Websites:
http://www.sciencepub.net
http://www.sciencepub.net/researcher

Emails:
editor@sciencepub.net
marslandresearcher@gmail.com

Researcher

MARSLAND PRESS
Multidisciplinary Academic Journal Publisher

Evaluation of Recognition-Based Graphical Password Schemes in Terms of Usability and Security Attributes

Touraj Khodadadi[1], A.K.M. Muzahidul Islam[2], Shozo Komaki[3], Sabariah Baharun[4]

[1234]Malaysia-Japan International Institute of Technology (MJIIT) Universiti Teknologi Malaysia, Jalan Semarak, Kuala Lumpur, Malaysia.
E-mail: ktouraj2@live.utm.my[1], mmmislam@ic.utm.my[2], pkomaki@ic.utm.my[3] ssabariah@ic.utm.my[4]

Abstract: User Authentication is a critical component in information security. Several widely used mechanisms for security to protect services from illegal access include passwords and alphanumerical usernames. However, there are several drawbacks attached to this method. For instance, the users themselves normally use passwords that are easy to guess. Their reasoning for this is that difficult passwords would be difficult to recall as well. A new alternative is the graphic-based password and there has been a growing trend in the use of such a password. The human psychology study reveals that humans find it easier to remember pictures as opposed to words. There are two main aspects to the graphical password scheme namely security and usability. This study comprises of a comprehensive research in the current Recognition-Based graphical password schemes. The common usability attributes and possible attacks on the Recognition-Based graphical password are reviewed, identified and examined in detail. Lastly, a comparison table is revealed to put forth the limitations and strengths of each approach in terms of security and usability.

[Touraj Khodadadi, A.K.M. Muzahidul Islam, Shozo Komaki, Sabariah Baharun. **Evaluation of Recognition-Based Graphical Password Schemes in Terms of Usability and Security Attributes**. *Researcher* 2022;14(6):38-49] ISSN 1553-9865 (print); ISSN 2163-8950 (online) http://www.sciencepub.net/researcher. 6. doi:10.7537/marsrsj140622.06.

Keywords: Authentication, Recognition-Based; Security and Usability; Graphical Password.

1. Introduction

The alphanumeric passwords have been traditionally used to ensure the user's authenticity. Even though, at the present time other techniques of identification such as smart cards and biometrics are available, the password system will most probably be dominant given the issues of security, ease of use, privacy, and reliability of the other approaches [1, 2]. The most often used singular method of user authentication of a system is the textual password. At present, most computer systems, internet-based environments, and networks use this approach for user authentication [3]. However, the weaknesses of this approach are commonly known to all. It is easy to guess or crack most passwords. For instance, a commonly used method of hacking to crack an alphanumeric password is the dictionary attack. This attack works efficiently as it requires very little time to find out the password of the user [4, 5]. An additional weakness of this approach is the effort required to remember a password. Studies carried out recently portray that the capacity of a human to remember a number of passwords is limited [6]. The key challenge with using an alphanumeric password is that after one has been used, the user must recall it again to login to a system where the password has been used. However, humans have the tendency to forget their passwords and more so if it is not used frequently. Thus, given this scenario, a user might write down the password, use a similar password for various applications and their choice something that short, simple and often easily guessed such as family members' names, pets' names, and birthdays [3, 4, 7]. A useful alternative that has been proposed is the graphical password technique. The graphical password is possibly easier to remember and more secure compared to traditional alphanumeric password as they make use of humans' capability of memorizing and recalling images better. This approach was developed to solve the problems associated with the conventional password using alphanumeric schemes. This approach also makes it easier to memorize the password, simpler to use and has more security. Given the two assumptions that humans can recall images better than numbers and words and the notion that a picture is more valuable than a thousand 'passwords', software companies and psychological researches appear to concur with this

approach [6, 8]. A user is given a group of images in the Recognition-Based technique and authentication is achieved by remembering and identifying the selected image at the initial stage of registration. This study intends to review the security and usability aspects of the currently available Recognition-Based graphical password schemes. This study comprises of a comprehensive research in the current Recognition-Based graphical password scheme. The common usability attributes and possible attacks on the Recognition-Based graphical password is reviewed, identified, and examined in detail. The following sections will review the strengths and weaknesses of the current Recognition-Based schemes.

2. Summary of the Present Recognition-Based Graphical Password schemes

Passface Scheme

In 2000 [9], the Real User Corporation developed a technique called the Passface scheme. The Real User Corporation using the assumption that humans recall faces better than any other images designed a commercial product called the Passfaces. With Passfaces, basically users have to choose human face they have seen before from a choice of nine faces; only one face is known to them, the rest act as a decoy. This stage is repeated continuously repeated till they are able identify all four faces. A comparative research that was carried out on Passfaces password found that it was easier recall Passfacess rather than text-based passwords and the users were highly influenced by the gender, attractiveness and race of the faces used [10]. The Passfaces password would be predictable in this way. This issue may be controlled by assigning faces to the users arbitrarily but then it would be more difficult for the users to recall such passwords. Another setback with this technique is that the login and registration processes take time and which will cause this method to be more time consuming compared to the text-based password system. Additional studies were carried on the security features of PassFaces to find out if the Passfaces was susceptible to social engineering threats whereby the hackers could persuade the user to explain the image they were using [11, 12]. It was revealed that when a decoy image was chosen carefully that was just like the user's chosen images, it was not possible for another person having heard the description of the image to enter the password accurately just based on this information.

