**International Journal of Electrical and Computer Engineering (IJECE)**
Vol. 6, No. 6, December 2016, pp. 2939~2948
ISSN: 2088-8708, DOI: 10.11591/ijece.v6i6.11227 

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

**Touraj Khodadadi, A. K. M. Muzahidul Islam, Sabariah Baharun, Shozo Komaki**
Malaysia-Japan International Institute of Technology (MJIIT), Universiti Teknologi Malaysia, Kuala Lumpur, Malaysia

**Article Info**

***Article history:***

Received Mei 11, 2016
Revised Oct 7, 2016
Accepted Oct 21, 2016

***Keyword:***

Graphical password
Recognition-based graphical
User interface
Security and usability attributes

**ABSTRACT**

User Authentication is a critical component in information security. Several widely used mechanisms for security to protect services from illegal access include alphanumerical usernames passwords. However, there are several drawbacks attached in this method. For instance, the users themselves usually those passwords that are easy to guess. As difficult passwords are difficult to recall. 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. There are several previous surveys on the graphical passwords. The latest research review and summarize graphical password systems concisely and at the same time, analyze usability features for every design. However it was found that there is not a single method that has the most resounding usability attributes. Therefore, this research suggests a set of usability attributes that can be applied into a single Recognition-Based graphical password system. In addition, this study examines and compares success rates on login, login time and memorability of existing systems which are the usability measures most often reported in user studies of graphical passwords. Lastly, a comparison table is revealed to put forth the limitations and strengths of each approach in terms of security and usability.



***Corresponding Author:***

Touraj Khodadadi,
Malaysia-Japan International Institute of Technology (MJIIT),
Universiti Teknologi Malaysia,
54100, Jalan Semarak, Kuala Lumpur, Malaysia.
Email: ktouraj2@live.utm.my

## 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 [1-3]. 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 [4-6]. 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 [7-9]. 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 [10-11]. 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 [12-15]. 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 [16-18]. Searchmetric or Cognometric systems, also called Recognition-Based systems, request users to learn and recall image portfolios during password generation, and next in order to log in, identify pictures among the decoys. In other words, 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 various image types are used by the suggested Recognition-Based systems, including icons, random art, faces and everyday objects.

However, since there is not yet wide deployment of Recognition-Based graphical password systems, the vulnerabilities of this schemes are still not fully understood. Overall, the current Recognition-Based graphical password techniques are still immature. Much more research and user studies are needed for this techniques to achieve higher levels of maturity and usefulness. This study comprises of a complete research in the current Recognition-Based graphical password scheme and review their strengths and weaknesses. The common usability attributes and possible attacks on the Recognition-Based graphical password is reviewed, identified, and examined in detail. In addition, we have conducted a comprehensive and comparative study of existing Recognition-Based graphical password techniques from the point view of usability features, login time and login success rate which are missed in previous related works.

## 2. SUMMARY OF THE PRESENT RECOGNITION-BASED GRAPHICAL PASSWORD SCHEMES

### 2.1. Passface Scheme

In 2000 [19], 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 [20]. 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 [21-22]. 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.

### 2.2. Déjà vu Scheme

Developed in 2000, the déjà vu algorithm allows the users select and recall an image subset from a larger sample to prepare the portfolio [23]. In order to login, users should remember the selected portfolio's images from a decoy image collection. In the test system, a panel including 25 pictures is presented; out of these, 5 images are included in user's the portfolio. The users should remember all images of their portfolio but only one panel is displayed. When "Randomart" images are employed, the users have difficulty disclose their password to others through image portrayal or jotting it. It is claimed that a set of 10,000 fixed images is sufficient; nevertheless, eye-catching images should be selected accurately so that users have higher chances of picking similar probable image. A study reported that this authentication technique was successfully used

by 90% of the users, while textual passwords and PINS were only successful in 70% of the cases [24]. On average, it takes longer time to login compared to the standard method, yet the failure rate is lower. Some weaknesses of the Déjà vu method have been reported. Considering the huge amount of saved images on the server, the authentication process is slower as network traffic causes delays. Moreover, while the Déjà vu's space size for password is less than the text passwords, it is not necessarily easier to recall that.

