IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

Impact Factor 8.021 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 3, March 2025

DOI: 10.17148/IJIREEICE.2025.13357

GRAPHICAL PASSWORD IMAGE SEGMENTATION: A NOVEL APPROACH TO ENHANCED ONLINE SECURITY

OMPRAKASH T[1], Dr.R. PRABA[2]

Department of Information Technology,

Dr.N.G.P. Arts and Science College, Coimbatore, Tamil Nadu, India[1]

Associate Professor, Department of Information Technology,

Dr.N.G.P. Arts and Science College, Coimbatore, Tamil Nadu, India[2]

Abstract: Captcha technology with graphical password systems, which are also known as Captcha as Graphical Passwords (CaRP), the project "Graphical Password Image Segmentation" enhances security online. The project, designed using ASP.Net as the front end, Microsoft SQL Server as the back end, and Windows 8 as the platform, is made up of modules such as File Upload/Download, Graphical Password, Captcha in Authentication, Registration, and Key Generation (Cued Click Points). CaRP provides more secure password selection by solving the hotspot problem of the image in traditional graphical password schemes. By restricting unauthorised file downloads and uploads, providing secure file sharing between users, and restricting system access to only authorised users through image-based Captcha authentication, it provides greater security

Keywords - Graphical Password, Captcha as Graphical Password (CaRP), Cued Click Points, Secure Authentication, File Management.

I.INTRODUCTION

In the rise of using digital platforms, online safety is important. Password systems are prone to brute-force and phishing because of weak or previously used passwords. Graphical password systems provide a more secure solution by utilizing human visual memory. But they experience problems such as image hotspots and shoulder surfing. Captcha technology prevents automated attacks by posing tasks simple for humans but difficult for bots. However, with the advancements in machine learning, some Captchas have become easier to circumvent. To counter these vulnerabilities, the Captcha as Graphical Passwords (CaRP) system integrates graphical passwords and Captcha challenges to provide stronger security against both human and automated attacks. CaRP alleviates image hotspot problems and enhances authentication by asking users to complete a Captcha during the input of their graphical password. This work aims at creating a secure and easy-to-use CaRP system that also encompasses secure file management, allowing only authenticated users to upload, download, or share files. The aim is to offer a strong solution for online authentication, especially for small businesses by enhancing security and usability.

II. LITERATURE REVIEW

Password authentication is extensively employed to secure user accounts and sensitive information. Yet, numerous users opt for weak, easily guessable passwords or use them on many websites, leaving them open to brute-force and phishing attacks (Bonneau et al., 2012). As computational power grows, attackers can try millions of password combinations quickly, exposing the weakness of conventional password systems in securing sensitive information. While used extensively, text-based passwords are no longer becoming adequate to safeguard sensitive information against sophisticated cyber attacks.

Graphical passwords are a possible answer using the human capacity to remember pictures more effectively than text. PassPoints and Draw-A-Secret systems provide users with points on an image or drawing patterns, making more intricate and recollective passwords possible (Sushmita & Rao, 2015). Yet, there are weaknesses including the image hotspot problem, wherein users select expectable locations in an image to make them simple to predict (Sui & Zhang, 2012). Graphical passwords are also subject to shoulder surfing, wherein an attacker watches and mimics the password entry.

DOI: 10.17148/IJIREEICE.2025.13357

Captcha technology, intended to discriminate between human beings and robots, is meant to ward off automatic attacks but less so since more advanced machine learning breakthroughs permit robots to tackle most Captcha challenges (Wang & Yin, 2010).

To overcome these constraints, Captcha as Graphical Passwords (CaRP) integrates graphical passwords and Captcha challenges to boost authentication security (Bonneau & Herley, 2012). Users are required to select image points when performing a Captcha task in CaRP systems, thereby making it hard for both human and automated attackers to circumvent the system. This method avoids the image hotspot problem and reinforces resistance against automated attacks (Chiasson & Van Oorschot, 2007). In addition, combining secure authentication mechanisms such as CaRP with file systems guarantees authorized users to have access to, upload, or share confidential information, minimizing data breaches and unauthorized tampering (Thorpe & Herbert, 2013).

III. METHODOLOGY

This study seeks to create a safe authentication system that combines Captcha and Graphical Passwords (CaRP) to improve online security, minimize vulnerabilities, and facilitate secure file management. The research involves system design, development, testing, and evaluation to guarantee the efficiency and usability of the system.

