Australian Journal of Basic and Applied Sciences, 7(4): 688-695, 2013
ISSN 1991-8178

Pixel Value Graphical Password Scheme-Graphical Password Scheme Literature Review

Mohd Afizi Bin Mohd Shukran, Mohd Sidek Fadhil Bin Mohd Yunus, Kamaruzaman Bin Maskat, Wan Sharil Sham Bin Shariff and Mohd Suhaili Bin Ariffin

Faculty of Defense Science and Technology, Universiti Pertahanan Nasional Malaysia

Abstract: Pixel Value Graphical Password Scheme is designed to offer a new method for graphical password. This paper presents literature review of graphical password scheme including recall-base scheme and recognition-base scheme. Recall-base scheme are involving user to sketch or draw on password input. While recognition-base require user to click on specific area on an image. Each scheme base can be categorized into several methods where each method was developed with different user-case method. Findings from existing graphical password scheme were used to determine the competencies focus on Pixel Value Graphical Password scheme based on user-case comparison. Final goal of this study is to produce a solid proof that Pixel Value Graphical Password Scheme being a unique and competitive scheme in graphical password category.

Key words: Pixel-Value, Graphical-Password, access-control, authentication, log-in.

INTRODUCTION

Pixel Value Graphical Password Scheme is a knowledge base password scheme that requires an image file pixel value extraction as authentication subject. Through this graphical password scheme, users need to determine an image file and username during enrolment stage as authentication key to a system. Then, on log in procedure, user once again input a username and feed image file on log in page. System will extract pixel value from fed image file, and validate the username and pixel value to authenticate a user to a system. Pixel value graphical password scheme is not click-based graphical password which widely applied to existing graphical password scheme method. This scheme gives a freedom to user to determine an image file, based on certain requirements, to be use on this access control system. However, pixel-value graphical password scheme can be implemented on a system where others graphical password scheme rationally implemented such as online banking system, internet mail system, operating system logon, and more.

This paper presents a literature review of graphical password and negative aspect discussion on current graphical password scheme. Topic covered here includes Graphical Password Scheme discussion including techniques, types, and method in section two (2), section three (3) will discuss on current graphical password scheme in negative aspects and the impact of pixel value graphical password solution implementation. Section four (4), will conclude all discussion and findings of this study.

2. Graphical Password Schemes:

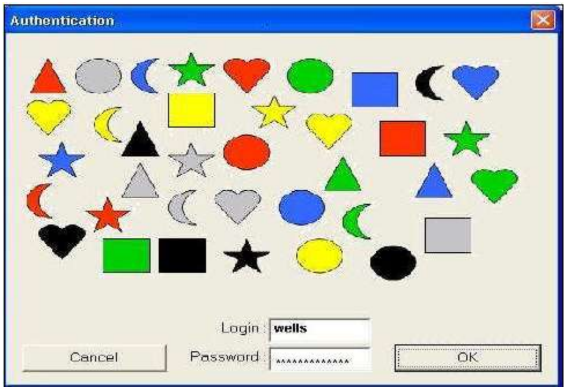
Graphical password scheme were introduced to reduce the human memory burden on text-based password. Research in the psychology discipline suggests that humans are better at recognizing visual information than recalling meaningless text-based strings (Dhamija, R. and A. Perrig, 2000), whether for authentication or otherwise (Pierce, J.D., 2004). This natural ability in humans can be use for authentication in a similar way to recalling passwords. A graphical authentication technique where users enter their login to a text box and then select screen artifacts, appearing among other control artifacts, is considered as a part of the graphical password (Pierce, J.D., 2004).

In 1999, a technique where users identify previously seen RandomArt is proposed by Perrig and Song. RandomArt hashes users' passwords and root keys in public key infrastructures and creates a visual representation of that hash. Later, this technique is enhanced by R.Dhamija that assembling the RandomArt images into a sequence of images that users identify in sequence before they are authenticated. Dhamija and Perrig called their suite Déjà Vu (2000) and validated it as a viable alternative paradigm using images.

