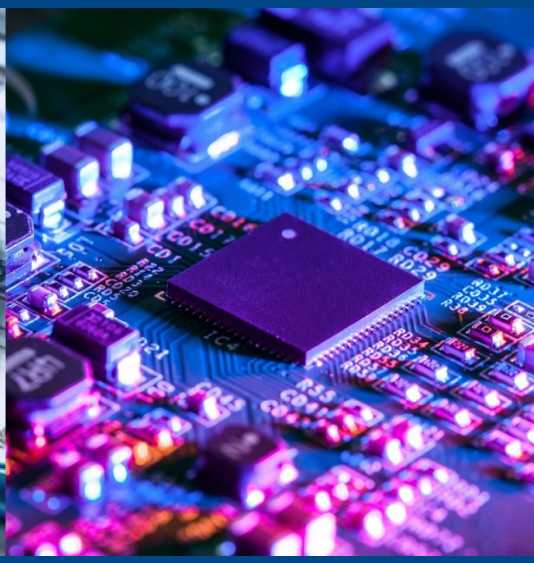
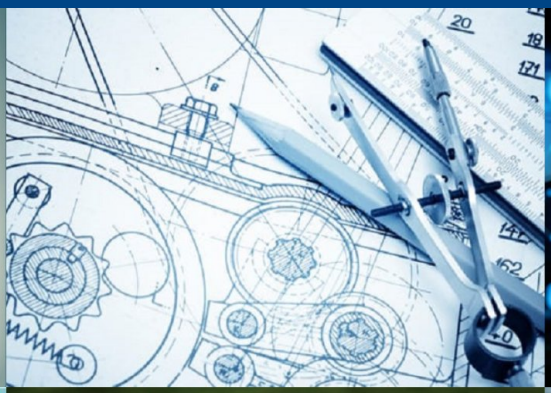
ISSN: 2582-7219

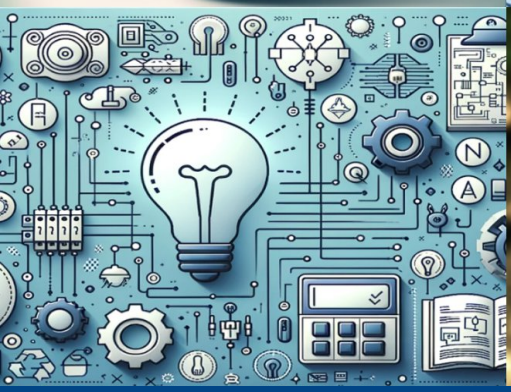




International Journal of Multidisciplinary Research in Science, Engineering and Technology

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.206 **Volume 9, Issue 4, April 2026**

© 2026 IJMRSET | Volume 9, Issue 4, April 2026 | DOI:10.15680/IJMRSET.2026.0904368

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Picture Password Authentication System

Mohammed Jalaluddin .M[1], Aravindhan RP[2], Nehan I[3]

Assitant Professor, Department of Computer Applications, B.S.A.Abdur Rahman Institute of Science and Technology, Chennai, Tamil Nadu, India[1]

BCA (CTIS) III year, Department of Computer Applications B.S.A.Abdur Rahman Institute of Science and Technology, Chennai, Tamil Nadu, India[2]

BCA (CTIS) III year, Department of Computer Applications B.S.A.Abdur Rahman Institute of Science and Technology, Chennai, Tamil Nadu, India[3]

ABSTRACT: Authentication is essential for protecting digital systems and user data from unauthorized access. Traditional text-based passwords are widely used but suffer from several security issues such as weak password selection, password reuse, and vulnerability to brute-force and dictionary attacks. To overcome these limitations, graphical authentication techniques have been introduced .This paper proposes a Picture Password Authentication System that allows users to authenticate using images instead of conventional text passwords. In this system, users click on specific locations in an image during registration, which act as their graphical password. During login, the user must reproduce the same click pattern to gain access. Since humans tend to remember visual information more effectively than textual data, graphical passwords improve memorability and reduce the likelihood of forgotten credentials .The proposed system enhances security by incorporating encrypted storage of click coordinates, tolerance-based matching for accurate verification, and session management mechanisms. Additional features such as time-based authentication control and limited login attempts further strengthen resistance against common attacks such as brute force, shoulder surfing, and guessing attacks.Overall, the system increases password complexity while maintaining usability, providing a secure and user friendly alternative to traditional password-based authentication methods.

