Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 45 (2015) 477 – 484

Procedia Computer Science

International Conference on Advanced Computing Technologies and Applications (ICACTA-2015)

# Shoulder-Surfing Resistant Graphical Password System

Amish Shah[a],Parth Ved[a],Avani Deora[a], Arjun Jaiswal[b], Mitchell D'silva[b]

[a]Student, Information Technology Department, DJSCOE, Vile Parle (W), Mumbai-56, India
[b]Assistant Professor, Information Technology Department, DJSCOE, Vile Parle (W), Mumbai-56, India

## Abstract

Graphical passwords consist of selecting images or drawing symbols rather than entering textual characters. They can be considered as an alternative to overcome the problems that arise from the text-based passwords system. It has been suggested that graphical passwords are harder to guess or to be broken by brute force attack. Also, the dictionary attacks are difficult. After a comprehensive study on various graphical password schemes, we propose a design to minimize the search time to find the pass-images on a login screen. The scheme proposed is currently under implementation and will be tested for usability and security verification.

Peer-review under responsibility of scientific committee of International Conference on Advanced Computing Technologies and Applications (ICACTA-2015).

*Keywords:* passwords;graphical; authentication; pass-objects; login

## 1. Introduction

Text based passwords are the most widely used for authentication. But this traditional technique has its own flaws and is vulnerable to attacks. One of them is the shoulder surfing attack that can be performed by an antagonist to obtain the user's password by watching over the user's shoulder as he enters his password. Traditionally, shoulder surfing attacks also called "peeping attacks" concerns moved from telephone calling card fraud to automated teller machine (ATM) fraud, and more recently to mobile computer users.

* Corresponding author. Tel.:+91-9619220036.
*E-mail address:* shahamish150294@gmail.com

Peer-review under responsibility of scientific committee of International Conference on Advanced Computing Technologies and Applications (ICACTA-2015).
doi:10.1016/j.procs.2015.03.084

Most graphical authentication systems are based on either recognition or recall [14]. In recognition-based systems a user must recognize images chosen during registration phase from a bulkier group of decoy images. There can be only 2 possibilities that the image is recognized or unknown [13]. In recall-based password systems users must click on several areas chosen at the time of registration in an image, cued by viewing the image. It is known that recognition memory is better than unaided recall [7].

Furthermore, psychological studies show that images are recognized with very high accuracy (up to 98 per cent) after a two hour delay, which is much higher than accuracy for words and sentences [8]. Hence, we propose a scheme to improve some recognition based systems which not only reduce the threat of shoulder-surfing but also has an added benefit of expeditious recognition and usability, thus reducing some flaws of recognition based systems.

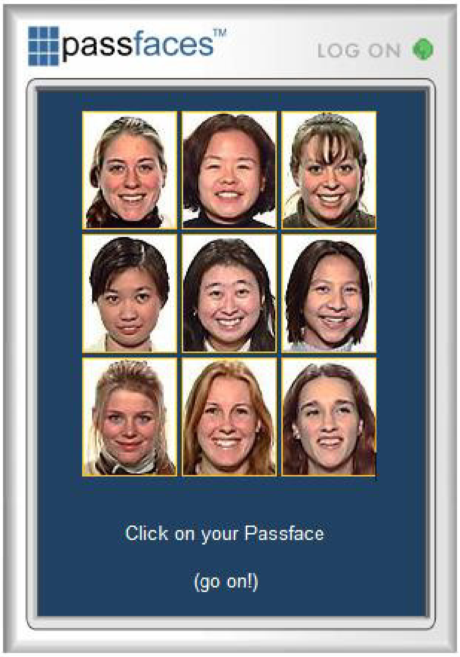
The paper discusses related work in the field of password authentication followed by the description of the proposed scheme. The future work and development in the proposed system concludes the paper.

## 2. Related Work

Some of the graphical password systems are given below:

### 2.1 Passfaces$^{TM}$[2]:

It is a commercial product by Passfaces Corporation. It requires user to select previously seen human faces picture as password. During the login process, the user is required to choose the correct face out of other faces to login. However, such systems are easily anticipated as they are affected by race, gender and attractiveness.