Blonder patented a graphical password that required users to touch predetermined areas or known as clickpoints grids of an image in sequence for authentication in 1996. Blonder method was later being an inspirational idea for graphical password scheme development. His technique was designed to suited computer based application. Passlogix Inc. distribute v-go, an authentication application that requires users to do such things as enter the time on a clock, draw cards from a deck, and entering phone numbers. Real User (formerly IDArts, 1999) distributes Passfaces, an authentication system based on recognising previously seen images of

Corresponding Author: Mohd Afizi Bin Mohd Shukran, Faculty of Defense Science and Technology, Universiti Pertahanan Nasional Malaysia
E-mail: afizi@upnm.edu.my

faces (Pierce, J.D., 2004). Most of reproducing a drawing graphical password scheme was developed that initially for mobile handheld devices. In year 1999 Jermyn, Mayer, Monrose, Reiter and Rubin proposed a graphical password scheme that consisted of simple pictures drawn on a grid. This graphical password scheme category require a precise and accurate drawing that also require a specified input tools such as stylus did not bring a huge impact for graphical password scheme development competition.



Login : wells
Password : *************

Fig. 1: Coloured shape authentication dialogue.

2.1 Type of Graphical Password Schemes:

Knowledge based techniques are the most widely used authentication techniques and include both text-based and picture-based passwords (Suo, X., 2006). The picture based techniques can be categorized into two:
Recall Base Graphical Password Schemes.
Recognition Base Graphical Password Schemes.

Recall Base Graphical Password Scheme:

In recall based techniques user is asked to reproduce something that user created or selected earlier during the enrolment stage. Two types of Recall based password techniques:
Reproducing a drawing.
Repeating a selection.

Reproducing a Drawing:

There are three methods under this category which are:

A. DAS (Draw-a-secret):

This method is proposed by Jermyn, Mayer, Monrose, Reiter and Rubin in 1999, which allows user to draw their unique password as in Figure 2. A user is required to draw a simple picture on a grid. The coordinates of the grids occupied by the picture are stored in the order of the drawing. During authentication, the user is asked to re-draw the picture. If the drawing touches the same grids in the same sequence, then the user is authenticated. Jermyn, et al. suggested that given reasonable-length passwords in a 5 X 5 grid, the full password space of DAS is larger than that of the full text password space (Suo, X., 2006).

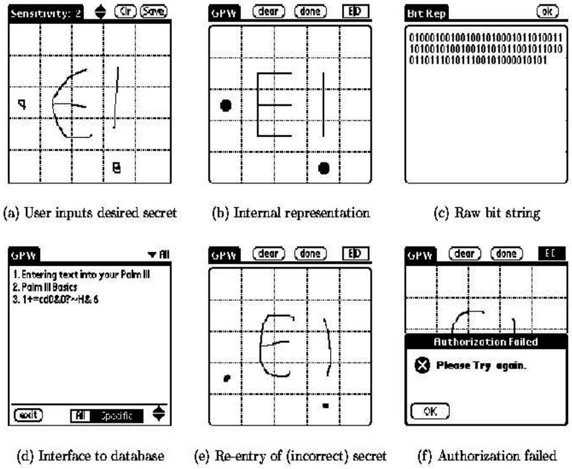
B. Passdoodle Method:

This is developed by J.Goldberg. This is a graphical password comprised of handwritten designs or text, usually drawn with a stylus onto a touch sensitive screen. Their study concluded that users were able to remember complete doodle images as accurately as alphanumeric passwords (Suo, X., 2006).

C. Syukri Method:

This method is a system where authentication is conducted by having user drawing their signature using mouse.

Their technique included two stages, enrolment and verification. On enrolment stage: user will first be asked to draw their signature with mouse, and then the system will extract the signature area and either enlarges or scale-down signatures, rotates if needed, (also known as normalizing). The information will later be saved into the database. The verification stage first takes the user input, and does the normalization again, and then extracts the parameters of the signature. After that, the system conducts verification using geometric average means and a dynamic update of database. According to the paper, the rate of successful verification was satisfying (Suo, X., 2006). The biggest advantage of this approach is that there is no need to memorize one's signature and signatures are hard to fake.



