Graphical Password: Usable Graphical Password Prototype

Ali Mohamed Eljetlawi[1], **Norafida Bt.Ithnin**[2]

1- Faculty of Computer Science and Information Systems,
Centre for Advanced Software Engineering (CASE),
Universiti Teknologi Malaysia, City Campus, Jalan Semarak,
54100 Kuala Lumpur, Malaysia.
2- Faculty of Computer Science and Information Systems, Universiti Teknologi Malaysia, 81300 Skudai, Johor.
Email: jetlawei@yahoo.com1, afida@utm.my2

Abstract. Recently, graphical passwords have become a viable alternative to the conventional passwords due to their security and usability features. However, there are very limited researches in classifying, analyzing and development of the graphical password techniques. In this paper, we will propose a new usable graphical password prototype of the recognition base graphical password. In this design we will focus on the usability features of the system to give new usable graphical password system. Graphical passwords schemes are an alternative authentication method of the conventional password scheme in which users click on images to authenticate themselves rather than type the conventional passwords as letters or numbers or mixed. This research aims to design and come out with a new usable graphical password prototype with the major important usability features. In this paper we will focus on implementation of the usability features on the new graphical password prototype design. This usability set includes the easy of use, memorize, creation, learning and satisfaction. Moreover, this work proposes to build a new system of graphical password system that provides promising usability features.

1.0 Introduction

The password is a very common and widely authentication method still used up to now but because of the huge advance in the uses of computer in many applications as data transfer, sharing data, login to emails or internet, some drawbacks of normal password appear like stolen the password, forgetting the password, week password, etc so a big necessity to have a strong authentication way is needed to secure all our applications as possible, so researches come out with advanced password called graphical password techniques where they tried to improve the password techniques and avoid the weakness of normal password. Alphanumeric passwords were first introduced in the late 1960s (Sobrado and Birget, 2002), today, many networks, computer systems and Internet-based environments used this technique to authenticate their users. The vulnerabilities of this technique have been well known generally. Dictionary attack is the commonly method used by hackers to break or crack the alphanumeric password, such attack is very efficient mechanism because its only need a little time to discover the users passwords. Another major drawback of this method is the difficulty of remembering the passwords. As studied by Gilhooly (2005), the good and hard to guess or break passwords basically difficult to memorize. Recent studies from Dhamija et al (2000) showed that humans are only capable to memorize a limited number of passwords, because of this syndrome, they often to write down, share and use the same passwords for different current account. Graphical password techniques have been proposed as an alternative to conventional based techniques. It has been designed to overcome the known weakness of conventional password. It also designed to make the passwords more memorable, easier for people to use and therefore more secure. Based on the two assumptions; first, humans can remember pictures better than alphanumeric characters and second, a picture worth a thousand passwords; some psychological studies and company software seem to agree with these assumptions (Shepard, 1967; Real User Corporation, 2007). As known generally, the main drawbacks for the current graphical password schemes are the shoulder-surfing problem and usability problem. Even though graphical passwords are difficult to guess and break, if someone direct observe during the password enter sessions, he/she probably figure out the password by guessing it randomly. Nevertheless, the issue of how to design the authentication systems which have both the security and usability elements is yet another example of what making the challenge of Human Computer Interaction (HCI) and security communities. (Shepard, 1967). Even though the main argument for graphical passwords is that humans are better at memorizing graphical passwords than conventional passwords, the existing user studies are very limited and there is not yet convincing the fact to support this argument. We have found that the existing recognition base graphical passwords schemes does not have attractive usability features for the users which mean that the usability features needed to be studied more and develop more usable systems for the Graphical Password. A collection of usability features will be implemented in the new graphical password prototype to be more usable for the users where this usability set includes the easy of use, memorize, creation, learning and satisfaction. Finally we propose a new graphical password scheme known as Jetlfida graphical password scheme.

2.0 Summary of the Existing Recognition Base Graphical Password Techniques.

2.1 Recognition Base (Multiple-image schemes)

In recognition based techniques, users are given a set of pictures and they pick and memorize some of them. During authentication, the users need to recognize and identify the pictures they have picked earlier.

PassfacesTM, a commercial product by Passfaces Corporation, requires a user to select previously seen human face pictures as a password (Passfaces, 2007), as shown in Figure 3.1 problem with PassfacesTM is that some faces displayed might not be welcomed by certain users. In other words, if a user has to look at some faces he/she does not like or even dislike, the login process will become unpleasant. Another drawback of PassfacesTM is that it cannot be used by people who are face-blind (a disease which affects a person’s ability to tell faces apart).

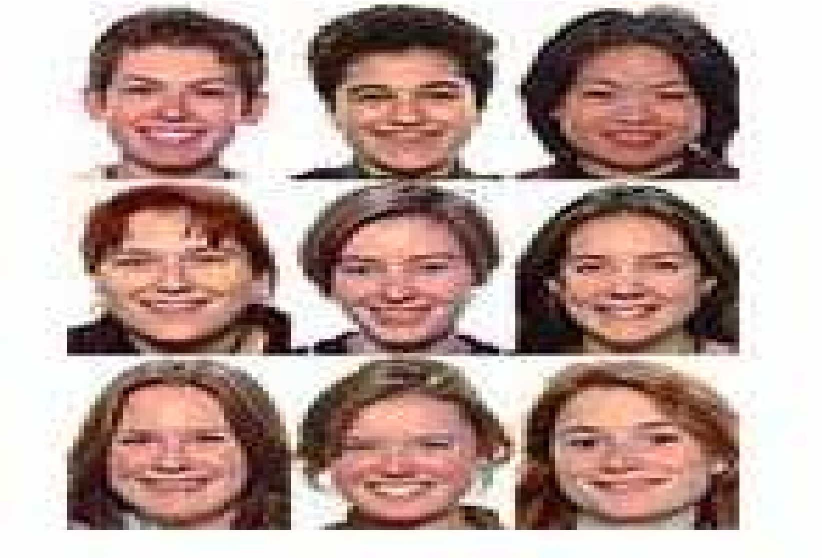


Figure 3.1 PassfacesTM [Passfaces 2006]

Brostoff, S. and Sasse (2000) conducted a user study (34 subjects involved) on this scheme and their result suggests that PassfacesTM is easier to remember than textual passwords. Davis, D., Monrose, F., and Reiter, M. K. (2004) suggested a similar scheme, the story scheme, in which a user’s password is a sequence of *k* images selected by the user to make a story, as shown in Figure 3.2.

