# A review of the recognition-based graphical password

Amanul Islam[1], Lip Yee Por[1], Fazidah Othman[1], Chin Soon Ku[2]

[1]University of Malaya, Kuala Lumpur 50603, Malaysia
[2]University of Tunku Abdul Rahman, Kampar 31900, Malaysia,

aman.um16@siswa.um.edu.my, porlip@um.edu.my, fazidah@um.edu.my, kucs@utar.edu.my

**Abstract:** This paper reviews the recognition-based graphical password system. Twenty-five recognition-based graphical password systems are studied and analyzed with regards to their security threats. Countermeasures and suggestions are given to prevent and reduce the security threats. A comparison summary of the selected recognition-based graphical password system is deliberated at the end of this paper.

**Keywords:** Graphical, Password, Authentication, Recognition, Method, System

## 1 Introduction

With accelerated the evolution of systems and applications, the urge for a potent computer security is growing [1].The majority of the computer systems and applications are preserved with user identification & authentication. However, many of them are having flaws due to an acquiescent and proficient user. Although, there are many ways to authenticate a person, the most commonly used means of authentication method is passwords.

Passwords always comply two fundamental contradicted requirements where they must be secure and easy to remember [2]. However, this is hard to achieve using alphanumeric passwords because a long and random password is secure but it is hard for the users to remember. Therefore, most of the users tend to use weak password [3]. Graphical password was then introduced as an alternative authentication method for alphanumeric passwords to overcome the memorability issue [3].

Back in 1996, Greg Blonder first explained the concept of graphical passwords [4]. Graphical password is easier to remember than alphanumeric password, which is an important advantage of it [4]. Graphical passwords utilize images in place of the alphanumeric passwords since humans are readily able to recognize images than a series of characters [5]. Human beings have the capability to recognize places they visit, other people's faces, and things [6]. Therefore, graphical password system paves a path by presenting a lot easier to use passwords whilst enhancing the security level [7]. Except for these improvements, the most acclaimed issue with graphical passwords is the shoulder-surfing attack [3]. Shoulder-surfing leads to employing direct observation methods, for instance, eyeballing over someone's shoulder, to obtain information [3]. Numerous researchers have endeavored to resolve this obstacle by giving distinct procedures. Hence, we started this research to find out the problem of algorithmic level of different recognition-based graphical password schemes how they implemented these schemes and why the problem of shoulder-surfing and other attacks arise in the field of recognition-based graphical passwords.

## 2 Methodology

This research begins with gathering information about existing recognition-based graphical password systems. The information is amassed from different sources, for example – journals, conference papers, and legitimate sites. The perceived systems are dissected to discover their qualities and inadequacies. Results from the investigation permit a prevalent perception of the present issues and troubles impacting existing graphical password systems. This information is used as a piece of the way toward making and specifying the research objectives.

## 3 Research Background

A graphical password system is a system that uses objects (images/icons/symbols) to perform authentication [8]. There are two main procedures in a graphical password system – enrolment procedure and authentication procedure. In the enrolment procedure, users are required to register certain objects from a database as their password [9]. In the authentication procedure, the users are given a challenge set to perform authentication. The users are required to identify the correct objects before they can access into a secure system.

Graphical password can be categorized into three categories – recognition-based, recall-based, and cued recall-based [10]. Recognition-based graphical password systems generally require users to register and memorize objects during enrolment procedure. The users are compelled to click the correct objects during the authentication procedure. The correct objects in each challenge set can be the registered objects, part of the registered objects or pass-objects that identify using certain methods. In recall-based graphical password systems, based on the registered objects, users are needed to remember and portray a covert drawing within a given grid or a blank canvas. On the other hand, cued recall-based graphical password systems needed users to remember and pinpoint target on specific locations within a picture.

In this paper, we only focus on the study of recognition-based graphical password systems because based on our reviewed, majority of the articles were found belongs to this category. The selected recognition-based graphical password systems are reviewed as below.

