



Paper Type: Original Article

## Enhancing Cybersecurity Through Graphical Password Authentication: A Hybrid Approach to Usability and Security

Soheil Fakheri<sup>1\*</sup> , Omar Mar Cornelio<sup>2</sup> , Haoran Yu<sup>3</sup>

<sup>1</sup> Department of Computer Engineering, Ayandegan Higher of Education Institute, Tonekabon, Iran; jfakherisoheil@iau.ac.ir.

<sup>2</sup> Centro de Estudio de Matematica Computacional, Universidad de las Ciencias Informaticas, La Habana, Cuba; omarmar@uci.cu.

<sup>3</sup> School of Economics and Management, China Three Gorges University, China; fatianyuff@163.com.

### Citation:

Received: 18 April 2024

Revised: 07 June 2024

Accepted: 29 August 2024

Fakheri, S., Mar Cornelio, O., & Yu, H. (2024). Enhancing cybersecurity through graphical password authentication: a hybrid approach to usability and security. *Computational engineering and technology innovations*, 1(3), 170-177.

### Abstract


Graphical Password (GP) is one of the techniques for authentication of computer security. Nowadays digital/computer security is one of the most important things in computer science for protected user or customer data. And shoulder-surfing is one of the threats where a criminal can steal a password by direct observation or by recording the authentication session. There are several techniques available for this authentication, the most prevalent and simple of which is the GP technique. So, we suggest a new technique to combat this problem. We have developed two concepts to combat shoulder surfing attacks. First, the user must register if the registration does not exist. Second, you must log in with a valid user ID and password. The password is a grouping of characters and numbers. Third, the user has to cross Image-Based (IB) authentication where the user can choose their password and this method has higher chances to offset each other. You should choose a password according to the registration password; it must match at login time. In color-based authentication, there should be several color-based passwords and depending on the color, you need to remember the password sequence. And it's like three-factor authentication. So, here is proposed a new GP authentication technique that is resilient to shoulder surfing and also to other types of probable attacks.

**Keywords:** Authentication process, Graphical password, Keylogger, Shoulder surfing.

## 1 | Introduction

One method of computer system authentication is a Graphical Password (GP). Establishing a secure environment for electronic devices is the goal of computer security. One method for ensuring the security of

 Corresponding Author: jfakherisoheil@iau.ac.ir

 10.48314/ceti.v1i3.37



Licensee System Analytics. This article is an open-access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0>).

our digital devices or critical data is the use of GP. Despite being extensively used, traditional alphanumeric passwords have been shown to be susceptible to a number of security risks, including brute force attacks, phishing, and guessing.

As previously mentioned, an image or Image-Based (IB) password may be stored or remembered by the human brain with ease. Therefore, experts suggest a GP for users who can create a random, extremely secure account and who have no trouble remembering it.

By leveraging our brain's ability to store and recall visual information easily, GP offer a more user-friendly and secure alternative for authentication in computer systems. The process of authenticating a user's identity prior to allowing them access to systems or data is known as authentication.

It serves as a critical layer of security in protecting consumer information. Token-based Authentication (TBA), Biometric Authentication (BA), and Knowledge-Based Authentication (KBA) are among the several kinds of authentication techniques.

Token-based methods rely on the possession of a physical device or key, while biometric methods use unique human characteristics, such as fingerprints or facial recognition.

KBA, such as passwords, is the most common approach, and GP fall into this category by using images or shapes as credentials rather than text-based characters. TBA uses tokens as a Hidden Key.

The idea behind GP is rooted in the psychological advantage that humans have when it comes to remembering images. The password is a collection of shapes and images. An image is also easier for the human brain to remember than text, according to scientists. The human brain easily processes images.

IB password this inherent capability makes GP more resistant to common cyber-attacks like dictionary attacks, keylogging, and social engineering.