Click on your Passface

Fig. 1.Passfaces$^{TM}$ (passfaces$^{TM}$, 2006)

### 2.2 Pattern Lock[3]:

Nine points are presented to the user. He is supposed to form a pattern by selecting all or some of these points. This pattern is registered and every time the user wants to log in he should enter the same password by joining to points. If the pattern formed is correct the user is granted further access. This scheme is commonly used in smartphones.

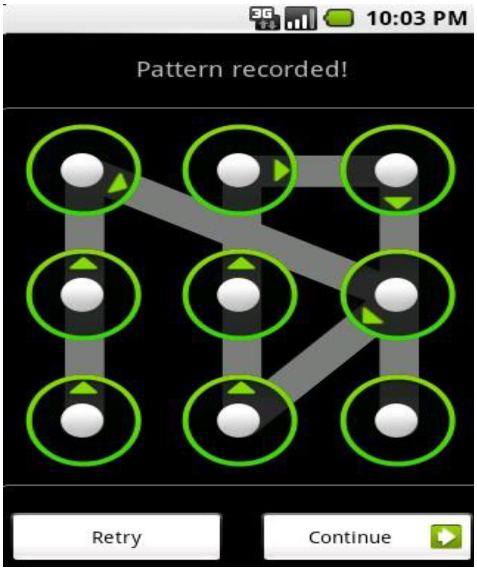


Fig. 2.Pattern Lock (free animation hub, 2012)

## 2.3 Jensen et al. Method[4]:

Based on image selection, a numerical sequence is registered to form a password. At login time user has to recognize same images in same sequence at login time. Main flaw was that password space was small since, the no of images were limited to 30.

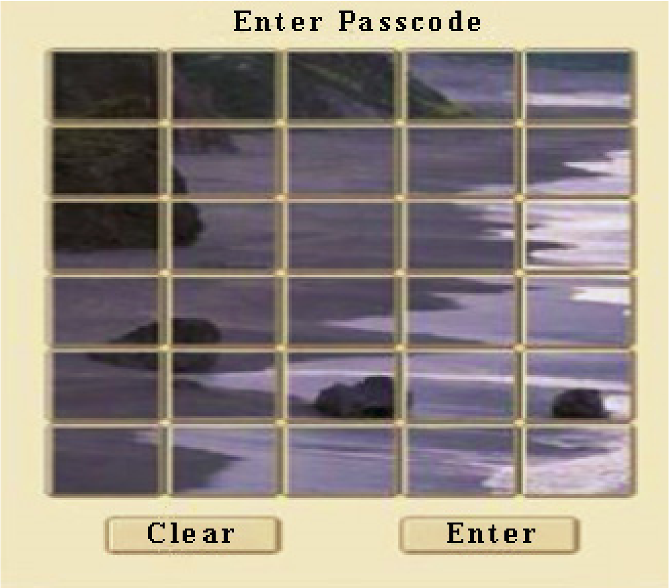


Fig. 3. Cats and dogs theme

## 2.4 Dhamiga and Perrig Method[5]:

Dhamiga and Perrig proposed a scheme called “Déjà vu”. It is based on human ability to remember previously seen pictures. User has to select few pictures from a set of previously. User has to perform same at login time. All abstract images were generated using Andrej Bauer’s random Art. They showed 90 % success rate using “Déjà vu” while only 70% using text-based password and pins. Perhaps shoulder surfing problem is one of the biggest problem for existing graphical authentication. If a person observes a few login rounds can deduce the password. The method stated leaks the pass-images to anybody watching the login screen. Due to susceptibility to such attacks, graphical passwords could never be used in situations where the login is to be done in the presence of people other than the users. However, it is feasible to develop schemes to impede the shoulder surfing problems.

