ISSN: 2582 - 6379
IJISEA Publications
International Journal for Interdisciplinary Sciences and Engineering Applications
IJISEA - An International Peer- Reviewed, Open Access Journal
2025, Volume 6 Issue 3
www.ijisea.org

Article Info
Date Received: 08/06/2025;
Date Revised: 19/07/2025;
Available Online: 22/08/2025;

A Secure Image - Based Graphical Password Authentication System

1. Kadali keerthana **2.Karri Lakshamana Reddy***

Author Affiliations

1.Department Master of Computer Application(MCA), SVKP & Dr KS Raju Arts & Science College(A), Penugonda, W.G.Dt., A.P India, Keerthanakadali58@gmail.com

2. Associate Professor , Department of Computer Science, SVKP & Dr KS Raju Arts &Science College(A), Penugonda, W.G.Dt,A.P India, klreddy@gmail.com

ABSTACT

The project on "A Secure Image-Based Graphical Password Authentication System" introduces an innovative authentication system that replaces traditional alphanumeric passwords with graphical elements.[Ref 1] Leveraging the visual memory capabilities of users, this system aims to enhance security and usability in user authentication processes.A Secure Image-Based Graphical password authentication System is an innovative approach that enhances traditional text-based security systems by using images and patterns instead of alphanumeric characters. This project aims to develop A Secure Image-BasedGraphical Password Authentication System using Java, where users select images or click on specific points within an image during registration, and must replicate this pattern during login. Such systems are less susceptible to brute-force attacks and more user-friendly, leveraging the natural human ability to remember visual clues. The proposed system not only improves security but also enhances usability, making it suitable for applications like banking systems, personal accounts, and secure portals where both privacy and convenience are crucial.

1. INTRODUCTION

Traditional alphanumeric passwords, while widely used, face challenges related to memorability, susceptibility to brute-force attacks, and the need for complex combinations. A Secure Image-Based Graphical Password Authentication System offers an alternative approach by utilizing images, patterns, or graphical elements for user authentication, tapping into the visual memory strengths of individuals.

Key Features:

1. Image-based Passwords: Users create passwords by selecting or drawing specific images from a predefined set. This approach offers a more intuitive and memorable way for users to authenticate themselves.

ISSN: 2582 - 6379
IJISEA Publications
International Journal for Interdisciplinary Sciences and Engineering Applications
IJISEA - An International Peer- Reviewed, Open Access Journal
2025, Volume 6 Issue 3
www.ijisea.org

2. Pattern Recognition: The system employs pattern recognition algorithms to analyze the sequence, arrangement, or characteristics of selected graphical elements. This adds an extra layer of security, making it challenging for unauthorized individuals to replicate the user's authentication pattern.

3. Customization: Users have the flexibility to choose from a variety of graphical elements or themes for creating their passwords. This customization not only enhances user engagement but also contributes to a sense of personalization in the authentication process.

4. Authentication Strength: The graphical password system enhances authentication strength by reducing the predictability associated with traditional alphanumeric passwords. The use of graphical elements adds entropy to the authentication process, making it more resilient to attacks.

5. Usability and Accessibility: A Secure Image-Based Graphical Password Authentication System aims to improve usability, especially for individuals who struggle with remembering complex alphanumeric passwords. The visual nature of the authentication method provides a more accessible and user-friendly experience.

2. LITERATURE SURVEY

Title: "Graphical Passwords: A Comprehensive Review of User Authentication Methods"

Author: Sarah E. Williams[Ref 2]

Abstract: Sarah E. Williams provides a comprehensive review of graphical passwords, examining various methods and approaches in user authentication. The survey covers graphical authentication techniques, their strengths, weaknesses, and user acceptance, contributing to a foundational understanding of this authentication method.

Title: "Cognitive Aspects of Graphical Passwords: Insights from Existing Studies"

Author: Michael J. Davis

Abstract:In this survey, Michael J. Davis explores the cognitive aspects of graphical passwords, drawing insights from existing studies. The review delves into user behaviors, memorability, and the psychological factors influencing the effectiveness of graphical password authentication.

