smartwatches and browsers, enhancing its versatility.

A **sensor-driven model** uses mobile device orientation sensors to create a touchless interaction where users guide a ball into a specific target by tilting their device. Human movement patterns are analyzed using Dynamic Time Warping (DTW) to differentiate them from automated behaviors. This model achieves high accuracy in distinguishing bots from humans while offering a user-friendly experience on mobile platforms.

Another study focused on the vulnerability of text-based CAPTCHAs by training **deep neural networks using transfer learning**. The model demonstrated that with only a small dataset, it could achieve high success rates in solving even distorted CAPTCHAs. This reveals a critical weakness in traditional systems and emphasizes the need for more dynamic and adversarially resistant CAPTCHA methods.

## 3. Methodology

The self-adaptive CAPTCHA system employs a multi-layered architecture designed to dynamically adjust CAPTCHA challenges based on user interactions and performance metrics. The system's primary objective is to maintain a balance between security and usability while enhancing accessibility through adaptive challenge formats.

### 3.1 System Architecture

The proposed system architecture comprises the following components:

- **User Interaction Module**: Captures real-time user responses and interaction patterns, including typing speed, mouse movements, and response accuracy.
- **Challenge Generation Engine**: Generates CAPTCHA challenges using text, images, or audio formats, dynamically adjusting difficulty based on user behaviour.
- **Machine Learning Module**: Utilizes OCR and CNNs to process and analyse user input and evaluate the likelihood of human versus bot activity.
- **Adaptation Layer**: Adjusts challenge complexity in real time based on user

performance data and historical interaction patterns.

- **Database Management**: Stores user interaction data, challenge logs, and performance metrics for ongoing analysis and system optimization.

### 3.2 Adaptive Challenge Generation

The challenge generation engine utilizes a scoring algorithm that assigns difficulty levels based on the user's previous interactions. Low-risk users are presented with simpler challenges, while high-risk users encounter more complex, multi-modal CAPTCHAs. This adaptability ensures both user convenience and robust security.

### 3.3 Machine Learning Techniques

The system employs OCR for text-based CAPTCHA recognition and CNNs for image-based challenge analysis. These models are trained on large datasets to accurately distinguish between human responses and automated attacks. Additionally, the system incorporates data augmentation techniques to improve model robustness.

### 3.4 Real-Time Adaptation

The adaptation layer continuously monitors user responses, dynamically adjusting challenge formats and difficulty levels. This real-time adaptation minimizes user frustration while maintaining security against bots.

### 3.5 Accessibility Considerations

To ensure inclusivity, the system supports multi-modal challenges, including text, audio, and graphical formats. Accessibility options, such as adjustable font sizes and audio speed controls, are integrated to accommodate diverse user needs.

### 3.6 Adaptive CAPTCHA System Pipeline

**Data Collection:**

The system begins with the collection of real-time interaction data from users engaging with various CAPTCHA types, including text, image, and audio-based challenges. It gathers input such as mouse movements, keystrokes, click timings, and overall task completion time. Both human user interactions and known bot behaviors are logged to create a well-labeled and diverse dataset. To ensure inclusivity, accessibility-focused interaction data—like keyboard-only navigation and screen reader usage—is also recorded.

**Data Preprocessing:**

The collected data is then cleaned and standardized to ensure consistency. Noisy or irrelevant data is removed, and timestamps are normalized. CAPTCHA inputs such as image- or audio-based responses are transformed using OCR or audio-to-text techniques to extract usable features. The goal is to convert all challenge formats into machine-readable representations suitable for model training.

**Feature Extraction and Behavioral Profiling:**

At this stage, the system analyzes user interaction behavior to extract significant features. Characteristics like cursor movement paths, typing rhythms, response times, and error frequencies are computed to differentiate between human users and bots. These behavioral traits provide valuable indicators for the machine learning models that follow.

**Model Training:**

With preprocessed data and extracted features, the system trains multiple machine learning models. Convolutional Neural Networks (CNNs) are applied for image-based CAPTCHA recognition, while models like Support Vector Machines (SVM), Random Forest, or LSTM are used to classify user behavior as either human or bot. For adaptive CAPTCHA generation, reinforcement learning may also be used to dynamically optimize CAPTCHA difficulty based on user performance.