010001001001001010001011010011
101001010010010101011001011010
011011101011100101000010101

1. Entering text into your Palm III
2. Palm III Basics
3. 1+=cd0&0?~H& 6

(a) User inputs desired secret (b) Internal representation (c) Raw bit string

(d) Interface to database (e) Re-entry of (incorrect) secret (f) Authorization failed

Fig. 2: Draw-a-Secret (DAS) method.

Repeating a Selection:

In this group of authentication algorithms, a user is asked to repeat sequences of actions originally conducted by the user during the registration stage. There are four methods is review under this category which is:

A. Blonder Method:

In this method Blonder designed a graphical password scheme in which a password is created by having the user click on several locations on an image. During authentication, the user must click on the approximate areas of those locations (Blonder, G., 1996). The image can assist users to recall their passwords and therefore this method is considered more convenient than unassisted recall (as in text-based password).

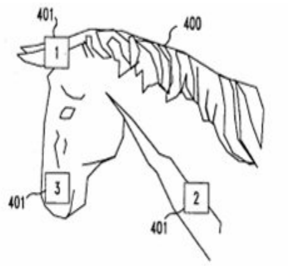


Fig. 3: Clickpoints on Blonder method.

B. PassGo Method:

Based on predetermined clickpoint grids graphical password scheme, an improvement on DAS (in term of grids) techniques was developed by Hai Tao in 2006. This technique was known as PassGo. It design based on old Chinese board game known as GO. PassGo was design to suite computer based used and can be implement on bigger grids that increase password space for DAS-type graphical password scheme. This method however does not show any similarity with DAS technique where there is no free move drawing work requires on authentication process. This method is better suite repeating a selection technique. In this technique, user is requiring to touch on grid intersection instead of grids cells symmetry drawing (Tao, H., 2006) on authentication process. The touch grid is determined by user during enrolment process. This method was also designed with graphical referencing aided which look like a checker board for each 9 by 9 grids.

C. Passpoint Method:

This system proposed by Wiedenbeck, and Wiedenbeck, extended Blonder's idea by eliminating the predefined boundaries and allowing arbitrary images to be used (Wiedenbeck, S., 2005). As a result, a user can click on any place on an image (as opposed to some pre-defined areas) to create a password. A tolerance around each chosen pixel is calculated. In order to be authenticated, the user must click within the tolerance of their chosen pixels and also in the correct sequence.

This technique is based on the discretization method proposed by Birget, because any picture can be used and because a picture may contain hundreds to thousands of memorable points, the possible password space is quite large. Wiedenbeck conducted a user study, in which one group of participants was asked to use alphanumerical password, while the other group was asked to use the graphical password. The result showed that graphical password took fewer attempts for the user than alphanumerical passwords (Wiedenbeck, S., 2005).

D. Passlogix Method:

Passlogix, Google has developed a graphical password system based on blonder idea. In their implementation, users must click on various items in the image in the correct sequence in order to be authenticated. Invisible boundaries are defined for each item in order to detect whether an item is clicked by mouse.

It has also developed several graphical password techniques based on repeating a sequence of actions (Suo, X., 2006). For example, its v-Go includes a graphical password scheme where users can mix up a virtual cocktail and use the combination of ingredients as password. Other password options include picking a hard at cards or putting together a “meal” in the virtual kitchen.

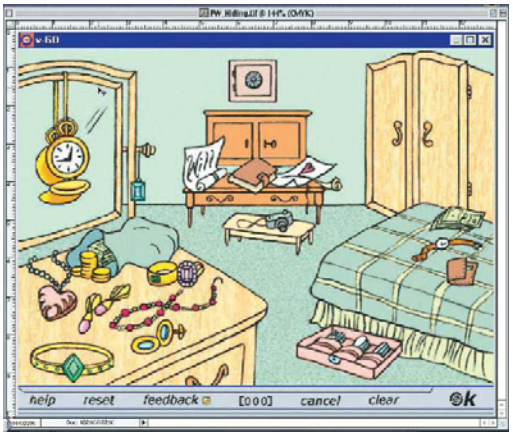


Fig. 4: PassLogix dialogue.

