AENSI Journals

Australian Journal of Basic and Applied Sciences

ISSN:1991-8178

Journal home page: www.ajbasweb.com

A Hybrid Graphical Password Scheme for High-End System

Liew Tze Hui, Housam Khalifa Bashier, Lau Siong Hoe, Wee Kuok Kwee, Md Shohel Sayeed

Faculty of Information Science & Technology, Multimedia University, Melaka-Malaysia.

ARTICLE INFO

Article history:
Received 25 December 2013
Received in revised form 22 February 2014
Accepted 26 February 2014
Available online 15 March 2014

Keywords:
Graphical Password, Authentication, Security

ABSTRACT

Background: Password is an important concept in information security application. Nowadays; a strong password should have included alphabet, numeric and special character to ensure that the password cannot be easily hacked. However, past researches shown that a graphical password scheme have a better security and easier to remember features compare to textual password. In this paper, we propose a new reliable and secure graphical password scheme for high end system. Our new scheme is based on the combinations of different schemes into one to form a secure authentication algorithm. The experiments results demonstrated the effectiveness of the proposed algorithm. Moreover, the complexity and combination of this password suggest that it's extremely difficult to be broken. Our prototype proved that the password consist of graphics has more combination and therefore, extremely difficult to be hacked, but with the hints, it's easy for the assigned user to remember.

To Cite This Article: Liew Tze Hui, Housam Khalifa Bashier, Lau Siong Hoe, Wee Kuok Kwee, Md Shohel Sayeed., A Hybrid Graphical Password Scheme for High-End System. ***Aust. J. Basic & Appl. Sci.,*** *8(2): 23-29, 2014*

INTRODUCTION

Graphical password schemes started around 1999 as an alternative solution to text based password. The reason is that, human memory finds difficulties in remembering and memorizing text-based password; as a result users tend to choose easy password. On the other hand, there are many drawbacks for text-based password (H. Rowley *et al, 2002).*

The main goal of authentication is to provide adequate security for its intended environment. The conventional way of verification/authentication system is by asking a legitimate user to input in his/her username and password. This scheme is well developed and used in many systems for instance browsers, applications that use multi-touch technology (large displays in public spaces) and ATM machines. However, there are many weaknesses for such a system; for example passwords can be easily guessed by an attacker and also vulnerable to spyware and key-logger attacks. Furthermore, Researchers showed that legitimate users tend to choose easy password (Adam and Sasse., *1999).*

Generally, graphical password is simply an authentication method which uses pictures as password instead of the traditional alphanumerical passwords. So during the login session, the system presents a set of pictures and then asks the user to select the pass-image. Psychology studies suggested that human brain is better in recognizing images; thus graphical password is proposed as an alternative solution to text-based password. However, shoulder surfing problem remained a challenge and need to be considered when working in graphical password (wu *et al*, 2013).

Past research had proven that alphanumerical password is very easy to be hacked compare to graphical password (*Biddle et al, 2011*). As an example, if we have 100 pictures for a graphical password system then the user is required to choose 8 pass-images, then there are 100^8 possible combination. If we use this example for high-end system with a built-in delay of only 0.1 second following the selection of each image until the selection of the next page, it would take millions of years to break into the system by hitting it with random image sequences. Therefore, hacking by random combination is impossible.

Therefore, the main focus of this paper is to examine a graphical password scheme that uses pictures as password instead of alphanumerical string. The main argument is that human brain is better in recognizing and memorizing pictures compared to text based password and it's very difficult to steal images with the elimination of shoulder surfing problem.

In this paper, we proposed a new hybrid scheme for high-end system; our method is based on applying different technique as one solution, so that we can increase the security level for high-end applications.