## 4 Recognition-Based Graphical Password Systems

Passfaces$^{TM}$ is a commercial product and it is one of the earliest recognition-based graphical password systems introduced by Passfaces$^{TM}$ Corporation [11]. During the enrolment procedure, users are required to register pictures of human faces. In the authentication procedure, the users are requested to click on the registered pictures to login. This system is simple and easy to use [12]. However, Passfaces$^{TM}$ is vulnerable to direct observation shoulder-surfing attack. Moreover, users who have prosopagnosia syndrome (face blindness) will find this system difficult to use.

In Déjà Vu system, users are needed to register several "random art" images during the enrolment procedure [1]. In the authentication procedure, the users are required to click on the registered images to login. This system is simple and easy to use. However, the direct selection of the pictures during authentication allows direct observation shoulder-surfing attack to be done successfully.

The Picture Password system, proposed by [13], is designed for mobile devices like the PDA. Users can either choose images from one of three predefined themes or provide their own images during enrolment procedure. In the authentication procedure, users are needed to click on the registered images to login. This system tries to increase the password space by allowing two images to be selected as one image. However, the direct selection of the pictures during authentication allows direct observation shoulder-surfing attack to be carried out.

Story system utilizes the same enrolment and authentication methods as in Passfaces$^{TM}$ system [14]. Despite using human faces images, this system uses non-human images. However, this system also suffer from direct observation shoulder-surfing attack.

In Triangle system, users are needed to register and remember three icons during the enrolment procedure [1]. In the authentication procedure, the users are required to form a polygon using the three registered icons virtually. The users need to click one of the icons (pass-icon) within the polygon area (convex hall) to complete a challenge set. The users are required to pass several challenge sets before they can login. This system uses other icons besides the registered icons to login. Thus, the system is able to resist direct observation shoulder-surfing attack.

In Moving Frame system [8], users are required to register and remember three icons during the enrolment procedure. In the authentication procedure, the users need to rotate the frame to ensure the two registered icons, which located within the frame, can form a straight line. The users are required to pass several challenge sets before they can login. This system does not required users to click on the registered icons. Therefore, it is able to resist direct observation shoulder-surfing attack. However, there are only four ways for the users to rotate the frame. Thus, chances for attackers to guess the correct rotation are quite high.

In Special Geometric Configuration (SGC) system [8], users are required to register four icons during the enrolment procedure. In the authentication procedure, users need to locate the registered icons. Then, the users need to use two of the registered icons to virtually form a line. The users need to click on the intersection icon that made by the two virtual lines to login. Similarly, this system does not required users to click on the registered icons. Therefore, the system is able to resist direct observation shoulder-surfing attack.

In Scalable Shoulder-Surfing Resistant Textual-Graphical Password (S3PAS) system [15], users are required to register at least three images during the enrolment procedure. In the authentication procedure, the users have to mentally construct a triangle using a group three characters, and then click on any character within the area of the virtual triangle formed. The process will be repeated for all possible groupings. For example, if a user's registered "L0V3", the possible groupings are, "L0V", "0V3", "V3L" and "3L0". Similar to the triangle system, this system is able to resistant direct observation shoulder-surfing attack because it does not use the registered images to login.

Visual Identification Protocol (VIP) version one and version two are two systems that predefined a set of registered images to the users instead of allowing the users to register themselves during the enrolment procedure [16]. In the authentication procedure, the users are required to identify the correct images in sequence before they can login. The difference between VIP1 and VIP2 is the arrangement of the pictures and the number of pictures used. VIP1 uses ten pictures and the arrangement of the picture is similar to the arrangement of keypad numbers in an ATM machine. On the other hand, VIP2 uses 3 x 4 grid cell interface to perform user authentication. These systems are simple and easy to use. However, the registered pictures chosen by the users can be shoulder-surfed easily as well. Therefore, both systems are vulnerable to direct observation shoulder-surfing attack. In the VIP version 3 [16], users are needed to register eight pictures during enrolment procedure. In the authentication procedure, only four of the registered pictures will be shown in a 4 x 4 grid cell. The rest of the grid cells are filled with decoy pictures. To login, the uses are required to click on the registered pictures in sequence. This system can reduce direct observation shoulder-surfing attack although the attackers can shoulder-surf the registered pictures clicked by the users every time they login. The main reason this system can reduce direct observation shoulder-surfing attack is because in every challenge set, only part of the registered pictures is shown. Therefore, it will take time and extra effort for the attackers to analyze the correct registered pictures used by the users.