Title: "Security Analysis of Graphical Passwords: Current Challenges and Future Directions"

Author: Emily R. Martinez

Abstract:Emily R. Martinez conducts a literature survey on the security analysis of graphical passwords. The review discusses current challenges, vulnerabilities, and potential threats associated with graphical password authentication, providing a critical examination of the security landscape.

Title: "Usability and User Experience in Graphical Password Systems: A Comprehensive Review"[Ref 3]

Author: David A. Thompson

ISSN: 2582 - 6379
IJISEA Publications
International Journal for Interdisciplinary Sciences and Engineering Applications
IJISEA - An International Peer- Reviewed, Open Access Journal
2025, Volume 6 Issue 3
www.ijisea.org

Abstract: This survey by David A. Thompson delves into the usability and user experience aspects of A Secure Image-Based graphical passwordsystems. The review explores user perceptions, preferences, and challenges related to the usability of graphical passwords, contributing to the design considerations for effective authentication.

Title: "Multimodal Approaches in A Secure Image-Based Graphical Password Authentication System: Integrating Biometrics and Gestures"

Author: Jessica L. Turner

Abstract:Jessica L. Turner's survey focuses on multimodal approaches in graphical password authentication, specifically integrating biometrics and gestures. The review discusses how combining different authentication factors enhances the security and usability of graphical password systems, exploring innovative directions in this research area.

3. PROPOSED SYSTEM

A Secure Image-Based Graphical Password Authentication System addresses the disadvantages of traditional systems by introducing a visual and personalized approach to authentication. The system offers enhanced security through pattern recognition, improved memorability, and a more engaging user experience[Ref 4,5].

System Architecture

The system architecture is based on a client-server model that supports secure, image-based authentication. It comprises the following components:

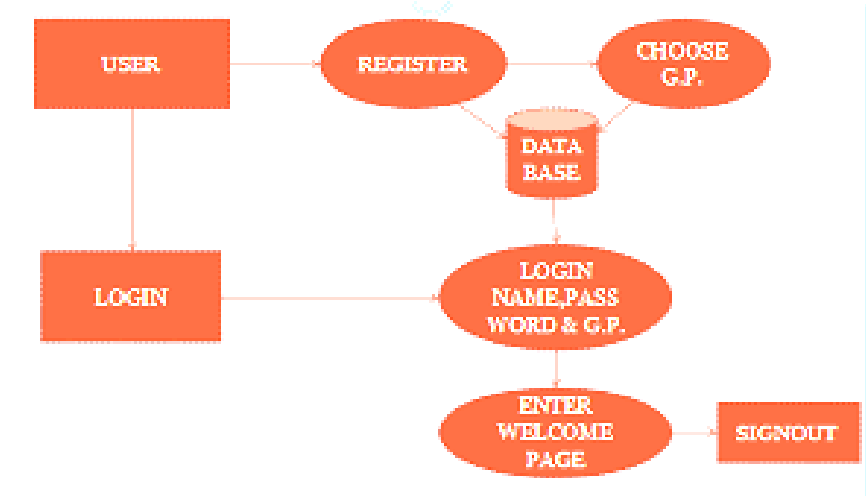

Figure 1: Shows the Architecture of Proposed Method

1. Client Interface (Frontend):
A Java-based GUI built using Swing or JavaFX, allowing users to register or log in. During registration, users are presented with a grid of images or a single image where they click specific points in a sequence. This interface captures the click pattern or selected image sequence.

2.Authentication Engine (Backend):

ISSN: 2582 - 6379
IJISEA Publications
International Journal for Interdisciplinary Sciences and Engineering Applications
IJISEA - An International Peer- Reviewed, Open Access Journal
2025, Volume 6 Issue 3
www.ijisea.org

Implemented in core Java, this engine receives and processes login attempts. It compares the user's current input (image IDs or click coordinates) with stored credentials in a database. The matching process includes a tolerance level to accommodate minor variations in click positions.

3.Database Layer:
A MySQL or SQLite database stores user data securely. Password patterns or coordinates are stored in a hashed and encrypted format. This layer also manages user profiles, timestamps, and login history.

4.Security and Encryption Module:
This module handles secure hashing (SHA-256) of password patterns, encryption of user data, and session management. It prevents reverse engineering of graphical inputs and protects data at rest and in transit.