Figure 1: Passface Scheme [9]

2.1 Déjà vu Scheme

The déjà vu algorithm was developed in 2000 [13] and it begins by letting the users choose and remember a subset of images taken from a bigger sample to make the portfolio on that they would use. Users must recall images of their chosen portfolio from a group of decoy images to login. A panel of 25 images is shown in the test system; 5 belong to the portfolio of the user. The users must recall all their portfolio images and displayed is only one panel. "Randomart" images are used so it is harder for users to jot their password or reveal it to others by way of image description. Researchers claim that it is sufficient to use a set of fixed 10000 images; however, the attractive images should be chosen meticulously to improve the chances of users choosing the same possible image. The findings of their study revealed that 90% of the participants were successful in utilizing this technique for authentication whereas only 70% were successful while utilizing PINS and textual passwords [14]. However, the average time for login is longer than the normal approach, but it has a lower failure rate. Studies on the Déjà vu technique have revealed certain weaknesses. One of them is given the large number stored pictures on the server, the process of authentication is slower due to delays caused by network traffic. The other weakness is that although the password space size of the Déjà vu is smaller in comparison to the text passwords, it does not mean that it is easier to remember the Déjà vu technique. Another observed weakness is the server requires storing the portfolio images' seeds of all the users in plain text format. Thus, the picture selection process form the image database can be time consuming and tedious. Lastly, time taken to create a password using the Déjà vu technique is 60 seconds while with the text password, it only takes 25 seconds [13, 14].

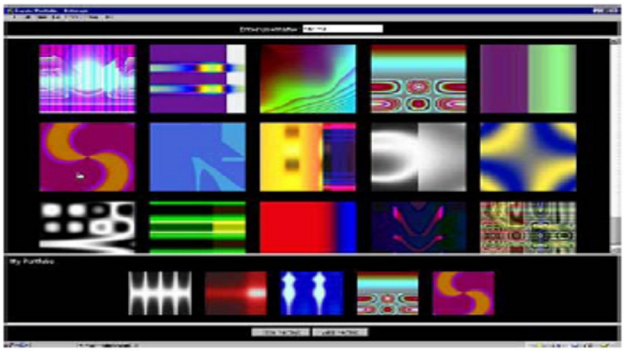

Figure 2: Déjà vu Scheme [13]

2.2 Triangle Scheme

Sobrado and Birget in 2002 [10], suggested a number of graphical password techniques to solve the problem of shoulder-surfing threats. Their first technique was known as the "triangle scheme"; the user has to choose his/her pass-object taken from the objects displayed. The users are required to identify the entire pre-chosen pass-objects that were chosen at the registration stage for authentication. The convex-hull designed by the pass-object has to be clicked by the users. Since the convex-hull's size is quite big, there may be a successful login based on random clicking [15, 16]. Sobrado and Birget proposed the usage of 1000 objects in the login process to make the space of password big enough and hard to guess. Nevertheless, increasing the quantity of objects would make the display to be hard and crowded to look for the pass-object while lowering the quantity of objects would cause the space of the password to be smaller since the convex-hull's size can be quite big. If this issue persists, it would be simple to guess and crack the password.

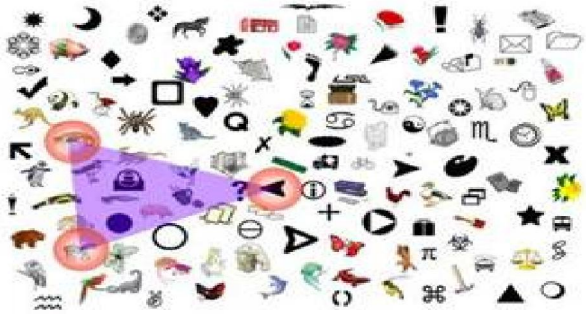

Figure 3: Triangle Scheme [10]

2.3 Moveable Frame Scheme

The last scheme by Sobrado and Birget in 2002 [10], is known as the Moveable Frame. In this scheme, there are just three pass-objects. One of the pass-objects will be directed to the moveable frame. Users are just required to move by rotating the frame till the entire pass-objects are places in a straight line to be authenticated. Sobrado and Birget proposed repeating the process a few times by randomly rotating or clicking it to minimize the chances of login. Nevertheless, this step is time consuming, confusing, and rather unpleasant given the numerous non-pass objects.

Figure 4: Moveable Frame Scheme [10]

2.4 Picture Password Scheme

In 2003 [17, 18], Bye Janesen, designed a graphical password scheme based on "picture password" particularly catered to mobile devices like PDAs. The users have to first choose the theme (cat and dog, sea and shore, and others) which comprise of thumbnail photos throughout the creation of a password. Then, the users choose and register a sequence of the chosen thumbnail photo to create a password. The users are required to remember and recognize the photos seen previously and touch in the right order utilizing a stylus for authentication purpose. The users can change the password, choose a new sequence, or change the theme after they succeeded in the authentication. The researchers also proposed that the process be repeated several times to lower the chances of logging in by randomly rotating or clicking. The disadvantage of this method is the small password space as the photos are limited to only thirty pieces. The designers added a second step to the algorithm to overcome this issue. The users can choose two thumbnails simultaneously to design the new alphabet component by utilizing the shift key to choose either special characters or uppercase. The recall process will be more complicated when the second step is added to the algorithm even though it overcomes the space problem.