### 2.3. Triangle Scheme

Sobrado and Birget in 2002 [20], 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 [25-26]. 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.

### 2.4. Moveable Frame Scheme

The last scheme by Sobrado and Birget in 2002 [20], 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.

### 2.5. Picture Password Scheme

In 2003 [27-8], 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.

### 2.6. Where is Waldo (WIW) Scheme

In 2003, Man, et al. proposed the shoulder-surfing resistant scheme [29]. In this technique, the users can select many pictures as the pass-items. Few variants are available for each pass-item and a unique code is given to each variant. During authentication, several scenes a few pass-items are given to the user. These include many decoys and a randomly selected variant. The users should input a string having a distinctive code that matches the variants of pass-item in the scene and a code that designates the pass-item's relative location in relation to a pair of eyes. Although the whole authentication process is recorded by video, it is almost impossible to guess this password type, because no mouse click exists to offer the pass-items information. However, the users using this technique should still memorize alphanumeric code of every pass-item variant. If there are, for example, 4 pictures with four variants, the user must memorize 16 codes. It is rather troublesome even if the pass-items provide some clues to recall the codes. Later, this method was improved to enable users to ascribe own codes to pass-item variants.

### 2.7. Story Scheme

Davis et al. proposed the Story scheme in 2004 [21] 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 [30],[31]. 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 [18],[30]. Time taken to login or create the password was not recorded.

### 2.8. Convex Hull Click (CHC) Scheme

Wiedenbeck et al. in 2006 [32], 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.

### 2.9. Weinshall Scheme

Weinshall in 2006 [33], 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.

### 2.10. Image Pass Scheme

Mihajlov (2011) [34] suggested the password pattern based on identifying visuals through single-object images to make graphical password. A username is chosen by the user as he/she keys in the desired choice of username in the textbox. If the username is accessible, the screen displays the graphical choice grid. For the selection of graphical password, the screen has 6x5 grid and shows the possible images that can be chosen. For the users' convenience, the ImagePass is supported by a gigantic image database for password selection. If the users do not favor the available images, they may upload a new image set and then choose. They click on x number of pictures in a particular order and the least allowed graphical lengths are 4 images. Following a successful enrolment, 16 fixed pictures including images from the graphical password selected by the users and chosen images chosen by the system for decoy are attached to the username permanently. Users should first key in the exact username for authentication purposes so that the personal set of image is loaded for instant authentication in the grid. Next, the users have to pick the graphical password properly based on the order of images. A drawback is that the large volumes of images should be stored in the server that might be relocated on the network, which makes the process of authentication time consuming [35].

### 2.11. WYSWYE Scheme

Khot et al. (2012) proposed a new secure scheme for recognition-based graphical passwords to avoid shoulder-surfing attack [36]. The WYSWYE strategy was used in this technique that required the users to recognize picture based password patterns from a picture grid and duplicate it on another one. The

WYSWYE stands for "Where You See (the password) is What You Enter (the position). This easy and effective strategy is based on the concept of tabular-based reductions and patterns identification. The pattern of N passwords images is identified inside the M×M grid, then the password image pattern recognized onto a separate N×N grid is mapped. The system generates an empty and random image grid while logging in and places them next to each other on the screen. The left picture grid M×M is known as the Challenge grid with N password pictures and the M2-N pictures for decoy. The users do not directly use this grid. Instead, for entering of the input, a distinct N×N grid called the Response grid is employed (on right hand side of the screen). In order to log in, the users should recognize pasterns of the password images and copy in the response grid accurately.

### 2.12. S-Passface Scheme

In the work by Towhidi et al. in 2013 [36] , 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.