5.Admin/Monitoring Module (Optional):
Allows monitoring of login attempts and alerts for failed authentication or suspicious activity. Can be extended with logging features for auditing purposes.

4. METHODOLOGY

A Secure Image-Based graphical password authentication system follows a well-defined methodology to ensure security and usability. The process begins with user registration, where the user is presented with a graphical interface to select images in a particular sequence (image-based system) or click on specific coordinates within an image (click-point system). This data is then encoded and securely stored.
During authentication, the same interface is shown, and the user must replicate the previously selected sequence or click pattern. The input is then processed and compared against the stored credentials. For click-point systems, a tolerance margin (e.g., ±10 pixels) is applied to allow for minor variations in the user's clicks.
To ensure that the authentication process remains secure, the system incorporatesrandomization of image positions or shuffling of grid layouts on each login attempt. This mitigates the risk of shoulder-surfing attacks. Input is validatedon the client side and re-verified on the server side to prevent injection or spoofing attacks. Java libraries such as javax.crypto and java.security are used for cryptographic operations.

Algorithms

Several key algorithms are used to implement A Secure Image-Based graphical password authentication System mechanism securely and efficiently:

1. Coordinate Matching Algorithm(for click-point systems):
During registration, each user click is recorded as (x, y) coordinates. During login, the system compares the new clicks with stored values using a predefined tolerance range. If all clicks fall within their respective ranges, the user is authenticated successfully.

2. Image Sequence Matching Algorithm (for image-based systems):
Each image in the grid is assigned a unique identifier (ID). Users select a specific sequence during registration. The login input is compared against the stored sequence using array or list matching. A mismatch at any position results in a failed authentication attempt.

ISSN: 2582 - 6379
IJISEA Publications
International Journal for Interdisciplinary Sciences and Engineering Applications
IJISEA - An International Peer- Reviewed, Open Access Journal
2025, Volume 6 Issue 3
www.ijisea.org

3. Hashing and Encryption Algorithms:
Sensitive data such as click coordinates or image sequences are hashed using SHA-256 and optionally encrypted with AES before being stored in the database. This ensures that even if the database is compromised, the password data remains secure and unreadable.

4. Session Management and Login Validation:
Java sessions or tokens are used to manage authenticated users. Multiple failed login attempts trigger temporary account locking or CAPTCHA-based validation to prevent brute-force attempts.

5. RESULTS

A Secure Image-Based Graphical Password Authentication System

In this project you ask to develop login and signup using image based password where application will shuffle 25 images for every login and signup users to make password more secured. At any time valid user can reset his password if forgot.

To run project install Java1.8 or higher and then install Tomcat7.0 web server and then install MYSQL to save user password details. After installation copy content from 'WEB_INF/database.txt and then paste in MYSQL console to create database Put Graphical Password folder inside Tomcat WEBAPPS directory and then start tomcat server from bin folder. Now open browser and enter URL as 'http://localhost:9999/GraphicalPassword' and then press enter key to get below page

