Jurnal Teknologi

Full paper

Security Analysis Method of Recognition-based Graphical Password

Touraj Khodadadi[a*], Mojtaba Alizadeh[a], Somayyeh Gholizadeh[b], Mazdak Zamani[c], Mahdi Darvishi[d]

[a]*Malaysia-Japan International Institute of Technology (MJIIT), Universiti Teknologi Malaysia, Kuala Lumpur, Malaysia*
[b]*Faculty of Computer Science and Information Technology, Universiti Putra Malaysia, Serdang, Malaysia*
[c]*Advanced Informatics School, Universiti Teknologi Malaysia, Kuala Lumpur, Malaysia*
[d]*Faculty of Computing, Universiti Teknologi Malaysia, 81310 UTM Johor Bahru, Johor, Malaysia*

*Corresponding author: ktouraj2@live.utm.my

Article history

Received : 15 August 2014
Received in revised form :
15 October 2014
Accepted :15 November 2014

Graphical abstract

Abstract

One of the most important primitive security mechanisms is the authentication system. Authentication through the use of password is a commonly utilized mechanism for authentication of users. In general, users utilize characters as their password; however, passwords based on texts are hard to recall and if the passwords are too simple and predictable, then there is the danger of being susceptible to threats. In order to overcome the problems with authentication, an alternative and new approach has been introduced utilizing images for passwords. The idea gains support from the knowledge that the human's brain is highly capable of remembering many detailed images, however remembering texts are more difficult. Users who utilize the graphic authentication carry out certain functions on the images such as to click, drag, and movement of the mouse and so on. This research reviews several common Recognition-Based graphical password methods and analyzes their security based on the estimation criteria. Moreover, the research defines a metric that would make it possible for the analysis of the security level of the graphical passwords that are Recognition-Based. Finally, a table comparing the limits of each method based on the security level is presented.

Keywords: Security; password space and entropy; recognition-based; metrics

1.0 INTRODUCTION

Lately, network and computer security has become a formidable technical challenge. One of the main areas in the research of security is authentication, which determines if users would be allowed to access a particular resource or system. Accordingly, it is common to use a password as an authentication tool even till today, however, at present it is not a very reliable security approach. Studies at presents reveal that the key challenges of using passwords are the remembering difficulty and users often use simple passwords that they can recall easily; however, these passwords are often predictable and risky. On the contrary, having a complicated password would mean that it would be difficult to recall [1, 2, 3]. One suggestion is the graphical password method as a potential alternative method compared to the text-based method partly due to the notion that people can recall images easier than texts. Users do not have to remember a long string of characters; users can just recall the set image password to be authenticated [4, 5].

Furthermore, when the possible quantity of images is large enough, the potential space for the graphical password method would be far larger than that used for a text-based method. The method of graphical password offers a higher security level compared to the text-based method. Graphical User Authentication Algorithm are divided into two categories namely Recall-based and Recognition-based. In the Recognition-based method, users are offered a set of images and users are authenticated by recognizing and identifying the image they had chosen while registering. In the Recall-based method, users are required to reproduce the image that they had chosen or created while registering. This research paper concentrates on the former Recognition-based method because the chances of creating a weak password are high using Recognition-Based passwords [6, 7, 8, 9, 10]. The work by Davis, *et al*. [11] found obvious patterns among the PassFace password. For example, most users tend to choose faces of people from the same race.

2.0 PRESENT RECOGNITION-BASED GRAPHICAL PASSWORD SCHEMES

2.1 Passface Scheme

Passfaces are the most commonly used choice-based method [12]. Users utilizing this method are required to select from a selection of images of faces for the purpose of authentication (refer Figure 1). This stage of selecting the faces is carried out several times to make sure that the space for the password is sufficiently large. Brostoff and Sasse [9] carried out studies in their laboratory and it was documented that Passfaces users could remember their

passfaces better than that those who used the text-based passwords. They also examined the Passface system and found that the users of the Passfaces took much longer to login in comparison to the normal password users. They found that users did not favor using Passface since the main login elements and the remembrance levels (memorability) and recall levels were the same as those using the normal text-based password. There are some disadvantages attached to this algorithm much like all the other authentication methods. First of all, after a password is chosen using the mouse device, it is easy for those with malicious intent to look at the password. Secondly, it is time taken during the login process, which is long, and during the registration stage which is also a long process which makes the algorithm to be slower compared to the text-based system.