Recognition Base Graphical Password Scheme:

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. There are six methods for this category which are:

A. Dhamija and Perrig Algorithm:

This method is proposed a graphical authentication scheme based on Hash Visualization technique. In their system, user will be asked to select certain number of images from a set of random pictures generated by a program. Later, user will be required to identify the pre-selected images to be authenticated. The results showed that 90% of all participants succeeded in the authentication using their technique, while only 70% succeeded using text-based passwords and PINS (Dhamija, R. and A. Perrig, 2000). The average log-in time, however, is longer than the traditional approach, but has a much smaller failure rate (Dhamija, R. and A. Perrig, 2000; Pierce, J.D., 2004).

B. Sobrado and Birget Algorithm:

They developed a graphical password technique that deals with shouldersurfing problem. In the first scheme, the system will display a number of pass-objects (pre-selected by user) among many other objects. To be authenticated, a user needs to recognize pass-objects and click inside the convex hull formed by all the passobjects (Sobrado, L. and J.C. Birget, 2002).

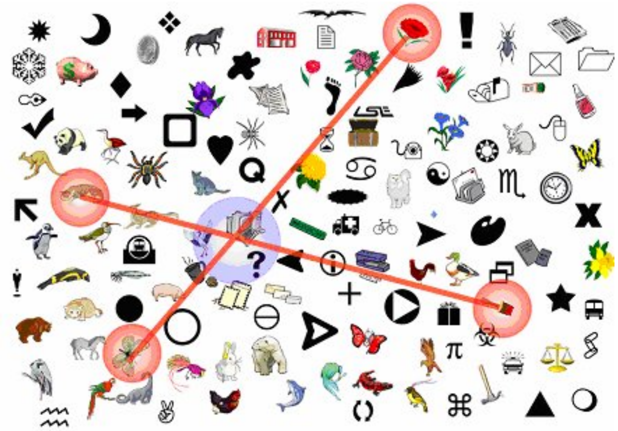


Fig. 5: Shoulder surfing resistance scheme.

In their second algorithm, a user moves a frame (and the objects within it) until the pass object on the frame lines up with the other two pass-objects. With this method, it is suggested repeating the process for a few more times to minimize the likelihood of logging in by randomly clicking or rotating.

C. Man, et al. Algorithm:

In this algorithm, a user selects a number of pictures as pass-objects. Each pass-object has several variants and each variant is assigned a unique code. During authentication, the user is challenged with several scenes. Each scene contains several pass-objects (each in the form of a randomly chosen variant) and many decoy-objects. The user has to type in a string with the unique codes corresponding to the pass-object variants present in the 24 scene as well as a code indicating the relative location of the pass-objects in reference to a pair of eyes. The argument is that it is very hard to crack this kind of password even if the whole authentication process is recorded on video because where is no mouse click to give away the pass-object information (Man, S., 2004).

D. Jansen Algorithm:

This algorithm graphical password mechanism proposed for mobile devices. During enrolment stage, a user selects a theme (e.g. sea, cat, etc.) which consists of thumbnail photos and then registers a sequence of images as a password. During the authentication, the user must enter the registered images in the correct sequence. After a successful authentication, the user may change the password, selecting a new sequence, or possibly change the theme. One drawback of this technique is that while the amount of thumbnail image is limited to 30, the password space is small. Each thumbnail image is assigned a numerical value, and the sequence of selection will essentially generate a numerical password (Jansen, W., 2004).

