Graphical Password to Avoid Shoulder Surfing

Santhosh S, Surya R, Vivin R, Sanjay Palani S, Ms. Poornima S

Department of Information Technology, Batchelor of Technology, Sri Shakthi Institute of Engineering and Technology (Autonomous) Coimbatore-641062

ABSTRACT

Traditional text-based passwords are vulnerable to attacks such as guessing, brute force, and particularly shoulder surfing, where an attacker can observe and replicate a user's password entry. To overcome these limitations, graphical password authentication provides a more secure and user-friendly alternative by leveraging human ability to remember images more effectively than text. In this project, a **graphical password scheme with spin-wheel/colour-wheel design** is implemented to resist shoulder surfing attacks. Users create a personalized password by selecting sequences of colors , patterns, or positions on an interactive graphical interface rather than typing characters. During authentication, the interface dynamically changes its layout, ensuring that even if an attacker observes the login process, the actual password sequence cannot be easily inferred. This approach enhances security while maintaining usability, making it suitable for applications where secure and intuitive authentication is essential.
.

INTRODUCTION

Password security is a major concern in today's digital world, where traditional text-based passwords are prone to attacks such as guessing, brute force, and shoulder surfing. Shoulder surfing, in particular, occurs when an attacker observes a user entering their password, making the system vulnerable in public spaces. To overcome this, graphical password systems are introduced as a more secure and user-friendly alternative. In this project, a graphical password using a **color-wheel mechanism** is proposed, where the interface changes dynamically during login. This makes it difficult for attackers to capture the actual password while ensuring better usability and stronger security.

Objective:

1. To develop a secure authentication system using **graphical passwords** instead of traditional text-based passwords.
2. To design a **color-wheel based interface** that resists shoulder surfing attacks.
3. To ensure the system provides **high usability and memorability** for users.
4. To make the login process **dynamic**, so the password cannot be easily observed or replicated.
5. To enhance protection against **common password attacks** such as guessing and brute force.
6. To provide a practical solution suitable for use in **public environments and mobile devices**.

LITERATURE SURVEY

1. Early Approaches
- **Sobrado & Birget (2002):** Introduced Movable Frame, Intersection, and Triangle schemes.
- **Issues:** High complexity, higher failure rates, usability concerns.

2. Modern Techniques
- **Randomized Pass Points (RPP):** Random click-points to resist pattern prediction.
- **Shifting Condition & Digraph Substitution:** Uses decoy images and calculations to confuse attackers.
- **Sequential Pass Point (SPP):** Sequence-based click-points; order reversal adds security.
- **Gaze-Assisted Authentication:** Eye-tracking to follow moving shapes, hard to mimic.

3. Comparative Studies
- Graphical passwords are more vulnerable to observation but not always to guessing.
- Studies with hundreds of participants confirm the effectiveness of randomized and sequence-based methods.

4. Usability
- Balancing security and usability remains a challenge.
- Schemes like Convex-Hull Click and Color Login aim to simplify user interaction while resisting shoulder surfing.

5. Conclusion
- Shoulder-surfing resistant graphical passwords are evolving.
- Future trends: Integration of biometrics (eye-tracking, gestures) and AI techniques for enhanced security.

METHODOLOGY

The methodology for designing a shoulder-surfing resistant graphical password system involves several key steps. First, the requirements are analyzed to understand the need for secure and user-friendly authentication while studying existing schemes and their vulnerabilities. Next, an appropriate graphical password scheme is designed, such as Randomized Pass Points, Sequential Pass Points, or gaze-assisted authentication, incorporating security features like randomization, decoy images, or sequence reversal while ensuring usability. The prototype is then implemented using web or mobile technologies, enabling image-based password selection, interactive feedback, and security mechanisms. After implementation, usability and security testing is conducted to evaluate memorability, ease of login, and resistance to shoulder-surfing and observation attacks. Finally, the system is optimized based on test results to balance security and user convenience, and conclusions are drawn regarding its effectiveness and potential for future enhancements such as biometric or AI-based integration.

Existing system:

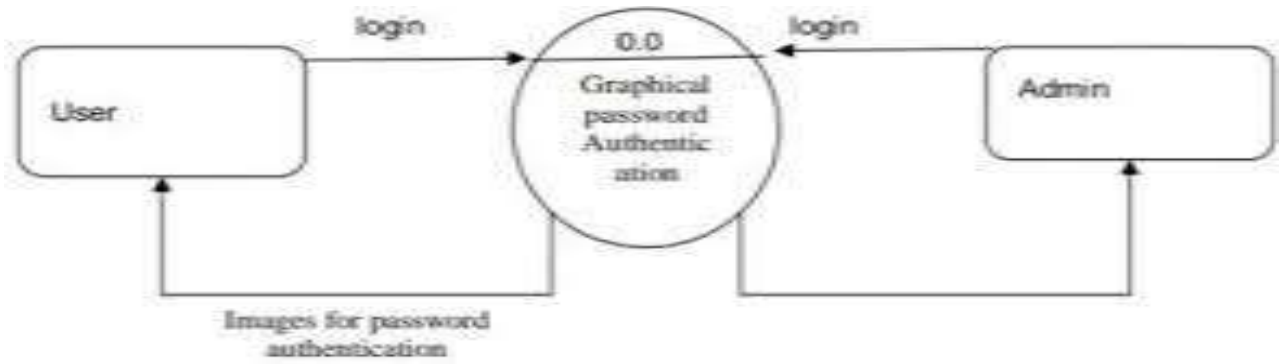
In existing authentication systems, traditional **text-based passwords** are widely used but are vulnerable to shoulder-surfing and keylogging attacks. Some **graphical password schemes** like PassPoints, Draw-A-Secret (DAS), and basic click-based image passwords have been introduced to improve memorability. However, these systems still face security issues as attackers can observe the user selecting points or drawing patterns. Many schemes lack additional protection mechanisms such as randomization, decoy images, or gaze-based interaction, making them susceptible to **shoulder-surfing attacks**.