Figure 1 A Sample of passface scheme [12]

2.2 Déjà Vu Scheme

The déjà vu algorithm was developed by Dhamija [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 (refer Figure 2). 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 [12]. 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, 15]. 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 [4, 12].

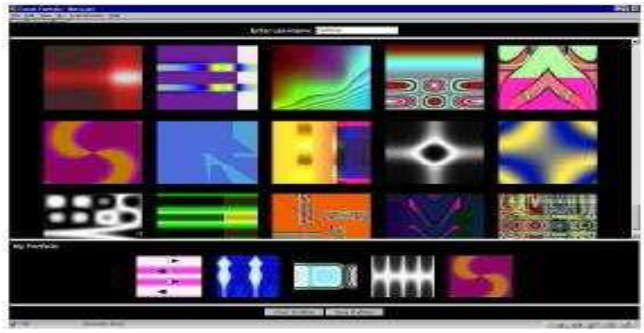

Figure 2 A Sample of déjà vu scheme [13]

2.3 Triangle Scheme

Sobrado and Briget [10] introduced an algorithm to overcome the problem of shoulder surfing security issue. Users in this algorithm are required to select the pass-images that were chosen at the registration stage out of a set of objects that are displayed. Users utilizing this algorithm have to click the inner part of the convex hull that shapes the pass-object (refer Figure 3). This algorithm’s author proposed that the objects that are displayed during the login phase ought to be raised to one thousand objects to enable the password space to be big enough and harder to predict. The algorithm proposes that users should discover just 3 of the pass-objects out of all the objects that are displayed to formulate a triangle form in order for authentication to take place. When conducting it for real, the amount of objects must be scattered randomly on the computer screen and the objects must vary sufficiently so that users would be able to differentiate them. This algorithm’s disadvantage is that if there are too many objects that are displayed, it would be harder for the users to pin point the pass-objects and if there too few objects, then the space used will be smaller and hence become simpler to predict or hack.

Figure 3 A Sample of triangle scheme [10]

2.4 WIW Scheme

Man, *et al*. [16], 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.

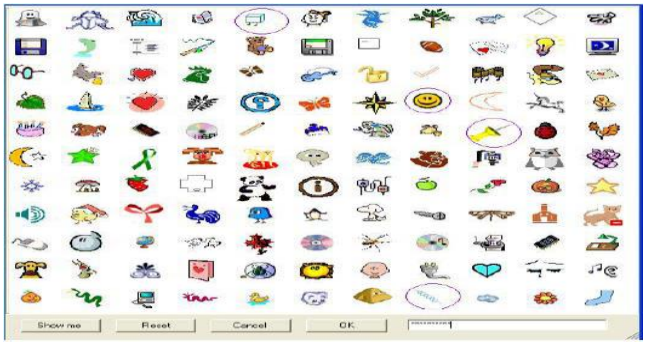

Figure 4 A sample of WIW scheme [16]

2.5 Picture Password Scheme

The picture password [17, 18] was developed particularly for devices that are handheld such as Personal Digital Assistants or PDAs. Figure 5 demonstrates that while registering for the first time, users choose a theme to identify the thumbnail pictures that would be utilized and after that register the arrangement of the thumbnail pictures to be utilized as the password from here on end. When the handheld device is turned on, users must enter the correct arrangement of the pictures and the users can change the passwords after they have successfully logged in. In this method, the number of images are only 30 so the space used is small [19]. To overcome this problem, another stage was added to the algorithm by the designer. Here, the users are able to choose two thumbnails simultaneously to create the new alphabet component by utilizing the shift keys to choose special characters or the uppercase. It is more complicated to memorize the password especially after the second stage that assists in the space problem is added to the whole process.