**Adaptive CAPTCHA Generation:**

Using the trained models, the system generates CAPTCHA challenges in real-time, adjusting their complexity to match the user's ability. A user who performs well may receive more difficult CAPTCHAs, whereas a struggling user is offered simpler challenges. This adaptability ensures both security and usability, especially for users with accessibility needs.

**Real-Time Classification and Feedback:**

During user interaction, the system performs real-time classification to determine whether the current session is likely human or bot activity. It uses the model's predictions along with historical user performance to decide the next CAPTCHA difficulty level or to block the session if suspicious.

**Continuous Learning:**

The system incorporates a feedback loop where new user interaction data is continuously added to retrain and fine-tune the models. This enables the CAPTCHA system to evolve and respond to new bot behaviors, keeping the defense mechanisms current and robust.

## 4. Existing System

The existing CAPTCHA recognition systems have significantly evolved with the advent of deep learning techniques. One notable approach is presented in the paper titled **"Research on CAPTCHA Recognition Technology Based on Deep Learning"**. This system primarily employs **Convolutional Neural Networks (CNNs)** and **Recurrent Neural Networks (RNNs)** to break CAPTCHAs by recognizing distorted text and patterns within images. By utilizing advanced deep

learning architectures, the system aims to enhance the accuracy and efficiency of CAPTCHA recognition, addressing challenges posed by complex and distorted CAPTCHA designs. The methodology of the existing system revolves around leveraging deep learning models to decode CAPTCHA images effectively.

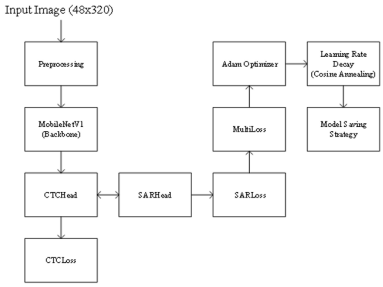



Figure 1. Overall Architecture and Training Process of the Model

CNNs are employed to recognize image-based CAPTCHAs by extracting spatial features from distorted and noisy CAPTCHA images. These neural networks are adept at capturing essential visual patterns that aid in decoding text and object-based CAPTCHAs, even when characters are cluttered or intertwined. On the other hand, RNNs are applied to text-based CAPTCHAs, where the sequential recognition of characters is crucial for accurate interpretation. The hybrid approach combining CNN and RNN models enables the system to processboth spatial and sequential data effectively, significantly improving recognition rates, especially for CAPTCHAs with complex structures or interconnected characters. The system utilizes multiple CAPTCHA datasets, comprising both text-based and image-based CAPTCHAs, commonly used in security research. These datasets encompass a wide range of distorted text and graphical CAPTCHAs designed to challenge automated recognition systems. The effectiveness of the existing system is demonstrated through its impressive accuracy, achieving recognition rates of over **90%** for text-based CAPTCHAs. However, the accuracy of image-based CAPTCHA recognition varies depending on the complexity and distortion level of the CAPTCHA.

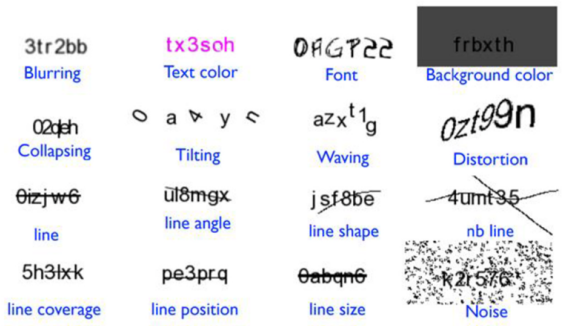



Figure 2. A main set of Text CAPTCHA

Despite its success, the existing system has some notable drawbacks. One significant limitation is the **lack of real-time adaptation**. Since the models are trained offline, they remain static and cannot adapt to new CAPTCHA patterns or evolving threats. This poses a risk when CAPTCHA generators employ novel techniques to counter automated recognition. Additionally, the combination of CNN and RNN models demands substantial computational resources, leading to high computational costs during both training and inference. This could hinder real-time CAPTCHA verification, especially in resource-constrained environments.