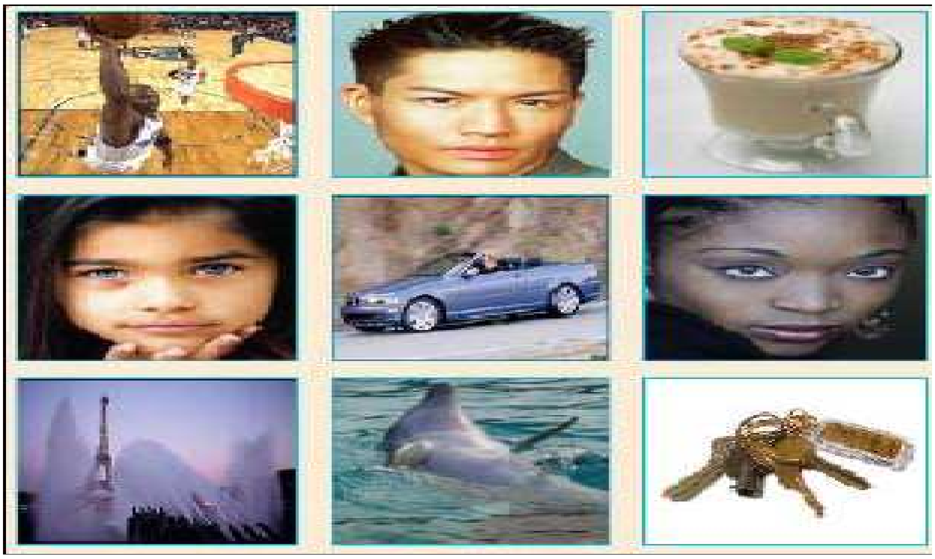


Figure 3.2 Story scheme [Davis et al. 2004]

Davis et al.(2004) empirically studied and compared these two schemes by surveying 154 computer engineering and computer science students from two universities. Their result shows that in PassfacesTM the user's choice is highly affected by race, the gender of the user, and the attractiveness of the faces.

By exploiting hash visualization techniques (Perrig and Song, 1999), another scheme called Déjà Vu (Dhamija and Perrig, 2000) was designed with non-describable abstract images (see Figure 3.3), rather than photographs. The advantage of introducing these kinds of images is that they can be generated deterministically by small initial seeds through a method called Random Art, thus removing the need to store and transmit those cumbersome images back and forth. A user study was also conducted and 20 participants were asked to create Déjà Vu (selecting 5 images among 20 "decoy" images) and textual passwords (at least 6 characters) simultaneously and authenticate themselves by using both respectively. The results showed that it took longer to create a graphical password then a textual password. In addition, 90% of the authentication attempts using Déjà Vub succeeded compared to 70% using textual passwords. Considering the fact that the password space of textual passwords is much larger than that of Déjà Vu (which is only 53,130), it is not convincing to conclude that Déjà Vu is easier to remember.

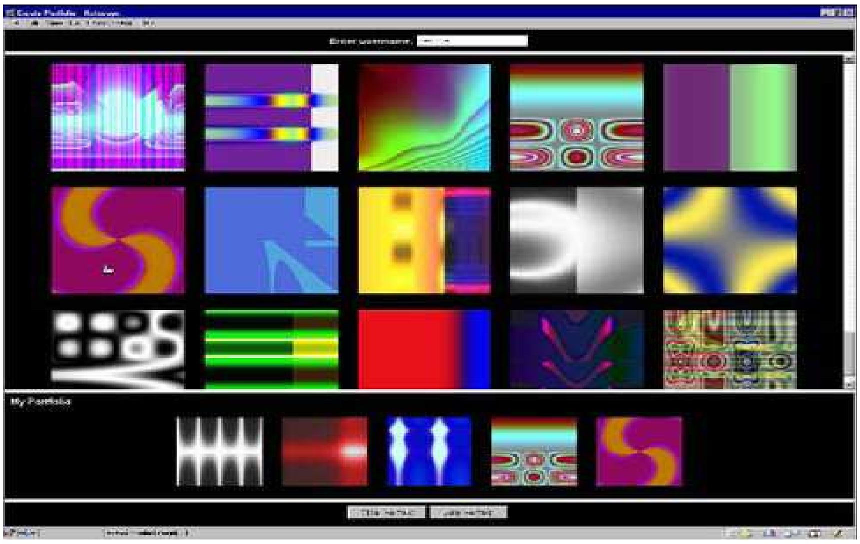


Figure 3.3 Déjà Vu [Dhamija and Perrig 2000]

“Picture password” was suggested by Jansen et al. (Jansen ,et al, 2003). The scheme was also designed for mobile devices (PDAs). When a password is to be created, a user selects a theme first (e.g. seashore, kitten and so on) which consists of thumbnail photos.