3.1 System Design

The system will integrate Captcha technology with graphical password schemes to create an integrated authentication process. The Captcha aspect will leverage dynamic challenges in the form of image recognition tasks to stop automated bots from penetrating the system. The graphical password scheme will use the image-based approaches such as Pass Points or Draw-A-Secret, which will ask users to click certain zones on an image or draw a sequence. Randomized points of clicks will inhibit pre-emptive hotspots. One of the major features of key generation through Cued Click Points (CCP) will provide dynamic cues during password generation to prevent selection patterns. The system will also have a secure file management module that will only permit authenticated users to upload, download, or share files and will impose stringent access controls and encryption.

3.2 Development Tools and Technologies

The CaRP system will be constructed on the ASP.NET framework for front-end implementation and Microsoft SQL Server for back-end functions. ASP.NET will be used to manage user interaction with the Captcha and graphical password fields, while SQL Server will securely manage user data such as hashed passwords and encrypted documents. The system will be created to run on the Windows 8 operating system to be compatible with regular desktop environments and browsers.

3.3 User Authentication Process

User authentication has two steps: Captcha challenge and graphical password entry. While logging in or registering, users are first asked to complete a Captcha challenge through image recognition or puzzle-solving exercise. In this way, human users alone can pass on to the subsequent step. After solving the Captcha, users will enter their graphical password by clicking points over an image or drawing a pattern. Randomized click points and cryptographic hashing (such as SHA-256) will also protect user credentials, keeping passwords secure even in the event of a compromised database.

3.4 Secure File Management

The file management module adds security through the limitation of file access to authenticated users. Users will have to undergo the double authentication process before they can upload, download, or share files. Access control policies will check for ownership of the files and permissions. Files will be encrypted during transmission (through SSL/TLS protocols) and even when stored in the database to restrict unauthorized access. Audit logs will be maintained for all file-based activities, thus providing transparency and security.

3.5 Testing and Evaluation

Security and usability of the system will be tested with thorough testing. Security will entail penetration testing to uncover weaknesses, Captcha resistance against automated attacks, and testing graph password security. Usability will entail user trials to determine the ease of use and efficiency of the system's interface. Performance will test response times when generating Captcha, taking in passwords, and file operations under different workloads.

IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

Impact Factor 8.021 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 3, March 2025

DOI: 10.17148/IJIREEICE.2025.13357

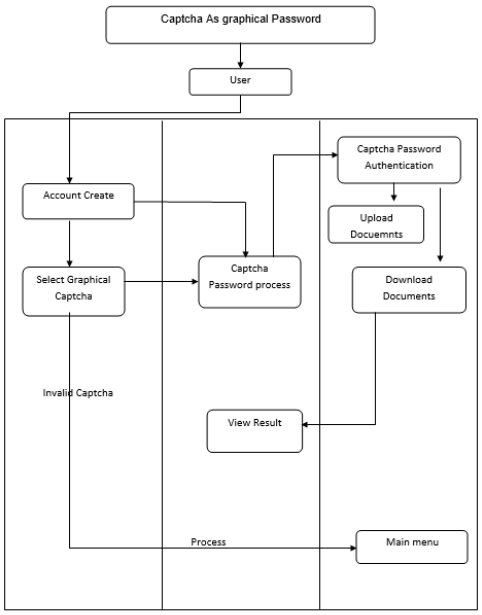

Fig 3.1.1: Flowchart

IV. IMPLEMENTATION

4.1 System Configuration and Setup

The system will be set up on the Windows 8 operating system using ASP.NET and Microsoft SQL Server. The database will hold user credentials, Captcha logs, and file metadata. This configuration allows for easy integration between the authentication and file management modules.

4.2 Captcha System Implementation

The Captcha process will create dynamic, image-type challenges based on distortion and noise to avoid being recognized by robots. Every Captcha will differ, and end users will be required to accurately solve the challenge in order to continue. Captcha verification will match user response against saved answer, and session management will exclude session hijacking.

4.3 Implementation of Graphical Password System

The users will create graphical passwords by choosing points on a picture or scribbling patterns. Randomized clues (Cued Click Points) shall avoid familiar patterns. The passwords will be saved as cryptographic hashes to secure them. When logging in, users will trace their graphical password, which the system will compare with the stored hash. Other security features involve the use of multiple pictures and a secure password recovery mechanism.

4.4 Implementation of Secure File Management

Authenticated users shall be permitted to upload, download, and share files. Access to files will be managed through checking permissions. Upload files will be checked for type and size conformance. Transfer and storage of files will be encrypted, and user activities shall be monitored through audit logs.

4.5 Testing and Debugging

Each component of the system will be unit tested to ensure functionality. Penetration testing will reveal weaknesses, particularly in Captcha and graphical password implementations. Usability testing involving a representative user group will test for interface clarity and simplicity, and the system will be customized according to feedback.

