Volume 5, Issue 7, July 2015 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

A Comparative Study of Graphical Passwords and Their Security Issues

Mokal Pranita Haridas*, R. N. Devikar
Information Technology & Pune University
Maharashtra, India

Abstract—For providing security to information and computer the passwords are important unit of authentication. The majority method used for authentication was alphanumeric password in ancient times. This scheme has some considerable drawbacks. For example, If user choose a passwords that can be remember then password can be easily guessed. Alternatively if a user choose a long or strong password then password is hard to guess. Alphanumeric passwords are also prone to different attacks such as such as shoulder surfing attack, online guessing attacks, brute force attacks, dictionary attacks, social engineering attacks etc. To overcome the vulnerabilities of alphanumeric password scheme graphical password schemes have been developed as possible solutions to alphanumeric password scheme. The graphical password scheme uses the images, pictures as a password. Many graphical password schemes have been proposed until now. In this paper, we accomplish a widespread survey of the existing graphical password schemes. We can classify these schemes into recognition-based, pure recall-based, cued-recall based and hybrid approaches. We also examine the strengths and drawbacks of every method. This paper signifies a analysis on the security and usability features of graphical password schemes. In this paper we surveyed about 30 papers. We also clarified the problems, their solutions, results and future work recommended in each paper.

Keywords—Graphical Password, Recognition-Based Graphical User Authentication, Recall-Based Graphical User Authentication

I. INTRODUCTION

Now a day's security is major issue in information security. Authentication is important factor for providing security. The most convenient method for providing security is use of password for authentication. There are various schemes are developed for providing security during authentication. The most widespread authentication method is to submit first username and password. Textual password is the most commonly used scheme. Textual password uses alphabets, numbers for selecting the password. Textual passwords are easy to remember and easy to use but having some drawbacks such as: If user selects short password then it is easy to remember but it is also easy for an attacker to guess [2]. As state in Computerworld news article, at lager number of companies the security panel had ran the password cracker and 80% passwords are indentified by this panel within 30 seconds [3]. If user selects long password then it is difficult for attacker to guess but it is also very difficult for user to remember. Furthermore, textual passwords are susceptible to various attacks such as shoulder surfing attack, spyware attack and social engineering attack etc. So that to overcome these drawbacks and provide security, new scheme is developed which uses images, clickpoints etc. as a password known as graphical password [4, 5]. To deal with the problems of textual password scheme, another authentication schemes like biometrics [3, 7], have been used. In this paper, we will concentrate on a different option i.e. graphical passwords.

Graphical password is developed as an alternative for textual password scheme. Graphical password scheme uses the images or pictures as a password. As images are easy to remember and recognized than text. Graphical password is developed by Greg Blonder 1996. In Blonder's scheme image is displayed in front of user and then user clicks on it. If clickpoints are same on the appropriate region then access is given to user. In graphical password scheme, the user has to select the memorable image and user has to remember the click locations. For providing memorization, contents of image should be meaningful.As images are used in graphical password scheme,the space required by graphical password is more than the textual password. Graphical passwords are more memorable than to the textual passwords.

Graphical password may categorized into recognition-based, recall-based and hybrid. To achieve a good authentication system Usability and security should be considered. Derived from the present research of password security, we studied Various existing graphical password schemes and accomplished a broad survey of usability and security of graphical password schemes.

II. GRAPHICAL PASSWORD METHODS

The graphical password schemes are categorized into three categories viz.

1) Recognition Based Scheme
2) Recall Based Scheme
3) Hybrid Scheme

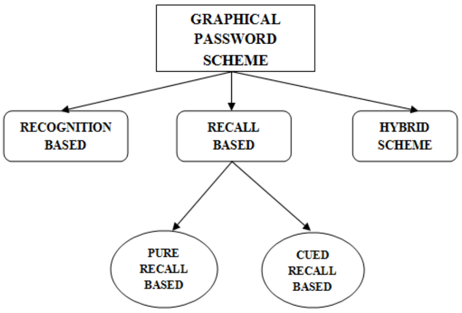


Figure.1: Graphical Password Techniques

1) Recognition Based Technique:

In this category, users will choose first images, icons or symbols from a set of images. During authentication, users should recognize their images, symbols or icons which are chosen during registration amongst a collection of images. The research illustrates that 90% of users can remember their passwords after one or two month also[15].