The user then selects a sequence of thumbnail photos as a password (see Figure 3.4). To repeat the password, the user needs to recognize and identify the thumbnail photos (previously selected) in the same order as in the registration stage. A numerical value is assigned for each thumbnail photo, and the sequence of selection will generate a numerical password. The concept of “akin” was introduced, which serves as a shift key in a traditional keyboard for each thumbnail photo in the theme. For example, instead of picking only one thumbnail photo, a user can select one or two thumbnail photos as one single action. The corresponding alphabet size is then expanded (e.g., from 30 to 930 if the theme consists of 30 thumbnail photos, as in Figure 3.4). Such expansion significantly enlarges the full password space, and makes an exhaustive search infeasible in practice.

However, the difficulty to remember a password is also increased significantly at the same time. The authors also discussed the use of the “Zooming” technique (which magnifies the area of the screen close to the cursor and facilitates the handling of small objects on a display). While “Zooming” can make small thumbnail photos easy to choose, it introduces great complexity in creating and handling themes.

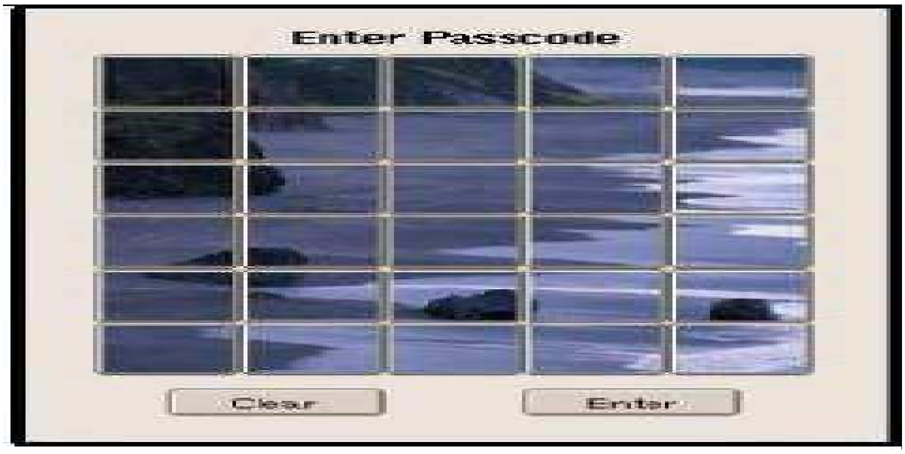
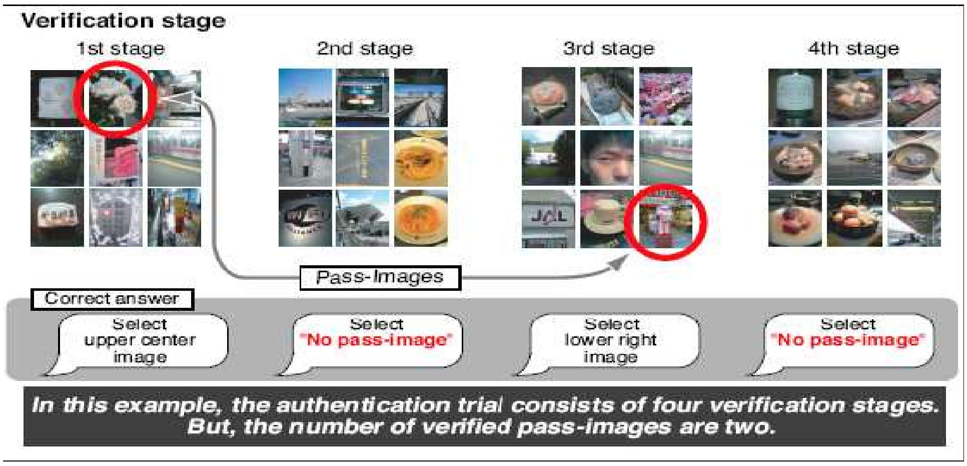


Figure 3.4 Picture password [Jansen et al. 2003].

Takada and Koike(2003) discussed image-based authentication for mobile phones using users’ own images. In the password registration phase, a user chooses his/her own images as pass-images, and then is required to recognize and identify them among decoy images in the authentication phase (see Figure 3.5). The user needs to go through several rounds of verification to ensure the password is secure enough. For each round, the user has to select a pass-image or choose nothing if there is not any pass-image displayed. The authentication will succeed if all verifications are successful.



In this example, the authentication trial consists of four verification stages. But, the number of verified pass-images are two.

Figure 3.5 Image-based authentication for mobile phones [Takada and Koike 2003]

In general, recognition base schemes suffer from following common shortages:

a) Considerably large display space is needed to hold multiple images;
b) The password space is small. For example, if one image needs to be distinguished from a 3×3 image matrix for 6 rounds, the full password space is only 531,441, which is even smaller than that for a 3 printable ASCII character textual password (953=857,375). Such a small password space is subject to off-line attack;
c) Passwords have to be stored in the clear; therefore the authentication server is required to be strongly protected;
d) The password is difficult to write down. While this was claimed as a desirable feature, as it could be an effective measure to prevent social engineering attacks, it makes password sharing difficult, thus making system-generated passwords difficult to be sent to a human user. In other words, this security feature is achieved by sacrificing some degree of usability.