Corresponding Author: Liew Tze Hui, Faculty of Information Science and Technology, Multimedia University, Jalan Ayer Keroh Lama, 75450 Melaka, Malaysia.
E-mail: thliew@mmu.edu.my

Related Work:

Graphical password can be classified into two types; recall based and recognition based approaches (Jemyn *et al*, 1999). In the recall based approach, a legitimate user is required to generate/reproduce an event or to select something he/she has chosen during the registration phase. However, the major weakness in this approach is that it relies heavily on the precise recall of the secret information. Therefore, if the user makes an error during the log in session; the authentication fails (Dhamija and Perrig, 2000). Moreover, (Jemyn *et al*, 1999) proposed a solution called (DAS). In this solution, the user is asked to draw a pattern or a picture in order to be verified. At the server side, the system verifies the coordinates of the grids and if grids are the same in the same sequence, the user is verified and access will be granted.

In 2004, authors proposed an improved version of DAS which is a Grid Selection (Thrope *et al*,2004). The difference is users need to determine a drawing grid; this is means that the password space will gradually increase. Moreover, there are others solutions for instance pass-Go (Tao *et al*, 2008) and BDAS (Dunphy *et al*, 2008).

Another method was developed by wiedenbeck *et al*, in their approach the legitimate user is supposed to choose a pre-registered point in the test image (Wiedenbeck *et al*, 2005). However, it's easy for observers to see the input password.

On the other hand, Recognition approach is quite applied and developed. The main idea in this approach is that, there will be a challenge set which contains a set of pictures (decoy images and pass-images). The decoy pictures are randomly produced by the algorithm during the authentication session. As for the pass-images, it will be the users selected pictures (user password). The authentication is straightforward; the user needs to recognize all the presented images in the challenge set.

In (Dhamija and Perrig, 2000) authors proposed an algorithm named Deja Vi, this scheme relies on a hash visualization algorithm which produces random pictures (abstract). On the other hand, the user is required to recognize the pass-images from a challenge set in order to be verified.

The other considerable work is proposed by (Harada *et al*, 2004), simply their algorithm generates a monochrome from the legitimate user pass-images and the idea here is to make the pictures look noisy as shown in Fig.1. Both the decoy and the pass-images are processed by an alpha blending algorithm. The problem in this method is that the images look unclear and noisy which makes it difficult for users to recognize their pass images as shown in Fig.1 and also the authentication takes much time.

Fig. 1: A scheme proposed by (Harada *et al*, 2004) (from left to right: Foreground, middle: background blended unclear image).

Another work proposed by the researcher in (eiji *et al*, 2008) in Fig2, used an oil filter to degrade pass-images and decoy images. The concept here is that users can identify a degraded version of a previously seen clear image. However, observers can still see the degraded version and also pass-image will be difficult to remember. Furthermore, authors in (Bashier, *et al*, 2013) proposed a graphical password scheme based on applying image processing algorithm to the input pass-image.

Fig. 2: A graphical password method proposed by (eiji *et al*, 2008).

GOTP (One Time Password generator) (CDTI, 2007)is an experimental application proposed by Safe layer that uses the new mechanism based on one-time passwords generated from graphical passwords that are far more secure and easy to use with compare to text-based. Another solution proposed in (passfaces, 2000), named passface; in this scheme authors rely on using human faces for authentication. The statement here is easy for the user to remember a face picture. In addition, there are others graphical password methods proposed for touch screen and mobile d*evices using the same scheme (Chang et al, 2012) (Chinag et al, 2013).*

Proposed Scheme:

In this section we study the proposed solution; our idea is based on allowing the legitimate users to decide which password is comfortable for them in order to remember and at the same time imposed some restriction for the password chosen by the user to maintain high security level.

The scheme relies on the psychology studies which say that pictures that are generated by users are better than those that are not. Moreover, users will find it interesting to select their pass-images. The aim of the design of the graphical user interface (GUI) of the prototype is to make it as easier as possible for the user. It include the username text field, check button, checkbox options of the methods, images, rotate buttons, resize dropdown menus, login and cancel button.

The solution combines many features such as applying blurring, sequence, rotation and resizing to the input image. This will greatly increase the security level of the system.

