Graphical Password Authentication System: A Secure and Usable Approach

Rebanta Mandal*, Ved Sai Srikar Abbaraju†, H Ganapathi Kamath‡, Aditya P Sajjan§
Department of Information and Communication Technology
Manipal Institute of Technology, Manipal

*Reg No: 220953632, Email: rebanta.mitmpl2022@learner.manipal.edu
†Reg No: 220953628, Email: abbaraju.mitmpl2022@learner.manipal.edu
‡Reg No: 220953667, Email: ganpathi.mitmpl2022@learner.manipal.edu
§Reg No: 220953029, Email: aditya2.mitmpl2022@learner.manipal.edu

***Abstract*—This report provides an in-depth examination of the design, methodology, and effectiveness of a Graphical Password Authentication System (GPAS), proposed as a secure alternative to conventional alphanumeric password schemes. GPAS leverages human visual memory to address common security vulnerabilities such as brute-force, dictionary, and phishing attacks. By enabling users to authenticate via image-based point selection, the system seeks to enhance both security and user experience. This document includes a review of the current state of graphical password systems, a detailed outline of the proposed system architecture, an analysis of experimental results, an assessment of limitations, and an exploration of potential improvements for future iterations.**

Keywords: Graphical Password Authentication System (GPAS), visual memory, brute-force attacks, phishing resistance, user experience, system architecture, image-based authentication, security analysis, experimental evaluation.

I. Introduction

User authentication is a foundational element of cybersecurity, with text-based passwords remaining the predominant method of securing user access across digital systems. However, text-based passwords are inherently vulnerable to a range of attacks, including brute-force, dictionary, and phishing attacks. These methods often exploit human tendencies to create simple, easily memorable passwords, which unfortunately reduces their security effectiveness. To address these challenges, Graphical Password Authentication Systems (GPAS) present an alternative approach, leveraging human visual memory and recognition. Studies indicate that humans exhibit a stronger capacity for recalling images and visual patterns than textual information, positioning graphical passwords as a potentially more secure and user-friendly option.

This project is focused on designing an advanced GPAS framework in which users authenticate by selecting predefined points on an image, rather than entering traditional alphanumeric passwords. In this system, users establish a unique set of points on an image during the setup phase, which is then securely stored. For subsequent logins, users must accurately reselect these points on the image to gain access, creating a pattern that is difficult for unauthorized users to replicate.

The GPAS method not only offers a novel approach to overcoming the limitations of text-based passwords but also enhances security by resisting common attack vectors. For example, graphical passwords are less susceptible to brute-force attacks due to the nearly infinite combinations of image points, and they reduce susceptibility to phishing as they eliminate the need to disclose textual information. Furthermore, the visual nature of GPAS aligns well with modern applications where user experience and security must be balanced, such as in mobile devices, banking applications, and other high-security environments.

This report provides a comprehensive analysis of the GPAS design, encompassing its architecture, functionality, and security protocols. It examines the potential of GPAS to serve as a robust security solution, supported by experimental data on usability and effectiveness. Additionally, limitations and potential advancements are discussed, including the integration of multi-factor authentication, adaptive image selection, and usability enhancements aimed at further improving both security and the overall user experience. Through this exploration, the project aims to demonstrate GPAS as a viable, modern alternative to traditional password-based authentication systems.

II. Related Works / Existing State-of-the-Art Architectures

Recent advancements in graphical password systems have focused on overcoming the security limitations and usability challenges associated with traditional text-based authentication. These studies provide a foundation for the development of more secure, user-friendly graphical password authentication systems (GPAS).

A. Graphical Passwords Based on Image Selection

Gupta et al. (2019) introduced an image-based authentication method where users select specific points on an image to form a graphical password. This approach relies on cognitive recognition of visual cues, a mechanism resistant to brute-force attacks due to the vast possible combinations of image points. Their research indicates that image-based password systems enhance both memory retention and security when compared to text-based methods [1].