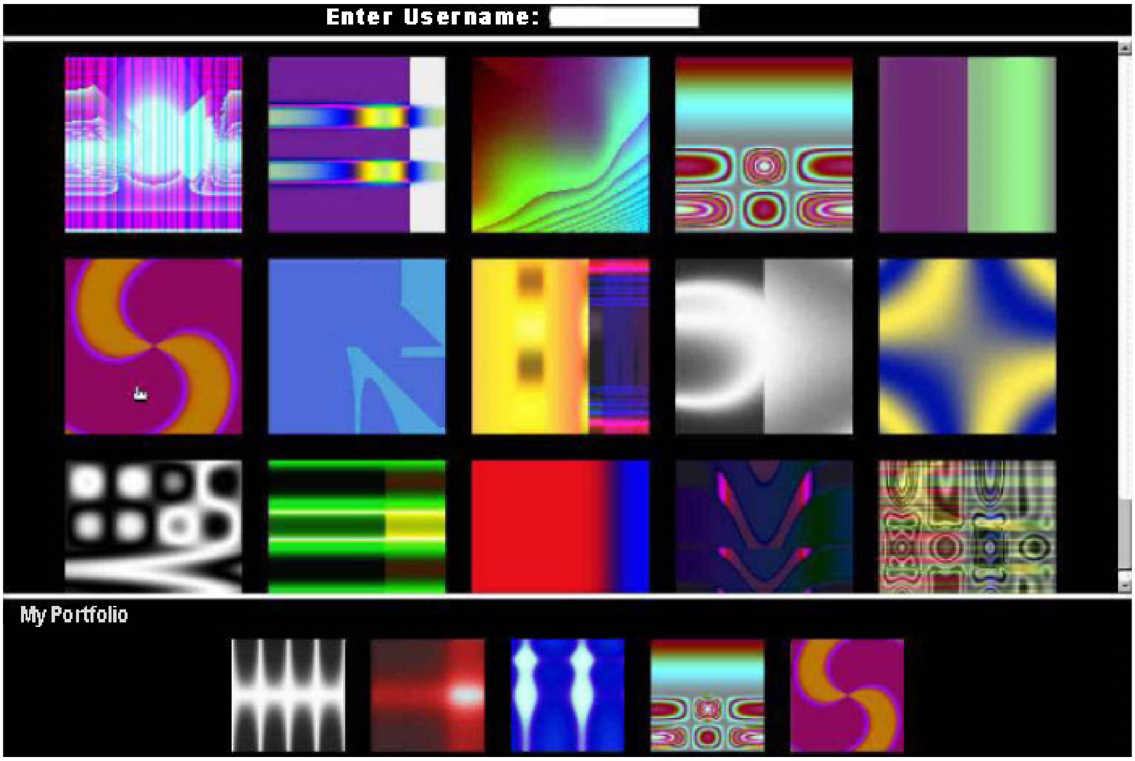


Fig. 4. Dhamiga and Perig Method

## 2.5 Pict-O-Lock[9]:

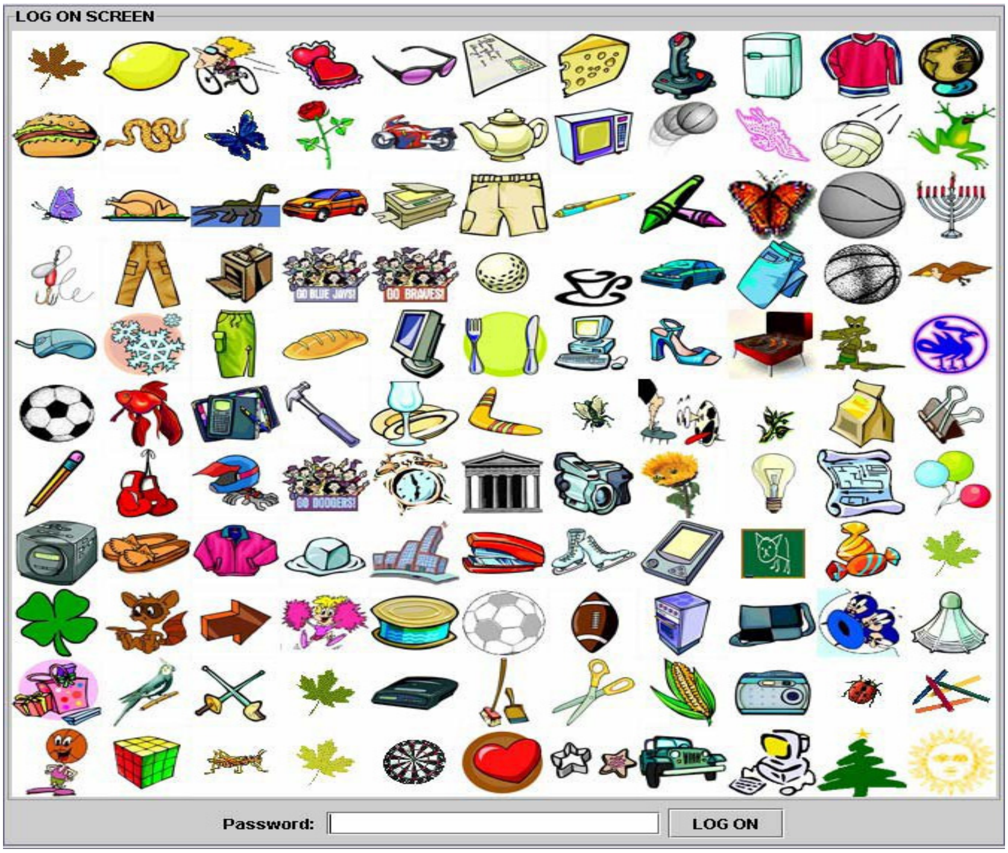


Fig.5.Pict O Lock

In this scheme, each word or character of a password was associated with a pass-image object. For example, if the password has a "0" then it could be associated with any symbol or object appearing as a "0". However, the registration process of this scheme is quite long. The login also becomes very exhausting and sluggish.