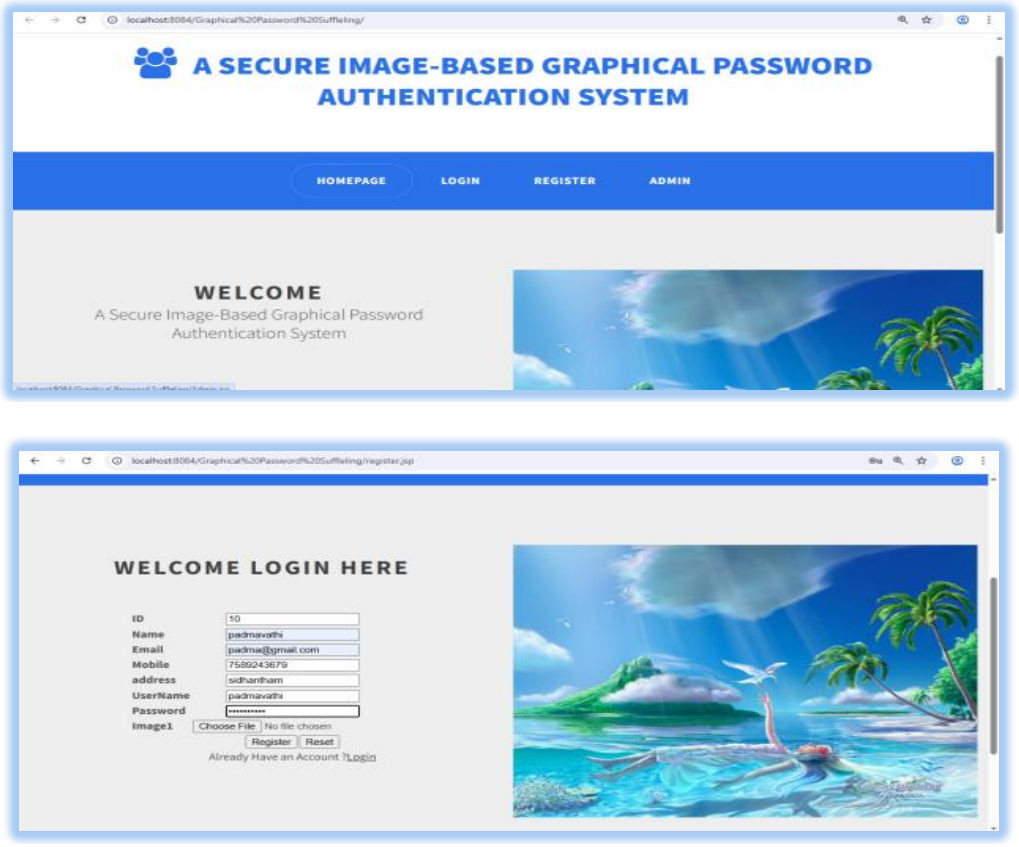

Figure 2: Shows Welcome to "A Secure Image-Based Graphical Password Authentication System"

ISSN: 2582 - 6379
IJISEA Publications
International Journal for Interdisciplinary Sciences and Engineering Applications
IJISEA - An International Peer- Reviewed, Open Access Journal
2025, Volume 6 Issue 3
www.ijisea.org

6. CONCLUSION

In conclusion, "A Secure Image-Based Graphical Password Authentication" presents a promising alternative to traditional password systems. By leveraging visual memory and customization, this approach aims to enhance security, usability, and overall user experience in the realm of authentication.

FUTURE WORK

In Future we will add some more features to our application to make it more secure and useful.

1. Extend this project with any application
2. Addition of OTP verification feature
3. Notification Alert during Login
4. Adding token based (cards) and biometric (like fingerprint or face) authentication techniques.

REFERENCES:

[1] J. Smith, Challenges in Text-based Password Systems: A Review of Vulnerabilities and Limitations.

[2] E. Johnson, A Secure Image-Based Graphical Password Authentication: An Overview of Approaches and Advancements.

[3] M. Brown, Usability Considerations in Authentication Systems: A Comparative Analysis.

[4] S. Davis, Pattern Recognition in Graphical Password Systems: Algorithms and Security Implications.

[5] D. White, Customization and Personalization in Authentication: Enhancing User Engagement.

ISSN: 2582 - 6379
IJISEA Publications
International Journal for Interdisciplinary Sciences and Engineering Applications
IJISEA - An International Peer- Reviewed, Open Access Journal
2025, Volume 6 Issue 3
www.ijisea.org

ABOUT AUTHORS

1. Kadali Keerthana is currently pursuing MCA at SVKP & Dr K S Raju Arts & Science College, affiliated with Adikavi Nannaya University, Rajamahendravaram, Her research interests include Cybersecurity, Graphical Password Authentication, Web Application Security, and Data Science.

2.Karri.Lakshamana Reddy Working as Associate Professor in SVKP &Dr.K.S Raju Arts & Science College(A), Penugonda, West Godavari District, A.P. He received Master's Degree in Computer Applications from Andhra University 'C' level from DOEACC, New Delhi and MTech from Acharya Nagarjuna University, A.P. He attended and presented papers in conferences and seminars. He has done online certifications in several courses from NPTEL. His areas of interests include Computer Networks, Network Security and Cryptography, Formal Languages and Automata Theory and Object-Oriented programming languages.