3.0 Usability over view

Usability is an important issue in order to develop a good scheme that can satisfy the user needs and requirements. As stated by the ISO 9241-11 standard, they defined usability as the extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use [14]. In graphical password scheme one of the main arguments for graphical passwords is that pictures are easier to remember than text strings (memorability). Preliminary user studies conducted by some researchers seem to agree with this opinion. However, recently user studies are still limited to support this view. There are many factors associated with the memorablity issues. In order to make the graphical password are more memorable, earlier researchers have suggested that the created password must be meaningful, frequently used and fun [Takada and Koike, 2003; Brostoff and Sasse, 2000; Passfaces, 2007). Nevertheless, there are some securities tradeoffs need to be aware if we agree with these suggestions. For example, it is easy to guess, break and predict the password if it is too meaningful. Additional usability issue is that the password registration and login process are time consuming, especially in recognition-based schemes. For example, user has to pick images from a large set of selections during the registration phase and user has to scan many images to identify a few pass-images in order to be authenticated (Sobrado and Birget, 2002). Because of this process, it will become unpleasant and difficult especially for the newbie's in graphical passwords environment.

4.0 Design of The Graphical Password Prototype

The design process will be divided into two stages, existing user and new user. If the user does not have password which means that he is a new user, so he has to enter his user name and start create his password. The usability features set will be transforming into a proposed graphical password prototype. The usability features that will be implemented in the proposed graphical password system prototype will be easy of use, memorize, creation, learning and satisfaction

To create the password the user should choose three images and sort them as he want in some order and save them or exist if he want to cancel the process. After the creation and saving of the password the user will exit the system to enter later with his password. But if the user name exists in the system which means that he is an existing user, so he has to enter his user name and start the verification process. If the password entered is correct so it will be accepted and the verification process will take the user directly to the application, otherwise when the password entered is incorrect the user can try three times to enter correct password or exit the system if he want to cancel the login process.

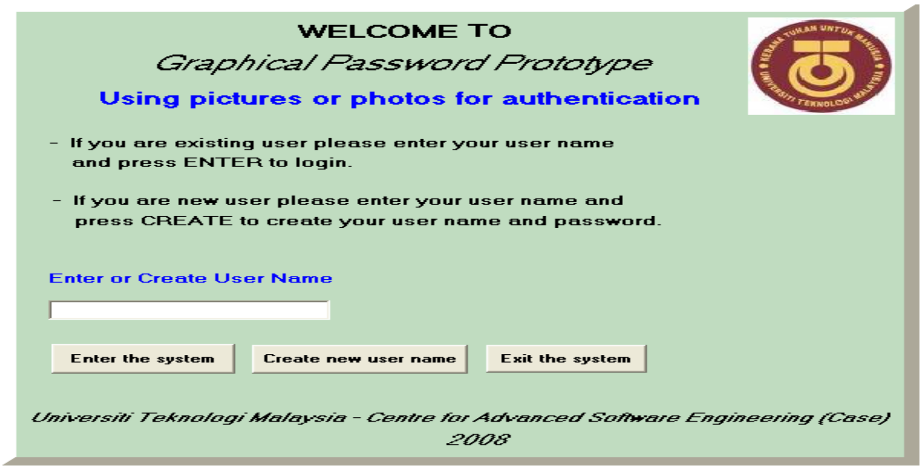
5.0 Graphical Password Protoype Interface Design

Interface design will be designed that help users to interact and communicate with the system, it also can be used as a presence of retrieving and sending information between the users and the computer.

5.1 Graphical Password login Interface.

5.1.1 New user Graphical Password login Interface.

The login interface is designed to login to the system for both the new user and existing user, there are two notice to the user either he is a new user or existing user to follow the entering or creation of the user name also there are three buttons in login interface to guide the user to inter the system, where these buttons are enter the system for existing user, create new user name for new user and exit the system. Figure 5.1show the login interface for the system.



WELCOME TO

Graphical Password Prototype

Using pictures or photos for authentication

- If you are existing user please enter your user name and press ENTER to login.
- If you are new user please enter your user name and press CREATE to create your user name and password.

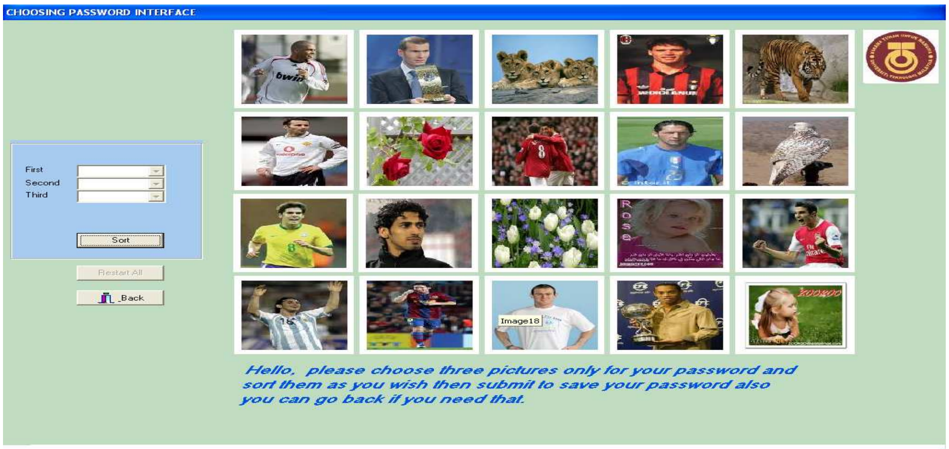
Enter or Create User Name

Universiti Teknologi Malaysia - Centre for Advanced Software Engineering (Case) 2008

Figure 5.1 Jetafida login interface for the system.

5.1.2 Graphical Password Registration Interface.

Then the system will direct the user to the reiteration or choosing the password interface as shown in Figure 5.3. In this interface there are twenty pictures mixed between natural, human and animal pictures and sort button to change the order of the pictures chosen also can go back for any user reason or restart all which means can reset the process also some hints will appear in the interface.