E. Takada and Koike:

Discuss a similar graphical password technique for mobile devices. This technique allows users to use their favourite image for authentication. The users first register their favourite images (pass-images) with the server. During authentication, a user has to go through several rounds of verification. At each round, the user either selects a pass-image among several decoy-images or chooses nothing if no pass-image is present. The program would authorize a user only if all verifications are successful. Allowing users to register their own images makes it easier for user to remember their pass-images. A notification mechanism is also implemented to notify users when new images are registered in order to prevent unauthorized image registration since it is viewable to the public (Takada, T. and H. Koike, 2003).

F. Passface Algorithm:

Which is a technique developed by Real User Corporation, Google RealUser. The basic idea is as follows. The user will be asked to choose four images of human faces from a face database as their future password. In the authentication stage, the user sees a grid of nine faces, consisting of one face previously chosen by the user and eight decoy faces. The user recognizes and clicks anywhere on the known face. This procedure is repeated for several rounds. The user is authenticated if he or she correctly identifies the four faces. The technique is based on the assumption that people can recall human faces easier than other pictures (Passface Corporation, 2005). User studies by Valentine have shown that Passfaces are very memorable over long intervals (Valentine, T., 1999). Comparative studies conducted by Brostoff showed that Passfaces had only a third of the login failure rate of text-based passwords, despite with about a third the frequency of use. Their study also showed that

Passface-based log–in process took longer than text passwords and therefore were used less frequently by users (Suo, X., 2006).

3. Finding and Discussion:

3.1 Recall-Base Scheme Negative Aspect:

Draw-a-secret method require user to recall in order of a drawing during authentication process. Based on study by J.Goldberg users do not like to repeat drawing in order on each authentication process (Suo, X., 2005). To overcome this matter, J.Goldberg come out with Passdoodle method where require user to draw freely on touch sensitive device. The work nevertheless provided useful information in terms of graphical password as a possible alternative for text password. However, the user study was done using paper prototype instead of computer programs, verifications were done by human rather than computer. Therefore the accuracy of this study is still uncertain. Shukri proposed a draw-password method that can be fit for computer. This method require user to draw their signature using mouse. However, not everybody is familiar with using mouse as a writing device; the signature can therefore be hard to drawn. One possible solution to this problem would be to use a pen-like input device, but such devices are not widely used, and adding new hardware to the current system can be expensive. Such technique is more useful to mobile handheld devices such as PDA.

Repeating-a-selection technique is developed in order to make recall-base scheme can be apply on computer application. This technique require user to repeat sequences of actions originally conducted by the user during the enrolment stage. In Blonder's method, users require to click on several image locations. This method offer limited choice of click-point image location. Blonder's method clickpoints grids limitation then inherit on PassGo method. Even PassGo was initially designed for enhancing DAS method, clickpoints on grids intersection show similarity on Blonder's limited clickpoints grids features. Passpoint method was introduced to overcome blonder method limitation. User may click on any click-point on a single provided image background. However, graphical password users had more difficulties learning the password, and took more time to input their passwords than the alphanumerical users. Later Wiedenbeck, also conducted a user study to evaluate the effect of tolerance of clicking during the re-authenticating stage, and the effect of image choice in the system. The result showed that memory accuracy for the graphical password is strongly reduced after using smaller tolerance for the user clicked points, but the choices of images do not make a significant difference. The result showed that the system works for a large variety of images (Wiedenbeck, S., 2005). Google introduce Passlogix that allow user to choose several image rather than clickpoints. However, this technique only provides a limited password space and there is no ease way to prevent people from picking poor passwords (for example, a full house of cards).