## 3. USABILITY ASPECTS

Usability is a critical component in developing a graphical password method that is good and meets the needs and requirements of its users. According to the ISO 9241-11 standard [17], [29], [36], usability is defined as the level at which a product is usable to particular users to reach their precise objectives efficiently and effectively and satisfactory in the required context. The major argument with the introduction of the graphical password is that images are easily remembered compared to strings of texts. Several researchers who conducted early studies in this area concur with this argument. Another usability issue that arises with the Recognition-Based approaches is the time taken in the registration and logging in process which is too long. Using this approach means that the users have to choose an image from a collection of images when registering initially and the users have to scan many images to pick several pass images for authentication purposes. Given the tediousness of this process, a newbie to the graphical password setting would find it difficult and complex. Following the comprehensive review of the usability attributes in the Recognition-Based graphical password, it was found that there is not a single method that has the most resounding usability attributes. Therefore, at the end of this research, a set of usability attributes that can be applied into a single graphical password system, which would be able to meet the requirements of the users, is suggested. In addition, this study examined and compared Success rates on login, login time and Memorability of the existing systems which are the usability measures most often reported in user studies of graphical passwords. The sections that follow will define and describe the major usability features that can be employed in the present and future techniques of the Recognition-Based graphical password 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.

### 3.1. Images that are Meaningful

Means that the images are well-known and familiar to the users.

### 3.2. 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.

### 3.3. Images Category

Means that users can select a category of images according to their preference.

### 3.4. 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.

### 3.5. 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.

### 3.6. 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.

### 3.7. 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.

### 3.8. 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.

### 3.9. 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 "O" symbol refers to a particular feature of a technique while the "×" symbol means that the technique is missing a specific function as shown in Figure 1.

| | Suggested Set of Usability features | | | | | | | | | usability measurement features | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 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 | Login Time | login Success Rate | Memorability |
| **Passface Scheme (2000)** | × | O | × | O | O | O | × | O | O | Fast | Moderate | High |
| **Déjà vu Scheme (2000)** | × | O | × | × | × | × | O | × | O | Slow | High | Low |
| **Triangle Scheme (2002)** | × | × | × | O | O | O | O | O | O | Fast | Moderate | Moderate |
| **Moveable Frame Scheme (2002)** | × | × | × | O | O | O | O | O | O | Moderate | Low | High |
| **Picture Password Scheme (2003)** | × | O | O | O | O | O | × | O | O | Moderate | Low | High |
| **Where Is Waldo scheme (WIW) (2003)** | × | O | × | × | × | × | × | O | O | Fast | Moderate | High |
| **Story scheme (2004)** | O | O | O | × | O | × | O | O | O | Slow | Moderate | High |
| **Convex Hull Click (CHC) Scheme( 2006)** | × | × | × | O | O | O | × | × | O | Slow | Moderate | Low |
| **Weinshall Scheme (2008)** | × | O | × | × | O | × | × | O | O | Slow | High | Low |
| **ImagePass scheme (2011)** | O | O | × | O | O | × | × | O | O | Slow | High | Low |
| **WYSWYE Scheme (2012)** | O | O | × | O | × | O | O | O | O | Slow | High | Low |
| **S-Passface Scheme (2013)** | × | O | × | O | O | O | O | O | O | Slow | High | Low |

Figure 1. The Usability Attributes on Existing Graphical password

## 4. SECURITY ASPECTS AND ATTACKS

Every authentication system should offer acceptable protection for its envisioned environment, or else it cannot satisfy its main goal. A suggested system must at least be assessed against usual attacks. Based on the standard offered by De Angeli et al. [40], we categorized the attacks on visual password into 3 groups. Guessability: The probability an attacker can guess the user's password. Observability: The probability of an attacker being able to observe the authentication Process. Recordability: The ease with which a user can record the user's 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 five kinds of attacks which are dictionary, brute force, spyware, social engineering, and shoulder-surfing. These are the present active attacks on the Recognition-Based schemes.

### 4.1. Dictionary Attack

These attacks are attempted by recognizing passwords that will be most probably selected and using them to hack the password systematically. The hackers attempt to guess the password space successfully. The ratio of success may be significantly increased by decreasing the number of probable speculations to find it. These threats can be mainly effective if ordered entries are employed to examine the most probable passwords. Recognition-based visual passwords are not as susceptible to dictionary attacks as textual passwords, because they comprise of a mouse input instead of a keyboard input. Only the Passface is not resilient against of the dictionary threat among the current techniques.