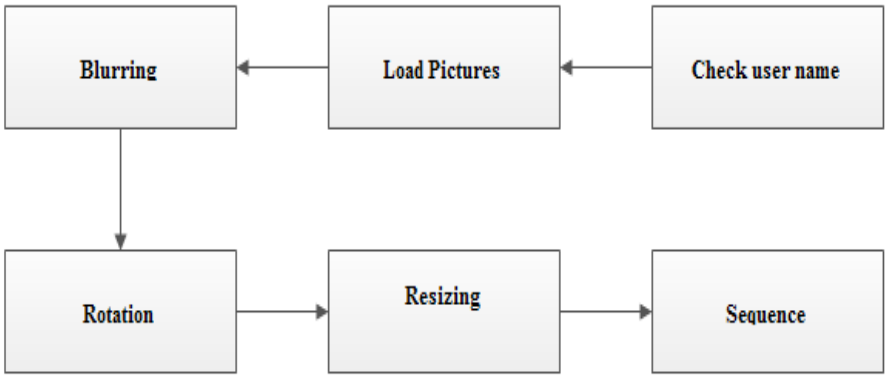

Fig. 3: Scheme Flow Chart.

The first input is the username; therefore our scheme will verify the username first.

Next, the random load function will be called; the system will randomly load the images from the database after users have typed in their username.

One of the major disadvantages of graphical password is shoulder surfing problem, easy for legitimate user to remember, also mean easy for others to remember and steal. This means direct observation techniques such as looking over someone shoulders to get information. For example, if there is someone stands beside the user during their login process, the graphical password may easily been stolen. In order to eliminate shoulder surfing problem, the blurring methods had been included in the system to prevent any attempt to steal password through shoulder surfing. Once the images loaded into the system, it will immediately become blurred. This can prevent the particular images seen by others. Legitimate users may also choose to disable the blurring methods afterwards.

Right after the blurring process, we proceed for the next step which is the graphic rotation step. There are a total of 8 options for different angle to let users choose in the system. Each image requires matching its preset angle in the database.

To make the system more secure, we had introduced the concept of resizing on the input pictures. Resize means resemble the size of each image to either small, medium which is the original size, or large. The size of the resized image also needs to match the preset size in the database.

Finally, sequences refer to the sequence of the images. Every time during the login process, users require to reallocated the sequence of the images until it match the preset sequence in the database. The system provides the option to let users choose either one of the method or combine two or more methods together. Combination of more methods will greatly increase the time requires for the attacker.

The aim of the design of the graphical user interface (GUI) is to give users as much convenient as possible. It includes the username text field, check button, checkbox options of the methods, images, rotate buttons, resize dropdown menus, login and cancel button as shown in the below figure.

The users need to type in their username. After that, the check button will be used to check either the user's username exist in the database or not. The images will be loaded if the username exist. The checkbox option gives users to choose which methods they have included in their preset data. The user is required to follow the methods they used in their registration phase in order to pass the authentication process. Rotate button used to rotate images and resize dropdown menus provide 3 options which are small, medium, and large for user to choose. After users finish input their data, login button will be used to check either the authentication process is success or not. Cancel button can be used to quit the program.

MD5 Hash will be used to encrypt the data such as sequences, rotated angle and size of the images before storing into the database. When users want to login to the system, they required to recall the sequence, rotate and resize the images. The input data will be hashed again and compared to the hash stored inside the database.

If the sequence method is chosen by the users, the data of all images will be combined in one string and hashed. If the hash matches the other hash inside the database, then the authentication processes is success. In the other hand, if the sequence method is not chosen, the data of each image will be hashed separately and compared one by one to the hashes inside the database. The authentication processes will only success when all of the hashes are matched. Therefore, introducing the hashing increases the security of the proposed solution. Moreover, it's very difficult for the attackers to get the plaintext from the hashed data.

Fig. 4: Proposed Login.

In order to make the scheme more convenient for users, we introduce the below table and diagram to help the users recall their pass-images size and rotation.