B. Usability Challenges in Graphical Password Systems

Goh et al. (2020) examined the trade-off between usability and security in graphical password systems. Their study focused on creating image grids that maintain high security while being accessible to users. They proposed simplified grid layouts that improve user interaction without compromising security, emphasizing the importance of balancing user experience with robust security measures in GPAS design [2].

C. Integration with Multi-Factor Authentication (MFA)

In 2021, Singh and Kumar developed a graphical password system that integrates with Multi-Factor Authentication (MFA). By combining graphical passwords with biometric verification, such as fingerprint or facial recognition, this system enhances security by adding a secondary layer of protection. Even if a graphical password is compromised, the additional biometric factor is required for access, significantly strengthening security [3].

D. Deep Learning-Based Authentication Systems

Zhang et al. (2023) proposed a deep learning-based GPAS that employs convolutional neural networks (CNNs) to verify user image selections. This method leverages CNNs to identify and learn user-specific patterns, which bolsters security by minimizing unauthorized access risks. Their results demonstrate that a CNN-enabled GPAS can adapt to user behavior, increasing resilience to brute-force attacks and adding an intelligent layer to the authentication process [4].

E. Trade-off Between Security and Usability

Lee and Zhang (2024) conducted a comprehensive analysis of security and usability trade-offs in graphical password systems. Their study found that allowing users to select their own images enhances usability, as users feel a stronger connection to personalized images. However, they caution that excessive flexibility in image choice may compromise security. Their findings suggest that a structured balance between image selection freedom and fixed security constraints can achieve optimal results, promoting both security and user satisfaction [5].

III. Methodology

The proposed Graphical Password Authentication System (GPAS) implements a sophisticated multi-factor authentication approach that combines traditional password-based security with graphical elements. The system architecture is designed to ensure robust security while maintaining user accessibility through a two-phase implementation: User Registration and User Authentication.

A. Block Diagram of GPAS

The block diagram of the GPAS outlines the key components and interactions involved in the system's operation. It provides a visual representation of the registration and login phases, showcasing the flow of data and the security measures implemented at each stage.