2) Pure Recall Based Technique:

In this category, users must reproduce his passwords and hints are not provided to remind the password. This scheme is easy and also convenient but it is hard to remember the password similar to DAS (1999) and Qualitative DAS (2007). This scheme is more secure than recognition based scheme.

3) Cued Recall-Based Technique:

This scheme is same as pure recall based but it is recall with cueing. Hints are provide scheme in this scheme. These hints or gestures help users to reproduce their password.

4) Hybrid Technique:

This scheme is combination of two or more schemes. These schemes are overcome the drawbacks of a single scheme.

III. RECOGNITION BASED SCHEME

Recognition based also called Cognometrics schemes or Search metrics schemes. In this section, we represent some recognition based algorithms.

a. Dhamija R. and Perrig A., [21] proposed Déjà vu in 2000. In this scheme user selects a certain random pictures from largse number of image set. This image set is generated by program in sign up phase. During authentication phase, first system presents number of images which contain both password images and decoy images. Then user must select the appropriate password images from displayed decoy and password images. It is suitable to store up and convey the images generated by small initial seeds but the images makes it difficult to record or share with others Déjà vu scheme has some weaknesses such as an ambiguous images are hard to remember and the space of password is much smaller than that of textual password passwords.

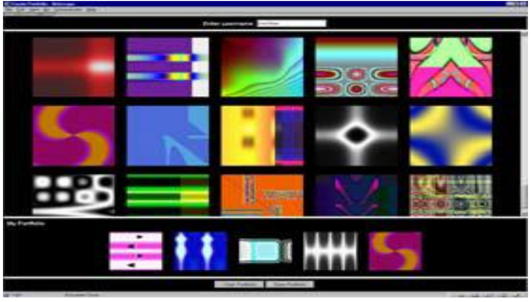


Figure.2: Déjà vu Scheme, 2000

b. Brostoff et al.[22] was proposed a PassFaces scheme in 2000.This scheme is provoked by fact that faces are more memorable for human. During registration phase, user has to select the passfaces from set of faces of male and female as a password. During authentication phase, a grid that contains 9 pictures is shown to the user as shown in Fig 3.

Figure 3: Passface Scheme, 1999

This grid just contains one of the user's passwords, and the other eight images are selected from the database.The users' password contain four faces, so that the grid is shown four times. Conversely, no grid contains faces found in the other grids, and the order of faces is also changed within each grid. These characteristics help to secure a user's Passface combination against detection through shoulder-surfing and packet-sniffing .

c. Jensen et al. [23] proposed a new graphical password scheme in 2003.This schme is known as picture password scheme.This scheme is developed for mobile PDAs. In this scheme, user has to select a theme.Images of size 40 x 40 are shown in a 5 X 6 matrix.The matrix is shown on the basis of selected theme, User should select images from that generated matrix with.

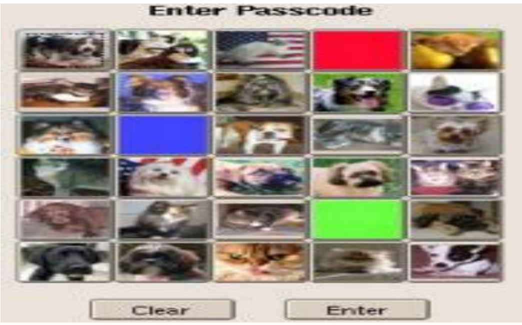


Figure 4: Jensen Scheme,2003

A order of image selection is also registered to form a password. During authentication phase, user should select the images in same sequence as in registration phase.

d. One more recognition based scheme, Story [24] is comparable to PassFaces.This scheme simply desires one phase of authentication.In this scheme,password pictures are a series of number of distinctive images that makes a story to enhance memorability. Durring authentication phase, users have to click the password pictures. The user should remember the story .In other words, order of images should be same Studies illustrate that, of over 80% of the all incorrect password entries in Story, contained all the correct images, but only their order is incorrect.