## 2.6 Sobrado and Birget (Movable Frame Scheme)[1]

User has to locate 3 pass-objects out of K pass-objects. Out of 3 pass-objects, 1 pass-object is placed in movable frame. The user needs to move the frame like a tape and line it up as per registered alignment with the other pass-object as shown below.

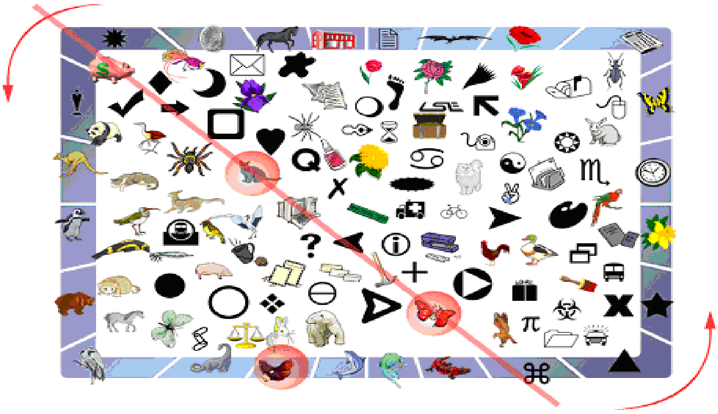
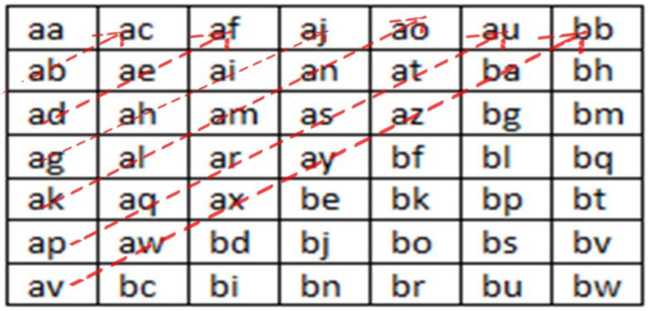


Fig.6. Movable frame scheme

The system recommends using about 1000 objects on the screen. However, detecting 3 objects from 1000 is tedious and time-consuming [1].