KEYWORDS: Authentication ,security ,Attacks, Click Points

I. INTRODUCTION

Authentication is an essential component of computer security that ensures only authorized users can access a system. Most existing systems rely on traditional text-based passwords; however, these passwords often suffer from several security and usability issues such as weak password creation, password reuse, and vulnerability to guessing and brute-force attacks. Additionally, complex passwords are difficult for users to remember, leading to poor password practices and reduced overall security.

To overcome these limitations, graphical authentication techniques have been introduced, where images or visual patterns are used instead of text. Humans generally remember images more easily than textual information, making graphical passwords more user- friendly and improving memorability. These methods reduce the cognitive load on users while enhancing resistance to common attacks such as shoulder surfing and password guessing.

In this paper, a Picture Password Authentication System is proposed, in which users create a graphical password by selecting specific points on an image during registration. During login, the user must reproduce the same click pattern to gain access. The system further enhances security by incorporating encrypted storage of click coordinates, tolerance-based matching for accurate verification, and controlled login attempts.

The proposed approach aims to provide a balanced solution that improves usability without compromising security. By combining ease of use with strong protection mechanisms, the system offers an effective alternative to traditional password-based authentication methods.

© 2026 IJMRSET | Volume 9, Issue 4, April 2026 | DOI:10.15680/IJMRSET.2026.0904368

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

II. LITERATURE SURVEY

Several research studies have focused on developing authentication systems that enhance both security and usability. However, achieving an effective balance between these two aspects remains a significant challenge.

Kausar et al.[1] proposed GRA-PIN, a hybrid authentication method that combines graphical passwords with PINs to defend against shoulder-surfing attacks. Although the method improves security, it increases user complexity due to the additional authentication step. Similarly, Kawamura et al. [5] introduced EyeDi , an image distortion-based graphical authentication system designed to resist screenshot attacks. While the approach enhances security, it may reduce usability because of the complexity involved in interpreting distorted images.

Vaishali [3] developed an authentication system that integrates image and video signatures. This method provides strong security; however, it makes the login process time-consuming and less user-friendly. Zujevs [8] proposed the HOPE graphical password system, which enhances security through graphical interactions but requires precise input, thereby reducing efficiency in quick authentication scenarios.

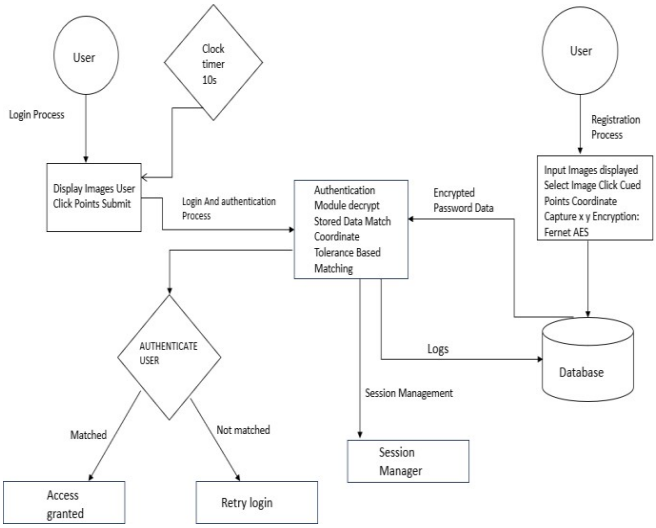
Albayati and Lashkari [5] introduced a **decoy-based graphical password system** to prevent guessing attacks. Although effective in improving security, it introduces additional steps during login, which may affect user convenience. Nizamani et al. developed a hybrid authentication scheme that improves memorability and usability, but at the cost of increased system complexity.