### 4.2. Brute Force (Exhaustive) Attack

These threats can be done similar to the dictionary attacks, but the difference is that every possible password is generated and used to attack the original password. These options are prioritized in much more strung threats to decrease the likelihood of being picked, if these options can be predicted whatsoever. Analogous to the dictionary threats, the Brute force attacks may be attempted either online or offline. The benefit is that a match will finally be identified with enough computing time and power (except if the location of online threat is found and halted before exhausting). But due to large password spaces, it may not be possible to be found all over the space. The exhaustive attack, unlike a dictionary threat, offers a greater coverage, yet requires more processing time or power. The main protection against such search is a password space that is large enough. Password space of textual passwords is 94^N, where 94 is the printable number of characters excluding the space and N is the length of password. Many visual password techniques provide a password space comparable to the textual passwords or bigger. Recognition-based visual passwords may have a smaller space than the recall-based methods. Compared to a textual password, it is much more difficult to attempt a brute force attack against a visual password. To create automatically precise mouse gestures to copy the user input, the attack programs are needed, which is quite challenging for the recall-based visual password.

### 4.3. Spyware Attack

In this attack, first tools are installed on the computer of the user and sensitive data is logged. This malware records any mouse or key movement. Then, the recorded data without the user's awareness is conveyed out of the computer. Apart from a few circumstances, mere use of key logging or key listening spyware does not crack visual passwords, because it is not verified whether a graphical password can be effectively cracked by the mouse spyware. Even though mouse tracing is effectively saved, it is not sufficient to discover and crack the visual password. Besides information timing, other extra data, such as window position and size, are essential to conduct this threat.

### 4.4. Shoulder Surfing Attack

Users' credentials are gained by attackers via external recording by video cameras or direct detection as the actual user calculates the information. Owing to the accessibility of high-resolution cameras with telephoto lenses and surveillance equipment, shoulder surfing is a great threat if invaders are explicitly aiming at users and can reach to geographic position of the users. In a public environment, this is mainly worrying, but in a private environment, it is a more severe threat. Like the textual passwords, most visual passwords are vulnerable to the shoulder surfing. At present, there are only few recognition-based methods to defend against the shoulder surfing. None of the Recall-based based methods is considered to be unaffected by the shoulder surfing.

### 4.5. Social Engineering Attack

These are comprising of any method that is used to tempt a person to disclose his/her credentials or private information to unreliable individuals. Phishing is an instance of social engineering using email and websites; however, it can also be implemented through false calls claiming to be from the users' credit card companies, banks or technical supports. Compared to hacking a secured system, it is easier to obtain a credential or password from a genuine. Users cannot disclose a visual password to another person as easy as a textual password. It is quite impossible, for instance, to disclose a visual password over the phone. To get a graphical password, more time is spent to prepare a phishing website.

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

| | Possible Attacks | | | | |
|---|---|---|---|---|---|
| | Dictionary Attack | Brute force Attack | Spyware Attack | Shoulder surfing Attack | Social engineering Attack |
| Passface Scheme (2000) | × | O | × | × | × |
| Déjà vu Scheme (2000) | O | O | × | O | O |
| Triangle Scheme (2002) | × | O | × | × | × |
| Moveable Frame Scheme (2002) | O | O | × | × | O |
| Picture Password Scheme (2003) | O | – | O | × | × |
| Where Is Waldo scheme (WIW) (2003) | × | O | O | × | O |
| Story scheme (2004) | × | – | O | × | × |
| Convex Hull Click (CHC) Scheme( 2006) | O | O | O | O | – |
| Weinshall Scheme (2008) | O | O | O | O | – |
| ImagePass scheme (2011) | O | O | O | × | × |
| WYSWYE Scheme (2012) | O | × | O | O | O |
| S-Passface Scheme (2013) | O | – | O | O | – |