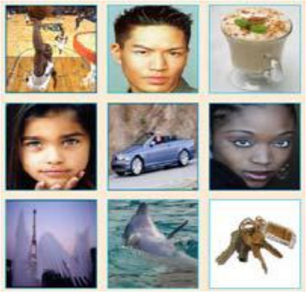


Figure 5: Story Scheme

e. Sobardo and Birget [25] developed a new scheme to resist shoulder surfing attack. During registration phase,user first selects only images from no of presented images. During authentication phase,the user should first select images same as that of selected in registration phase and then click inside that convex hull formed bythat selected images.

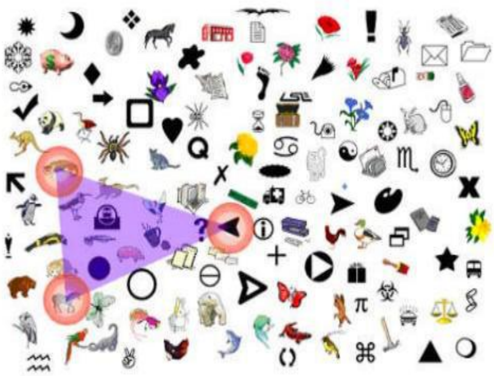


Figure 6: Sobardo and Birget Scheme,2003

f. In 2003, Man et al [26] proposed an algorithm as a new method for graphical password which is shoulder surfing resistant. In this algorithm a unique code is assigned to all the pictures. As shown in Fig 4, During authentication,the user is confrontd with numerous scenes which contain several password objects and many decoy one. There is a distinctive code for each password object, the user will enter the string of code for his own password.So that it is resistant to shoulder surfing attack.

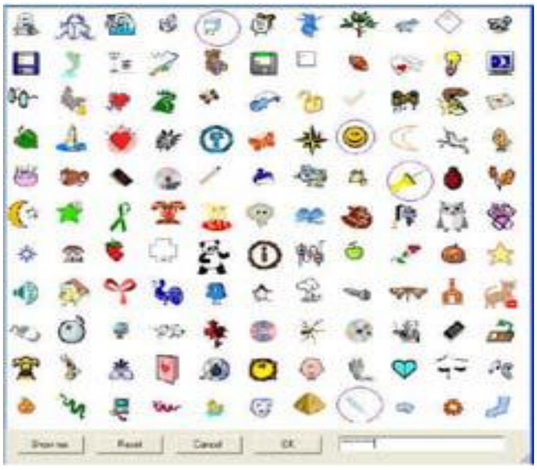


Figure 7: Man et al Scheme, 2004

IV. RECALL BASED SCHEME

Recall Based Scheme are also known as Drawmetric schemes .Some recall based schemes are studied in this section.

a. Jemryn et al. [27] proposed a scheme known as ”Draw asecret (DAS)”.In registration phase,user has to draw somewhat on a GRID of size Y X Y. The coordinates of (X,Y) of the grid were stored in the order of drawing. During login phase, user should redraw such that the drawing touches the registered series of coordinates. Password space is increased but traffic load is reduced, since images were not transferred over network.

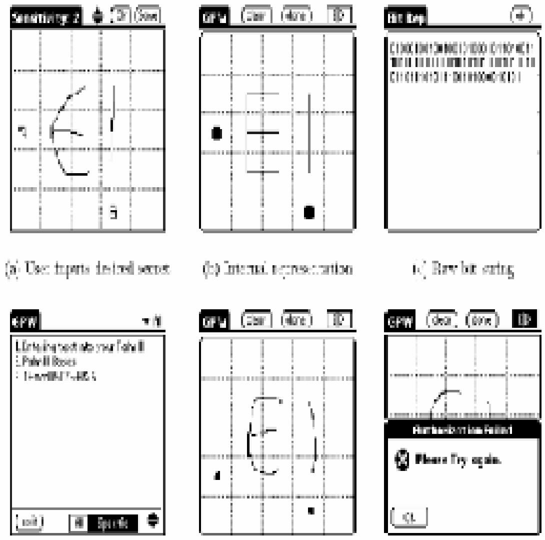


Fig. 8 Jermyn et al. DAS Scheme

b. G.E blonder [28] proposed a scheme in which a image is offered to user with tap regions. During authentication, user should click within those tap regions but user should click in a sequence. The drawbacks of this scheme was password space because , user cannot click anywhere he wants because of predetermined tap regions.

