Text and Image: A new hybrid authentication Scheme

Noor Afiza Mohd Ariffin¹, Akram Abduljabbar Abdulhalem¹, Nor Azura Husin¹

¹Faculty of Computer Science and Information Technology, University of Putra Malaysia, 43400 UPM Serdang, Selangor, Malaysia.

Abstract. Nowadays authentication considered the most vital field in term of security aspects because it represents the first line of defense in total process of our assets protection. In order to get access to any data especially when they are private, authentication is required as the first step of protecting accessing our assets. Therefore, many techniques been invented to create appropriate authentication process, for example the traditional textual password technique, the graphical passwords techniques and biometrics techniques. These techniques involved a sequence of procedures all aim to three things (confidentiality against attackers, acceleration of access time, simplification of the created technique). However, the rapid growth of threats for example the shoulder surfing attacks led to invent many techniques concentrated only on the confidentiality aspect and neglected other important aspects like easiness of utilization, as a result; these techniques suffered distinctly the issue of complexity. Many techniques been proposed in order to eliminate the complexity problem without losing their confidentiality purpose, however; most of them did not succeeded. For that reason, this research present a new hybrid technique that combines the maintenance of confidentiality against shoulder surfing attacks and the simplification of utilization at the same time, our technique consist of two simple techniques but effective to solve complexity issue with maintaining the confidentiality aspect, these two techniques are the traditional textual password and the graphical password.

Keywords:— graphical password, textual password, hybrid authentication, security

1. Introduction
One of the most famous types of authentication is using password. Passwords alongside previous years witnessed many developments phases, starting with simple textual password, graphical image passwords and ending with using biometrics devices to authenticate legitimate users. However, Graphical image passwords considered in recent years the most desired technique for most people due to the easiness to remember and the enjoyable experience the users can witness during performing authentication process. Graphical password can be defined as a technique of verification of an identity by using images as a password instead of traditional textual. This technique been considered as an alternative technique of the textual based in order to solve the problem of memorability, and since it uses pictures as a verification of an identity, it offers great flexibility of in term of memorability comparing to ordinary text. A textual password defined as a verification of an identity of legislated user by using simple alphanumeric characters, numbers, letter and symbols, it can be created in simple way or via using special techniques and graphical password is one of them [1].

Even when graphical passwords showed many advantages that covered some disadvantages of the text-based password, but it also revealed of issues related to certain attacks like shoulder surfing attacks and some other disadvantages related to space specified for the applications that perform such
technique. Shoulder surfing attacks defined as an ability of an attacker to observe password by his/her naked eyes from a short distance, the attacker performs his/her attack without the knowledge of the victim, and usually this attack performed during the time when the victim utilizes his of logging in process or registration process [1]. Even though, with developments applied on the graphical image passwords techniques in attempt to enhance confidentiality, there was a raise of complexity occurred on these techniques; as a result, this led to make users to reconsider of utilizing graphical image passwords technique frequently.

Scarce techniques been suggested in order to eliminate the complexity problem without losing their confidentiality purpose, however; most of them did not succeed. For that reason, we present our new hybrid technique “text and image: a new hybrid authentication scheme” that combines the maintenance of confidentiality against shoulder surfing attacks and the simplicity of utilization at the same time. Our technique consists of two simple techniques but effective to solve complexity issue with maintaining the confidentiality aspect, these two techniques are the traditional textual password and the graphical image password.

Here are some major differences between textual-based and graphical-based passwords.

| Graphical – based passwords | Textual – based password |
|-----------------------------|--------------------------|
| A group of images, shapes or pictures selected by the user to verify user identity or gain access. | A group of letters, alphanumeric characters or numbers typed by the user to verify user identity or gain access. |
| Easy to remember | Hard to remember |
| Hard to guess | Easy to guess |
| Less common | Most common |
| Vulnerability to attacks like shoulder surfing | Vulnerable to attacks like dictionary attacks, brute force attacks and spywares |
| More human friendly since it contains images | Less human friendly since it contains chars and symbols |
| Higher security | Less security |
| Registration and log in take long time | Registration and log in take short time |
| Requires more storage space because of the images | Requires less storage space because it is only uses chars, symbols and numbers |

The remaining of the paper is organized as follows. We first summaries related work in Section 2 and we introduce our methodology applied in this research in Section 3. In Section 4, some experiments are discussed and section 5 the results are presented to show the performance of proposed scheme in term of mean time. Finally, presents the conclusions of the research work carried out and points out several of recommendations for future works for exploration and open problems that have been discovered throughout the tenure of this research.