3.2 Recognition-Base Scheme Negative Aspect:

Recognition based scheme require user to pick and memorize some of a given set of pictures. During authentication, the users need to recognize and identify the pictures they have picked earlier. Dhamija and Perrig have proposed a scheme that require user to pick a series of image from provided image library for authentication. A drawback is that the server needs to store a large amount of pictures which may have to be transferred over the network, delaying the authentication process. Another weakness of this system is that the server needs to store the seeds of the portfolio images of each user in plain text. Interface-wise, the process of selecting a picture from picture database can be tedious and time consuming for the user. Sobrado and Birget proposed a method to deal with shoulder surfing exposed where user needs to recognize pass-objects and click inside the convex hull formed by all the passobjects. In order to make the password hard to guess, Sobrado and Birget suggested using 1000 objects, which making the display very crowded and the objects almost indistinguishable. On the other hand, using fewer objects may lead to a smaller password space, since the resulting convex hull can be large. Another technique to deal with shoulder surfing was developed by Man. User requires selects a number of pass-objects which has several variants and assigned to a unique code. However, this technique still requires users to memorize the alphanumeric code for each pass-object variant. For example, if there are 4 pictures each with 4 variants, then each user has to memorize 16 codes. Although the pass-objects provide some clues for recalling the codes, it is still quite inconvenient.

Remembering clip art or random arts might be difficult for user on authentication process after long intervals. Therefore, Google proposed a new method which is Passface. Although the preliminary user studies have shown some promising results for the Passface technique, the effectiveness of this method is still uncertain. Davis studied the graphical passwords created using Passface technique and found obvious patterns among these passwords. For example, most users tend to choose faces of people from the same race (Davis, D., 2004). In their study, female faces were preferred by both male and female users. Better looking faces were more likely to be chosen. All of these make the Passface password quite predictable. This problem may be alleviated by arbitrarily assigning faces to users, but doing so would make it hard for people to remember the password.

Development on recognition base scheme has been made for mobile device. Jansen has developed a technique that inherits similarity method with Dhamija and Perrig technique. This technique require user to choose image theme before proceed to choose image sequence. The result showed that the image sequence length was generally shorter than the textural password length. To address this problem, two pictures can be combined to compose a new alphabet element, thus expands the image alphabet size. Another mobile devices password scheme has been developed by Takada and Koike. This method require user to choose the correct image among decoy image from different image set stage. This method does not necessarily make it a more secure authentication method than text-based password. User registered image are viewable to others. User may use an image that might relate to personal thing such as car, house, and pet. That give hacker easier to guess if knows personal information of a user.

3.3 Pixel Value Graphical Password Impact:

Based on previous discussion, it can be conclude on some design flaw on Recall-base scheme and Recognition-base scheme which is:

Reproducing a drawing techniques are mostly developing to be appropriate for handheld device equipped with a stylus as PDA phone.

It's dealing digital pen or stylus input hardware and accurate drawing is an important issue.

Some of the method dealing with image background by clickpoints effecting clickpoints hotspot on a single image background.

Recognition based techniques require user to choose an image from a predetermined image library.

Some method require user to register their image file which user easily to memorize the image. However the image is exposed to all users which hacker can use it as sources to conduct identity study on a user.

Pixel Value graphical password scheme is designed to address solution on these graphical password scheme flaw. The solutions are described as follows:

Scheme interface design is suitable for both computer and handheld devices.

It does not require any specific input device where it is only require a specific image file as passobject.

Passobject for Pixel Value graphical password is determine by user based on users convenient.

It only requires single image file and not involving any image sequence to remember and indirectly reduce memory burden.

User registered image is not exposed to other user or publicly which make passobject clue remain unknown on a user.

Sources of passobject only owned by a user. It is being uploading by user from local storage drive that ensures the safety of the passobject.