Use Your Illusion system utilizes the same enrolment and authentication methods as in Passfaces$^{TM}$ system [17]. Despite using human faces images, this system uses distorted images. Although the distorted pictures are hard to be seen clearly but attackers can still shoulder-surf the clicked pictures. Thus, this system is vulnerable to direct observation shoulder-surfing attack. Moreover, this system suffers from a small password space.

In ColorLogin system [18], users are needed to choose a color and a set of icons in the enrolment procedure. The users can use the registered color as background to help them find their registered icons. In the authentication procedure, users are required to click on the rows that contain the registered icons in an N x N grid cell. Once clicked; the entire row will be locked. All the affected icons will change to a "lock" icon. To complete a challenge set, the users have to ensure all the registered icons are locked. The users have to perform several challenge sets in order to login. ColorLogin system is able to reduce direct observation shoulder-surfing attacks because the registered icons are not chosen directly during the login process. However, attackers can still shoulder-surf the row that clicked by the users. Moreover, this system is vulnerable to guessing attacks due to small password space.

Graphical Password with Icons (GPI) and Graphical Password with Icons suggested by the System (GPIS) are proposed by [19]. In GPIS, users are required to register six icons during the enrolment procedure. In GPIS, the six icons are assigned to the users during the enrolment procedure. In the authentication procedure, both systems required the users to identify and click on the registered/assigned icons among 150 icons to login. Therefore, both systems are vulnerable to direct observation shoulder-surfing attack because the registered/assigned icons chosen by the users can be easily shoulder-surfed.

There are two variations of What You See is What You Enter (WYSWYE) system [20]. In both variations, users are required to register four images during the enrolment procedure. For the first variation, called the Horizontal Reduce Scheme (HRS), users are presented with a 7x4 grid during the authentication procedure. The users have to find the columns and mentally eliminate columns that do not have their registered images. The result will be an Nx4 grid with the maximum size being a 4x4 grid. The users then need to key in the corresponding position of the registered images in the password input grid. The second variation, called the Dual Reduce Scheme (DRS), users are presented with a 5x5 grid. The users have to eliminate a row and a column that does not have their registered images. The result will be an M x N grid, again with the maximum size being a 4x4 grid. Similar to the first variation, users are required to key in the position of the registered images in the password input grid. WYSWYE-HRS and WYSWYE-DRS are able to reduce direct observation shoulder-surfing attack because the registered images are not selected during the authentication processes. However, attackers can still shoulder-surf the value of keyed in by the users and map with the position of the registered images.

In Por's system [21], users are required to register eight images in the enrolment procedure. In the authentication procedure, the users are required to click four or five registered images to login. Similar to VIP3, this system can reduce direct observation shoulder-surfing attack because only part of the registered images is used for every challenge set.

In Manjunath's system [22], users are required to register a string (8 to 15 characters) and choose one color (eight colors are given) during the enrolment procedure. In the authentication procedure, eight color sectors are shown and each sector is filled with eight random characters. To login, the users are required to move the registered color sector to the registered characters. This system can prevent direct observation shoulder-surfing attack because the registered string and color are not directly used.

In Haque's scheme [23], users are required to register their username and at least several image during the enrolment procedure. After that, a set of questions will be given to the users. The users need to pair each question with three registered images. In the authentication procedure, the users are required to recognize the correct images based on the question asked. This system is easy and simple to use. However, this system cannot prevent direct observation shoulder-surfing attack because the direct selection of the registered images during an authentication process can be easily observed and shoulder-surfed.

In Pooja system [24], users are required to register several images during enrolment procedure. During the authentication procedure, the users are required to identify the registered images from the 4 x 4 grid cell. This system is simple and easy to use. However, this system is vulnerable to direct observation shoulder-surfing attack because the direct selection of the registered images during an authentication process can be easily observed and shoulder-surfed.