Figure 5: Picture Password Scheme [18]

2.5 Where Is Waldo (WIW) Scheme

Man, et al. in 2003 [19], suggested another scheme that was shoulder-surfing resistant. The users choose several images as the pass-objects in this technique. Every pass-object has a few variants and every variant is given a unique code. The user is provided with several scenes during authentication the stage. Every scene has a few pass-objects which were a randomly chosen variant and many decoys. The users have to key in a string with the unique code that corresponds with the pass-object variants available in the scene and a code that indicates the relative location of the pass-objects in reference to a pair of eyes. This was carried out since it is very difficult to guess this type of password even if the entire process of authentication is video recorded because there is no mouse click to give away the information on the pass-objects. Nevertheless, this technique still needs the users to memorize each pass-object variant's alphanumeric code. For instance, if there are 4 images with 4 variants, 16 codes must be memorized by the user. It is quite inconvenient even though the pass-objects offers some hints for remembering the codes. This approach was later extended to permit users to assign their own codes to pass-object variants. Figure 6 reveals the graphical password scheme on the log-in screen. This method however, still requires the users to memorize many text strings and therefore it has many of the setbacks of the textual passwords. For example, if there are 4 pictures each with 4 variants, then each user has to memorize 16 codes.

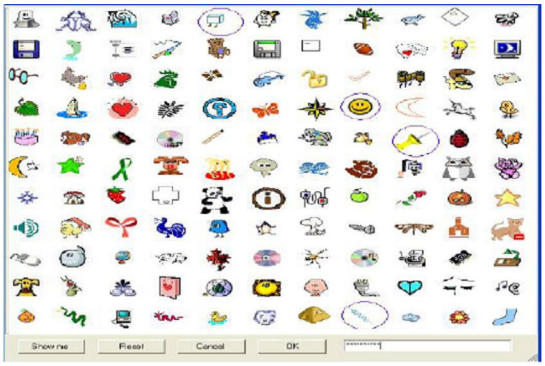
Figure 6: WIW Scheme [19]

2.6 Story scheme

Davis et al. proposed the Story scheme in 2004 [11] as a comparable technique to PassFaces. Here in Story, firstly, the user chooses an image sequence for their portfolio. The user is given an image panel which they should use to identify their portfolio images among other decoys in order to log in. The images consist of people, places or everyday objects. A sequential component was also introduced in Story by having the users choose their images in the right order. Users were told to construct a story mentally to link the images in their set in order to easily memorize the scheme. A panel comprising of 9 images and user's password comprising of 4 images sequence must be chosen from this panel for the test system. Research on Story revealed that users' selections in Story had more variations but still had patterns that could be exploited such as differences between female and male selections. The users found it difficult to remember their Story passwords (85% success rate) and many of them frequently made errors in the orders [8, 20]. Surveys that were carried out revealed that it was not possible to formulate a story as a memory aid, despite the intentions of the designers, which explains the many errors in ordering; using a different instruction or gaining more experience using the system might enable the users to solve this problem [3, 8]. Time taken to login or create the password was not recorded.

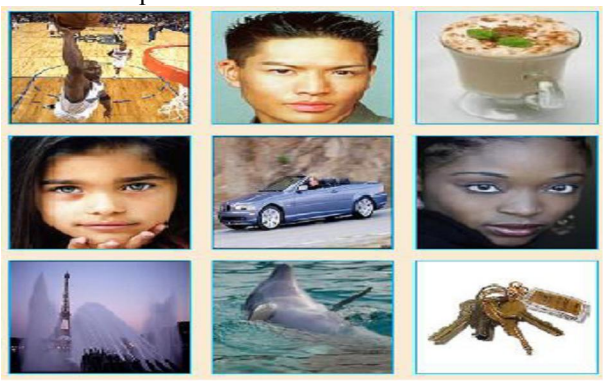
Figure 7: Story Scheme [11]

2.7 Convex Hull Click (CHC) Scheme

Wiedenbeck et al. in 2006 [21], proposed the CHC scheme which is just like the triangle technique. It is a graphical password technique that safeguards against the shoulder-surfing threats by video recording, electronic capturing, or human observation. Several rounds of challenge-response authentication are used in CHC. The graphical features utilized for authentication in CHC are icons that appear in a screen window. The users must identify a minimum number of their password icons, or "pass-icons," out of a large number of icons arranged randomly in a challenge. The users respond by clicking within the pass-icons convex hull to address the challenge. A few of these challenges appear in a sequence, and if the users respond accurately to each one, then user authentication is done. This approach needs the user to undergo a training session and learn how the pass-icons should be placed. It is important that the users are able to locate their pass-icons in a large group of icons and if the users are not used to it, this can cause the login process to be time-consuming and affect the usability feature of this technique.