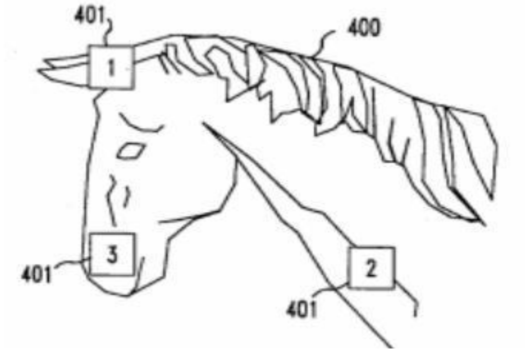


Fig. 9. Blonder Scheme

c. Passlogix [29] has proposed various graphical scheme.These schemes are base on the fact of repeating a series of actions. In the v-Go scheme, user,, bedroom bathroom.Then user can do different actions with objects shown in image such as clicking, dragging etc. Clicks on object is identified with the help of invisible boundaries on them. The drawback of this scheme is users may select weak passwords. Second is password space is small.

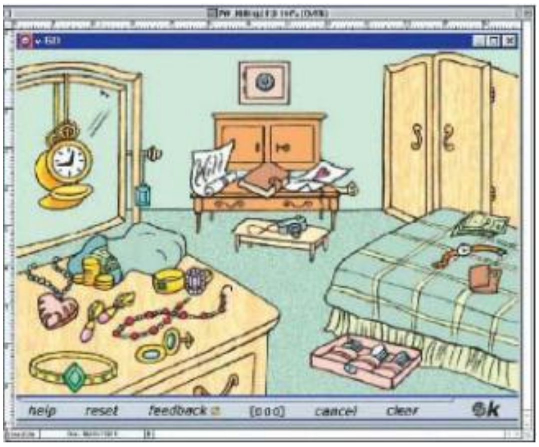
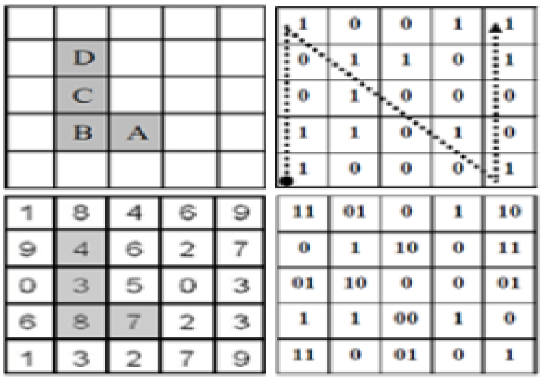


Fig. 10 v-Go Scheme

V. HYBRID SCHEME

a. GrIDsure [30] proposed a new scheme as a commercial product known as graphical one-time PIN scheme.This scheme is scheme which makes PINs more resistant to shoulder-surfing attacks. In this scheme grids are used fornpassword. During registration phase, users first choose the shape and then memorize the shape (e.g. an “L” shape) and the order in a *5×5* grid, and then enter the series of numbers using a keyboard. This selected shapes and their order of cells is known as user’s pattern, representing the secret to authenticate. After that during each succeeding login attempt, the grid is settled by arbitrary numbers from 0 and 9. Users should enter the numbers that come into view in his pattern in the earlier selected order GrIDsure password is more secure.This scheme provides shoulder-surfing resistance.



	D			
	C			
	B	A		

1	0	0	1	1
0	1	1	0	1
0	1	0	0	0
1	1	0	1	0
1	0	0	0	1

1	8	4	6	9
9	4	6	2	7
0	3	5	0	3
6	8	7	2	3
1	3	2	7	9

11	01	0	1	10
0	1	10	0	11
01	10	0	0	01
1	1	00	1	0
11	0	01	0	1

Fig. 11. GrIDure Scheme

b. Man, et al. [31] proposed one more shoulder surfing attack resistant scheme. In this scheme, user first select number of images as pass-objects.