2. Literature Review
[2] defined the authentication, as the ability to make an identity that belongs to an entity is valid. The authentication usually take the form of credentials, such as passwords or certificates that used as evidences to verify certain identities. Authentication aims to make sure that an entity is who they claim to be. One of the earlier forms of authentication is using passwords and during decades, these passwords were a subject of many types of attacks some of these attacks occurred directly via extracting password information from the victim him/herself by sharing it with neglecting or via using tools and techniques all aim to reveal the password. [2] defined password as a form of secret authentication data that is used to control access to a resource, these resources represented as ATM machines, personal computers, servers and phone mobiles. Passwords are not for accessing purposes only, but also to retrieve accounts like email from servers, accessing files, and even reading the morning newspaper online. This research categorized password into two types, textual and graphical passwords.
A- Textual Password
It represents the common and most used technique in authentication process; it involves using characters, digits, numbers, alphanumeric characters and symbols. Although the wide utilization of this category, it still holds vulnerabilities in confidentiality and usability aspects; therefore, new technique been suggested end of the 20th century the graphical password to replace traditional textual password.

B- Graphical Password
The motivation behind the idea of using graphical passwords is to find an alternative technique to the textual that easy to remember, less to lose and more secure.

[10] Defined graphical password as a technique of verification of a certain identity by using images as a password instead of traditional textual that use characters. This technique been considered as an alternative technique of the textual based password in order to solve the problem of memorability, and since it uses pictures as a verification of an identity , it offers great flexibility in term of memorability comparing to ordinary text passwords. A textual password defined as a verification of an identity of legislated user by using simple alphanumeric characters, numbers, letter and symbols, it can created in simple way or via using special techniques and the graphical password is one of these techniques. Even when graphical password showed many advantages that covered some disadvantages of the text-based password, but it also revealed of issues related to certain attacks like shoulder surfing attacks and some other disadvantages related to space specified for the applications that perform such technique. Shoulder surfing attacks defined as an ability of an attacker to observe password by his/ her naked eyes from a short distance, the attacker performs his/her attack without the knowledge of the victim, and usually this attack performed during the time when the victim utilizes his of logging in process or registration process.

This research [14] suggested using new textual based technique named it as “A Stroke-based Textual Password Authentication Scheme”. The suggested technique based on the idea of developing textual based passwords via using key strokes instead of using graphical images as an alternative technique, the reason of his choice due to his opinion that both textual and graphical passwords techniques are vulnerable to shoulder surfing attacks. Thus, using graphical password with images will not solve the problem and instead of that he preferred to continue using textual based password but with the enhancements in technique.

From research [3] has suggested an authentication technique that used for banking application, ATM services and other such application where user can interact with private data controlled by means of password authentication. The suggested scheme named as (3LAS Three Level Authentication Scheme). The 3LAS technique involved 3 levels of authentication, Level 1 Random Character in Grid, Level 2 Random Character in Grid with Session password. Level 3 Random Character in Grid with Session password and grid variations. Although Level 1 showed us resistance to shoulder surfing attack, it also has a vulnerability represented by the ability of the attacker to take snapshots of the key logger, which in return could help him to recognize the password. Once the attacker obtain multiple snapshots from many log in sessions, he/she will be able to identify the password when perform a comparison among these snapshots which eventually leads to compromise the technique itself specification was to prevent the attacker from realizing what character dedicated to each image unless watches login several times.