Figure 2. The Possible Attacks on Existing Graphical password

## 5. DISCUSSION

This study revealed that several suggested Recognition-Based graphical schemes of authentication have some benefits and drawbacks. Not surprisingly, the majority of them are memorable, because the purpose of graphical passwords is to avoid the textual passwords' cognitive burdens. Usability and security are generally seen as trade-off items in a way that decreasing one inevitably increases the other. To date, most mechanisms and products for several visual password schemes only provided fixed levers. For instance, integrating additional rounds to the Passfaces rises security at the expense of extra burden of memorability, because every added round presents a new set of decoys to the users. Efficient and secure graphical password schemes permit passwords that are easy to recall but complex at the same time to resist against attacks like shoulder-surfing and engineering attacks. Login needs to be simple and quick, because it is the most usual task that authentication system users should do. Our study has shown that, when it comes to the login performance, the memorability becomes important, because it is the key factor of login success. Memorability measures deal with the issue of ability to remember passwords with different login frequencies and over long- and short terms. Although research on graphical password has focused on enhancing memorability, new usability issues have raised. For example, authentication by the users using these mechanisms takes longer time. The users mainly complain that the log-in process and password registration takes long time, particularly in-approaches based on Recognition-Based. During the registration, for example, a user must select pictures from several choices. During authentication, a user must scan several pictures to recognize pass-images, which can be long and tedious. Moreover, most of the users do not know graphical passwords; thus, graphical passwords are often less convenient to them compared to text-based passwords.Text-based passwords need much less storage space than graphical passwords; thus, huge number of images must be kept in a central database. Another concern is the delay in the network transfer, particularly for Recognition-based techniques that require display of large number of pictures for every verification round. Changing or resetting passwords are not normally inspected during testing the usability of

current visual password schemes, yet these passwords are usually essential when users fail to recall passwords.

## 6. CONCLUSION AND FUTURE RESEARCH

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. We note from Table 2 that several existing Recognition-Based graphical password schemes believed to be resistant or immune to existing attacks such as shoulder-surfing attack have significant usability drawbacks, usually in the slow login time and high login success rate required to login, and memorability problem making them less suitable for everyday authentication. This problem is especially revealed in the Recognition-Based graphical password technique, as users must select particular images that are all seen on the screen. 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 work is partially supported by grants GUP Tier 1, 2014-2015 with Vote No. 05H61, GUP Tier 1 with Vote No. 11H39, 2015-2017, and Malaysia-Japan and International Institute of Technology and (MJIIT) of Universiti Teknologi Malaysia (UTM) Research Grant with Vote No. 4J044, Ministry of Higher Education (MoHE), 2012-2017.

## REFERENCES

[1] A. P. Sabzevar and A. Stavrou, "Universal multi-factor authentication using graphical passwords," in *Proceedings of the 2008 IEEE International Conference on Signal Image Technology and Internet Based Systems*, pp. 625–632, 2008.
[2] P. Shi, *et al.*, "A PIN entry scheme resistant to recording-based shoulder-surfing," in *Proceedings of the 2009 Third International Conference on Emerging Security Information, Systems and Technologies*, pp. 237–241, 2009.
[3] L. Sobrado and J. C. Birget, "Graphical passwords," *The Rutgers Scholar, An Electronic Bulletin of Undergraduate Research, Camden New Jersey*, vol/issue: 4(2002), 2007.
[4] X. Suo, *et al.*, "Analysis and design of graphical password techniques," *Adv. Visual Comput.*, vol. 4292, pp. 741–749, 2006.
[5] T. Takada, "Fake Pointer: an authentication scheme for improving security against peeping attacks using video cameras," in *The Second International Conference on Mobile Ubiquitous Computing, Systems, Services and Technologies*, pp. 395–400, 2008.
[6] F. Tari, *et al.*, "A comparison of perceived and real shoulder-surfing risks between alphanumeric and graphical passwords," in *Proceedings of the Second Symposium on Usable Privacy and Security*, pp. 56–66, 2006.
[7] S. Wiedenbeck, *et al.*, "Pass Points: design and longitudinal evaluation of a graphical password system," *Int. J. Hum. Comput. Stud.*, vol. 32, pp. 102–127, 2005.
[8] S. Wiedenbeck, *et al.*, "Authentication using graphical passwords: effects of tolerance and image choice," in *Symposium on Usable Privacy and Security*, pp. 1–12, 2005.
[9] S. Wiedenbeck, *et al.*, "Design and evaluation of a shoulder-surfing resistant graphical password scheme," in *Proceedings of theWorking Conference on Advanced Visual Interfaces*, pp. 177–184, 2006.
[10] H. Zhao and X. Li, "S3PAS: A scalable shoulder-surfing resistant textual-graphical password authentication scheme," in *Proceedings of the 21st International Conference on Advanced Information Networking and Applications Workshops*, vol. 2, pp. 467–472, 2007.
[11] H. L. Arash, *et al.*, "Security evaluation for graphical password," 2011.
[12] N. Wright, *et al.*, "Do you see your password?: applying recognition to textual passwords," in *Proceedings of the Eighth Symposium on Usable Privacy and Security*, pp. 8, 2012.