Figure 5 A sample of picture password scheme [17]

2.5 Imagepass Scheme

In a study by Mihajlov [20], 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.

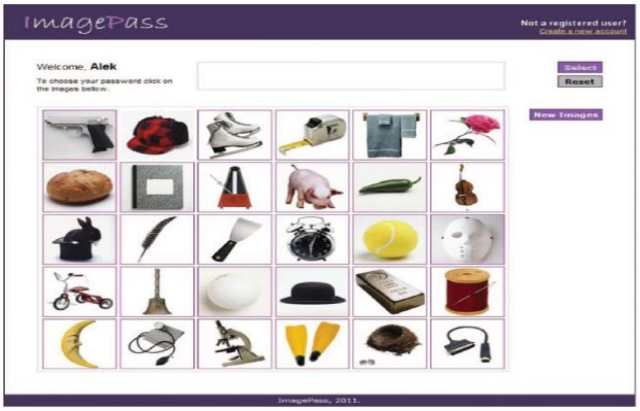

Figure 6 A sample of imagepass scheme [20]

2.6 WYSWYE Scheme

According to Khot *et al*. [21], 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 × M grid (where N < M) and then maps the pattern of password images that have been identified onto an N × 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 7. The image grid on the left hand side M × M is called the Challenge grid and it has the N password images and the M2-N images for decoy. This grid is not directly utilized by the users. A

separate N × 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.

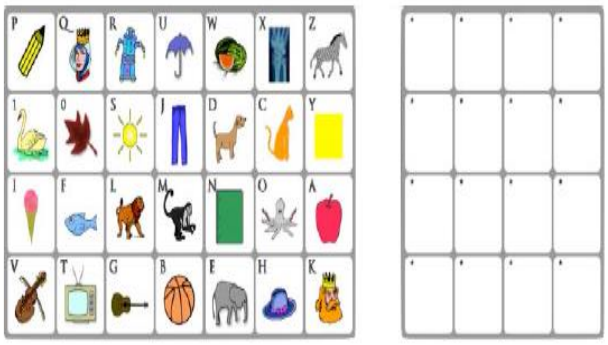

Figure 7 A sample of WYSWYE scheme [21]

■3.0 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 based on the Common Attack Pattern Enumeration and Classification (CAPEC) and three aspects of password security which are observability, recordability, and guessability. The possible attacks are mapped to the Recognition-Based schemes in Table 1. 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.

3.1 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.

3.2 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 [23]. 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.

3.3 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 [24, 25]. 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.

3.4 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.

3.4 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.

3.5 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.

■4.0 EFFECTIVE LEVEL OF SECURITY

4.1 Password Space

A user can choose any feature as password in the GUA. The password space's raw size is the upper part of the content of the information in the distribution that are used by users in real time. A formula for the password space cannot be defined but one can measure the password space or the amount of passwords that can be created using this algorithm [25, 26]. The following part will describe and measure the password for the past algorithms. The techniques based on recognition in the password space are mainly dependent on the content size. Many of the techniques based on recognition do not pay attention to the selection's order or sequence. The normally include a lot of stages of authentication where the user has to go through a few pages of images. The space for password for the technique based on recognition is provided below; it is assumed that an image can be chosen more than a single time. In the below formula, Y is the total number of pictures, Z is Password length and X is the maximum password length.

$$Passowrd\_Space = \sum_{z=1}^{x} \binom{y+z-1}{y-1} = \sum_{z=1}^{x} \frac{(y+z-1)!}{z!\,(y-1)!}$$

4.2 Password Entropy

The password entropy is normally utilized to calculate the security of a password that is developed, which really relates to how difficult it would be to predict a password [28]. To make the matter easier to understand, it is assumed that all passwords are distributed evenly; the password entropy of a password with a graphic image can then be measured. Likewise, the Graphical password entropy attempts to calculate the probability that the hacker would be able to find the right password using random prediction. In the below formula, N is the length or number of runs, L is locus alphabet as the set of all loci, O is an object alphabet and C is colour of the alphabet.