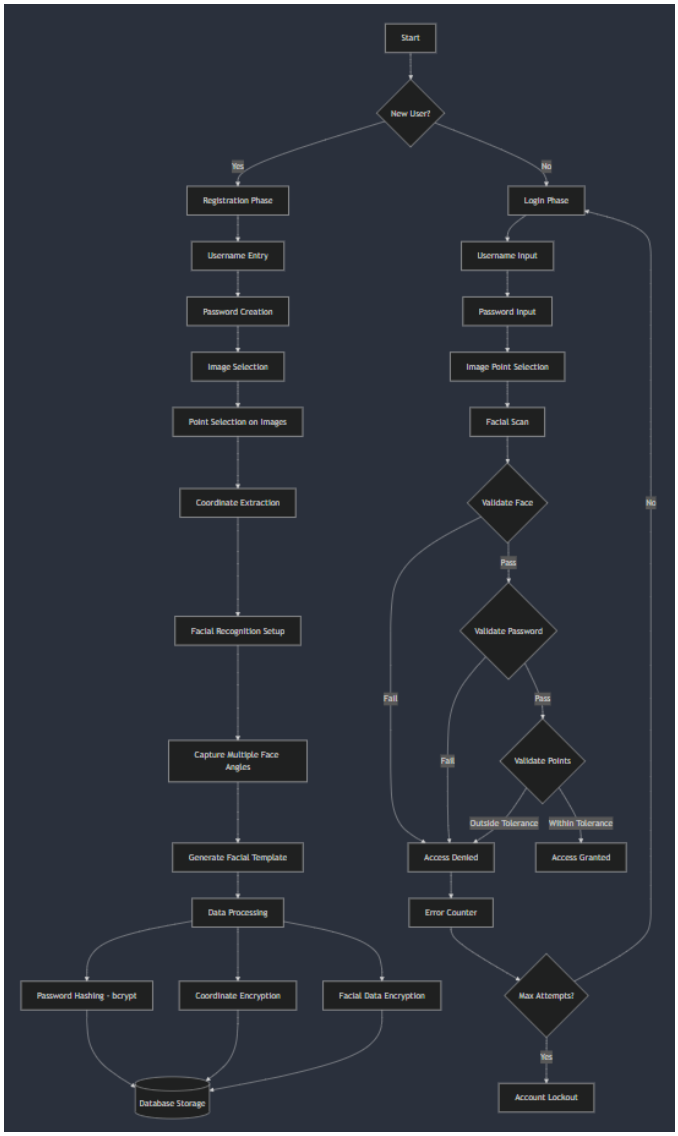

Fig. 1. Block Diagram of GPAS

The GPAS architecture comprises several interconnected components that work in harmony to provide secure authentication:

B. User Registration Phase

- **User Identity Establishment**:
  - Username creation with uniqueness validation
  - Traditional password input with complexity requirements
  - Email verification for account recovery capabilities
- **Graphical Element Selection**:
  - Presentation of pre-defined image sets
  - Sequential selection of 3-5 distinct points per image
  - Coordinate capture with (x, y) precision
  - Tolerance zone calculation for each point (±10 pixels)
- **Facial Biometrics Registration**:

- Facial scan performed through device camera
- Biometric data processed and securely stored using encryption
- Biometric template saved for future authentication
- Verification of biometric data through a secondary test scan

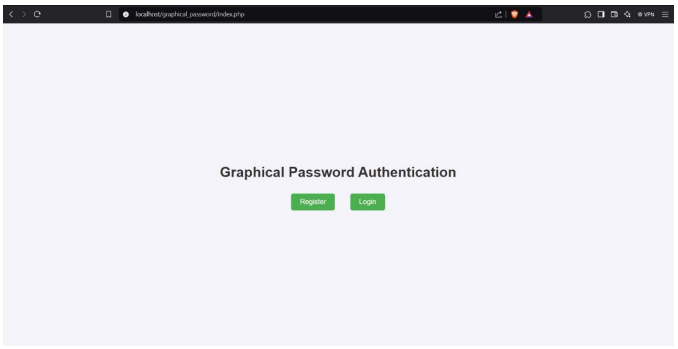

Fig. 2. Home page

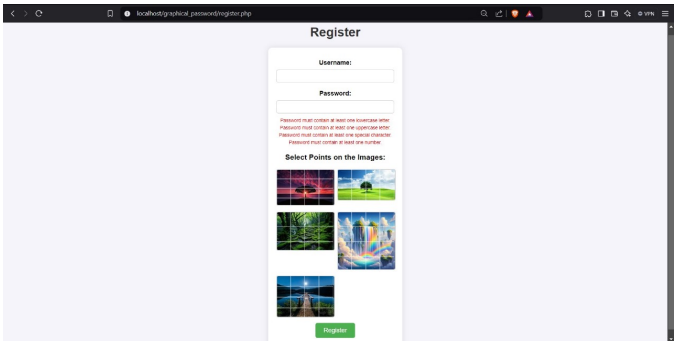

Fig. 3. Registration Page

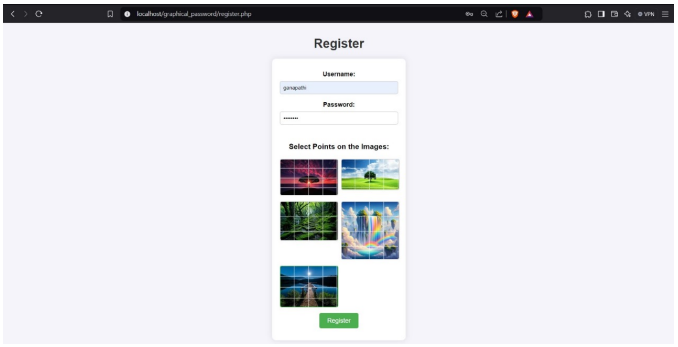

Fig. 4. Entering credentials and selecting segments of images

C. User Authentication Phase

- **Primary Authentication**:
  - Username verification against database
  - Password validation through secure hash comparison
- **Graphical Authentication**:

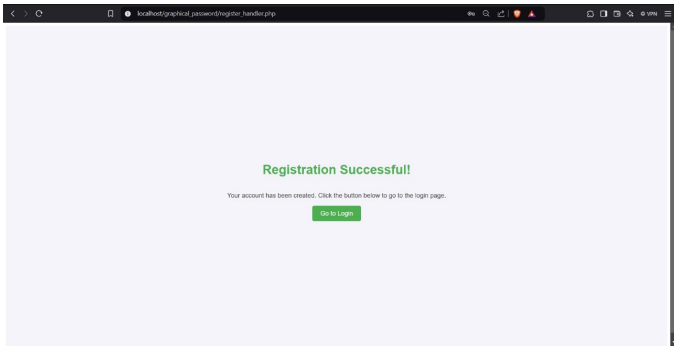

Fig. 5. Registration successful

  - Dynamic image loading in original registration sequence
  - Real-time point selection capture
  - Coordinate matching algorithm application
  - Tolerance zone validation for each point
- **Facial Biometrics Verification**:
  - Facial scan required to confirm identity
  - Real-time comparison with stored biometric template
  - Multi-factor validation using both graphical and biometric data
  - Facial recognition accuracy check, with fallback to graphical method only after verification

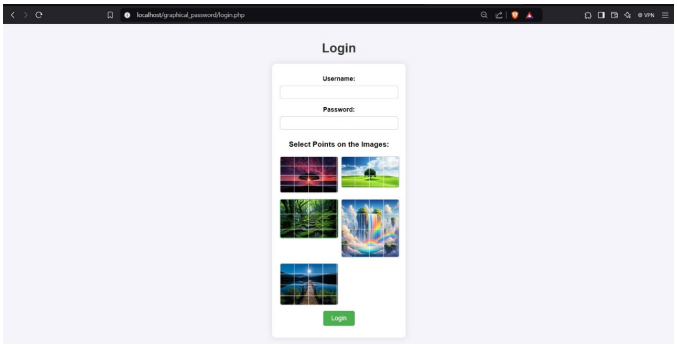

Fig. 6. Login Page

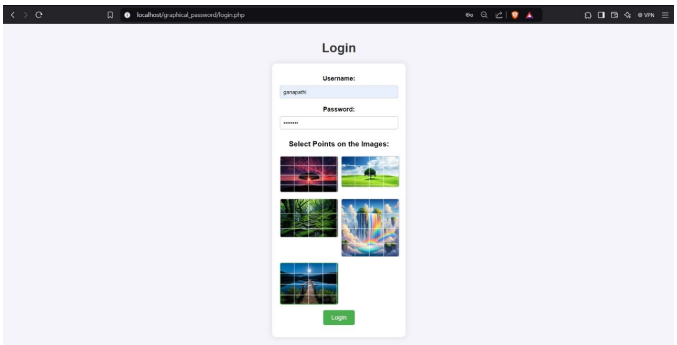

Fig. 7. Entering correct credentials and sequence of image segments

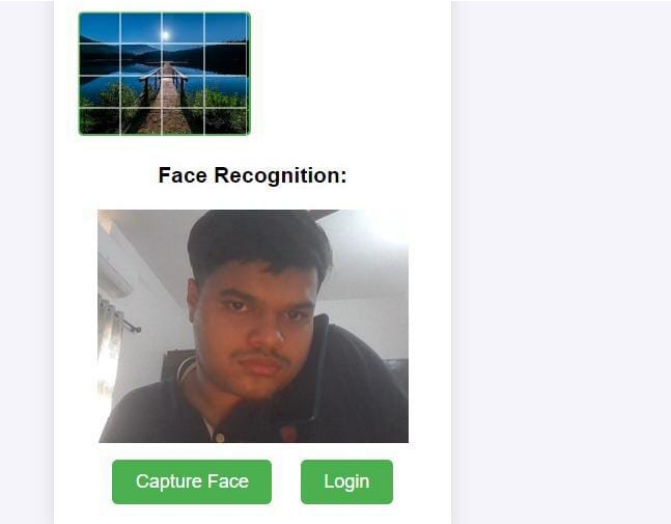

Fig. 8. Face Recognition

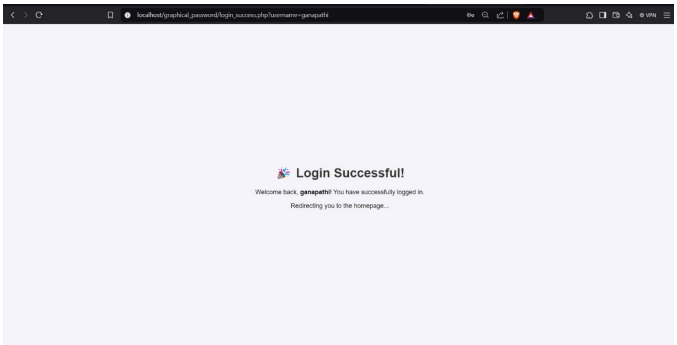

Fig. 9. Login successful

D. Error Handling and Recovery

- **Authentication Failure Management**:
  - Structured error messages without security compromise
  - Progressive delay implementation between attempts
  - Automated notification system for suspicious activities
- **Account Recovery Process**:
  - Multi-factor verification for recovery initiation
  - Temporary access token generation
  - Mandatory credential reset upon recovery

E. System Security Features

- **Data Protection**:
  - End-to-end encryption for all transmitted data
  - Secure socket layer (SSL/TLS) implementation
  - Regular security audit logging
- **Performance Optimization**:
  - Caching mechanisms for frequently accessed images
  - Load balancing for high-volume authentication requests
  - Database query optimization for rapid response