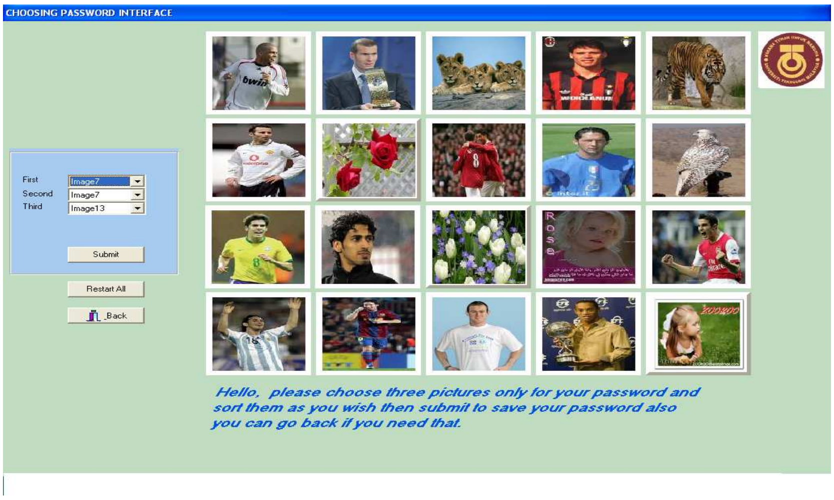


CHOOSING PASSWORD INTERFACE

Hello, please choose three pictures only for your password and sort them as you wish then submit to save your password also you can go back if you need that.

Figure 5.3 Jetafida registration interface

When the user choose the images for password the image will arise to make it easy to the user to know which pictures he has chosen then he can sort them as he wish as shown in Figure 5.4

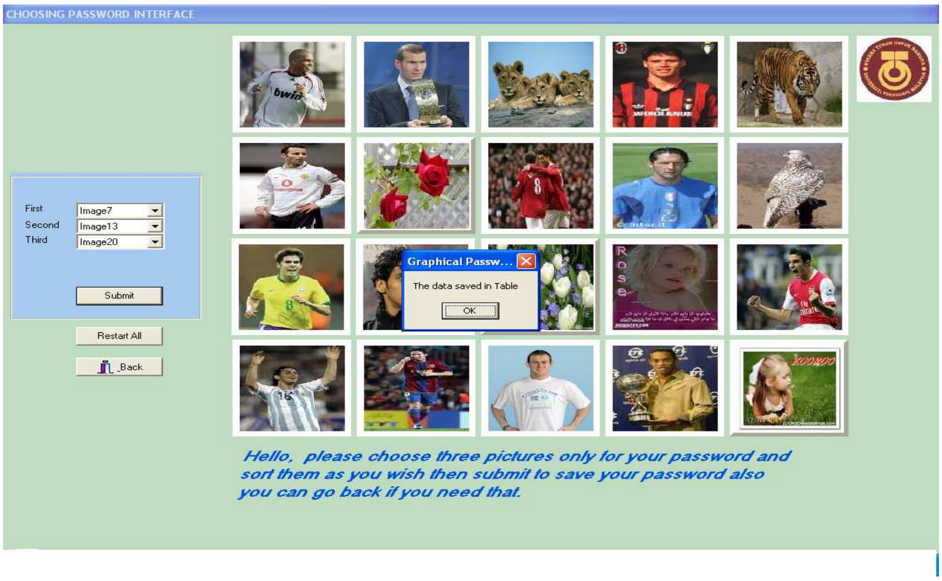


First Image7
Second Image7
Third Image13

Hello, please choose three pictures only for your password and sort them as you wish then submit to save your password also you can go back if you need that.

Figure 5.4 Jetafida Choosing and sorting password interface

When finishing the pictures selection the sort button will replaced by submit button to submit the chosen password, then message box indicate that the password has been saved and click ok as shown in Figure 5.5.



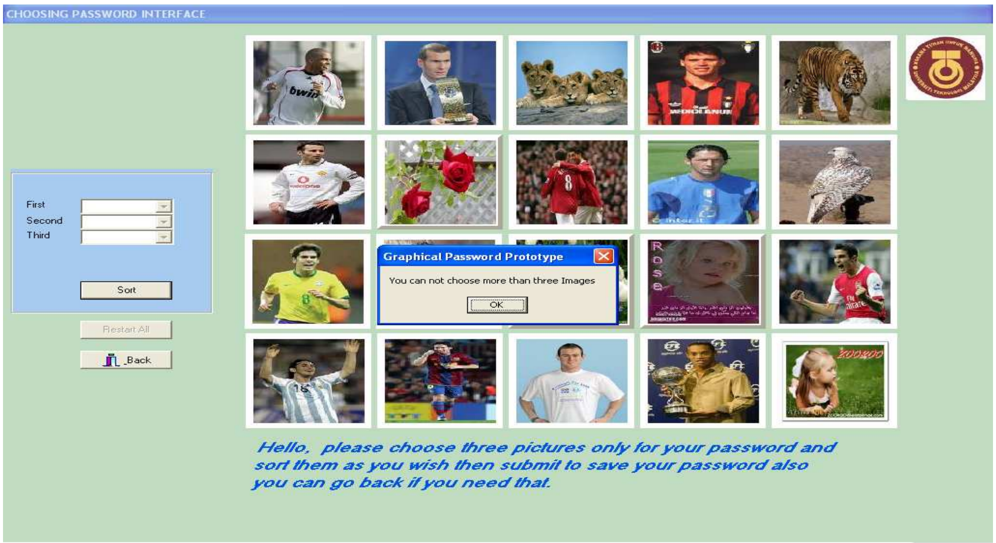
First Image7
Second Image13
Third Image20

The data saved in Table

Hello, please choose three pictures only for your password and sort them as you wish then submit to save your password also you can go back if you need that.

