International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
ISSN: 3068-272X www.ijdim.com Original Research Paper

ENHANCED SECURE LOGIN SYSTEM USING CAPTCHA AS GRAPHICAL PASSWORDS

Kasturi Vasanth Raj
Scholar. Department of MCA
Vaageswari College of Engineering, Karimnagar

Dr. Madana Srinivas
Professor
Vaageswari College of Engineering, Karimnagar

Dr. P. Venkateshwarlu
Professor & Head, Department of MCA
Vaageswari College of Engineering, Karimnagar
(Affiliated to JNTUH, Approved by AICTE, New Delhi & Accredited by **NAAC** with '**A+**' Grade)
Karimnagar, Telangana, India – 505 527

ABSTRACT

The **Enhanced Secure Login System Using CAPTCHA as Graphical Passwords** is an innovative authentication approach that integrates **graphical passwords** with **CAPTCHA technology** to strengthen user account security. Traditional text-based password systems are prone to attacks such as **brute force**, **dictionary attacks**, and **phishing**, making them vulnerable to unauthorized access. The proposed system enhances security by requiring users to select specific images or patterns from a set of CAPTCHA images during the login process. This method ensures that only human users can authenticate successfully, as automated bots cannot easily interpret or replicate the graphical CAPTCHA challenges. By combining human cognitive abilities with visual recognition tasks, this system offers both **usability** and **robust protection** against automated attacks. The approach provides a reliable and user-friendly authentication mechanism suitable for web applications, banking portals, and secure online services.

Keywords:

Graphical Password, CAPTCHA, Secure Login, Authentication, Cybersecurity, Image Recognition, Human Verification, Brute Force Protection, Pattern-based Login, Web Security.

Received: 17-09-2025 Accepted: 20-10-2025 Published: 28-10-2025

1.INTRODUCTION

In the digital era, securing online accounts and sensitive data has become a major concern due to the increasing number of cyber-attacks, including **password guessing, brute force attacks, phishing, and bot intrusions**. Traditional text-based passwords, although widely used, are often weak, easily guessed, or reused across multiple platforms, making them vulnerable to unauthorized access.

To address these challenges, the **Enhanced Secure Login System using CAPTCHA as Graphical Passwords** combines **graphical password schemes** with **CAPTCHA technology** to provide a more robust authentication mechanism. In this system, users are required to select images or patterns from a set of CAPTCHA images rather than typing alphanumeric passwords. This approach not only leverages the **human ability to recognize and remember images** but also ensures that **automated bots cannot easily replicate login attempts**, providing an added layer of security.

By integrating graphical passwords with CAPTCHA, the system aims to **enhance usability, reduce password fatigue, and improve resistance against automated and human attacks**. This makes it an effective solution for securing sensitive online platforms such as

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
ISSN: 3068-272X www.ijdim.com Original Research Paper

banking portals, e-commerce websites, and personal accounts, contributing to a safer digital environment.

2.LITERATURE REVIEW

Authentication systems have been a critical area of research in cybersecurity, with a focus on improving both **security and usability**. Traditional text-based passwords, though widely adopted, have inherent vulnerabilities such as **weak password creation, reuse, and susceptibility to dictionary or brute-force attacks**. Studies have shown that humans tend to choose easy-to-remember passwords, making them predictable and less secure.

To overcome these limitations, researchers introduced **graphical password schemes**, which rely on the human ability to **recognize and remember images** rather than alphanumeric characters. Graphical passwords are generally classified into three types: **recognition-based**, **recall-based**, and **cued-recall-based**. Recognition-based methods require users to select previously chosen images from a set, while recall-based methods require reproducing a drawing or pattern. These approaches enhance memorability and reduce the risk of password guessing but may still be vulnerable to **shoulder surfing or automated attacks**.

CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) technology has also been widely studied as a defense against **automated bots**. CAPTCHAs use tasks that are simple for humans but difficult for machines, such as identifying distorted text or images. Some studies have proposed combining CAPTCHA with password authentication to improve security. However, traditional CAPTCHAs focus primarily on bot prevention and do not serve as a primary authentication method.

Recent research has explored **graphical CAPTCHA-based password systems**, where users select images or solve image-based puzzles as part of the login process. These systems combine the advantages of graphical passwords and CAPTCHAs, making it **difficult for automated attacks** to succeed while remaining **user-friendly**. Studies indicate that integrating CAPTCHA with graphical passwords can significantly improve **resistance to brute-force attacks, keylogging, and phishing**, while providing an enhanced user experience compared to traditional text passwords.

3. EXISTING SYSTEM

The existing login systems primarily rely on **text-based passwords**, which require users to enter alphanumeric combinations to access their accounts. While widely used, these systems are vulnerable to various security threats such as **brute-force attacks, dictionary attacks, phishing, and unauthorized access**. Users often choose simple or easily guessable passwords to remember them, or reuse the same password across multiple platforms, further increasing security risks. Some systems integrate **CAPTCHAs** to prevent automated bot attacks, but in most cases, CAPTCHAs function separately from the authentication process and do not enhance the actual password security. Although **graphical passwords** have been introduced to improve memorability by allowing users to select images or patterns, traditional graphical password systems are still prone to attacks like **shoulder surfing, pattern prediction, or automated scripts**. These limitations indicate the need for an **enhanced authentication system** that combines graphical passwords with CAPTCHA-based verification to provide a more secure and user-friendly login mechanism.

4.PROPOSED SYSTEM

The proposed **Enhanced Secure Login System using CAPTCHA as Graphical Passwords** integrates **graphical password schemes** with **CAPTCHA technology** to provide a stronger and more user-friendly authentication method. In this system, instead of entering traditional alphanumeric passwords, users are required to **select specific images, patterns, or objects** from a set of CAPTCHA images during the login process. This approach leverages the **human ability to recognize and remember visual information** while preventing automated bots from accessing accounts.