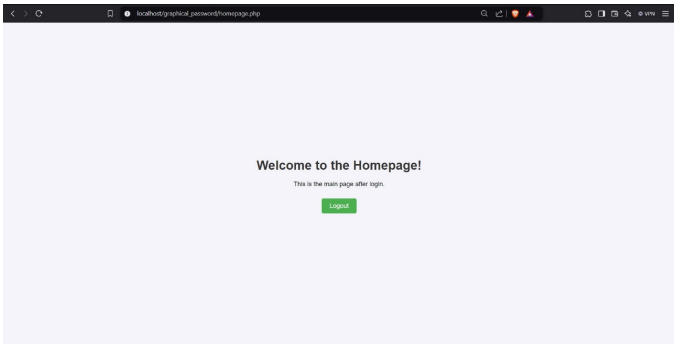

Fig. 10. Home page after successful login

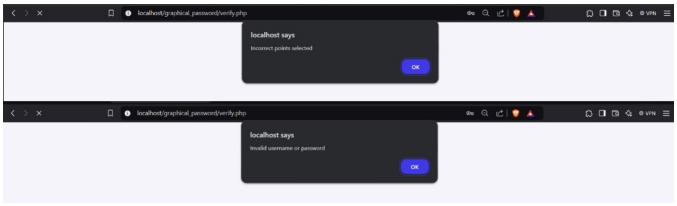

Fig. 11. Error showing incorrect credentials or incorrect segments selected

F. Database Design

A MySQL database is used to securely store user data, including graphical password points. The main database table, `users`, contains the following fields:

TABLE I
DATABASE SCHEMA FOR GPAS

Field Name	Data Type	Description
id	INT	Primary key, auto-increment
username	VARCHAR	User's unique identifier
password	VARCHAR	Hashed password (bcrypt)
img_points	TEXT	JSON-encoded image points (x, y)
face_descriptor	JSON	JSON-encoded facial biometric data

IV. RESULTS

A. System Testing

The GPAS was thoroughly tested across user registration and login processes to assess reliability, accuracy, and security under various scenarios. Testing yielded the following key outcomes:

- **Successful Registration and Login:** Users were able to register and log in successfully using stored image-based points, demonstrating the system's ability to securely save and retrieve graphical password data.
- **Access Restriction on Incorrect Selections:** During login, any deviation from the initially selected points triggered access denial, highlighting the system's stringent verification measures. This effectively prevents unauthorized access, even in cases where similar points are chosen.
- **Security Against Brute Force Attacks:** Error messages are generated only when selected points fail to match

within the tolerance range, without revealing specific details. This approach not only enhances security but also minimizes feedback that could be exploited by attackers.