Attackers often exploit weak alphanumeric passwords by guessing or intercepting them, but GP present an additional layer of complexity, making it harder for malicious actors to crack them. Many users tend to create weak passwords that are easy to guess, reuse the same password across multiple platforms, or rely on simple combinations, leaving themselves vulnerable to attacks. Moreover, the unique visual nature of these passwords adds resistance against techniques like shoulder surfing and phishing. A conventional, widely used authentication mechanism is an alphanumeric password. This traditional method is a system that is too insecure in practice. For instance, if the user is not using a strong password, the attacker might select one that is simple to figure out. Users may use the same password for multiple devices or sites [1].

As security threats continue to evolve, it has become clear that traditional passwords are no longer sufficient to protect sensitive data. This growing realization has led to the exploration of alternative authentication methods, with GP emerging as a promising option that balances security and usability. For typical users, all of these features are insecure. Additionally, one of the key security areas where users actively manage the security of their personal data is authentication.

Generally, GP techniques are two types: 1) recognition-based and recall-based graphical techniques, and 2) recall-based graphical techniques.

During the registration process, the user must select one or more images to authenticate themselves using recognition-based approaches.

In recall-based GP require users to recreate a pattern or draw an image they initially registered, relying on their ability to remember the image from memory. Both techniques offer advantages in terms of security and ease of use, with the potential to improve the overall security of personal and corporate systems, reducing reliance on easily compromised alphanumeric passwords.

## 2 | Literature Review

Bhand et al. [2] created GPA. The GP method was created in which they provided some ineffective GP techniques. For instance, they created a multiple-IB password, in which the user is shown a number of images from which they must choose one or more. There are no more displays needed for the grid-based system, which is an easy object. It's difficult to decide between the Triangle scheme, which has a protruding surface and almost the same amount of images displayed. The most useless parts of this paper are the username calculation bases. Thus, this novel approach frequently addresses the many problems with the current system.

Bhand et al. [2] collaborated on enhancement of password authentication system using graphical image. The construction of a GP system with several authentication methods is the primary subject of this study [3]. Additionally, this method's main objective is to increase security while making it easier for users to use and harder for hackers to figure out. Thus, they create three distinct types of authentication systems: 1) Cued Click Points (CCP), 2) pass points, and 3) persuasive CCP.

### Pass point

The user must select five points from a single image during this system, and they must repeat the same order of points from the same image both during the selection process and during the login process. The Cued Click Point and the Pass Point share the same structure, but they differ primarily in that the former awards five points on five distinct images, one point for each. One possible authentication method is PCCP. Despite being the finest technology, PCCP contains problems with security.

A new GP scheme resistant to Gao et al. [4] discussed Shoulder-Surfing. The security properties of graphical authentication are discussed in this study [5]. Different GP schemes employ various strategies to reduce cyberattacks. GP is easy to remember and offers good security and usability, as you are aware. Thus, compared to text-based passwords, GP schemes offer greater security.

Shoulder surfing, brute force, dictionary, guessing, malware, and social engineering attacks are some of the defenses against GPA risks. This article provides a brief overview and categorization of different GP schemes, followed by details on their drawbacks and recommendations for further advancement.

The paper "Graphical passwords: learning from the first twelve years" by Biddle et al. [6] presents a comparative analysis of various GP techniques, including Pass Points, CCP, story-based passwords, and Draw a Secret (DAS) [7]. They evaluate the techniques based on various factors, such as usability, memorability, security, and resistance to attacks. The study concludes that Pass Points and CCP techniques are more user-friendly, but they may not provide high security against shoulder-surfing attacks. On the other hand, Story-based Passwords and DAS techniques are more secure but may not be as easy to use.

The paper "A Systematic Literature Review of Graphical Password Schemes" by Shammee et al. [8] provides a comprehensive analysis of various graphical password (GP) schemes. The authors evaluate these techniques based on factors such as usability, memorability, security, and resistance to attacks. This systematic literature review evaluates the usability and security of GPA techniques [9]. The authors analyzed 51 research papers published between 2005 and 2017 and categorized them based on the type of GP techniques and the evaluation criteria. They found that GP techniques provide better usability than traditional text-based passwords, but they may not offer sufficient security against various attacks. The review also suggests that there is a need for standardized evaluation criteria and user studies to improve the design of GP schemes.