Figure 5.5 Jetafida Submit and save the password interface

But if the user chooses more than three images, a message will appear to show the user that he can only choose three images regarding to the system design usability features as shown in Figure 5.6.



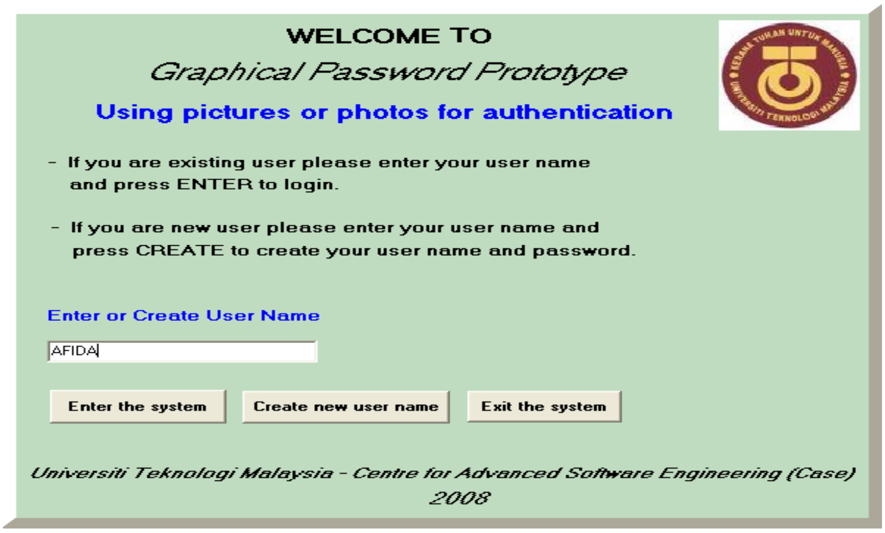
You can not choose more than three Images

Hello, please choose three pictures only for your password and sort them as you wish then submit to save your password also you can go back if you need that.

Figure 5.6 Jetafida error choosing pictures

5.1.3 Existing user Graphical Password login Interface.

In the existing user case, the login interface is same login interface for new user just we need to remember our user name and write it in enter user name space and press enter the system button as shown in Figure 5.7.


WELCOME TO

Graphical Password Prototype

Using pictures or photos for authentication

- If you are existing user please enter your user name and press ENTER to login.
- If you are new user please enter your user name and press CREATE to create your user name and password.

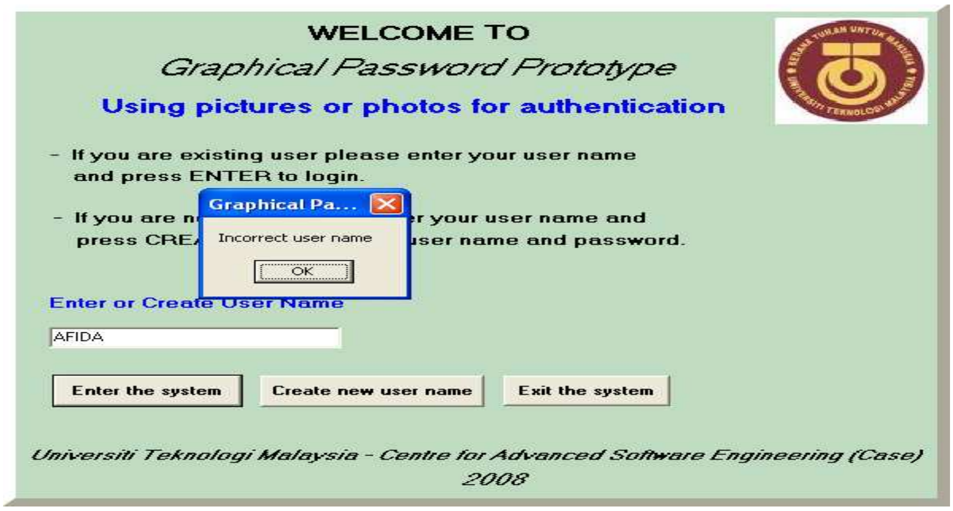
Enter or Create User Name

AFIDA

Universiti Teknologi Malaysia - Centre for Advanced Software Engineering (Case) 2008

Figure 5.7 Jetafida existing user login interface

In case of entering incorrect user name a message box will appear to show that you enter incorrect name as shown in Figure5.8.



WELCOME TO

Graphical Password Prototype

Using pictures or photos for authentication

- If you are existing user please enter your user name and press ENTER to login.
- If you are n r your user name and press CRE user name and password.

Graphical Pa...

Incorrect user name

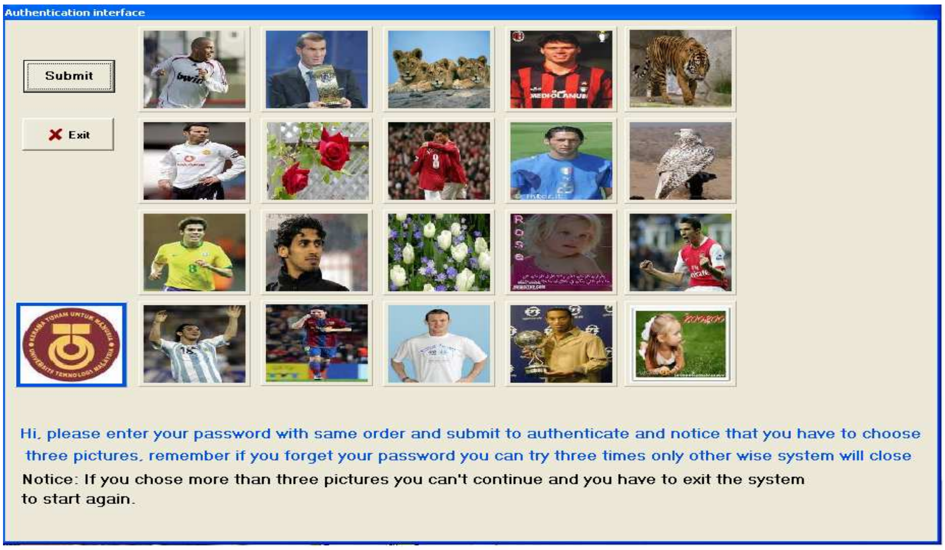
Enter or Create User Name

AFIDA

Universiti Teknologi Malaysia - Centre for Advanced Software Engineering (Case) 2008