Furthermore, the existing system presents **accessibility challenges**. Most of the CAPTCHAs utilized in the system are purely visual, which makes them inaccessible to users with visual impairments. This limitation highlights the need for a more inclusive multi-modal approach that accommodates diverse user needs, such as incorporating audio or interactive CAPTCHAs.

Overall, while the existing system demonstrates high accuracy and efficiency in CAPTCHA recognition, it falls short in terms of adaptability and accessibility. Addressing these challenges is crucial to developing a more resilient and inclusive CAPTCHA recognition framework.

## 5. Proposed System

The self-adaptive CAPTCHA system dynamically adjusts challenge difficulty based on user performance metrics, such as response time and accuracy. It incorporates advanced image and text recognition models to differentiate between human and automated inputs. The primary components of the system are OCR for text-based CAPTCHA recognition and CNN for image-based CAPTCHA analysis.

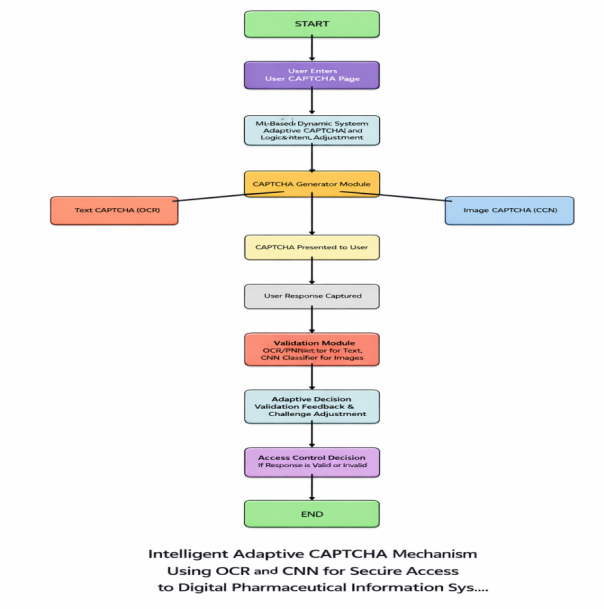



Figure 3. Workflow of the Self-Adaptive CAPTCHA System

**5.1 Optical Character Recognition (OCR)**

OCR is employed to recognize and extract text from images, playing a critical role in CAPTCHA analysis and verification. The OCR process typically involves the following steps:

1. **Image Preprocessing:**
   - Converts the input CAPTCHA image to grayscale.
   - Applies noise reduction techniques (e.g., Gaussian filtering) to enhance text clarity.
   - Uses thresholding to binarize the image, isolating text from the background.
2. **Text Localization:**
   - Detects regions containing text using contour detection or region-based methods.
   - Segments characters individually for accurate recognition.
3. **Character Recognition:**
   - Utilizes trained deep learning models (e.g., Tesseract or CNN-based OCR) to identify characters.
   - Maps recognized characters to ASCII or Unicode values.
4. **Post-Processing:**
   - Corrects errors using language models and dictionaries to improve accuracy.

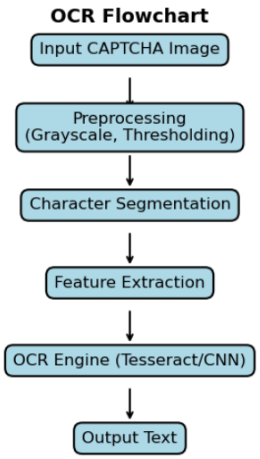



Figure 3. OCR Flowchart for CAPTCHA Text Recognition

OCR enhances the system's ability to analyse text-based CAPTCHA challenges by accurately recognizing characters, even when they are distorted or obfuscated.