## 3 | System Design

Any user attempting to access the homepage of this project will be presented with three options: register, log in, and about the developer. Clicking the Register option is necessary if you haven't already.

Then, the register page will appear; you have to provide a first text-based password and necessary information like first name, last name, email, password, security question etc.

After clicking the next Second color, the base GP security page will appear, and then you have to select the password squatly. And you have to remember squatly based on color.

After clicking next, the image base password page will appear; you have to select multiple images as a password and save it.

After that, you must return to the main page and click the login button. You must then enter the right password and username. You have successfully logged in with your text-based password if your username and password match.

You must then enter the Color-Based (CB) password after the page requesting it appears. If it's accurate, you've successfully logged in using the CB password.

After the page with the IB password appears, you must choose the IB password. You have successfully logged in with the IB password, if it is correct.

Then, the main page will come.

The human brain easily processes images. As a result, engineers provided a GPA system that is easy to use and remember. Additionally, GP is more secure than text-based ones since they are resistant to social engineering, dictionary attacks, keyloggers, and other threats. In general, there are two kinds of GP techniques: recall-based and recognition-based.

Both CB and IB authentication are utilized in GP, which are the greatest substitute for text passwords because they are simple to remember and hard to figure out. GP takes advantage of the fact that humans are visual beings who process and retain visual cues more well than most other types of data.

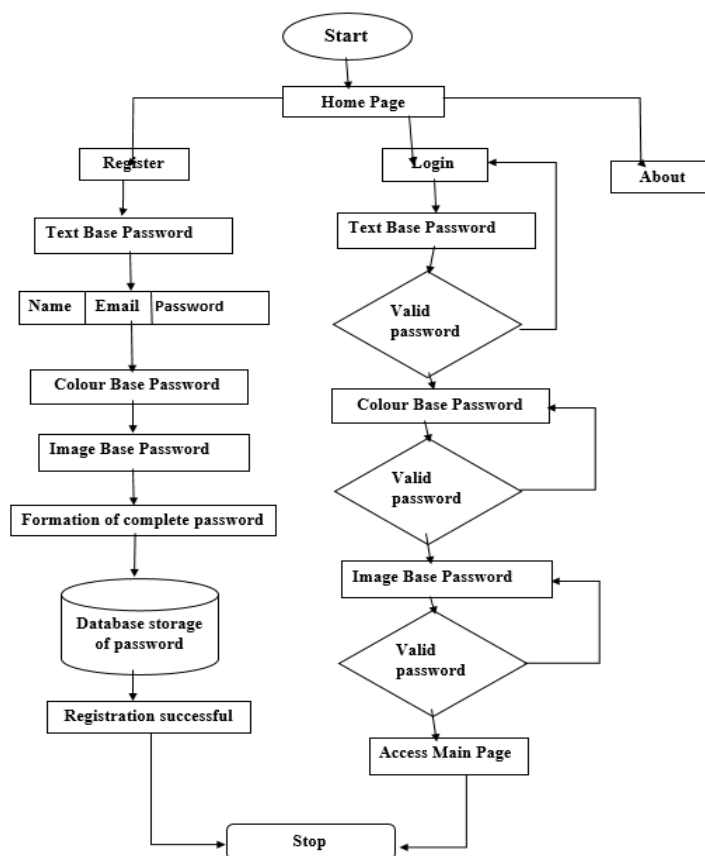


Fig. 1. Flowchart for graphical password authentication [10].

### 3.1| Schemes

Using images and various colors as passwords is known as a GP. Because people recall visuals better than words, GP is simpler to remember. Brute-force attacks are less likely to succeed with the GP. Instead of using text or alphanumerical characters, GP is sometimes more visually appealing.

#### 3.1.1| Image based scheme

The user must choose images as the password in this system, which will supply a certain number of images. For authentication, the user must choose the real images from the grid in the right sequence. The images make it easy for the user to remember the password. Images are placed for each login attempt, and IB passwords are more visually appealing. Thus, shoulder surfing attacks were also prevented by this plan. These classes define an attack dictionary's suitable weak password subspaces.