In CuedR system [25], users are required to register six animal images during the enrolment procedure. In the authentication procedure, the users are required to key in the character associated with the registered images in sequence. This system is vulnerable to direct observation shoulder-surfing attack because attackers can decompose the password string then associated each character with the unique animal image in a challenge set.

In Digraph Substitution Rules (DSR) system [3], users are needed to register a username and register two images in the enrolment procedure. In the authentication procedure, users need to click on a pass-image based on the registered images and the three digraph substitution rules. The users have to complete several challenge sets before they can login. This system can prevent direct observation shoulder-surfing attack because the users will never click on the registered images.

In WordPassTile system [26], users are required to register five Tiles (a unique word) in the enrolment procedure. In the authentication procedure, users are required to click on the Tiles provided in a specific sequence. This system is vulnerable to direct observation shoulder-surfing attack because the direct selection of the Tiles during an authentication process can be easily observed and shoulder-surfed.

In Graphical-Text Password Authentication (GTPA) system [27], users are required to register four images in the enrolment procedure. In the authentication procedure, the users have to click on the first pass-image within a 10 x 10 grid cell based on the pair of numbers associated with the first registered image. After clicking, the images and the pair of numbers will be re-shuffled using uniform randomization algorithm. The user then has identified the second pass-image based on the pair of numbers associated with the second registered image. The same process keeps repeating until the users click on the fourth pass-image before the user can login. This system can prevent direct observation shoulder-surfing attack because the images clicked by the users could be the registered image or the decoy image.

## 5 Common attacks in recognition-based graphical password system

The following are the common security threats for recognition-based graphical password systems: -

Guessing attack – It is the process of getting the password of a user by predicting or resolving the password [1, 28]. Most of the recognition-based graphical password systems, which have small password space usually, will encounter such security threat. There are several ways to overcome such attack. For example, increase the password space, use partial registered objects (images/icons/symbols) or pass-objects (pass-images/pass-icons/pass-symbols) to login.

Direct observation attack – It is a type of shoulder-surfing attack for example eyeballing over someone's shoulder to obtain information [3]. Most of the recognition-based graphical password systems, which uses direct registered objects, will encounter such security threat. To overcome or reduce this attack, indirect objects for example pass-objects can be used to login.

Frequency of Occurrence Analysis (FOA) attack – It only happens in recognition-based systems that use uniform randomization algorithm to perform selection [21]. Due to the fact that the sampling size of the registered objects is relatively smaller than the decoy objects sampling size, when uniform randomization algorithm is used, the probability the registered objects will always appear in a challenge set while the same distracter image will only appear occasionally in every challenge set [21]. To overcome or reduce this attack, an authentication system can use fix objects or prevent using large amount of decoy objects in every challenge set.

## 6 Result and Discussion

**Table 1.**Recognition-based graphical password and its security threats

| Graphical Password Schemes | Direct observation attack | FOA | Guessing attack |
|---|---|---|---|
| Passfaces$^{TM}$ | ✗ | ✗ | ✗ |
| Déjà Vu | ✗ | ✗ | ✗ |
| Picture Password system | ✗ | ✗ | ✗ |
| Story | ✗ | ✗ | ✗ |
| Triangle system | ✓ | N/A | ✓ |
| Moving Frame system | ✓ | N/A | ✗ |
| SGC | ✓ | N/A | ✓ |
| S3PAS | ✓ | N/A | ✓ |
| VIP1 | ✗ | N/A | ✗ |
| VIP2 | ✗ | N/A | ✗ |
| VIP3 | can reduce | ✗ | ✓ |
| Use your illusion | ✗ | ✗ | ✗ |
| ColorLogin | ✓ | ✗ | ✗ |
| GPI | ✗ | N/A | ✓ |
| GIPS | ✗ | N/A | ✓ |
| WYSWYE-HRS | can reduce | N/A | ✓ |
| WYSWYE-DRS | can reduce | N/A | ✓ |
| Por's system | can reduce | can reduce | ✓ |
| Manjunath's system | ✓ | N/A | ✓ |
| Haque's system | ✗ | N/A | ✓ |
| Pooja's system | ✗ | ✓ | ✓ |
| CuedR | ✗ | N/A | ✓ |
| DSR | ✓ | ✓ | ✓ |
| WordPassTile | ✗ | ✓ | ✓ |
| GTPA | ✓ | ✓ | ✓ |