Figure 5.8 Jetafida incorrect user name interface

After enter the correct existing user name and press enter the system an authentication interface will open to enter the chosen password as shown in Figure 5.9. Also some hints will appear in the interface to guide the user.



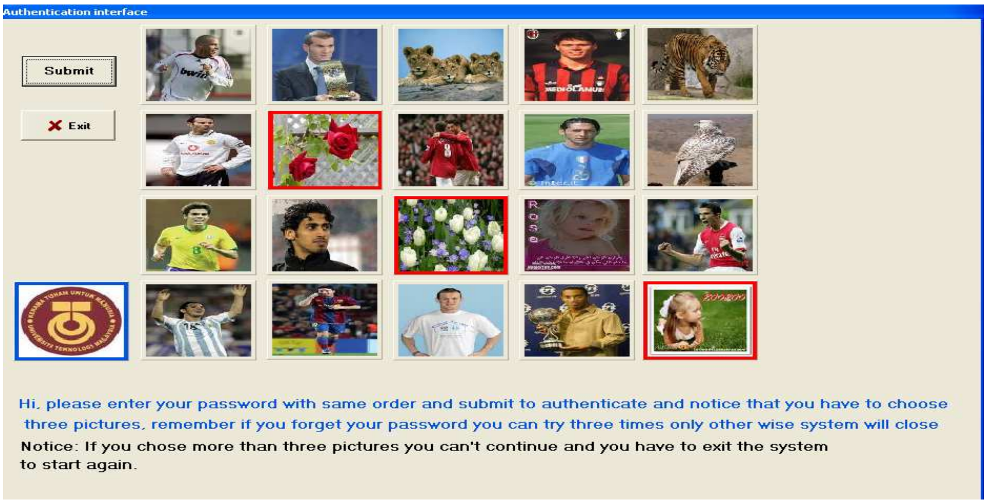
Authentication interface

Hi, please enter your password with same order and submit to authenticate and notice that you have to choose three pictures, remember if you forget your password you can try three times only other wise system will close

Notice: If you chose more than three pictures you can't continue and you have to exit the system to start again.

Figure 5.9 Jetafida Authentication interface

Then the user has to press his saved password with same order and the pictures pressed will appear with red framework to be easier to the user to recognize his password as shown in figure 5.10. After that the user will press submit button to directly go to his application if the password was correct or exit button to cancel the process**.**

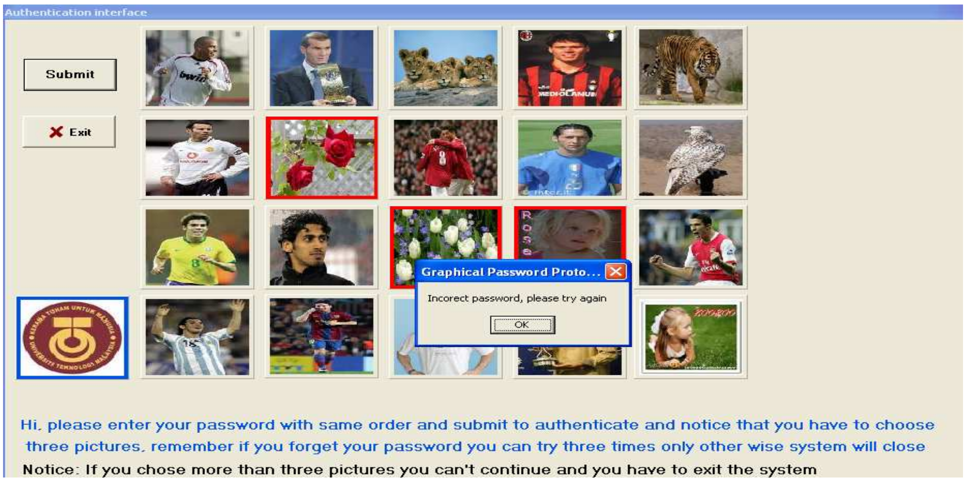


Hi, please enter your password with same order and submit to authenticate and notice that you have to choose three pictures, remember if you forget your password you can try three times only other wise system will close

Notice: If you chose more than three pictures you can't continue and you have to exit the system to start again.

Figure 5.10 Jetafida Authentication process interface

But if the password entered is not match the saved password under that user name then a message will appear to show that the password is incorrect and the user can try again as shown in Figure 5.12.