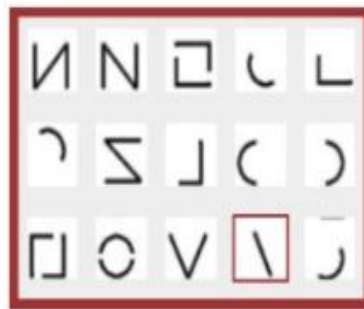


Fig. 2. Image based scheme.

#### 3.1.2| Color base scheme

The user must choose colors as the password in this scheme, which will supply a number of colors. Different colors are utilized in this system to confound imposters, yet authorized users can easily use it. The colors make it easy for the user to remember the password. It can withstand attacks that involve shoulder surfing. For authentication, the user must choose the actual colors in the right order. The database will then store the password.

#### 3.1.3| Recognition based scheme

During the registration process, customers utilize this technique to set an image as their password. No tips are provided to help users remember their passwords because they must replicate or remember them themselves. The password requires the user to choose a certain amount of the images in this collection. The user must accurately identify these pre-selected images during authentication.

#### 3.1.4| Signature based scheme

This approach uses the user's signature in place of the system-specified password. No one can just copy someone else signature. Access may be blocked by a small error in the signature.

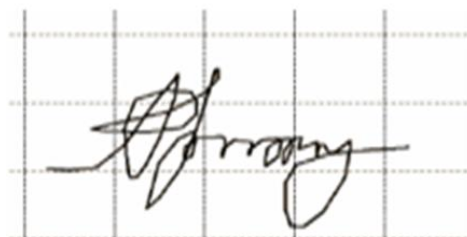


Fig. 3. Signature based scheme.

## 4 | Discussion

A key element in the majority of computer security scenarios is user authentication. Researchers suggested a straightforward GPA mechanism in this expanded abstract. In an attempt to combine the finest features of both text-based and GP, the system:

- I. Performance evaluation: describe how the performance of the system was evaluated, including the criteria and metrics used to assess its effectiveness. Provide quantitative and quantitative results that demonstrate the performance of the system. The quantitative results include tables and graphs that show a comparison of your system's performance against standard metrics. Report on failure rates during the test; false acceptance rates (FAR) are determined. The qualitative results discuss the feedback received from users during performance testing.
- II. User evaluation: discuss how the system was evaluated from a user perspective, including feedback and opinions from users. Analyze the usability of the system and how well it meets the needs of users. Present data can be collected from user studies. It includes quotes from user interviews that highlight strengths and areas for improvement. Reports on specific usability metrics, such as registration completion time and success rate, are determined. This proposed system helps the user to memorize passwords better.
- III. Comparison with existing systems: compare the developed system with other GPA systems in terms of security, usability, and performance. Discuss the advantages and disadvantages of the developed system in comparison to existing systems. Assess the strength of the proposed system against traditional text-based and graphical-only systems in terms of susceptibility to various attacks like brute force, dictionary, or shoulder-surfing attacks. Compare system performance in terms of processing load and time-to-login. If your system performs slower than pure text-based systems, it explains why the increased security justifies the tradeoff.
- IV. Strengths and weaknesses: analyze the strengths and weaknesses of the developed system. Identify areas for improvement and suggest potential solutions to address these weaknesses. Highlight how the combination of graphical and text-based passwords increases password entropy and resists attacks better than traditional methods. The hybrid nature increases the overall password space, making it more resistant to brute-force attacks. The weakness includes Acknowledgement of any potential disadvantages of combining two authentication methods. Multi-device support or improvements explain how users enter GP on different platforms.
- V. Future directions: discuss potential future directions for the development of GPA systems. Consider emerging technologies and new methods for enhancing security and usability. Suggest adding a biometric layer to enhance security further. By combining biometrics with graphical-text authentication, we can further reduce the risk of impersonation or unauthorized access. It investigates how blockchain could be used to decentralize authentication data storage, improving security. It also suggests future systems where the password strength requirement dynamically adapts based on user behavior or the sensitivity of the action.