Note: ✗ = vulnerable to the attack
✓ = invulnerable to the attack

N/A=not applicable

Table 1 shows the comparison table among the reviewed system. From the table, majority of the reviewed systems are vulnerable to direct observation shoulder-surfing attack. Only systems that used partial objects to login can reduce such attack. For example VIP3, WYSWYE-HRS, WYSWYE-DRS, and Por's system. Systems that use indirect input or pass-objects instead of the registered objects to login can prevent this attack. Examples of these systems are – Triangle system, Moving Frame system, SGC, S3PAS, ColorLogin, Manjunath's system, DSR, and GTPA.

In terms of FOA attack, there are only few systems get affected because these systems used uniform randomization to perform selection. For example Passfaces$^{TM}$, Déjà Vu, Picture Password system, Story, Photographic authentication, VIP3, Use your illusion and ColorLogin. There are few systems are able to resist such attack because they used fix number of objects every time to login. Examples of these systems are – Pooja's system, DSR, WordPassTile and GTPA. Other systems are not relevant because they are not using uniform randomization to perform selection.

In terms of FOA attack, there are only few systems get affected because these systems have small password spaces. Example of these systems are – Passfaces$^{TM}$, Déjà Vu, Picture Password system, Story, Moving Frame system, VIP1, VIP2, Use your illusion and ColorLogin.

## 7 Conclusion

In this study, several specific security threats such as guessing attack, direct observation and FOA that encountered by recognition-based graphical password system were highlighted. The countermeasures for each of the security threat were discussed. We believed this study could help the researchers who would like to do research on graphical password especially on recognition-based graphical password. In future, besides security aspects, we will focus on usability aspects research such as user login time and methods that can help users to recall their passwords.

## Acknowledgement

This project was supported by the Postgraduate Re-search Grant (PPP) - PG005-2015B from the University of Malaya and also Fundamental Research Grant Scheme (FRGS) - FP071-2015A from the Ministry of Higher Education, Malaysia.

## References

1. Por L. Y. and Lim X. T.: Issues, threats and future trend for GSP. in Proceedings of The 7th WSEAS International Conference on Applied Computer & Applied Computational Science, Hangzhou, China, 627–633 (2008)

2. Ho, P. F., Kam, Y. H. S., Wee, M. C., Chong, Y. N., Por, L. Y.: Preventing Shoulder-Surfing Attack with the Concept of Concealing the Password Objects' Information. The Scientific World Journal, (2014)
3. Por, L.Y., Ku, C.S., Islam, A., Ang, T.F.: Graphical password: Prevent shoulder-surfing at-tack using digraph substitution rules. The Frontiers of Computer Science, Accepted (2016)
4. Blonder, G. E.: ``Graphical Passwords", United States Patent 5559961, Lucent Technologies, Inc. (Murray Hill, NJ), (1996)
5. Biddle, R., Chiasson, S., Van Oorschot, P. C.: Graphical passwords: Learning from the first twelve years. ACM Computing Surveys (CSUR), 44(4), 19 (2012)
6. Por, L. Y., Wong, K., Chee, K. O. : UniSpaCh: a text-based data hiding method using Unicode space characters. Journal of Systems and Software, 85(5), 1075–1082 (2012)
7. Por, L. Y., Delina, B.:Information hiding a new approach in text steganography. In Proceedings of the 7th WSEAS International Conference on Applied Computer and Applied Computational Science, 2008, 689–695.
8. Por, L. Y., Delina, B., Ang, T. F., Ong, S. Y.: An enchanced mechanism for image steganog-raphy using sequential colour cycle algorithm. The International Arab Journal of Information Technology, 10(1), 51–60 (2013)
9. Por L. Y., Lai W. K., Alireza Z., Delina B.: StegCure: an amalgamation of different steganographic methods in GIF image. In Proceedings of the 12th WSEAS International Conference on Computers, Heraklion, Greece, 420–425 (2008)
10. De-Angeli, A., Coventry, L., Johnson, G., and Renaud, K.: Is a picture really worth a thou-sand words? Exploring the feasibility of graphical authentication systems. International Journal of Human-Computer Studies, 63, 128-152 (2005)
11. Passfaces$^{TM}$: The Science behind Passfaces, White paper. http://www.passfaces.com/enterprise/resources/white_papers.htm. Accessed 10 July 2017 (2000)
12. Brostoff, S., Sasse, M. A.: Are Passfaces more usable than passwords: a field trial investigation. In People and Computers XIV—Usability or Else! , 405-424: Springer London (2000)
13. Jansen, W., Gavrila, S., Korolev, V., Ayers, R., Swanstrom, R.: Picture password A visual login technique for mobile devices. (2003)
14. Davis, D., Monrose, F., Reiter, M. K.: On user choice in graphical password schemes. In USENIX Security Symposium, 13, 1-14 (2004)
15. Zhao, H., Li, X.: S3PAS: A Scalable Shoulder-Surfing Resistant Textual-Graphical Password Authentication Scheme. Proceedings of the International Conference on Advanced In-formation Networking and Applications Workshops, 2, 467-472 (2007)
16. De-Angeli A., Coutts M., Coventry L., Johnson G.: VIP: A Visual Approach to User Authentication. Proceedings of the Working Conference on Advance Visual Interfaces, 316-323 (2002)