Figure 8: CHC Scheme [21]

2.8 Weinshall Scheme

Weinshall in 2006 [22], introduced a graphical password technique where users are required to identify images from their portfolio in order to login. The login process includes outlining a path on the computer through an image panel based on if specific images belong to the portfolio of the user. The instructions state that they are to compute a path beginning from the top-left corner of the image panel, then moving down if one is standing on a picture from their portfolio, and moving right if it is not. After reaching the bottom edge or right of the panel, they have to identify the corresponding label for that column or row. A multiple-choice question is asked, which involves the accurate end-point of the path's label. Several rounds are performed by users, each time being presented with a panel, differently. After completion of each round, the cumulative probability is computed by the system to affirm that the accurate answer was not computed by chance. When a certain threshold is passed by the probability, the user authenticated is complete. Some user error is allowed but the user is rejected if the threshold is not reached within a fixed number of rounds. The input uses the keyboard instead of a mouse, to help lower the threat of shoulder-surfing. System assigned image portfolios are given to users and they receive a thorough training to initially memorize this portfolio as it involves many images (about 100), but time taken was not recorded for this initial phase of training. In a study done with 9 users, an overall 95% rate of successful login was achieved, where users logged in for 10 weeks. On average the login process takes about 1.5 to 3 minutes. Weinshall reported that the main advantage of this technique was the avoidance of observation (shoulder-surfing) attack or threat [23, 24].

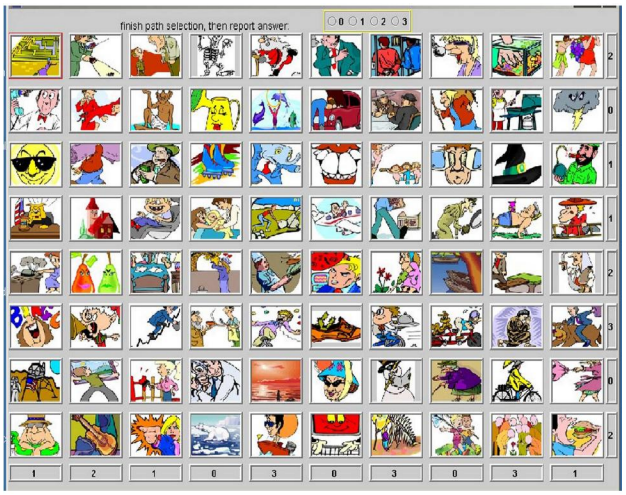

Figure 9: Weinshall Scheme [22]

2.9 Use Your Illusion Scheme

Hayashi and Christin in 2008 [25], introduced a graphical password technique that permitted image usage that was self-chosen which the users were familiar with but which an attacker cannot easily predict. Psychology studies revealed that self-generated images are better recognized compared to those that are not; this technique permits the users to choose their own images for the graphical password. Besides, the users get to enjoy the possibility of selecting and personalizing their portfolios' images, and users are likely to select images that are meaningful to them, semantically. Users can select and generate images by uploading pictures from their computers or from the existing database. In the

mobile devices' context, the users can take a picture with their own camera attached to the mobile device. After the pictures are chosen, they are distorted by utilizing an algorithm that non-photorealistic that removes most of the images' details while some features are preserved such as rough shapes and color. It is not possible to revert back mathematically to the original image from the distorted version as the information is lost in the rendering algorithm. Thus, the distortion feature is similar to the one-way function that cryptography uses. The main disadvantage of this technique is that users are required to memorize images that have been chosen in the registration phase and if users cannot recall the images, authentication does not take place, so inevitably the users have to still memorize.

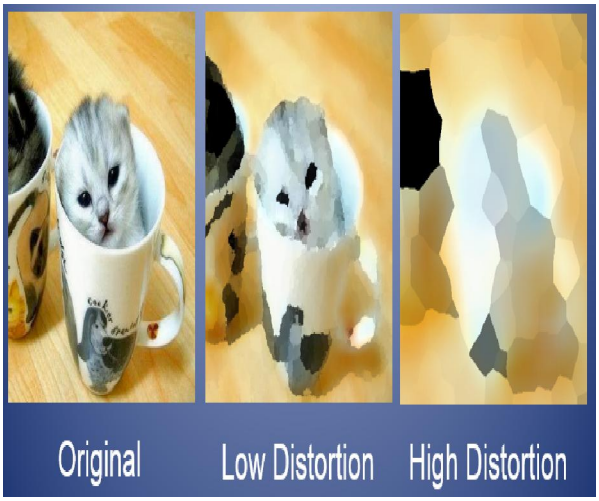

Figure 10: Use Your Illusion Scheme [25]

2.10ImagePass scheme

In a study by Mihajlov in 2011 [26], he proposed the password scheme based on recognizing graphics which utilized images that were single-object to create the graphical password. Users select a username by inputting the preferred choice in the textbox for username. The graphical choice grid is shown on the screen if the username is available. The screen for the graphical password selection has a 6x5 grid with a graphical password selection which reveals the images possible to be selected. A huge image database supports the ImagePass for the convenience of the users while selecting their passwords. If the images available are not what users are searching, users can load a set of images that are new and then make a selection. The users click on x number of images with a specific order where 4 images are the minimum graphical length allowed in choosing the graphical password. After an enrolment that is successful, a set of sixteen specifically fixed images that consist of pictures from the users chosen graphical password and system chosen images for decoy are attached permanently to the username. For authentication purposes, firstly users must input the accurate username; this would load the personal image set for immediate authentication in the authentication grid and after that users must choose the graphical password in the sequence of images correctly. A disadvantage is that the servers are required to store large volumes of pictures that may have to be moved on the network, thus making the authentication process time consuming.