## 5 | Conclusion

In this system design, a new GPA technique is proposed and implemented. It aimed at enhancing security against shoulder-surfing attacks. The technique involves three key steps: user registration, user login, and the use of IB and CB password authentication. By incorporating these steps, the method increases the chances of resisting shoulder-surfing attacks through multi-factor authentication. This approach, with its focus on graphical and CB authentication, provides a resilient alternative to traditional password methods. The system also enhances security by increasing password complexity through the use of graphical elements while maintaining familiarity with traditional text-based passwords. The performance evaluation demonstrated that the system strikes a balance between usability and security, showing higher resistance to attacks such as brute force and shoulder-surfing compared to text-only or graphical-only systems.

In comparison with existing systems, our hybrid approach provides enhanced password entropy and security, though it introduces a modest increase in authentication time. This work serves as a foundation for more robust and user-friendly authentication systems, paving the way for more secure digital environments. In future research, further improvements could involve exploring the integration of BA methods to enhance security. Testing the effectiveness of the proposed technique across diverse devices and platforms would also help assess its real-world application. Additionally, evaluating user experience and usability, as well as the resilience of the system under more advanced cyber-attacks, would be valuable in refining the method for broader adoption in secure authentication systems.

## Funding

This study did not receive any dedicated funding from public, commercial, or non-profit organizations.

## Data Availability

The data and materials utilized in this research, including prototypes of the authentication scheme and testing results, can be obtained from the corresponding author upon a reasonable request. Access to user-specific login test data is limited due to privacy issues.

## Conflicts of Interest

The authors indicate that there are no conflicts of interest regarding this research. The study was carried out in an independent academic environment, free from any external influences.

## Reference

- [1] Zakaria, N. H., Griffiths, D., Brostoff, S., & Yan, J. (2011). Shoulder surfing defence for recall-based graphical passwords. *Soups 2011-proceedings of the 7th symposium on usable privacy and security*, 6, 1–12. <http://dx.doi.org/10.1145/2078827.2078835>
- [2] Bhand, A., Desale, V., Shirke, S., & Shirke, S. P. (2015). Enhancement of password authentication system using graphical images. *2015 international conference on information processing (ICIP)* (pp. 217–219). IEEE. <https://doi.org/10.1109/INFOP.2015.7489381>
- [3] Darbanian, E., & others. (2015). A graphical password against spyware and shoulder-surfing attacks. *2015 international symposium on computer science and software engineering (CSSE)* (pp. 1–6). IEEE. <https://doi.org/10.1109/CSICSSE.2015.7369239>
- [4] Gao, H., Ren, Z., Chang, X., Liu, X., & Aickelin, U. (2010). A new graphical password scheme resistant to shoulder-surfing. *2010 international conference on cyberworlds* (pp. 194–199). IEEE. <https://doi.org/10.1109/CW.2010.34>
- [5] Gokhale, M. A. S., & Waghmare, V. S. (2016). The shoulder surfing resistant graphical password authentication technique. *Procedia computer science*, 79, 490–498. <https://doi.org/10.1016/j.procs.2016.03.063>
- [6] 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. <https://doi.org/10.1145/2333112.2333114>
- [7] Irfan, K., Anas, A., Malik, S., & Amir, S. (2018). Text based graphical password system to obscure shoulder surfing. *2018 15th international bhurban conference on applied sciences and technology (IBCAST)* (pp. 422–426). IEEE. <https://doi.org/10.1109/IBCAST.2018.8312258>
- [8] Shammee, T., Mou, M., Chowdhury, F., & Ferdous, M. S. (2020). A Systematic literature review of graphical password schemes. *Journal of computing science and engineering*, 14, 163–185. <http://dx.doi.org/10.5626/JCSE.2020.14.4.163>
- [9] Sonkar, S., Paikrao, R., Kumar, A., & Deshmukh, M. S. (2014). Minimizing shoulder surfing attack using text and color based graphical password scheme. *International journal of engineering research and technology*, 3, 835–839. <https://B2n.ir/e98988>
- [10] Nandi, P., & Savant, P. (2022). Graphical password authentication system. *International Journal for Research in Applied Science & Engineering Technology (IJRASET)*, 10(5). <https://doi.org/10.22214/ijraset.2022.41621>