[8] Proposed a technique used for smart hand held devices (smart phones i.e. PDAs, iPod, iPhone, etc). This technique based on the idea of combination of recognition and pure recall based techniques. This scheme suggested as a new method to resist shoulder surfing attacks represents the
major threat of using graphical password authentication techniques. But in this research, there have some limitation seems that graphical passwords are often predictable, a serious problem typically associated with text based passwords. Encryption and transferring over the internet are two vital issues that remain un-discussed among all the works we encountered.

According to [5] has proposed a version of PassPoints by tapping on the correct sequence of click-points. Users may define settings such as the size of the tolerance regions, and which image is displayed. But this research have some disadvantage which is the process is too long and may take a lot of time and Users cannot click where they wants because of predetermined tap regions.

In 2015, [6] has proposed a scheme that combines Captcha and graphical password. For example, suppose the password is “Mango”. During sign in user see the Captcha challenge. The m, a, n, g, o are at different locations and there are different alphabets too. User clicks on the locations of the m, a, n, g, o in correct sequence. But this research have some limitation such as, it is nonresistant to shoulder-surfing attack.

Research from [11] suggested in his article “Graphical password: prevent shoulder-surfing attack using digraph substitution rules”, the scheme based on the idea of using the digraph substitution rules in order to secure and hide the process of password-images creation. The user demanded to click on only one pass image instead of clicking both pass images within a challenge set or three consecutive sets. The whole idea of this technique based on locating the correct password images in indirect way while they distributed within the grid of images. Disadvantages of this research are the password will be exposed to anyone with access to the database storing the users’ credentials.

Research from [7] also proposed a hybrid password scheme based on shape and text. The proposed scheme uses shapes of strokes as origin passwords and allows users to login with text passwords via traditional input devices. Although the researchers claim that the scheme is resistant to shoulder surfing, hidden camera and brute force attacks and that it has variants to strengthens the security level through changing login interface of the system, the scheme still has some security and usability drawbacks. It is not familiar to users so they may adopt simple and weak strokes. This increases the chance of attackers to obtain the passwords. Also, the password creating step is vulnerable to attacks since users have to tell the system the original shapes and strokes. Moreover, the login process of this scheme is longer than other graphical schemes. For these reasons, more advanced authentication system should be proposed to improve this method.

In a recent study, a comprehensive survey on shoulder surfing resistant text based graphical password schemes is conducted [12]. This study explained the existing security problems, possible solutions and limitations of some of these schemes. These studies primarily focused on the existing shoulder surfing attacks in text based graphical password approach. However, a guessing attack is also a potential problem for graphical password schemes because of the predictability of user-chosen graphical passwords [14].

3. Research Methodology

The research is conducted with a methodology which consists of 3 steps as shown in Figure 1, and the descriptions are as the following.
**Step 1: User registration and execution of the proposed scheme**

In Registration phase, user is required to enter his private information that make him able to open a unique account within the application, the information represents user name, textual password and graphical image password; for this reason, there are two mini phases involved in this stage, the Registration of textual password and the Registration of image password. Both mini phases share the same Registration interface. The whole Registration process performed just once and for one user only for confidentiality purposes.

Upon successful registration, user is required to re-enter his private information that elected in the Registration Phase, the use should recall information within his/her mind and type them in the correct way. On the other hand, recalling the Pass Images performed not by clicking them with mouse, but to use them within the mind via observation to indicate the Prime Images within the new distributed grid. This phase also divided into two sub phases, the Login of the textual password and the Login of the graphical image password. Finally, each sub phase considered as a gate to other phase, for instance, if the user finish the Login of the textual password, then he/she will move to the next sub phase which is Login of the graphical image password, and once the user finish both sub phases then the accessing process will complete. The mean time for successful login attempts will be recorded to measure the effectiveness of the scheme.

**Step 2: Analysing the result**

After all users have tested the proposed scheme, all the mean time for successful login statistics from the users will be analysed. The measured time will be in seconds. Measured mean time will be the accumulative time from when user inputs in their details, the scheme interacts with the database and finally until the result is shown. Detail layout in graph form will be presented to show a more linear pattern for execution time representing statistics from all the users.