Figure 10: ImagePass scheme [26]

2.11WYSWYE Scheme

According to Khot et al. in 2012 [27], they examined and suggested the new defensible scheme against shoulder-surfing attack for graphical passwords that are based on Recognition. These techniques use the WYSWYE strategy, whereby the users have to identify patterns of image based passwords from an images grid and copy it on another grid. WYSWYE is the acronym for "Where You See (the password) is What You Enter (the position). It is an effective and easy strategy which uses the notion of identification of patterns and tabular based reductions. It identifies the pattern of N images of passwords within the $M \times M$ grid (where $N < M$) and then maps the pattern of password images that have been identified onto an $N \times N$ grid that is separate. While logging in, the system creates an image grid that is random and empty and puts them on the screen side by side as illustrated in Figure 11. The image grid on the left hand side $M \times M$ is called the Challenge grid and it has the N password images and the M^2-N images for decoy. This grid is not directly utilized by the users. A separate $N \times N$ grid is used instead for entering of the input, which is on the screen's right hand side. This part of the grid is known as the Response grid. For logging in purposes, the users are supposed to identify the password images' pasterns within the challenge grid and accurately copy them onto the response grid. The key benefit of the suggested technique is that even if the entire process of logging

in is monitored by an attacker, only the *N* random positions marked in the response grid can be seen and it is hard to link them back to the images of the passwords. In addition, the positions marked as *N* are only valid for one session and with each new logging in session, a grid with a new challenge is generated, which makes the *N* positions that were captured earlier obsolete. The main drawback of this scheme is that choosing images for authentication can be time consuming and difficult for users.

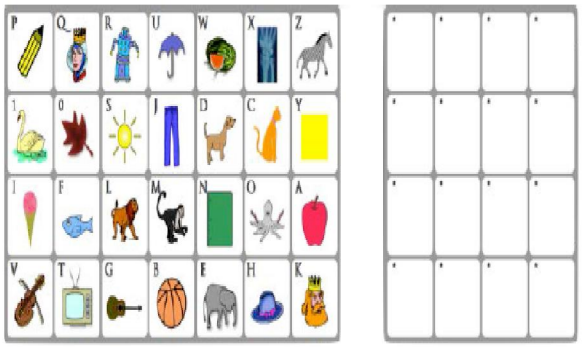

Figure 11: WYSWYE Scheme [27]

2.12S-Passface Scheme

In the work by Towhidi et al. in 2013 [28] , they enhanced the Passface scheme and introduced the S-Passface scheme. S-Passface was designed to improve the usability and security algorithm of the Passface, by enhancing the Passface algorithm's vulnerability to shoulder-surfing attacks, and improving usability in the logging in stage. Using the Passface approach, the nine decoy pictures are randomly selected from a face database with password faces of the same age. However, with the S-Passface approach, the selection of decoy pictures is done using visual similarity with the password face. In order to identify the images that are more similar, a group of people examined the images' resemblance. With the S-Passface, the images used for decoy were selected according to the similarity to the verbal depiction of the password's picture with eight decoy images. The findings of the research revealed that Passface can be utilized by accurate decoy selection which lowers this method's vulnerability to description attacks. Thus, the decoy images do not have any characteristic associated to the individuals or their faces so that this would make it difficult for users to describe the password to another person. The algorithm for the S-Passface which was designed to be impenetrable to shoulder surfing attacks, using the research which reveals that moving the configuration from mouse based input to keyboard input, lowers the possibility of being attacked using the shoulder surfing method. Furthermore, the algorithm of "WIW", was proven to be resilient to shoulder surfing attacks, when a random text that is unique is assigned for every image, users need to key in a string of codes that correspond with the images in the password, instead of choosing their passwords using a mouse directly. In these findings, it was shown that during the login stage of the S-Passface algorithm, no option is available to select the password with a mouse, and in return, two characters are assigned randomly beneath every face. Users are successfully authenticated if they are able to identify their password images and enter the text that appears beneath their passwords. The disadvantage of this approach is that all the attackers have to do is to identify the images that were selected, and as such randomly assigning text for every image becomes useless as the attackers can see which text is linked to a particular image and hack the password, easily.

Figure 12: S-Passface Scheme [28]

3. Usability Attributes in Recognition-Based Graphical Password schemes

Usability is sometimes defined as "easy to use" but this definition does not accurately identify the problem and offers little to the user interface designer to change the interface. A better definition should be used to identify the users' requirements, design usability aims and determine the best approaches to evaluate the usability functions. In computer science and human computer interaction, usability normally relates to the clarity and elegance with which the communication with a web site or computer program is developed. Therefore, usability is a critical component in developing a good technique that can meet the users' requirements [29]. A comprehensive study of the usability attributes of Recognition-Based graphical password techniques has been carried out and the common usability attributes have been identified and determined in this study. The usability attributes are mapped to the Recognition-Based techniques and various similarities and differences of the usability attributes

in each technique are noticeable. Table 1 depicts the major usability attributes that have been utilized in the current Recognition-Based graphical password techniques which can be classified into nine categories such as User assigned Images, Meaningful Images, Category of Images, Easy and Fun to Use, Easy to Create, Easy to Execute, Easy to learn and Understand, Easy to Correct, and Nice and Simple Interface. The following sections describe the definition of the usability function in detail:

- Images that are Meaningful: means that the images are well-known and familiar to the users.
- Images Assigned by Users: research on memorability suggests that when a password is randomly assigned to users, they have difficulty recalling their passwords compared to the scenario where users are allowed to choose their own passwords.
- Images Category: means that users can select a category of images according to their preference.
- Easy to Create: means users can create their graphical passwords easily when the registration steps are simple. Having a few rounds of choosing and creating a password as in the Story password, makes the process slow and complicated for the users.
- Fun to Use and Easy: means that the system should offer a good platform to create the password. As an example, the challenge-respond or training session approach is used to make users feel that the system is easy to use.
- Easily Executed: means users can execute the algorithm with ease when the registration and login is described in simple easy steps. Having a few rounds of choosing and creating a password, makes the process slow and complicated for the users thus the suggested algorithm for the registration and login should be done in a single step.
- Nice and Simple interface: concentrates on the users' interactions besides making the interface attractive. The aim of having a nice and simple interface is to make the users' interactions as efficient and simple as they can. A good interface design for users facilitate the completion of the task at hand by staying away from unnecessary attention with a good, eye catching and bold graphic design.
- Easily understood and learnt: means that when understandability and learnability functions are added to an algorithm, the system will be easier to understand and utilize, hence lowering training and support expenses; it also improves the user satisfaction and lowers pressure and uneasiness. Besides, the learnability function will increase the users' productivity and the overall organization's operational effectiveness.
- Easy to Correct: this feature assists the users to easily utilize the system without any difficulty by giving hints to users or opening some windows while executing to reveal mistakes made by the users.

The " √ " symbol refers to a particular feature of a technique while the " X " symbol means that the technique is missing a specific function.

Table 1. The usability attributes on graphical

Recognition-Based Graphical Password Schemes	Usability Attributes								
	Memorability								
	Meaningful Image	User Assign Image	Category of Images	Ease to Create	Ease and Fun to Use	Easy to Execute	Simple and Nice Interface	Easy to learn and Understand	Easy to Correction
Passfaces	X	✓	X	✓	✓	✓	✓	✓	✓
Déjà vu	X	✓	X	X	X	X	X	✓	✓
Triangle	X	X	X	✓	✓	✓	X	✓	✓
Moveable Frame	X	X	X	✓	✓	✓	X	✓	✓
Picture	X	✓	✓	✓	✓	✓	✓	✓	✓
Story	✓	✓	✓	X	✓	X	✓	✓	✓
WIW	X	✓	X	✓	X	X	X	✓	✓
Use Your Illusion	✓	✓	X	✓	✓	✓	✓	✓	✓
CHC	X	X	X	✓	✓	✓	X	✓	✓
Weinshall	X	✓	X	X	✓	X	X	✓	✓
ImagePass	✓	✓	X	✓	✓	X	X	✓	✓
WYSWYE	✓	✓	X	✓	X	✓	✓	✓	✓
S-Passface	X	✓	X	✓	✓	✓	✓	✓	✓

4. Possible attacks on Recognition-Based graphical password

In the following section, a detailed study of the possible attacks on Recognition-Based graphical password techniques has been conducted and the attacks have been identified and determined. The possible attacks are mapped to the Recognition-Based schemes. Possible attacks are classified into six kinds of attacks which are dictionary, brute force, spyware, guessing, social engineering, and shoulder-

surfing. These are the present active attacks on the Recognition-Based schemes.

- Dictionary attack

Dictionary attacks are conducted by attackers by identifying passwords that users will most likely choose and utilizing this list to attempt systematically to hack the password. The hackers try to estimate the password space effectively. The success ratio can be dramatically increased in comparison to an exhaustive attack by reducing the number of expected guesses to succeed. Dictionary threats can be particularly successful if prioritized entries are used to first test the most likely passwords. As recognition based graphical passwords include a mouse input rather than a keyboard input, these techniques are not as vulnerable to dictionary threats as textual passwords. Among the current techniques, only the Passface technique is not resistant against this type of threat.

- Brute force (Exhaustive) attack

Exhaustive threats can be carried out just like the dictionary attacks, except that each potential password possibility is created and utilized to attack the genuine password. In more high strung threats, these possibilities are also prioritized to reduce the possibility of being chosen by the user, if at all these possibilities can be guessed. Similar to the dictionary threats, exhaustive attacks can be carried out either offline or online. The advantage of this kind of threat is that with sufficient computing power and time, a match will eventually be found (unless the online threat is located and stopped before exhausting the list), but given the big password spaces, it might not be feasible to find throughout the whole space. Contrary to a dictionary threat, the exhaustive attack provides a higher coverage but needs more processing power or time. The major defense tool against a brute force search is to possess a large enough password space. Textual passwords have a password space of 94^N, whereby N is the password length and 94 is the printable characters' number not including the space. Several graphical password methods offer a similar password space to that of textual passwords or even larger. Graphical passwords that are recognition-based are likely to contain a smaller password space compared to the recall based techniques. It is much harder to conduct a brute force attack against a graphical password compared to a textual password. The attack programs are required to generate automatically accurate mouse motions to copy the human input, which is rather hard for the recall based graphical password.

- Spyware attack

This is a specialized type of attack where tools are installed initially on the user's computer and sensitive data is recorded. Any key or mouse movement is recorded using this malware. The data that has been recorded without the user's knowledge is then reported back outside the computer. Except in a few cases, just using key listening spyware or key logging cannot be utilized to crack graphical passwords since it's not proven if the mouse spyware is an effective mechanism to crack a graphical password. Even if mouse tracking is successfully saved, it is not enough to find and crack the graphical password. Other additional information is required to complete this type of threat such as window size and position, besides information timing.