### 3. Our Proposed Scheme:

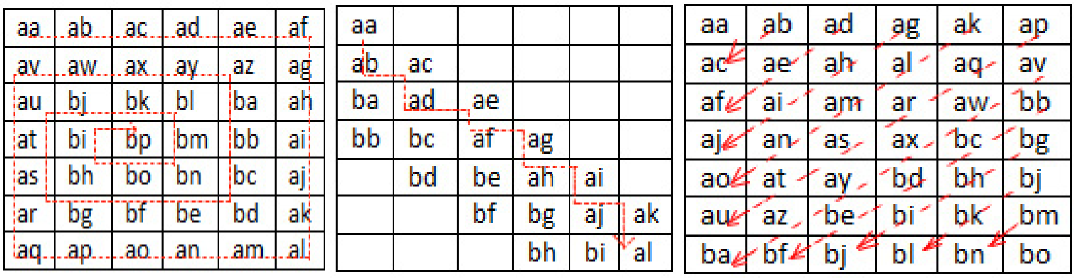
In this section, we will consider a shoulder surfing resistant graphical password scheme based on Sobrado and Birget scheme (Mobile frames scheme).The movable frame scheme by Sobrado and Birget[1] is a recognition-based graphical password authentication scheme. To allow the user to quickly recognize the password symbols on the screen, we propose that instead of using objects in images use texts in images which will lead to quicker recognition and hence we can make use of more images that will in turn lead to higher password space [17]. A simple login screen can be shown below:



| | | | | | | |
|---|---|---|---|---|---|---|
| aa | ac | af | aj | ao | au | bb |
| ab | ae | ai | an | at | ba | bh |
| ad | ah | am | as | az | bg | bm |
| ag | al | ar | ay | bf | bl | bq |
| ak | aq | ax | be | bk | bp | bt |
| ap | aw | bd | bj | bo | bs | bv |
| av | bc | bi | bn | br | bu | bw |

Fig.7. Simple login screen example

The user can select an alphanumeric passphrase at the time of registration. For simplicity, we assume that the user will choose a password containing only alphabets with length of six. Also, we consider that each image on the login page contain two characters in it. Suppose if the password is "abbcbz". The user will have move the frames with characters "ab", "bc" and "bz" and arrange them as per the alignment chosen during registration. The user can move each frame (a row or a column) in the grid which would increase usability and reduce random login. To enhance recognisability, we can arrange the alphanumeric characters in specific patterns for every new login session. Some examples of the patterns are displayed below.



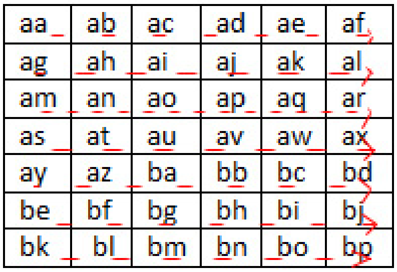
|  |  |  |  |  |  |
|---|---|---|---|---|---|
| aa | ab | ac | ad | ae | af |
| av | aw | ax | ay | az | ag |
| au | bj | bk | bl | ba | ah |
| at | bi | bp | bm | bb | ai |
| as | bh | bo | bn | bc | aj |
| ar | bg | bf | be | bd | ak |
| aq | ap | ao | an | am | al |

|  |  |  |  |  |  |
|---|---|---|---|---|---|
| aa |  |  |  |  |  |
| ab | ac |  |  |  |  |
| ba | ad | ae |  |  |  |
| bb | bc | af | ag |  |  |
|  | bd | be | ah | ai |  |
|  |  | bf | bg | aj | ak |
|  |  |  | bh | bi | al |

|  |  |  |  |  |  |
|---|---|---|---|---|---|
| aa | ab | ad | ag | ak | ap |
| ac | ae | ah | al | aq | av |
| af | ai | am | ar | aw | bb |
| aj | an | as | ax | bc | bg |
| ao | at | ay | bd | bh | bj |
| au | az | be | bi | bk | bm |
| ba | bf | bj | bl | bn | bo |

Fig. 8.(a) Spiral Inward pattern (b) Downward Zig-Zag pattern (c) -45 degree pattern

We can have many such patterns. However, we cannot include patterns with all characters arranged horizontally or vertically as shown below because it will give a hint about the password depending upon the frames being moved in left-right or top-down directions.