To calculate the numbers in the table above, we followed these equations:

- \( \text{Average} = \frac{\text{maximum} + \text{minimum}}{2} \)
- \( \text{Standard Deviation} = \)
- \( \text{Median} = \frac{\text{maximum} + \text{minimum}}{2} \)

**Step 3: Comparative Analysis**

In this step, the obtained result for step 2 will be compared with previous published researches. This comparison is done manually.
4. **Evaluation of Efficiency of Proposed Scheme**

A user study was conducted to test the effectiveness of the proposed method in reducing shoulder-surfing attacks. The 15 participants in order to test our new hybrid authentication scheme and comparing it with previous research, Lip Yee POR scheme. All the participants need to choose among four ways which is identify the location of image on the grid, guessing, direct observation and identify based on the algorithm in proposed method to identify the both our textual based password and our Prime image password each in its phase. Participants were asked to spend a maximum of 15 minutes in the user study. First they were taught the concept of the system and the steps that they should use in order to login. The participants first underwent a tutorial before creating their password and logging into the system.

In the registration phase, the participants were required to select two images which called “pass-image” from a group of images all contained within a grid, these two images represents the clue images used identify the real prime images during the log in phase. The participants now has to specify the order of the two images been selected in the previous step, which one will represent “pass-image 1” and which one will represents “pass-image 2”. After selecting the order, the participants has to click on submit button to store all the information related to user name and the pass-image in the system file. In login phase, the participants now have to recognize the two pass-images been selected in the registration phase via using proposed algorithm of three cases. The participants have the freedom to identify the first or the second pass image as a start.

After the participants had completed ten successful logins, they were instructed to watch a demonstration of a login session to perform shoulder-surfing test. The resources available to them as the attackers are the images shown in the challenge set and the images clicked by the authorized user during login. Then, they were given three attempts to guess the password pictures used for the login session in the demonstration. Each of the participants was tested separately.

5. **Result and Discussion**

We were able to test our scheme on 15 participants from different ages. First, we tried to ask the participants about their background knowledge of Graphical password and Shoulder surfing attack. Related to the term “Graphical password”, only two persons were able to recognize this term from total 15 and that means they form 13.3333% only, while the other 13 participants who never heard about this term form 86.6667% from total participants. Related to the term of “Shoulder Surfing Attack”, also only two persons were able to recognize the term and they form 13.3333% of total participants while the rest 13 form 86.6667% from total 15 participants.

Figure 2 shows the mean time of ten successful logins. The chart shows that the time taken for participants to login decreases significantly over the ten login attempts. This indicates that as the participants become more familiar with the system, the time for login becomes shorter.
Table 1 shows the minimum, maximum, average, standard deviation and median for all successful login attempts. The minimum time taken for a successful login by the participants is 4.0 seconds, while the maximum time taken is 27.0 seconds. The average time taken by the participants for a successful login is 10.9 seconds with a standard deviation of 5.9 seconds. The median for all the successful login attempts is 7.25 seconds. This shows that 50% of the login attempts require less than 6.25 seconds to login. After the participants has completed ten successful logins, they were instructed to watch a demonstration of a login session. The participants could watch the demonstration of the login session as many times as they wanted. Then they were given three attempts to figure out the password pictures used for the login session in the demonstration. The shoulder-surfing test resulted in none of the participants being able to identify the password images used in the demonstration session. One would suspect that if the adversary would have the advantage if he/she knew the algorithm used. However, the results of the shoulder-surfing test in the user study suggest that the proposed system is resistant to shoulder-surfing attacks (both traditional and video recorded shoulder-surfing attacks), despite the fact that the attackers knew about the proposed system and the underlying algorithm.
Figure 3 shows the strategies used by the participants and the percentage of the participants who used them. 17.2% of the participants did not manage to figure out the pass-images used although they knew how the underlying proposed algorithm works, while 71.3% of the participants used direct observation and clicked according to the images used in the demonstration. 7.4% of the participants simply guessed the pass-images and the remaining 7.4% of them used simple and commonsense shoulder-surfing strategies such as identifying the location of the selected images on the grid based on the demonstration.