- Shoulder surfing attack

Attackers gaining knowledge of users' credentials via direct observing, or via external recording through video cameras, as the real user computes the information is known as Shoulder surfing. The availability of high-resolution cameras with surveillance equipment and telephoto lenses cause shoulder-surfing to be a major threat if attackers are specifically targeting users and have access to these users' geographic location. This is particularly troublesome in a public environment, but it is a more serious threat in a private environment. Similar to textual passwords, most graphical passwords are at risk of shoulder surfing. Right now there are just several recognition-based techniques designed to confront the issue of shoulder-surfing. Not one of the Recall-Based based techniques is regarded as being resistant to shoulder-surfing.

- Social Engineering Attack

Social engineering involves any approach that is utilized to trick a person into revealing his/her private information or credentials to untrustworthy people. An example of social engineering utilizing websites and email is known as Phishing however social engineering can also be carried out through other means, such as fake phone calls claiming to be from the users' banks, credit card companies, or technical supports. It is easier to get a password or credential from a legitimate user than attempting to hack into a secured system. Compared to a textual password, it is not as easy for users to reveal a graphical password to somebody else. For instance, it is almost impossible to reveal a graphical password over the telephone. It would be more time consuming to set up a phishing website just to gain a graphical password.

- Guessing Attack

Since users normally choose their passwords according to some personal information such as pet names, passport numbers, and family names, hackers attempt to guess passwords by trying out the possible passwords. Attacks using Password guessing can be broadly classified into offline dictionary and online password guessing attacks. The attacker searches

exhaustively for the password through manipulation of inputs by one or more oracles in an offline dictionary attack. On the other hand, the attacker attempts an already guessed password through manipulation of inputs of one or more oracles in an online password guessing attack. However, it appears that a graphical password can be easily guessed, just like with textual passwords. For instance, researches on the Passface method revealed that users frequently select predictable and weak graphical passwords.

Table 2 reveals the comparative Recognition-Based schemes according to common attacks; " √ " in this table refers to resistance to attack, and "X" refers to non-resistance to attacks.

Table 2. The attacks on graphical password

Recognition-Based Graphical Password Schemes	Possible Attacks					
	Dictionary	Brute force	Spyware	Shoulder surfing	Social engineering	Guessing
Passfaces	✓	✓	X	✓	X	✓
Déjà vu	X	✓	X	✓	X	✓
Triangle	X	✓	X	X	X	✓
Moveable Frame	X	✓	X	X	X	✓
Picture	X	✓	X	✓	X	✓
Story	X	✓	X	X	X	✓
WIW	X	✓	✓	X	X	X
Use Your Illusion	X	X	X	X	X	✓
CHC	X	✓	X	X	X	✓
Weinshall	X	✓	X	✓	X	X
ImagePass	X	✓	X	✓	X	X
WYSWYE	X	X	✓	X	X	X
S-Passface	X	✓	X	✓	X	✓

5. Conclusion and Future Research

These days, user authentications are a major area of concern in information security. Password schemes that are strong text-based could offer some level of security. Nevertheless, since strong passwords are hard to remember frequently makes the users to jot them down or even keep them in their computer files. Graphical authentication methods have been suggested as a possible alternative solution to solve the problem with textual authentication, particularly motivated by the reasoning that humans can recall images better than texts. Of late, many Internet based environments, computer systems, and networks, have attempted to use graphical authentication methods to authenticate their users. This research has reviewed twelve current graphical passwords that are Recognition-Based. The security and usability attributes of the recognition-based graphical passwords have been further addressed and reviewed and each attribute has been discussed in detail. Lastly, comparison tables of Recognition-Based algorithms were made based on the usability features and the potential of threats.

In conclusion, it was discovered that from the first authentication using graphical images that was suggested till now, many researchers have tried to come up with new techniques or make the previous ones better especially in improving usability and security. Unfortunately, improving usability has made the techniques to reduce the security element and when security is emphasized, the usability features are compromised. Although, both aspects are necessary and critical, in reality one or the other is compromised. The Recognition-Based graphical password techniques reveal this challenge. Therefore, designers are still challenged with creating a technique that covers both security and usability.

There is a possibility for future researches to proof this argument as the existing user researches are limited and not convincing enough to support the main argument that people are better at memorizing graphical passwords compared to textual passwords. Based on the usability viewpoint, more efforts should be placed on finding out the effects of a particular image utilized successfully as graphical passwords, studying speed of skilled users, and finding out the bad practices of insecure password practices that users carried out in coming up with graphical passwords.

Acknowledgements:

This research is in affiliation with Ministry of Higher Education, Universiti Teknologi Malaysia, Malaysian-Japan International Institute of Technology (MJIIT) and communication System and Network (CSN) research group.

Corresponding Author:
Touraj khodadadi
Malaysia-Japan International Institute of Technology (MJIIT) Universiti Teknologi Malaysia, Malaysia.
E-mail: ktouraj2@live.utm.my

References

[1]. S. Komanduri and D. R. Hutchings, "Order and entropy in picture passwords," in Proceedings of graphics interface 2008, 2008, pp. 115-122.

[2]. A. Patrick, A. C. Long, and S. Flinn, "HCI and security systems," 2003.

[3]. H. Gao, Z. Ren, X. Chang, X. Liu, and U. Aickelin, "A new graphical password scheme resistant to shoulder-surfing," in Cyberworlds (CW), 2010 International Conference on, 2010, pp. 194-199.