$$Password\_Entropy = N \log 2\ (|L||O||C|)$$

■5.0 DISCUSSION

Nowadays, graphical password has not been widely used in practical. Most of the graphical password authentication schemes are only discussed in laboratory. In our findings we can see that authentication process is slower in graphical password. Security of graphical passwords is a main challenges for researchers. Also our experience has demonstrated that the design of successful authentication mechanism is a complex task, as it requires considering and weighting several important factors to reach maximum level of security. It is possible to measure the level of security of a recognition-based graphical password scheme in a way which can accurately predict resistance to identified potential attacks.

The identified potential attacks are based on the Common Attack Pattern Enumeration and Classification (CAPEC) and three aspects of password security established by De Angeli *et al*. [27]: observability, recordability, and guessability. Observability relates to the ease with which an attacker can view the graphical password as it is being entered. Guessability relates to how easily the attacker can guess the graphical password. Finally, recordability relates to the ease with which the user can record the graphical password, making it easier for the attacker to capture and replay. Each of these aspects have been analysed to highlight the potential attacks which would exploit vulnerabilities. The possible attacks are mapped to the Recognition-Based schemes in Table 1. During our analysis we found that it is very difficult to perform attacks on graphical passwords like brute force, Dictionary attack, and spyware.

Table 1 Comparison of typical recognition-based schemes

Methods	Security issues	
	Authentication process	Possible attack methods
Passface	User needs to select four pictures of human face from the nine pictures to be authenticated.	Dictionary attack, brute force , guess , shoulder surfing
Déjà vu	Authentication process is based on Hash Visualization technique. User needs to pick several pictures out of many choices. The users must recall all their portfolio images and displayed is only one panel.	Brute force , guess, shoulder surfing
Triangle	Users in this scheme are required to select the pass-images that were chosen at the registration stage out of a set of objects that are displayed and click the inner part of the convex hull that shapes the pass-object.	Brute force, guess,
Picture Password	Users choose a theme to identify the thumbnail pictures that would be utilized and after that register the arrangement of the thumbnail pictures to be utilized as the password from here on end.	Brute force guess, shoulder surfing
WIW	Users in this scheme are required to select several pictures as pass-objects. Each pass-object has several variants and each variant is given a unique code.	Brute force, spyware
ImagePass	select a username, a 6x5 grid with a graphical password selection which reveals the images possible to be selected	Brute force , shoulder surfing
WYSWYE	Users need to select N images of passwords within the M × M grid (where N < M)	Brute force, shoulder surfing, guess

6.0 CONCLUSION

The past decade has seen a growing interest in using graphical passwords as an alternative to the traditional text-based passwords. We believe that main reason for using graphical password is they can be easily recalled. Furthermore, graphical passwords are more secure than text based passwords. In this paper, we have conducted a comprehensive study and focuses on security aspects of existing Recognition-Based algorithms and try to define their security features and attributes. This study first introduced some typical Recognition-Based graphical passwords authentication schemes. Then under its estimate criterions, the security analysis of graphical passwords was given. In addition, we try to define tow method, password space and password entropy which would allow analysis of the level of security of Recognition-based graphical passwords. Finally, a comparison of current typical graphical password techniques is presented in Table 1 based on their authentication process and possible attack methods.

References

[1] S. Komanduri and D. R. Hutchings. 2008. Order and Entropy in Picture Passwords. In Proceedings of Graphics Interface 2008. 115–122.

[2] A. Patrick, A. C. Long, and S. Flinn. 2003.. HCI and Security Systems.

[3] H. Gao, Z. Ren, X. Chang, X. Liu, and U. Aickelin. 2010. A New Graphical Password Scheme Resistant to Shoulder-Surfing. In Cyberworlds (CW), 2010 International Conference on. 194–199.