Table 1: Hints.

Age	Image Size
10-25	Small
26-35	Medium
36-60	Large

We relied on the user's birthday to determine the angle as shown in Fig5. This is an attempt to combine biological data with graphical images for ease of memorability.

Experiments and Results:

The aim of the experiments is to prove the following 3 points: i) Memorability ii) Usability of the proposed solution. And iii) Security.

Memorability:

Below table illustrate the results of our evaluation, we have asked the users to determine after they have tested the system, whether is easy to understand and remember the password. The average result obtained is quite satisfactory for both memorability and understanding even though this system is mainly designed for high-end system.

Table 2: Understanding and memorability.

User	Experiment 1	
	Understanding	Memorability
1	5	4
2	4	4
3	5	4
4	5	4
5	3	3
6	5	4
7	5	5
8	4	4
9	3	2
10	5	3
Average	4.4	3.7

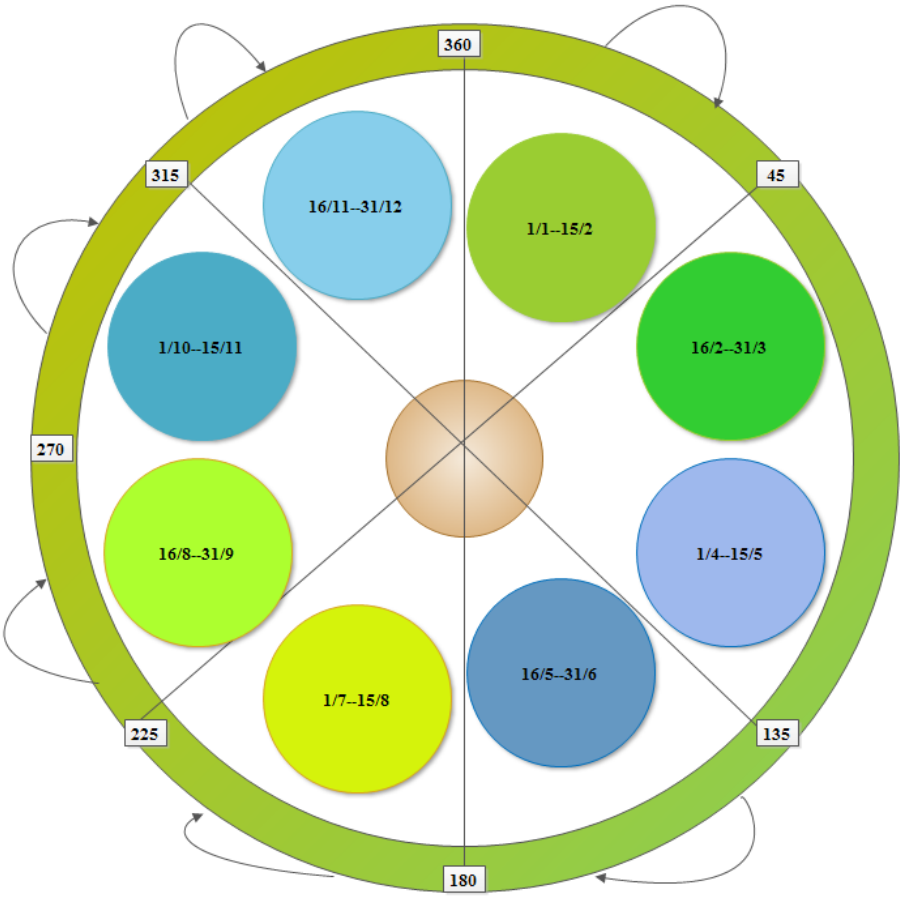

Fig. 5: Rotation hint.

Understanding:
5=Understood completely; 1=Do not understand at all
Memorability
5=Very memorable; 1=Not memorable at all

We have found that more than half of the examined users have memorized their assigned password and their ratio is about 60% to 100%. This indicates that the system is eligible to be memorized by the users and the difficulty will be faced only by minority of users.