17. Hayashi, E., Dhamija, R., Christin, N., Perrig, A.: Use Your Illusion: secure authentication usable anywhere. Proceedings of the 4th Symposium on Usable Privacy and Security, 35-45 (2008)
18. Gao, H., Liu, X., Wang, S., Liu, H., Dai, R.: Design and Analysis of a Graphical Pass-word Scheme. The 4th International Conference on Innovative Computing, Information and Control, 675-678 (2009)
19. Khot, R. A., Kumaraguru, P., Srinathan, K.: WYSWYE: shoulder surfing defense for recognition based graphical passwords. Paper presented at the Proceedings of the 24th Australian Computer-Human Interaction Conference, Melbourne, Australia (2012).
20. Perkovic, T., Cagalj, M., Rakic, N.: SSSL: Shoulder Surfing Safe Login. 17th International Conference on Software, Telecommunications & Computer Networks, 2009. SoftCOM (2009)
21. Por, L.Y.: Frequency of occurrence analysis attack and its countermeasure. The International Arab Journal of Information Technology, 10(2), 189-197 (2013)
22. Manjunath, G., Satheesh, K., Saranyadevi, C., Nithya, M.: Text-based shoulder-surfing resistant graphical password scheme. International Journal of Computer Science and Information Technologies, 5(2), 2277-2280 (2014)
23. Haque, M.A., Imam, B.: A New Graphical Password: Combination of Recall & Recognition Based Approach. World Academy of Science, Engineering and Technology, International Journal of Computer, Electrical, Automation, Control and Information Engineering, 8(2), 320-324 (2014)
24. Pooja K. S., Prajna V. D., Prathvi, Ashwini N.: Shoulder Surfing Resistance Using Graphical Password Authentication in ATM Systems. International Journal of Information Technology & Management Information System (IJITMIS), 6(1), 1-10 (2015)
25. Al-Ameen M. N., Wright M., and Scielzo S.: Towards making random passwords mem-orable: leveraging users' cognitive ability through multiple cues. CHI `15 Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems, pp.2315-2324 (2015)
26. Assal, H., Imran, A., Chiasson, S.: An Exploration of Graphical Password Authentication for Children. https://arxiv.org/abs/1610.09743. Accessed Date: 16 June 2017 (2016)
27. Agrawal, S., Ansari, A. Z., Umar, M. S.: Multimedia graphical grid based text password authentication: For advanced users, 2016 Thirteenth International Conference on Wireless and Optical Communications Networks (WOCN), 1-5 (2016)
28. Por L. Y., Kiah M. L. M.: Shoulder surfing resistance using penup event and neighbouring connectivity manipulation. Malaysian Journal of Computer Science, 23(2), 121–140 (2010)