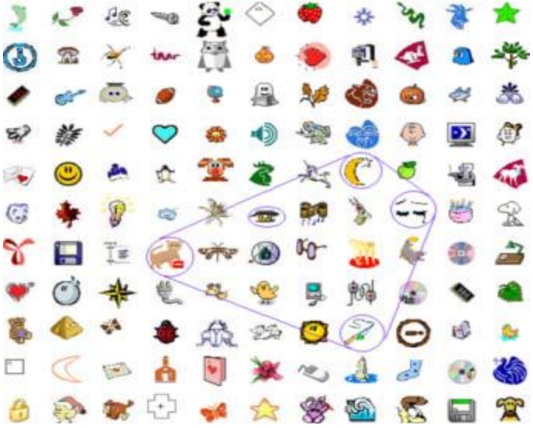


Fig. 11. Man, et al Scheme

Each pass image have several variants. Each variant has a unique code assigned. In authentication phase, users first enter a string with the unique code of the pass-objects variants. This code representing the relative location of the pass-objects with reference to a pair of eyes in numerous rounds provided by the system. This scheme is also totally resistant to shoulder surfing attack. It needed users to remember a significant amount of code analogous to the pass-objects variants.

TABLE I DIFFERENT GRAPHICAL PASSWORD SCHEMES

SCHEMES	**Login Interface**	**PASSWORD SPACE**	**DICTIONARY ATTACK**	**SHOULDER SURFING ATTACK**	**SPYWARE ATTACK**
Deja Vu	Identify correct pass images	16	Y	N	Screen
Jensen et al.	Select images based on a theme	11	Y	N	Screen
Passfaces	Select face from of grid of faces	13	N	N	Screen
Story	User has to remember the sequence of images which form a story	12	Y	N	Screen
Sobardo and Birget	Select object from number of display	32	Y	Y	Y
Hong et al.	login screen divided in to grids each grid containing a icon	Unknown	Y	N	Screen
Blonder	Click within those tap regions and in a sequence.	Unknown	Y	N	N
DAS	Redraw such that the drawing touches the registered sequence of coordinates	Unknown	N	N	Y
v-Go	Repeating a sequence of actions	Unknown	N	N	Y
GrIDsure	The order that user want to enter the corresponding numbers in a 5×5 grid, and enter the sequence numbers using a keyboard.	18	N	Y	Y
Man et.al.	In this scheme, users select several images as pass-objects which have many variants.Each variant is assigned with a unique code.	Unknown	Y	Y	Y

VI. CONCLUSION

In this paper, different graphical password schemes are studied. An algorithms of recognition-based, pure recall-based, cued recall-based, and hybrid schemes of graphical password schemes are analyzed and studied. During our research, we discover login interface, password space required and resistance against various attacks such as shoulder surfing attack, dictionary attack etc.Therefore, it can be concluded that the common drawbacks on these graphical password methods and how to overcome these attacks. Then, we tried to survey on attack patterns and define common attacks in graphical password authentication methods. Finally we make a comparison table among various graphical password authentication techniques based on attack patterns.

ACKNOWLEDGMENT

I have a great pleasure in presenting the paper on ” A Comparative Study Of Graphical Passwords And Their Security Issues ”under the guidance of Mr. R.N. Devikar I am truly indebted and grateful to Head of Department Prof. B. S. Borkar for their valuable guidance and encouragement. I take an opportunity to thank all the staff members of our department. Finally I express my sincere thanks to all those who helped me directly or indirectly in many ways in completion of this seminar work.

REFERENCES

[1] K. Renaud. “Evaluating authentication mechanisms”. In L. Cranor and S. Garnkel, editors, *Security and Usability: Designing Secure Systems That People Can Use*, chapter 6, pp.103-128. O'Reilly Media, 2005.

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

[3] D. Feldmeier and P. Karn. “UNIX Password Security-Ten Years Later”. *In Crypto'89*, August 1989.

[4] R. Morris and K. Thompson. “Password Security: A Case History”. *Communications of the ACM*, 22(11):594-597, 1979.

[5] D. Florencio and C. Herley. “A large-scale study of WWW password habits”. *In 16th ACM International World Wide Web Conference (WWW)*, May 2007.

[6] A. Adams, M. A. Sasse, and P. Lunt. “Making passwords secure and usable”. *In HCI 97: Proceedings of HCI on People and Computers*, pp.1-19, London, UK, 1997.

© 2015, IJARCSSE All Rights Reserved

[7] G. Blonder. “Graphical passwords”. *United States Patent*, 5,559,961, 1996.

[8] B. Kirkpatrick. “An experimental study of memory”. *Psychological Review,* 1:602-609, 1894

[9] S. Madigan. “Picture memory”. In J. Yuille, editor, *Imagery, Memory, and Cognition: Essays in Honor of Allan Paivio*, chapter 3, pp.65-89. Lawrence Erlbaum Associates, 1983.