Figure 3: Strategies used

6. Conclusion
We proposed our research to overcome the efficiency issue and lack of defensive mechanism against multi attempts and frequent attacking cases. Our research is provide the user security defensive mechanism allow this user to recognize whether there was an attempt to unauthorized access, this mechanism represented with ability to lock the system for a period of time that allows the user to discover that his system was under attack. Our research also provided with easy usage, as proved in numbers of tests where the users became faster in their attempts to access the system especially at the beginning; this thing can provide more security and reduce time available to the attacker to perform shouldsurfing.

Although our research shows weaknesses related to shoulder surfing attack against textual password, the existing of the other graphical password as the next stage authentication is more than enough to prevent the an authorized accessing, and vice versa, even if the attackers succeeded to know the two PassImages, he has to know the textual password pattern. Furthermore, textual password still is the most desired technique to most people and using only graphical passwords as a security technique it will not encourage the user to use or trust this kind of protection, therefore; using the hybrid technique can encourage the user to accept the graphical password as a replacement to textual password in the near future.
References

[1] Abdul Rahim M and Anandhavalli D, “Implementation of image based authentication to ensure the security of mail server,” in 2014 IEEE International Conference on Advanced Communications, Control and Computing Technologies, 2014.

[2] Anitha, M., & Mahalakshmi, B. Graphical Password Authentication Using for Multistage Image Recognition Captcha. in 2015 International Journal of Computer Science and Engineering Communications, 2015.

[3] V. Ravi and Dayananda Sagar University, “Integration of image and video signature in graphical password authentication system,” Int. J. Eng. Res. Technol. (Ahmedabad), vol. V9, no. 05, 2020.

[4] H. Shirazi, B. Bezwada, I. Ray, and C. Anderson, “Adversarial sampling attacks against phishing detection,” in Data and Applications Security and Privacy XXXIII, Cham: Springer International Publishing, 2019, pp. 83–101.

[5] R. Biddle, S. Chiasson, and P. C. Van Oorschot, “Graphical passwords: Learning from the first twelve years,” ACM Comput. Surv., vol. 44, no. 4, pp. 1–41, 2012.

[6] E. Darbanian and G. Dastghaiby fard, “A graphical password against spyware and shoulder-surfing attacks,” in 2015 International Symposium on Computer Science and Software Engineering (CSSE), 2015.

[7] H. Gao, Z. Ren, X. Chang, X. Liu, and U. Aickelin, “A new graphical password scheme resistant to shoulder-surfing,” arXiv [cs.CR], 2013.

[8] Haque, A., & Imam, B. A New Graphical Password: Combination of Recall & Recognition Based Approach. International Journal of Computer, Electrical, Automation, Control and Information Engineering, 2014.

[9] Mulwani, K., Naik, S., Gurnani, N., Giri, N., & Sengupta, S. 3LAS (three level authentication scheme). International Journal of Emerging Technology and Advanced Engineering, 2013

[10] L. Y. Por, C. S. Ku, A. Islam, and T. F. Ang, “Graphical password: prevent shoulder-surfing attack using digraph substitution rules,” Front. Comput. Sci., vol. 11, no. 6, pp. 1098–1108, 2017.

[11] S. Saeed and M. S. Umar, “PassNeighbor: A shoulder surfing resistant scheme,” in 2016 2nd International Conference on Next Generation Computing Technologies (NGCT), 2016.

[12] H. Umar Suru and P. Murano, “Security and user interface usability of graphical authentication systems – A review,” Int. j. comput. trends technol., vol. 67, no. 2, pp. 17–36, 2019.

[13] Towhidi, F., & Masrom, M. A survey on recognition based graphical user authentication algorithms in 2009 International Journal of Computer Science and Information Security, 2009.

[14] Z. Zheng, X. Liu, L. Yin, and Z. Liu, “A stroke-based textual password authentication scheme,” in 2009 First International Workshop on Education Technology and Computer Science, 2009.