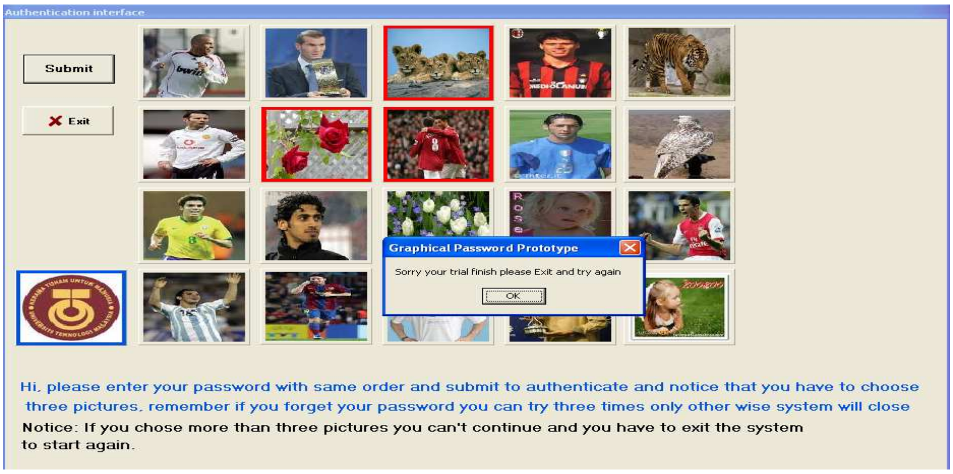
Incorrect password, please try again

Hi, please enter your password with same order and submit to authenticate and notice that you have to choose three pictures, remember if you forget your password you can try three times only other wise system will close

Notice: If you chose more than three pictures you can't continue and you have to exit the system

Figure 5.12 Jetafida incorrect password selection interface

The user only can try three times to enter the saved password, but if he fails to remember his password three times the system will show a message indicate that the trials has been finished as shown in Figure 5.13 and the system will close and he has to exit to start again.



Sorry your trial finish please Exit and try again

Hi, please enter your password with same order and submit to authenticate and notice that you have to choose three pictures, remember if you forget your password you can try three times only other wise system will close

Notice: If you chose more than three pictures you can't continue and you have to exit the system to start again.

Figure 5.13 Jetafida trials finish interface

6.0 Result and discussion

In this paper, we have proposed a usable design (as prototype) of graphical password technique. Even though the main argument for graphical passwords is that humans are better at memorizing graphical passwords than alphanumeric character passwords, the existing user studies are very limited and there is not yet convincing the fact to support this argument. We have found that the existing recognition base graphical passwords techniques does not have attractive usability features for the users which mean that the usability features needed to be studied more and develop more usable systems for the Graphical Password. In this paper a graphical password prototype designed and implemented with the most usable features of usability but the system not focus on the security side of the graphical password systems and that may need more researches and time to develop a complete systems provide both the security and usability features. A usability questionnaire survey had been conducted with thirty computer science students in different times and the results were very good and the system is achive the usability features builtin.The following table illustrate the usability features and the survey results.

No	Categories	Percentsge
1	Evaluation of Whole GRP	51.67%
2	Ease of Use	40%
3	Ease to Create	38.33%
4	Ease to Memorize	55%
5	Ease to Learn	56.67%
6	Screen Design	53.33%

7.0 Conclusion

In this paper we present and describe the implementation process and the executing stages of the graphical password creation and authentication. We can rely on the new graphical password prototype model for using as authentication method between the users and their applications with the possible usable features which provide easiest factors to deal with this type of authentication**.**

References

1. Brostoff, S. and Sasse, M. A. 2000. Are PassfacesTM more usable than passwords? A field trial investigation. In *Proceedings of Human Computer Interaction*, 405–424
2. Davis, D., Monrose, F., and Reiter, M. K. 2004. On User Choice in Graphical
3. Password Schemes. In *Proceedings of the 13th USENIX Security Symposium*. 151-164.
4. D. Davis, F. Monrose and M.K. Reiter. (2004). "On User Choice in Graphical Password Schemes," in Proceedings of the 13th USENIX Security Symposium. San Diego, California.
5. Dhamija , R. an Perrig, A. August (2000). *"Déjà vu: A User Study Using Images for Authentication"*. In Proceedings of the 9th USENIX Security Symposium,.
6. Dhamija, R. and Perrig, A. 2000. Déjà Vu: A User Study Using Images for
7. Authentication. In *Proceedings of the 9th USENIX Security Symposium.*
8. Gilhooly, K. (May, 2005). *"Biometrics: Getting Back to Business"*, in Computerworld.
9. ISO-International Organization for Standardization, http://www.iso.org, Accessed on May 2007.
10. Jansen, W., Gavrila, S., Korolev, V., Ayers, R., and Swanstrom, R. 2003. Picture Password: A Visual Login Technique for Mobile Devices. *NIST Report - NISTIR7030.*
11. PASSFACES.(2006). The science behind passfacesTM for windows.
12. http://www.realuser.com/resources/white%20papers.htm, site accessed on Jan 29, 2006.
13. Perrig, A. and Song, D. (1999) Hash Visualization: a New Technique to Improve Real- World Security. In *International Workshop on Cryptographic Techniques and ECommerce*,pages 131–138
14. Real User Corporation, Passfaces TM "http//:www.realuser.com," Accessed on June 2007.
15. Shepard, R. N. (1967). "Recognition memory for words, sentences, and pictures," *Journal of Verbal Learning and Verbal Behavior*, vol. 6, pp. 156-163.
16. Shepard, R. N. (1967) "Recognition memory for words, sentences, and pictures," *Journal of Verbal Learning and Verbal Behavior*, vol. 6, pp. 156-163, 1967.

17. Sobrado, L and Birget, J. (2002). "*Graphical Passwords,*" The Rutgers Scholar , An Electronic Bulletin of Undergraduate Research, Rutgers University, Camden New Jersey , Vol. 4. Accessed on June 2007.
18. Takada, T. and Koike, H. (2003) Awase-E: Image-based Authentication for Mobile Phones using User's Favorite Images. In *Human-Computer Interaction with MobileDevices and Services*, vol. 2795 / 2003: Springer-Verlag GmbH, 2003, pp. 347 - 351.