Usability:

The next experiment we have conducted is to evaluate whether this scheme can be used for high-end system or normal applications. From the feedback we have received from the users 70% of them said that the system is better for high end system where's 30% of them said it is better for end users. We can conclude from that, majority of the users agreed to use this scheme for high-end. The system was intermediate in usage for the majority of the users by about 60%, where a 30% of them found it hard. And only 10% said it's easy as shown in table 3.

Table 3: Evaluating the scheme.

	What do you think the system should work?		*How difficult is the possessed scheme?*		
	High-end system	End user system	hard	Intermediate	Easy
User1	✓			✓	
User2	✓			✓	
User3	✓			✓	
User4		✓		✓	
User5		✓			✓
User6	✓		✓		
User7	✓		✓		
User8	✓		✓		
User9		✓		✓	
User10	✓			✓	

Table 4 shows that, the learning process takes on average of 2.63 min to understand the whole system. From this study, the users do not depend on their age instead of their ability to memories the pictures and moreover the learning process also varies based on the difficulty of the passwords.

Table 4: Learning Time vs. Age.

User	Learning Time	Age
1	02:21	25
2	01:59	20
3	02:45	23
4	02:30	24
5	03:36	23
6	02:55	26
7	03:34	22
8	03:00	27
9	02:48	21
10	03:00	28
Average	02:63	23.9

Table 5: Learning Time vs. Age.

	Login Time Experiment 1	Remarks	Login Time Experiment 2	Remarks	age
1	00:32	yes	01:35	Failed remember	25
2	00:30	yes	00:45	yes	20
3	00:31	yes	01:25	yes	23
4	00:47	yes	00:50	yes	23
5	01:02	yes	00:45	yes	27
6	01:40	yes	00:50	yes	22
7	01:45	yes	01:02	yes	28
8	00:42	yes	00:35	yes	24
9	02:50	yes	00:28	yes	21
10	00:25	no	1:23	yes	26
Average time	01:01		01:14		

The difference between average of the two experiments in table 5 is because users were exposed to the system and ask to login immediately at the second experiment. The user needs to recall the password as shown in the above table.

The successful login for the users was 90% for first and second experiment. Users with background in computer found it easy to login with compare to others.

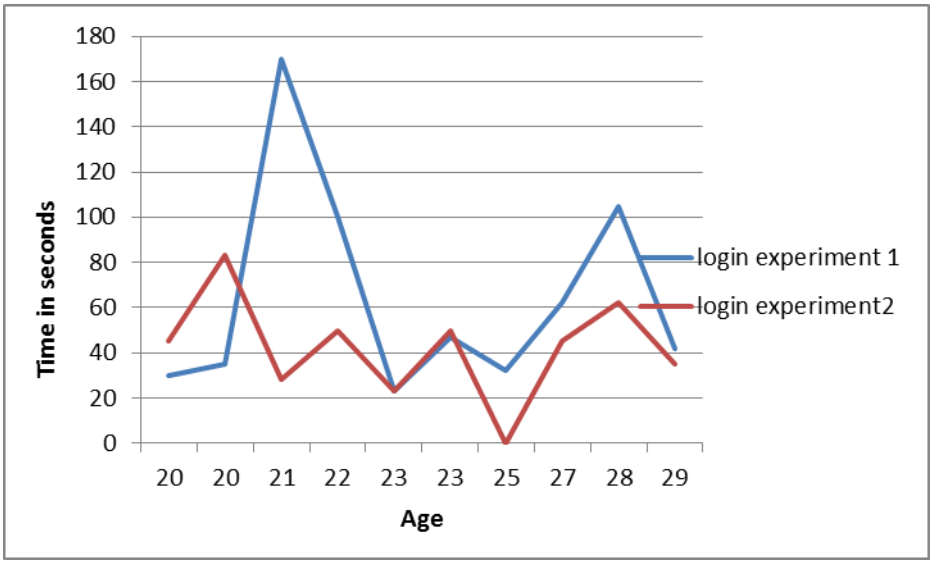

Fig. 6: Authentication time vs Age.