4.6 Deployment

The system will be installed on a secure web server with adequate firewalls and encryption methods. Periodic backups will guarantee data safety and ease of recovery in case of failure. The installation will guarantee the system's stability and availability for real-world utilization.

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering
Impact Factor 8.021 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 3, March 2025
DOI: 10.17148/IJIREEICE.2025.13357

V. RESULTS AND DISCUSSION

5.1 Security Evaluation

Several factors were employed to analyze the system:

•Brute-force resistance: The system is made more resistant to automated attacks by combining graphical passwords with Captcha.

•Effectiveness of Cued Click Points: The graphical password is hard to guess because the cued points are randomised.

•Captcha Integration: Through blocking automated login attempts, captcha-based authentication renders it harder for bots to gain access to the system.

5.2 Usability

Surveys were used to gather user responses to assess the usability and effectiveness of the system. The participants reported no major problems with file management or authentication, and all participants stated the system was easy to use.

5.3 Comparative Analysis

CaRP was more secure than conventional graphical password schemes. Conventional schemes are prone to automated attacks since they typically depend on static images or pointed locations. By integrating dynamic Captcha challenges and random key generation, CaRP addresses this problem.

VI. CONCLUSION

Captcha as Graphical Passwords (CaRP) is an important improvement in online security through the integration of the advantages of Captcha technology and graphical password schemes. By combining the two approaches, the system effectively responds to widespread weaknesses like weak passwords and bot attacks, offering a strong barrier against unauthorized access. The application of Cued Click Points reduces the image hotspot issue inherent in standard graphical password systems, making password selections more secure. The application of a dynamic Captcha test strengthens user authentication even further, guaranteeing that only legitimate users can access the system.

Besides, the system has integrated secure file management capabilities, through which approved users can download, upload, and share files in a secure manner, both while in transit and when at rest. Constructed using ASP. NET and Microsoft SQL Server, the CaRP system is reliable, scalable, and simple to deploy, rendering it an ideal solution for small enterprises looking to enhance security without compromising convenience. Although the system is effective in its goal of security, enhancements like multi-factor authentication and better user interfaces in the future could further improve its effectiveness and ease of use. In general, the CaRP system presents a solid basis for current authentication and secure file handling, showcasing how mechanisms of multiple kinds can collaborate to safeguard user data and foreclose unauthorized access.

REFERENCES

[1]. R Praba, “Cyber Crime and Media Awareness in India”, International Journal of Innovative Research in Technology (IJIRT), International Journal of Engineering Research and Technology (IJERT), Volume: 14, Issue: 2, 2024.
[2]. Priti C. Golar, Rika Sharma, "An Advanced Knowledge Based Graphical Authentication Framework with Guaranteed Confidentiality and Integrity", International Journal on Recent and Innovation Trends in Computing and Communication, Volume: 11, Issue: 8s, 2023.
[3]. Ashutosh Kumar, Maina Changeriwal, "Graphical Password Authentication Using PassPoint and PTC Scheme", Journal of Operating Systems Development & Trends, Volume: 9, Issue: 3, 2023.
[4]. Priti C. Golar, Rika Sharma, "Security Analysis of the Graphical Password-Based Authentication Systems with Different Attack Proofs", International Journal of Intelligent Systems and Applications in Engineering, Volume: 11, Issue: 10s, 2023.
[5]. Mohd Afizi Mohd Shukran, et al., "Pixel Value Graphical Password Scheme: K-Means as Graphical Password Fault Tolerance", Journal of Information and Organizational Sciences, Volume: 45, Issue:1, 2021.
[6]. Mary Ogbuka Kenneth, Stephen Michael Olujuwon, "Web Application Authentication Using Visual Cryptography and Cued Clicked Point Recall-based Graphical Password", Journal of Computer Science Research, Volume:3, Issue: 3, 2021.
[7]. Maw Maw Naing, Ohnmar Win, "Graphical Password Authentication using Image Segmentation for Web-Based Applications", International Journal of Trend in Scientific Research and Development, Volume: 3, Issue: 4, 2019.
[8]. P.G. Scholar, “Graphical Password Authentication System Based on Persuasive Cued Click-Points”, International Journal of Recent Trends in Engineering and Research, Volume: 4, Issue: 3, 2018.
[9]. A. Shaikh, et al., "Implementation of Authentication Using Graphical Password in Cloud Computing", International Research Journal of Engineering and Technology, Volume: 5, Issue: 5, 2018.