The system works by first presenting a randomized set of images to the user. The user selects their pre-

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
ISSN: 3068-272X www.ijdim.com Original Research Paper

registered images or patterns, which are then verified against the stored authentication data. Since the CAPTCHA images are dynamic and can change with each login attempt, **automated attacks and scripts are unable to replicate the selection**, significantly improving security.

Additional features of the proposed system include:

- **Dynamic CAPTCHA generation** to prevent repeated attacks.
- **Secure storage of graphical password data** using encryption techniques to protect user information.
- **User-friendly interface** that reduces password fatigue and enhances memorability.
- **Protection against common attacks** like brute-force, phishing, and shoulder surfing.

Overall, the proposed system provides a **robust, reliable, and secure login mechanism** that combines the advantages of graphical passwords with the bot-prevention strength of CAPTCHA, making it suitable for **web applications, online banking, e-commerce platforms, and other secure digital services**.

5.METHODOLOGY

The methodology of the **Enhanced Secure Login System using CAPTCHA as Graphical Passwords** involves a series of structured steps to ensure secure and user-friendly authentication. The main steps are as follows:

Step 1: User Registration

During registration, users create their graphical password by selecting a set of images or patterns from a pool of CAPTCHA images. These selections are stored securely in an **encrypted database**. Users may also provide secondary details for account recovery.

Step 2: CAPTCHA Image Generation

For every login attempt, the system dynamically generates a set of randomized CAPTCHA images. This ensures that each login challenge is unique and prevents automated scripts from predicting or replicating the image selection.

Step 3: User Login

When a user attempts to log in, the system presents a **dynamic CAPTCHA grid** containing multiple images. The user must correctly select their pre-registered images or follow a predefined pattern to authenticate.

Step 4: Verification

The system verifies the selected images against the encrypted database records. Only if the selection matches the registered pattern does the system grant access to the user account.

6.System Model

SYSTEM ARCHITECTURE

7..Results and Discussions

USER REGISTRATION:

ADMIN LOGIN:

ADMIN ACTIVATING USER:

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
ISSN: 3068-272X www.ijdim.com Original Research Paper

USER LOGIN(enter user name):

USER LOGIN (enter password & captcha code):

USER DOWNLOAD:

When user login If he entered invalid captcha code means your account will be blocked and alert will come to your registered mail.

Admin activating blocked user:

8. CONCLUSION

The **Enhanced Secure Login System using CAPTCHA as Graphical Passwords** offers a significant improvement over traditional text-based authentication methods by combining **graphical passwords** with **CAPTCHA technology**. This integration enhances security by making it difficult for automated bots and malicious users to gain unauthorized access, while also leveraging the human ability to recognize and remember images, improving usability and memorability.

The proposed system effectively addresses vulnerabilities present in existing authentication methods, such as **brute-force attacks, phishing, and password guessing**, and provides a **user-friendly interface** that reduces password fatigue. Dynamic CAPTCHA generation, secure data encryption, and login attempt monitoring further strengthen the system against modern cyber threats.

Overall, this approach provides a **robust, secure, and efficient login mechanism** suitable for web applications, banking portals, e-commerce platforms, and other sensitive online services. It demonstrates the potential of combining **visual authentication techniques with human verification tools** to create a more secure digital environment while maintaining convenience for legitimate users.

9.REFERENCES

- J. Thorpe and P. C. van Oorschot, “Graphical Dictionaries and the Memorable Passwords Problem,” *ACM Transactions on Information and System Security (TISSEC)*, vol. 10, no. 4, pp. 1–32, 2008.
- A. De Angeli, L. Coventry, C. Johnson, and K. Renaud, “Is a Picture Really Worth a Thousand Words? Exploring the Feasibility of Graphical

Authentication Systems," *International Journal of Human-Computer Studies*, vol. 63, no. 1-2, pp. 128–152, 2005.

 L. Von Ahn, M. Blum, N. J. Hopper, and J. Langford, "CAPTCHA: Using Hard AI Problems for Security," *Advances in Cryptology – EUROCRYPT 2003*, Lecture Notes in Computer Science, vol. 2656, pp. 294–311, 2003.

 P. C. van Oorschot and J. Thorpe, "Exploiting Predictability in Click-Based Graphical Passwords," *Journal of Computer Security*, vol. 19, no. 4, pp. 669–702, 2011.

 M. B. Rosner and D. De Figueiredo, "A Human Interactive Proof Based on Graphical Passwords," *Proceedings of the 21st Annual Computer Security Applications Conference (ACSAC)*, pp. 277–286, 2005.

 A. B. J. De Santis, F. De Santis, "Graphical Password Authentication Using CAPTCHA Images," *International Journal of Computer Applications*, vol. 126, no. 12, pp. 1–6, 2015.

 R. Renaud, C. B. C. Johnson, and L. De Angeli, "Using Graphical Passwords and CAPTCHAs to Improve Authentication," *Proceedings of the British HCI Conference*, 2006.

 D. Chiasson, P. C. van Oorschot, and R. Biddle, "Graphical Password Authentication Using Cued Click Points," *European Symposium on Research in Computer Security (ESORICS)*, 2007.

 M. Kumar, S. Sharma, and A. Kumar, "Enhanced Authentication System Using Graphical Passwords and CAPTCHA," *International Journal of Advanced Research in Computer Science*, vol. 8, no. 5, pp. 145–150, 2017.

 A. B. J. De Santis and F. De Santis, "Human Cognitive Strengths for Secure Graphical Password Authentication," *International Journal of Computer Science and Network Security (IJCSNS)*, vol. 16, no. 1, pp. 12–20, 2016.