**5.2 Convolutional Neural Networks (CNN)**

CNNs are integral to image-based CAPTCHA analysis, processing complex visual patterns to distinguish between human inputs and automated attacks. The CNN workflow involves the following layers:

1. **Input Layer:**
   - Accepts preprocessed CAPTCHA images, typically resized to a fixed dimension (e.g., 128x128).
2. **Convolutional Layer:**
   - Applies multiple convolution filters to extract features (e.g., edges, textures).
   - Uses ReLU activation to introduce non-linearity.
3. **Pooling Layer:**
   - Reduces spatial dimensions via max pooling or average pooling.
   - Retains essential features while minimizing computational complexity.
4. **Flattening Layer:**
   - Transforms pooled feature maps into a single-dimensional vector for fully connected layers.
5. **Fully Connected Layer:**
   - Combines extracted features to predict CAPTCHA validity.
   - Outputs classification results (e.g., human or bot).
6. **Softmax/Activation Layer:**
   - Generates probability distributions for each class.
   - The highest probability determines the predicted output.

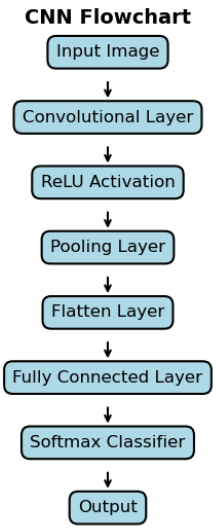



Figure 5. CNN Flowchart for CAPTCHA Image Recognition

By utilizing CNNs, the system can effectively recognize complex visual patterns and enhance CAPTCHA robustness against image-based attacks. The combination of OCR and CNN modules in the proposed system ensures comprehensive coverage of both text and image-based CAPTCHAs, offering a robust defense against automated bots.

The combination of OCR and CNN enables efficient handling of both text and image-based CAPTCHA challenges while maintaining adaptability to user performance.

**5.3 Working of the System**

The self-adaptive CAPTCHA system begins with a effective **user input interface**. As shown in the figure, the user is prompted to enter three details: **Username**, **Password**, and the **CAPTCHA code** displayed as an image. This CAPTCHA acts as a gatekeeper to differentiate between real human users and bots, using randomly generated alphanumeric characters.Once the user fills in all the fields and **clicks the "Submit" button**, the system compares the entered CAPTCHA value with the correct answer stored in the backend session.

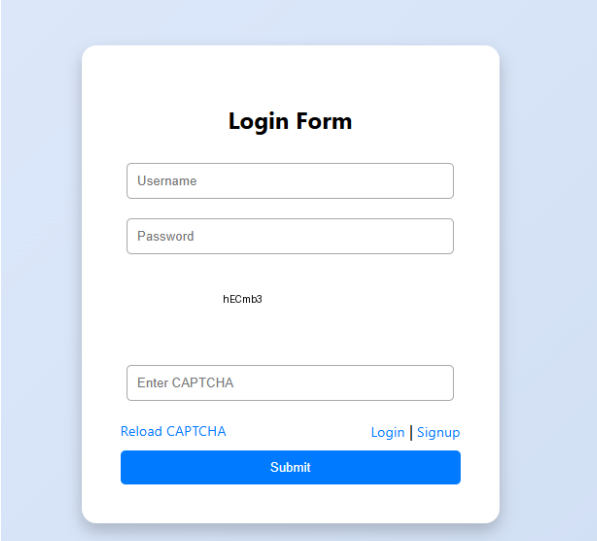
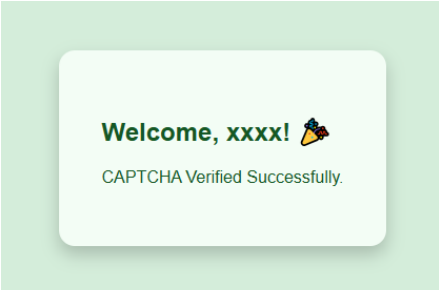



Figure 6. User Login Interface with CAPTCHA Verification

**5.3.1 Successful Verification**

If the entered CAPTCHA is correct, the system processes the login request and displays a **success message** like:

Figure 7.