[10] A. Paivio, T. Rogers, and P. C. Smythe. “Why are pictures easier to recall than words?”, *Psychonomic Science,* 11(4):137-138, 1968.

[11] R. Shepard. “Recognition memory for words, sentences, and pictures”. *Journal of Verbal Learning and Verbal Behavior,* 6:156-163, 1967.

[12] A. Paivio. “Mind and Its Evolution”, *A Dual Coding Theoretical Approach*. Lawrence Erlbaum: Mahwah, N.J., 2006.

[13] X. Suo, Y. Zhu, and G. Owen. “Graphical passwords: A survey”. *In Annual Computer Security Applications Conference (ACSAC)*, December 2005.

[14] R. Biddle, S. Chiasson, and P.C. van Oorschot. “Graphical passwords: Learning from the First Twelve Years”. *ACM Computing Surveys*, 44(4), Article 19:1-41.

[15] X.Y. Liu., J.H. Qiu., L.C. Ma., H.C. Gao., etc., “A Novel Cued-recall Graphical Password Scheme”, *In sixth International Conference on Image and Graphics (ICIG),* pp.949-956, 2011.

[16] H.C. Gao., Z.J. Ren., X.L. Chang., X.Y. Liu., etc., “A New Graphical Password Scheme Resistant to Shoulder-Surfing”, *International Conference on Cyberworlds (CW),* pp.194-199, December 2010.

[17] D. Nali and J. Thorpe. “Analyzing user choice in graphical passwords”. *Technical Report TR-04-01, School of Computer Science,* Carleton University, May 2004.

[18] H. Tao. “Pass-Go, a new graphical password scheme”. *Master's thesis, School of Information Technology and Engineering,* University of Ottawa, June 2006.

[19] H. Tao and C. Adams. “Pass-Go: A proposal to improve the usability of graphical passwords”. *International Journal of Network Security,*7(2):273-292, 2008.

[20] J. Thorpe. “On the Predictability and Security of User Choice in Passwords”. *PhD thesis, School of Computer Science*, Carleton University, January 2008.

[21] Dhamija R. and Perrig A., “Déjà vu: A User Study Using Images for Authentication”, *in Proceedings of 9th USENIX Security Symposium*, 2000.

[22] Sacha Brostoff, M. Angela Sasse, “Are Passfaces More Usable Than Passwords?:, *A Field Trial Investigation,* 2000.

[23] Jansen, W. Gavrila, S. Korolev, V. Ayers, R. Swanstrom, “Picture Password: A Visual Login Technique for Mobile Devices”, NISTt NISTIR 7030, 2003

[24] Davis, F. Monrose, and M. K. Reiter, “On user choice in graphical password schemes”, *in Proceedings of the 13th Usenix Security Symposium*.s San Diego, CA, 2004.

[25] Sobrado, L and Birget, J. “Grap hical Passwords”, The Rutgers Scholar, An Electronic Bulletin of Undergraduate Research, Ruthgers University, New Jersey, Vol.4, 2004.

[26] S. Wiedenbeck, J. Waters, L. Sobrado, and J. Birget.“Design and evaluation of a shoulder-surfing resistant graphical password scheme”. *In International WorkingConference on Advanced Visual Interfaces (AVI),* May 2006.

[27] I. Jermyn, A. Mayer, F. Monrose. M. K. Reiter and A. D. Rubin, “The Design and Analysis of GraphicalPasswords”, In Proceedings of the 8th USENIX Security Symposium,1999.

[28] G. Blonder, “Grap hical Password”, In Lucent Technologies,Inc., M urray Hill, NJ,United States Patent 5559961, 1996. Passlogix, http://www.passlogix.com, Accessed on February 2007.

[29]] Passlogix, http://www.passlogix.com, Accessed on February 2007.

[30] Brostoff, S., Inglesant, P., &Sasse, A. M. “Evaluating the usability and security of a graphical one-time PIN system”. *24th BCS Conference on Human Computer Interaction*.

[31] S. Man, D. Hong, and M. Mathews, "A shoulder surfing resistant graphical password scheme," in *Proceedings of Intenational conference on security.*