From the comparative analysis, it is evident that most existing systems prioritize either security or usability, often resulting in a trade-off between the two. Many approaches involve complex password mechanisms or extended authentication time, which reduces overall user convenience.

The proposed Picture Password Authentication System addresses these limitations by providing a balanced solution. It ensures secure authentication using encrypted graphical passwords while maintaining high usability and faster login times through intuitive image-based click points.

III. METHODOLOGY

The methodology of the proposed Picture Password Authentication System consists of two main processes: Registration and Login & Authentication. The workflow is designed to ensure secure password creation, encrypted storage, efficient matching, and session management.



a. Registration Process

During registration, the user selects an image that will serve as the basis for creating the graphical password. The system

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

displays the chosen image, and the user clicks on specific points to generate unique coordinate-based password data. These click coordinates are captured and encrypted using the AES encryption algorithm to ensure secure storage. The encrypted password data, along with the selected image information, is then stored in the database for future verification.

b. Login Process

In the login phase, the system displays the previously registered image to the user. The user clicks on the same predetermined points. A clock timer mechanism (10 seconds in the diagram) ensures that the user must complete the login action within a specified time frame, preventing brute-force and automated attacks.

Once the user submits the login attempt, the captured click coordinates are forwarded to the Authentication Module for verification.

c. Authentication Process

The Authentication Module retrieves the corresponding encrypted password data from the database and decrypts it for comparison. The received login coordinates are matched against the stored coordinates using a tolerance- based matching algorithm, allowing for minor variations in user clicking behaviour.
If the coordinates match, the system forwards the result to the Session Manager.
If the coordinates do not match, the user receives a retry prompt.

d. Session Management

Upon successful authentication, the Session Manager establishes a secure user session and grants access to the system. In the case of mismatched coordinates, the system denies authentication and redirects the user to retry the login process.

e. Access Control

The final stage consists of either:
Access Granted – if authentication is successful and a valid session is established.
Retry Login – if the authentication module detects mismatched or invalid click coordinates.

IV. PROPOSED SYSTEM

The proposed Picture Password Authentication System is built on the Cued Click Point (CCP) methodology, which enhances both usability and security when compared to traditional PassPoint techniques. Unlike PassPoint— where multiple click points are selected on a single image—the CCP approach requires the user to click one point on multiple images presented in a sequence. Each image appears one after another, and the next image in the sequence is determined by the click point chosen on the current image, making every authentication path unique.

ADVANTAGES OF PROPOSED SYSTEM

- **Resistant to brute-force attacks** due to the enlarged password space created by single-click points distributed across multiple images.
- **Enhanced usability through cued recall**, allowing users to remember click positions more naturally and accurately.
- **Improved security through image-sequencing logic, where each click determines the next image, making it difficult for attackers to reproduce the exact sequence.**

V. PERFORMANCE ANALYSIS

Table I compares different graphical password authentication systems based on key performance parameters. The proposed system outperforms existing methods in terms of login time and usability by providing faster and more intuitive authentication. Unlike other systems that require complex password patterns, the proposed system allows easy-to-remember graphical passwords while maintaining a high level of security. Additionally, it ensures consistent availability and a user- friendly interface, making it a balanced and efficient authentication solution.