|  |  |  |  |  |  |
|---|---|---|---|---|---|
| aa | ab | ac | ad | ae | af |
| ag | ah | ai | aj | ak | al |
| am | an | ao | ap | aq | ar |
| as | at | au | av | aw | ax |
| ay | az | ba | bb | bc | bd |
| be | bf | bg | bh | bi | bj |
| bk | bl | bm | bn | bo | bp |

Fig. 9.Horizontal Arrangement

## 4. Future Work and Conclusion:

In this paper, we presented a graphical shoulder surfing resistant scheme in which the user can efficiently and effortlessly complete the login process without being concerned about shoulder surfing attacks. From a security perspective, this exploration is anticipated to bolster the development of graphical passwords especially recognition-based. Our research shows that the future developments in the field of recognition-based should concentrate on enriching the login time, usability and cognizability. So, a method for contracting the time gap in the authentication process and balancing usability will lead to better graphical password systems. Also, making these schemes available on all platforms is another area for future research.

## 5. Acknowledgements

We would like to thank our honorable Principal Dr. Hari Vasudevan of Dwarkadas J. Sanghvi College of Engineering and Dr. A. R. Joshi, Head of Department of Information Technology, for giving us access to computer laboratories and other research materials. We would like to thank Prof. Arjun Jaiswal and Prof. Michelle D'silva for guiding us in this paper. We would also like to thank S.V.K.M. for encouraging and promoting such research activities.

## 6. References:

1.Sobrado, L and Birget, J. “Graphical Passwords”, The Rutgers Scholar, Ruthgers University, New Jersey, Vol.4, ’04

2. Shoulder Shuffling Free Graphical Locker for Android Graphical Pattern Lock with Text Support for Android Devices (International Journal of Advanced Research in Computer Science)

3. Real User Corporation, PassfacesTM, www.realuser.com, Accessed on January’07.

4. Jensen et al. Method, “Picture Password:- A Visual Login Technique for Mobile Devices”, National Institute of Standards and Technology, NISTIR 7030, 2003

5.Dhamiga and Perig Method R. Dhamija and A. Perrig. ‘Déjà vu: A User Study Using Images for Authentication’, USENIX Security Symposium, 2000.

6.“Recognition memory for words, sentences, and pictures” from the Journal of Verbal Learning and Verbal Behaviour, vol.6, 1967, pp. from 156 to163.

7.Norman- The Design of Everyday Things, Basic Books, NY, 1988.

8.Shepard, R.N. Recognition memory for words, sentences, and pictures. Journal of Verbal Learning and Verbal Behavior 6, 156-163.

9.“A password scheme strongly resistant to spyware”,B. Hawes, D. Hong, M. Mathews and S. Man in Proceedings of International conference on security and management at Las Vergas, Nevada, 2004.

10. https://sites.google.com/site/passdirections/Home/resources/comparision-table

11.S. Wiedenbeck, J. Waters, J.C. Birget, A. Brodskiy, N. Memon, ``Authentication using graphical passwords: Effects of tolerance and image choice'', Symposium on Usable Privacy and Security (SOUPS), 6-8 July 2005, at Carnegie-Mellon Univ., Pittsburgh.

12. S. Man, D. Hong, B. Hayes, M. Matthews, “A password scheme strongly resistant to spyware”, Proc. Int. Conf. on Security and Management, Las Vegas, 2004, pp. 94-100.

13. Jean Camille Birget, S. Wiedenbeck, J. Waters, A. Brodskiy, N. Memon, “Authentication using graphical passwords: Basic results” , Human-Computer Interaction International (HCII 2005), Las Vegas, July 25-27, 2005.

14. Graphical Passwords: A Survey by Xiaoyuan Suo,Ying Zhu, G. Scott. Owen.

15. B. Hoanca (University of Alaska Anchorage) and K. Mock.(University of Alaska Anchorage) Screen oriented technique for reducing the incidence of shoulder surfing. SAM05 in June 2005

16. Transparent User Authentication: Biometrics, RFID and Behavioural Profiling Pg 63.

17.Protecting the Login Session from Camera Based Shoulder Surfing Attacks By Varun Kartik Almaula Pg 7- Pg 9