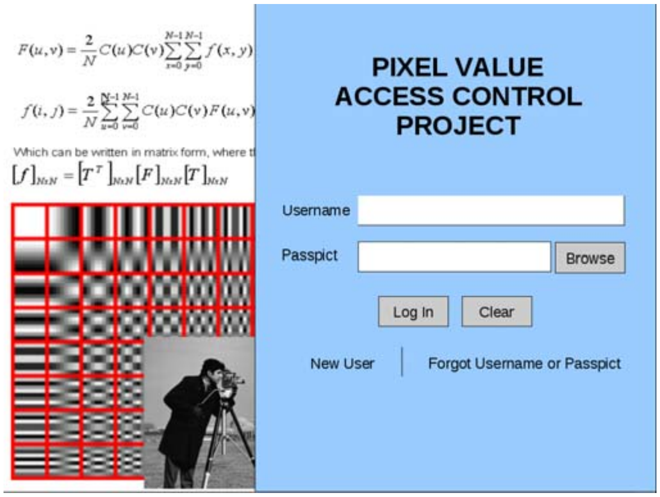

$F(u,v)=\frac{2}{N}C(u)C(v)\sum_{x=0}^{N-1}\sum_{y=0}^{N-1}f(x,y)$
$f(i,j)=\frac{2}{N}\sum_{u=0}^{N-1}\sum_{v=0}^{N-1}C(u)C(v)F(u,v)$
Which can be written in matrix form, where t
$[f]_{NxN}=[T^T]_{NxN}[F]_{NxN}[T]_{NxN}$
PIXEL VALUE
ACCESS CONTROL
PROJECT
Username
Passpict
Browse
Log In
Clear
New User
Forgot Username or Passpict

Fig. 6: Pixel value graphical password scheme log-in interface.

4. Conclusion:

Pixel Value Graphical Password scheme is a new method of graphical password scheme. It brings different framework and user case for graphical password scheme that bring improvement for current graphical password scheme in term of usability and security. Besides maintaining passobjects secrecy, this method authentication procedure is much simpler than other graphical password scheme. This method can be implementing on any system platform where there is no specific input hardware requirement during authentication procedure.

This research will be further on image compression algorithm such as Discrete Cosine Transform (DCT) for detailing in terms of increasing image accuracy and precision image pixel value extraction results.

REFERENCES

Blonder, G., 1996. Graphical Passwords. United States Patent, 5: 559-961.

Davis, D., F. Monrose, M.K. Reiter, 2004. On user choice in graphical password schemes. In 13th USENIX Security Symposium.

Dhamija, R. and A. Perrig, 2000. Deja Vu: A User Study Using Images for Authentication. Proceedings of 9th USENIX Security Symposium.

Jansen, W., 2004. Authenticating Mobile Device Users through Image Selection. Data Security.

Man, S., D. Hong, B. Hawes and M. Matthews, 2004. A graphical password scheme strongly resistant to spyware. In International conference on security and management.

Passface Corporation, 2005. Passface [Online] Avalaible: http://www.realuser.com/

Pierce, J.D., M.J. Warren, D.R. Mackay, J.G. Wells, 2004. Graphical authentication: justifications and objectives. In 2nd Australian Information Security Management Conference (p. 49).

Shepard, R.N., 1967. Recognition memory for words, sentences, and pictures. Journal of Verbal Learning and Verbal Behavior, 6(1): 156-163.

Sobrado, L. and J.C. Birget, 2002. “Graphical passwords,” In The Rutgers Scholar, an electronic Bulletin for undergraduate research, 4.

Suo, X., 2006. A design and analysis of graphical password. Master’s thesis, College of Arts and Sciences, Georgia State University.

Suo, X., Y. Zhu, G.S. Owen, 2005. Graphical passwords: A survey. In Computer Security Applications Conference, 21st Annual (pp. 10-pp). IEEE.

Takada, T. and H. Koike, 2003. Awase-E: Image-based Authentication for Mobile Phones using User’s Favorite Images. Human-Computer Interaction with Mobile Devices and Services, vol. 2795 / 2003: Springer-Verlag GmbH.

Tao, H., 2006. Pass-Go, a new graphical password scheme. Master’s thesis, Faculty of Graduate and Postdoctoral Studies, University of Ottawa.

Valentine, T., 1999. Memory for Passfaces after a Long Delay. Technical Report, Goldsmiths College, University of London.

Wiedenbeck, S., J. Waters, J.C. Birget, A. Brodskiy and N. Memon, 2005. Authentication using graphical passwords: effects of tolerance and image choice. In Proceedings of the 2005 symposium on Usable privacy and security, SOUPS ’05, pages 1–12, New York, NY, USA. ACM.