© 2026 IJMRSET | Volume 9, Issue 4, April 2026 | DOI:10.15680/IJMRSET.2026.0904368

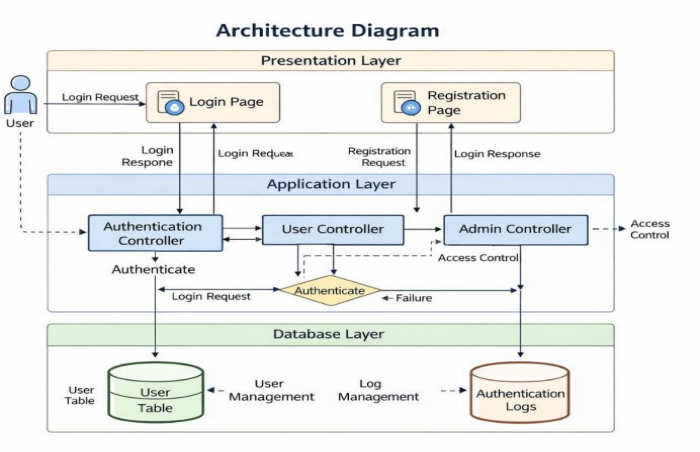
ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

PARAMETER	GRA-PIN	Graphical Password Method 'HOPE'	Proposed System
Login Time	More	More	Less(faster)
Usability	Less	Medium	High
Availability	High	Always	Always
GUI	User friendly	Less user friendly	User friendly
Security	High	High	High
Password Complexity	High(hard)	Hard	Easy

VI. SYSTEM ARCHITECTURE



1. Presentation Layer
- Includes Login Page and Registration Page.
- Accepts user inputs such as username and authentication actions (clicks on images).
- Sends requests to the application layer and displays responses to the user.

2. Application Layer
- Acts as the core processing layer of the system. Includes components such as:

1. Authentication Controller (handles login validation)
2. User Controller (manages registration and user operations)
3. Admin Controller (handles administrative tasks and access control)
4. Processes user requests and performs authentication logic.
5. Determines success or failure of login attempts.
6. Manages session handling and system flow.

3. Database Layer
- Responsible for data storage and retrieval.
- Stores user details in the User Table.

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

VII. IMPLEMENTATION

Frontend Technologies:

- HTML5 & CSS3
- Bootstrap Framework
- JavaScript
- Responsive Design Backend Technologies:
- Python Flask Framework
- SQLite Database
- Cryptography Library
- Session Management ALGORITHMS
- Cued Click Points Algorithm
- Image Coordinate Matching Algorithm

VIII.CONCLUSION

This paper presents a Picture Password Authentication System that enhances security and usability by replacing traditional text-based passwords with graphical authentication. The system allows users to authenticate by selecting specific points on images, leveraging human visual memory for improved recall and convenience. Security is strengthened through the use of hashing and encryption techniques, along with tolerance-based validation, session management, and timeout mechanisms.

The proposed system successfully addresses the limitations of existing authentication methods by achieving a balance between security and user friendliness. It reduces the complexity of password management while maintaining resistance against common attacks such as brute force and shoulder surfing. Overall, the system provides an efficient, secure, and user-centric authentication solution suitable for modern applications.

REFERENCES

[1]. S. Kausar, M. R. Naqvi, and A. Shahid, “GRA-PIN: A Hybrid Graphical Password System for Enhanced Security,” International Journal of Computer Applications, vol. 120, no. 5, 2015.
[2]. T. Kawamura, Y. Watanabe, and H. Iwasaki, “EyeDi: Image Distortion-Based Graphical Authentication System Resistant to Shoulder-Surfing Attacks,” in Proc. International Conference on Information Security, 2016.
[3]. Vaishali, “An Enhanced Authentication System Using Image and Video Signatures,” International Journal of Advanced Research in Computer Science, vol. 8, no. 3, 2017.
[4]. A. Zujevs, “HOPE: A Graphical Password Authentication System,” in Proc. International Conference on Computer Systems and Technologies, 2014.
[5]. M. Albayati and A. H. Lashkari, “A Decoy-Based Graphical Password Scheme for Improved Security,” Journal of Information Security, vol. 6, no. 4, 2015.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com