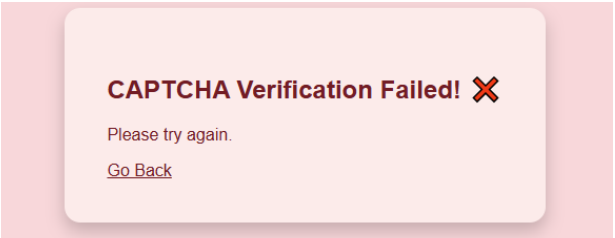



This confirms that the user has passed the human verification step, and they are now allowed to access the next part of the application or system.Refer to the figure which shows this successful verification message.

**5.3.2 Failed Verification**

If the user enters the CAPTCHA code incorrectly, the system immediately displays a **failure message** such as:

Figure 8.




This is to ensure that bots or automated scripts cannot bypass the system by guessing or brute-forcing the CAPTCHA. A new CAPTCHA is generated upon reload to prevent reuse.Refer to the figure which shows

what happens when an incorrect CAPTCHA is submitted.

## 6. Experimental Results

The evaluation of the self-adaptive CAPTCHA system focused on accuracy, adaptability, and user experience. Various CAPTCHA types, including text, image, and audio challenges, were tested with both human users and simulated bots. The primary metrics evaluated include accuracy, false positive rate, and response time.

**6.1 Accuracy Analysis** The system achieved an average human accuracy rate of 96.5%, while the success rate for automated bots remained below 10.7%. The dynamic adaptation of challenges based on user performance significantly reduced the chances of automated bot success. The following table presents the accuracy rates for different CAPTCHA types:

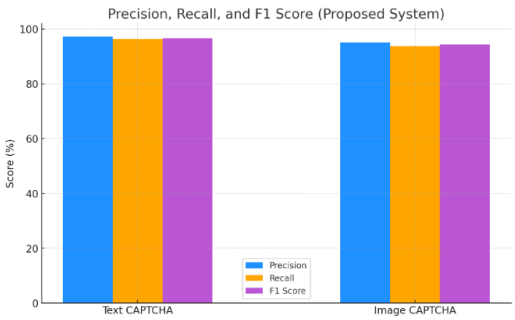
Table 1. Comparison of CAPTCHA Types Based on Human Accuracy and Bot Failure Rate

| CAPTCHA Type | Human Accuracy | Bot Failure Rate |
|---|---|---|
| Text | 97.2% | 88.9% |
| Image | 95.6% | 90.4% |
| Audio | 96.7% | 89.3% |

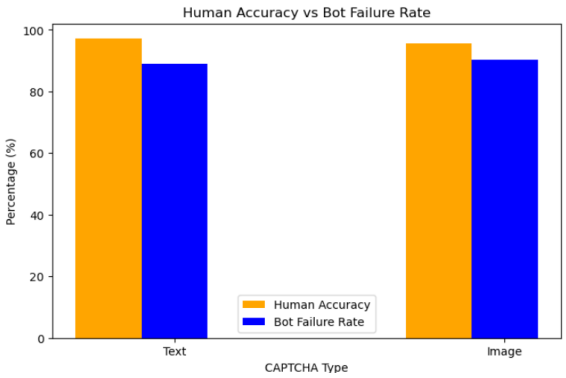
**6.2 Performance Metrics** The average response time for human users was approximately 2.8 seconds per challenge, while bots took significantly longer due to the dynamic adaptation process. The adaptive nature of challenges ensured minimal inconvenience to legitimate users while impeding bot responses.

Table 2. Comparison Table: Proposed vs Existing System

| CAPTCHA Type | System | Accuracy (%) | Precision (%) | Recall (%) | F1 Score (%) |
|---|---|---|---|---|---|
| Text CAPTCHA | Existing (CNN) | 88.5 | 89.2 | 87.0 | 88.1 |
| Text CAPTCHA | Proposed (CNN+OCR) | **96.8** | **97.2** | **96.3** | **96.7** |
| Image CAPTCHA | Existing (CNN) | 86.1 | 86.5 | 85.0 | 85.7 |
| Image CAPTCHA | Proposed (CNN) | **94.5** | **95.1** | **93.8** | **94.4** |