[13] 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.
[14] L. Lazar, *et al.*, "Personalized cognitive passwords: an exploratory assessment," *Information Management & Computer Security*, vol. 19, pp. 25-41, 2011.
[15] R. Biddle, *et al.*, "Graphical passwords: Learning from the first twelve years," *ACM Computing Surveys (CSUR)*, vol. 44, pp. 19, 2012.
[16] S. Komanduri and D. R. Hutchings, "Order and entropy in picture passwords," in *Proceedings of graphics interface 2008*, pp. 115-122, 2008.
[17] A. Patrick, *et al.*, "HCI and security systems," 2003.
[18] H. Gao, *et al.*, "A new graphical password scheme resistant to shoulder-surfing," in *Cyberworlds (CW), 2010 International Conference on*, pp. 194-199, 2010.
[19] 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*, pp. 405-424, 2000.
[20] L. Sobrado and J. C. Birget, "Graphical passwords," *The Rutgers Scholar, an electronic Bulletin for undergraduate research*, vol. 4, pp. 2002, 2002.
[21] D. Davis, *et al.*, "On User Choice in Graphical Password Schemes," in *USENIX Security Symposium*, pp. 11, 2004.
[22] 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, pp. 559, 2000.
[23] R. Dhamija and A. Perrig, "D´ej`a Vu: a user study using images for authentication," *Proceedings of the 9th conference on USENIX Security Symposium*, Denver, Colorado, vol. 9, 2000.
[24] X. Suo, *et al.*, "Graphical passwords: A survey," in *Computer Security Applications Conference, 21st Annual*, vol. 10, pp. 472, 2005.
[25] A. H. Lashkari, *et al.*, "A Secure Recognition Based Graphical Password by Watermarking," in *Computer and Information Technology (CIT), 2011 IEEE 11th International Conference on*, pp. 164-170, 2011.
[26] K. U. Wei-Chi, *et al.*, "A Sector-Based Graphical Password Scheme with Resistance to Login-Recording Attacks," *IEICE TRANSACTIONS on Information and Systems*, vol/issue: 98(4), pp. 894-901, 2015.
[27] W. Jansen, "Authenticating mobile device users through image selection," *The Internet Society: Advances in Learning, Commerce and Security*, vol. 1, pp. 183-194, 2004.
[28] W. Jansen, "Authenticating users on handheld devices," in *Proceedings of the Canadian Information Technology Security Symposium*, 2003.
[29] S. Man, *et al.*, "A Graphical Password Scheme Strongly Resistant to Spyware," in *Security and Management*, pp. 94-100, 2004.
[30] A. Fulkar, *et al.*, "A study of graphical password and various graphical password authentication schemes," *World*, vol. 1, pp. 04-08, 2012.
[31] M. Hlywa, *et al.*, "Facing the facts about image type in recognition-based graphical passwords," in *Proceedings of the 27th Annual Computer Security Applications Conference*, pp. 149-158, 2011.
[32] S. Wiedenbeck, *et al.*, "Design and evaluation of a shoulder-surfing resistant graphical password scheme," in *Proceedings of the working conference on Advanced visual interfaces*, pp. 177-184, 2006.
[33] D. Weinshall, "Cognitive authentication schemes safe against spyware," in *Security and Privacy, 2006 IEEE Symposium on*, vol. 6, pp. 300, 2006.
[34] M. Mihajlov, *et al.*, "Recognition-Based Graphical Authentication with Single-Object Images," in *Developments in E-systems Engineering (DeSE)*, pp. 203-208, 2011.
[35] R. Biddle, *et al.*, "Graphical passwords: Learning from the first twelve years," *ACM Comput. Surv.*, vol. 44, pp. 1-41, 2012.
[36] R. A. Khot, *et al.*, "WYSWYE: shoulder surfing defense for recognition based graphical passwords," in *Proceedings of the 24th Australian Computer-Human Interaction Conference*, pp. 285-294, 2012.