[4]. H. L. Arash, A. Abdul Manaf, and M. Masrom, "Security evaluation for graphical password," 2011.

[5]. N. Wright, A. S. Patrick, and R. Biddle, "Do you see your password?: applying recognition to textual passwords," in Proceedings of the Eighth Symposium on Usable Privacy and Security, 2012, p. 8.

[6]. Z. Erlich and M. Zviran, "Authentication methods for computer systems security," Encyclopedia of information science and technology 2nd ed, vol. 1, pp. 288-293, 2009.

[7]. L. Lazar, O. Tikolsky, C. Glezer, and M. Zviran, "Personalized cognitive passwords: an exploratory assessment," Information Management & Computer Security, vol. 19, pp. 25-41, 2011.

[8]. R. Biddle, S. Chiasson, and P. C. Van Oorschot, "Graphical passwords: Learning from the first twelve years," ACM Computing Surveys (CSUR), vol. 44, p. 19, 2012.

[9]. S. Brostoff and M. A. Sasse, "Are Passfaces more usable than passwords? A field trial investigation," in People and Computers XIV—Usability or Else!, ed: Springer, 2000, pp. 405-424.

[10]. L. Sobrado and J.-C. Birget, "Graphical passwords," The Rutgers Scholar, an electronic Bulletin for undergraduate research, vol. 4, p. 2002, 2002.

[11]. D. Davis, F. Monrose, and M. K. Reiter, "On User Choice in Graphical Password Schemes," in USENIX Security Symposium, 2004, pp. 11-11.

[12]. D. T. Levin, "Race as a visual feature: using visual search and perceptual discrimination tasks to understand face categories and the cross-race recognition deficit," Journal of Experimental Psychology: General, vol. 129, p. 559, 2000.

[13]. R. Dhamija and A. Perrig, " D´ej`a Vu: a user study using images for authentication," presented at the Proceedings of the 9th conference on USENIX Security Symposium - Volume 9, Denver, Colorado, 2000.

[14]. X. Suo, Y. Zhu, and G. S. Owen, "Graphical passwords: A survey," in Computer Security Applications Conference, 21st Annual, 2005, pp. 10 pp.-472.

[15]. A. H. Lashkari, A. A. Manaf, and M. Masrom, "A Secure Recognition Based Graphical Password by Watermarking," in Computer and Information Technology (CIT), 2011 IEEE 11th International Conference on, 2011, pp. 164-170.

[16]. A. Fulkar, S. Sawla, Z. Khan, and S. Solanki, "A study of graphical password and various graphical password authentication schemes," World, vol. 1, pp. 04-08, 2012.

[17]. W. Jansen, "Authenticating mobile device users through image selection," The Internet Society: Advances in Learning, Commerce and Security, vol. 1, pp. 183-194, 2004.

[18]. W. Jansen, "Authenticating users on handheld devices," in Proceedings of the Canadian Information Technology Security Symposium, 2003.

[19]. S. Man, D. Hong, B. Hawes, and M. M. Matthews, "A Graphical Password Scheme Strongly Resistant to Spyware," in Security and Management, 2004, pp. 94-100.

[20]. M. Hlywa, R. Biddle, and A. S. Patrick, "Facing the facts about image type in recognition-based graphical passwords," in Proceedings of the 27th Annual Computer Security Applications Conference, 2011, pp. 149-158.

[21]. S. Wiedenbeck, J. Waters, L. Sobrado, and J.-C. Birget, "Design and evaluation of a shoulder-surfing resistant graphical password scheme," in Proceedings of the working conference on Advanced visual interfaces, 2006, pp. 177-184.

[22]. D. Weinshall, "Cognitive authentication schemes safe against spyware," in Security and Privacy, 2006 IEEE Symposium on, 2006, pp. 6 pp.-300.

[23]. R. Biddle, S. Chiasson, and P. C. V. Oorschot, "Graphical passwords: Learning from the first twelve years," ACM Comput. Surv., vol. 44, pp. 1-41, 2012.

[24]. R. Biddle, S. Chiasson, and P. C. Van Oorschot, "Graphical passwords: Learning from the first generation," Technical Report

TR-09-09, School of Computer Science, Carleton University2009.

[25]. E. Hayashi, R. Dhamija, N. Christin, and A. Perrig, "Use Your Illusion: secure authentication usable anywhere," in Proceedings of the 4th symposium on Usable privacy and security, 2008, pp. 35-45.

[26]. M. Mihajlov, B. Jerman-Blazic, and M. Ilievski, "Recognition-Based Graphical Authentication with Single-Object Images," in Developments in E-systems Engineering (DeSE). 2011, pp. 203-208.

[27]. R. A. Khot, P. Kumaraguru, and K. Srinathan, "WYSWYE: shoulder surfing defense for recognition based graphical passwords," in Proceedings of the 24th Australian Computer-Human Interaction Conference, 2012, pp. 285-294.

[28]. F. Towhidi, M. Masrom, and A. A. Manaf, "An Enhancement on Passface Graphical Password Authentication," J. Basic. Appl. Sci. Res., 3(2)135-141, 2013.

[29]. S. Winter, S. Wagner, and F. Deissenboeck, "A comprehensive model of usability," in Engineering interactive systems, ed: Springer, 2008, pp. 106-122.

2/15/2022