[4] Farnaz Towhidi, Maslin Masrom. 2009. A Survey on Recognition-Based Graphical User Authentication Algorithms. *International Journal of Computer Science and Information Security*. 6(2).

[5] N. Wright, A. S. Patrick, and R. Biddle. 2012. Do You See Your Password? Applying Recognition to Textual Passwords. In Proceedings of the Eighth Symposium on Usable Privacy and Security. 8.

[6] Z. Erlich and M. Zviran. 2009. Authentication Methods for Computer Systems Security. Encyclopedia of Information Science and Technology. 2nd ed. 1: 288–293.

[7] L. Lazar, O. Tikolsky, C. Glezer, and M. Zviran. 2011. Personalized Cognitive Passwords: An Exploratory Assessment. *Information Management & Computer Security*. 19: 25–41.

[8] R. Biddle, S. Chiasson, and P. C. Van Oorschot. 2012. Graphical Passwords: Learning from the First Twelve Years. ACM Computing Surveys (CSUR). 44(19).

[9] S. Brostoff and M. A. Sasse. 2000. Are Passfaces More Usable Than Passwords? A Field Trial Investigation. In People and Computers XIV—Usability or Else! ed: Springer. 405–424.

[10] L. Sobrado and J.-C. Birget. 2002. Graphical Passwords. The Rutgers Scholar, An Electronic Bulletin for Undergraduate Research. 4.

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

[12] R. Biddle, S. Chiasson, and P. C. Van Oorschot. 2009. Graphical Passwords: Learning from the First Generation. Technical Report TR-09-09, School of Computer Science, Carleton University.

[13] R. Dhamija and A. Perrig. 2000. 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.

[14] X. Suo, Y. Zhu, and G. S. Owen. 2005. Graphical Passwords: A Survey. In Computer Security Applications Conference, 21st Annual. 10: 472.

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

[16] S. Man, D. Hong, B. Hawes, and M. M. Matthews. 2004. A Graphical Password Scheme Strongly Resistant to Spyware. In Security and Management. 94–100.

[17] W. Jansen. 2004. Authenticating Mobile Device Users Through Image Selection. *The Internet Society: Advances in Learning, Commerce and Security*. 1: 183–194.

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

[19] A. Fulkar, S. Sawla, Z. Khan, and S. Solanki. 2012. A Study of Graphical Password and Various Graphical Password Authentication Schemes. *World*. 1: 04–08,

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

[21] R. A. Khot, P. Kumaraguru, and K. Srinathan. 2012. WYSWYE: Shoulder Surfing Defense for Recognition Based Graphical Passwords. In Proceedings of the 24th Australian Computer-Human Interaction Conference. 285–294.

[22] M. Hlywa, R. Biddle, and A. S. Patrick. 2011. Facing the Facts About Image Type In Recognition-Based Graphical Passwords. In Proceedings of the 27th Annual Computer Security Applications Conference. 149–158.

[23] S. Wiedenbeck, J. Waters, L. Sobrado, and J.-C. Birget. 2006. Design and Evaluation of a Shoulder-Surfing Resistant Graphical Password Scheme. In Proceedings of the Working Conference on Advanced Visual Interfaces. 177–184.

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

[25] Suo, X., Y. Zhu, and G. S. Owen. 2006. Analysis and Design of Graphical Password Techniques. Proceedings of the 2nd International Symposium, Advanced in Vis. Comp., Nov. 6–8, Springer, Berlin Heidelberg. 4292: 741–749.

[26] Lashkari, A. H., *et al.* 2009. Shoulder Surfing Attack in Graphical Password Authentication. *International Journal of Computer Science and Information Security (IJCSIS).*

[27] A. De Angeli, L. Coventry, G. Johnson, and K. Renaud. 2005. Is a Picture Really Worth a Thousand Words? Exploring the feasibility of graphical authentication systems. *International Journal of Human-Computer Studies*. 63: 128–152.

[28] Lashkari, A. H., *et al.* 2011. Security Evaluation for Graphical Password, in The International Conference on Digital Information and Communication Technology and its Applications (DICT AP2011).