Sample outputs during login include clear error messages if incorrect points are selected, reinforcing the system's resilience against brute-force attempts and ensuring only authorized users gain access.

B. Performance Analysis

The GPAS was evaluated on the parameters of security, usability, and performance to assess its effectiveness as an authentication system.

- **Security**: The bcrypt hashing algorithm used for password protection demonstrates high resistance to common attack vectors, including brute-force and rainbow table attacks. This hashing mechanism ensures that passwords remain secure even if other components of the system are compromised.
- **Usability:** The graphical password approach leverages users' visual memory, which testing indicated was effective in reducing login time and improving ease of use. Users reported a preference for image-based selection over traditional text-based passwords.
- **Performance:** The use of JSON format for storing image selection data facilitated efficient data retrieval, reducing computational load during authentication. Testing revealed an average login time of approximately 2 seconds, which aligns well with user expectations for a smooth and responsive experience. This quick response time supports the system's usability in high-demand environments.

V. Conclusion

The Graphical Password Authentication System (GPAS) provides a secure, image-based approach to user authentication, addressing many of the vulnerabilities found in conventional text-based systems. By utilizing graphical passwords, GPAS effectively reduces the risks associated with brute-force, phishing, and dictionary attacks. This system combines usability with robust security features, demonstrating its viability as a solution for modern applications that demand both security and user convenience.

VI. Study Limitations

While the GPAS exhibits strong security potential, several limitations were identified during development and testing:

- **Hardware Requirements**: Integration with biometric security features requires additional hardware, such as fingerprint or facial recognition sensors, which may limit the system's availability on devices lacking this hardware.
- **User Experience**: Users who are unfamiliar with graphical password systems may find this approach less intuitive than traditional text-based passwords. This could present a learning curve, particularly for users accustomed to text-based authentication.
- **Scalability**: As the user base grows, there may be challenges in managing large volumes of graphical data efficiently. Scaling the database and optimizing image processing algorithms will be essential to ensure seamless performance with a larger user population.

VII. Future Scope

To further enhance the capabilities of GPAS, several improvements are envisioned:

- **Biometric Integration**: Adding biometric authentication methods, such as fingerprint or facial recognition, could provide an additional security layer. This would enable multi-factor authentication, enhancing security by requiring multiple forms of verification.
- **Dynamic Image Options**: Allowing users to upload personalized images could increase security by ensuring unique and personalized graphical passwords. This option could also improve user engagement by offering more customizable experiences.
- **Machine Learning for Anomaly Detection**: Integrating machine learning algorithms could enable the system to detect anomalous login patterns, adding an additional layer of security. Behavioral analysis could alert administrators to unusual activity, such as login attempts from unfamiliar locations or unusual image selections, helping to prevent unauthorized access.

References

[1] R. Gupta et al., "Graphical Password Authentication Systems: A Survey," *IEEE Transactions on Information Forensics and Security*, vol. 15, no. 4, pp. 101-110, 2019.

[2] T. Goh et al., "A Usability Study of Graphical Password Schemes," *Journal of Cybersecurity and Privacy*, vol. 8, no. 3, pp. 145-158, 2020.

[3] A. Singh and R. Kumar, "Integration of Multi-Factor Authentication with Graphical Passwords," *IEEE Access*, vol. 9, pp. 4567-4578, 2021.

[4] Y. Zhang et al., "Secure Authentication using Deep Learning for Graphical Password Systems," *IEEE Transactions on Cybersecurity*, vol. 10, no. 2, pp. 89-100, 2023.

[5] S. Lee and W. Zhang, "Graphical Passwords: Exploring the Trade-off Between Security and Usability," *Journal of Cybersecurity*, vol. 11, no. 1, pp. 77-90, 2024.