From Fig6, the variation seen in login time for the two experiments is because of the need for users of more time to login to the system in the second experiment. 40% of users have taken less time to login for the second experiment 10 % have failed to login. Moreover, Zero seconds for login time means the user failed to login.

Conclusions:

The combination of several methods greatly increases the security level of the system. The time requires by the attacker to break into the system will be longer due to the larger possibilities of password combination. Furthermore, the scheme is easy to be used when users follow the rotation angle and the table for image size; this solution makes it easier for user to use the scheme.

REFERENCES

Adams and M.A. Sasse, 1999. "Users are not the enemy: why users compromise computer security mechanisms and how to take remedial measures," Communications of the ACM, 42: 41-46.

Atsushi Harada, Takao Isarida, Masakatsu Nishigaki, 2004. "A proposal of user authentication using mosaic images," Proc. of Computer Security Symposium, pp: 385-390.

Bashier, H.K., L.S. Hoe, P.Y. Han, 2013. Graphical Password: Pass-Images Edge Detection.Signal Processing and its Applications (CSPA), 2013 IEEE 9th International Colloquium on 8-10.

Biddle, R., S. Chiasson and P. van Oorschot, 2011. Graphical Passwords: Learning from the first twelve years. ACM Computing Surveys, 44.

Chang, Ting-Yi, Cheng-Jung Tsai and Jyun-Hao Lin, 2012. "A graphical-based password keystroke dynamic authentication system for touch screen handheld mobile devices." Journal of Systems and Software, 85(5): 1157-1165.

Chiang, Hsin-Yi and Sonia Chiasson, 2013. "Improving user authentication on mobile devices: A touchscreen graphical password." Proceedings of the 15th international conference on Human-computer interaction with mobile devices and services. ACM.

Dunphy, Paul and Jeff Yan, 2007. "Do background images improve Draw a Secret graphical passwords?." Proceedings of the 14th ACM conference on Computer and communications security. ACM.

Eiji Hayashi, Nicolas Christin, Rachna Dhamija, Adrian Perrig, 2008. "Use Your Illusion: Secure Authentication Usable Anywhere," Proc. of the 4th symposium on usable privacy and security (SOUPS08), pp: 35-45.

Jermyn, I., A. Mayer, F. Monrose, M.K. Reiter and A.D. Rubin, 1999. "The Design and Analysis of Graphical Passwords," in Proceedings of the 8th USENIX Security Symposium.

Passfaces. 2000. Example of graphical password http://www.realuser.com/index.htm.

Dhamija, R. and A. Perrig, 2000. "Déjà vu: A user study, using images for authentication," Proc. 9th USENIX Security Symposium, August.

Wiedenbeck, S., J. Waters, J.C. Birget, A. Brodskiy and N. Memon, 2005. "Authentication using graphical passwords: Basic results," in Human-Computer Interaction International (HCII 2005), Las Vegas, NV.

Spanish government's Center for the Development of Industrial Technology (CDTI, Centro para el Desarrollo Tecnológico Industrial). 2007. gOTP - OTP generator for iPhone by Safelayer. http://sandbox.safelayer.com/en/experimental-applications/1-semantic-web-trust-portal/465-gotp-otp-generator-for-iphone.

Tao, Hai and Carlisle Adams, 2008. "Pass-Go: A Proposal to Improve the Usability of Graphical Passwords." IJ Network Security, 7(2): 273-292.

Thorpe, Julie and Paul C. van Oorschot, 2004.. "Towards secure design choices for implementing graphical passwords." Computer Security Applications Conference, 2004. 20th Annual. IEEE.

Wu, Tzong-Sun, *et al*., 2013. "Shoulder-surfing-proof graphical password authentication scheme." International Journal of Information Security, 1-10.