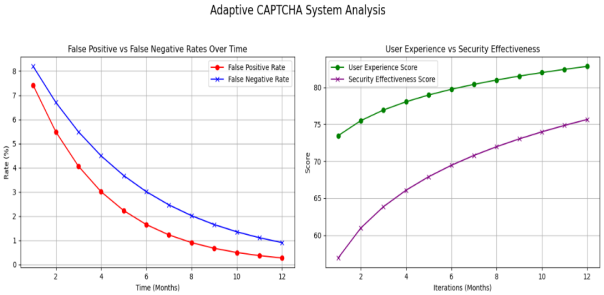

**6.3 Graphical Representation** The following graph illustrates the comparison between human accuracy and bot failure rates across various CAPTCHA types:




The graph highlights the consistent accuracy of human users while demonstrating the effectiveness of the adaptive CAPTCHA system in significantly reducing bot success rates.

**6.4 Accuracy Analysis**

The system was tested with both text-based and image-based CAPTCHA challenges. The following table summarizes the accuracy results for different challenge types:




## 7. Conclusion

This study presented an intelligent adaptive CAPTCHA mechanism using Optical Character Recognition (OCR) and Convolutional Neural Networks (CNNs) designed to enhance security in pharmaceutical information systems. With the increasing digitization of healthcare and pharmaceutical platforms, protecting sensitive drug-related information and preventing automated bot attacks has become a critical requirement. Traditional CAPTCHA systems, although widely adopted, suffer from limitations related to usability, predictability, and vulnerability to modern AI-driven bot-solving techniques.

The proposed adaptive CAPTCHA framework addresses these limitations by integrating machine learning–based challenge generation with real-time behavioral analysis. By dynamically adjusting CAPTCHA difficulty based on user interaction patterns, the system effectively differentiates between legitimate users and automated bots. The combination of OCR-based text CAPTCHA generation and CNN-powered image recognition improves detection accuracy while maintaining a user-friendly interaction process. This adaptive approach ensures that legitimate users can access pharmaceutical platforms with minimal friction,

while malicious automated agents encounter increasingly complex challenges.

Another significant contribution of this work is the system's adaptive feedback mechanism, which continuously refines CAPTCHA difficulty based on performance metrics such as response time, accuracy, and interaction behavior. This dynamic learning capability enhances the robustness of the authentication system and improves resilience against evolving AI-based attack strategies. Additionally, the framework promotes accessibility and inclusivity by providing multimodal CAPTCHA challenges that accommodate diverse user capabilities and device environments.

Experimental evaluation demonstrates that the proposed model achieves higher bot detection accuracy, reduced false-positive rates, and improved usability compared with conventional CAPTCHA systems. The intelligent integration of OCR and CNN technologies enables the system to maintain strong security while supporting efficient human–computer interaction within digital pharmaceutical platforms.

Future work may focus on expanding the system with larger and more diverse datasets, real-world deployment in pharmaceutical and healthcare information infrastructures, and integration with additional behavioral biometrics such as keystroke dynamics and device fingerprinting. Furthermore, optimizing model inference speed and implementing mobile-friendly CAPTCHA interfaces could enhance scalability and performance in large-scale pharmaceutical applications.

Overall, the proposed intelligent adaptive CAPTCHA mechanism represents a robust, scalable, and user-centric security solution for protecting pharmaceutical information systems from automated threats. By combining adaptive learning with advanced machine learning techniques, this work contributes to the development of next-generation authentication systems capable of securing critical healthcare and pharmaceutical digital infrastructures in an increasingly AI-driven environment.