Disadvantages:

1. Vulnerable to **shoulder-surfing attacks** as attackers can observe user actions.
2. **High failure rates** due to complex patterns or multiple click-points.
3. Limited **password space** in some schemes, reducing security.
4. Some methods are **time-consuming** and reduce usability.
5. Lack of **advanced protection mechanisms** like randomization or decoy images.

Proposed system:

The proposed system implements a **shoulder-surfing resistant graphical password scheme**. Users select click-points or follow visual patterns on images, enhanced with **randomization, decoy images, and sequence reversal** to prevent observation attacks. The system focuses on **usability**, ensuring the login process is simple and memorable, while maintaining strong security. Advanced methods like **gaze-assisted authentication** or interactive feedback may be incorporated to further reduce vulnerability to shoulder-surfing. Additionally, the system can **adapt to different devices** like mobile or web platforms, supports **error correction mechanisms** for misclicks, and includes **performance logging** to analyze login efficiency and user behavior. These features ensure a balanced approach between **security, convenience, and accessibility**.



SYSTEM REQUIREMENTS

1. Hardware Requirements

- **Processor:** Intel i3 or higher
- **RAM:** 4 GB minimum
- **Storage:** 100 MB free space
- **Display:** Monitor with minimum resolution 1024×768
- **Input Devices:** Mouse, Keyboard, or Touchscreen

2. Software Requirements

- **Operating System:** Windows 10/11, Linux, or macOS
- **Development Tools:** HTML, CSS, JavaScript (for web-based implementation) or Android Studio/Xcode (for mobile apps)
- **Database:** MySQL, MongoDB, or local storage for password data
- **Browser:** Latest version of Chrome, Firefox, or Edge (for web-based systems)

3. Additional Requirements

- Internet connection (optional, for cloud or web-based systems)
- Eye-tracking device (optional, if gaze-assisted authentication is implemented)
- Graphics support for image-based password display

Module Description

1.**User Registration:** Users create an account and set a graphical password by selecting points or patterns on images.
2.**User Login:** Users authenticate using their graphical password; includes randomization and decoy features to prevent shoulder-surfing.
3.**Password Management:** Allows secure password reset or change.
4.**Security Module:** Protects against shoulder-surfing, brute-force, and observation attacks; optional gaze-assisted authentication.
5.**Usability Module:** Ensures easy interaction, error correction, and a balance between security and convenience.

MAINPAGE:

LOGIN PAGE

CONCLUSION

In conclusion, the development of graphical password systems can greatly enhance the security and usability of authentication mechanisms. With the increasing demand for stronger and user-friendly security solutions, graphical passwords can provide personalized and reliable protection to users based on their ability to recognize and recall images. This can also bridge the gap between usability and security, making it easier for individuals to safeguard their digital information without relying on complex text-based passwords. The incorporation of graphical methods in authentication can also increase accessibility for a wider audience, promoting safer digital practices. However, it is important to continuously improve and update graphical password systems to ensure their robustness against evolving cyber threats. Additionally, proper regulation and oversight must be in place to ensure ethical implementation and protect user privacy.

Overall, graphical password systems have the potential to revolutionize the way we approach authentication and promote the use of innovative methods for a more secure digital lifestyle.

REFERENCES

[1] Blonder, G. E. (1996). Graphical passwords. *United States Patent 5559961*.

[2] Jansen, W., & Gavrila, S. (2001). *Graphical password authentication using cued click points*. Proceedings of the 21st National Information Systems Security Conference, 1–7.

[3] Sobrado, L., & Birget, J. C. (2002). Graphical passwords. *The Rutgers Scholar, 4*, 1–8.

[4] Wiedenbeck, S., Waters, J., Birget, J. C., Brodskiy, A., & Memon, N. (2005). Authentication using graphical passwords: Effects of tolerance and image choice. *Proceedings of the 2005 Symposium on Usable Privacy and Security*, 1–12. ACM.

[5] Biddle, R., Chiasson, S., & van Oorschot, P. C. (2012). Graphical passwords: Learning from the first twelve years. *ACM Computing Surveys (CSUR), 44*(4), 1–41.

[6] Chiasson, S., van Oorschot, P. C., & Biddle, R. (2007). Graphical password authentication using cued click points. *European Symposium on Research in Computer Security*, 359–374. Springer.