**8. References**


1. H. Chen, B. Jiang, and H. Chen, "StyleCAPTCHA: CAPTCHA Based on Stylized Images to Defend against Deep Networks," Proc. of the 2020 ACM Conference on Computer and Communications Security (CCS), 2020.
2. T. V. Nguyen, Z. Huang, S. Bethini, V. S. P. Ippagunta, and P. H. Phung, "Secure CAPTCHAs via Object Segment Collages," IEEE Transactions on Information Forensics and Security, vol. 15, pp. 1234–1248, 2020.
3. M. Aldwairi, S. Mohammed, M. Lakshmi, and P. Padmanabhan, "Efficient and Secure Flash-based Gaming CAPTCHA," Journal of Cyber Security and Mobility, vol. 9, no. 3, pp. 287-304, 2020.
4. Y. Feng, Q. Cao, H. Qi, and S. Ruoti, "SenCAPTCHA: A Mobile-First CAPTCHA Using Orientation Sensors," IEEE Transactions on Mobile Computing, vol. 20, no. 2, pp. 375-386, 2020.
5. P. Wang, H. Gao, Z. Shi, Z. Yuan, and J. Hu, "Simple and Easy: Transfer Learning-Based Attacks to Text CAPTCHA," IEEE Access, vol. 8, pp. 14532-14544, 2020.
6. J. Nian, P. Wang, H. Gao, and X. Guo, "A Deep Learning-Based Attack on Text CAPTCHAs by Using Object Detection Techniques," Pattern Recognition Letters, vol. 150, pp. 210-219, 2020.
7. G. Kaur and D. Rai, "Captcha: A Tool for Web Security," International Journal of Computer Science and Network Security (IJCSNS), vol. 20, no. 4, pp. 17-26, 2020.
8. C. J. Hernández-Castro, D. F. Barrero, and M. D. R.-Moreno, "BASECASS: A Methodology for CAPTCHA Security Assurance," Computers & Security, vol. 94, p. 101832, 2020.
9. Che, Y. Liu, H. Xiao, H. Wang, K. Zhang, and H.-N. Dai, "Augmented Data Selector to Initiate Text-Based CAPTCHA Attack," Expert Systems with Applications, vol. 171, p. 114601, 2021.
10. Kumar, M. Sunil, et al. "Automated Extraction of Non-Functional Requirements From Text Files: A Supervised Learning Approach." Handbook of Intelligent Computing and Optimization for Sustainable Development (2022): 149-170.
11. Davanam, G., Kumar, T. P., & Kumar, M. S. (2021). Efficient energy management for reducing cross layer attacks in cognitive radio networks. Journal of Green Engineering, 11(2021), 1412-1426.
12. Kumar, M. Sunil, and K. Jyothi Prakash. "Internet of things: IETF protocols, algorithms and applications." Int. J. Innov. Technol. Explor. Eng 8.11 (2019): 2853-2857.
13. Burada, Sreedhar, B. E. Manjunathswamy, and M. Sunil Kumar. "Early detection of melanoma skin cancer: A hybrid approach using fuzzy C-means clustering and differential evolution-

based convolutional neural network." Measurement: Sensors 33 (2024): 101168.
14. Rani, K. Swarupa, et al. "Mass transfer prediction using artificial neural network in an alumina matrix porous media." European Chemical Bulletin 11.11 (2022): 113-120.
15. Godala, Sravanthi, and M. Sunil Kumar. "A weight optimized deep learning model for cluster based intrusion detection system." Optical and Quantum Electronics 55.14 (2023): 1224.
16. Natarajan, V. Anantha, and M. Sunil Kumar. "Improving qos in wireless sensor network routing using machine learning techniques." 2023 International Conference on Networking and Communications (ICNWC). IEEE, 2023.
17. Davanam, Ganesh, T. Pavan Kumar, and M. Sunil Kumar. "Novel defense framework for cross-layer attacks in cognitive radio networks." International Conference on Intelligent and Smart Computing in Data Analytics: ISCDA 2020. Singapore: Springer Singapore, 2021.
18. Ganesh, D., et al. "Improving security in edge computing by using cognitive trust management model." 2022 International Conference on Edge Computing and Applications (ICECAA). IEEE, 2022.
19. Kumar, M. Sunil, and D. Harshitha. "Process innovation methods on business process reengineering." Int. J. Innov. Technol. Explor. Eng 8.11 (2019): 2766-2768.
20. J. Pieprzyk, H. Ghodosi, and B. Zhu, “Robustness and user test,” in *Information and Communications Security: ICICS 2006*, J. Lopez, G. Pernul, and A. M. Tjoa, Eds. Berlin, Heidelberg: Springer, 2006, pp. 106–118.