

# Graphical User Authentication System – An Overview

P. Baby Maruthi<sup>1</sup>, Dr. K. Sandhya Rani<sup>2</sup>

<sup>1</sup>Research Scholar: Dept of Computer Science  
S.P.M.V.V, Tirupati, Andhra Pradesh, India  
[mail2maruthi03@gmail.com](mailto:mail2maruthi03@gmail.com)

<sup>2</sup>Professor: Dept of Computer Science,  
[sandhyaranikasireddy@yahoo.co.in](mailto:sandhyaranikasireddy@yahoo.co.in)  
S.P.M.V.V, Tirupati, Andhra Pradesh, India

*Abstract- Authentication plays a vital role in information security. The traditional approach of authentication is text based authentication. Today, passwords easily guessed or broken by the attackers, so an alternative way to text passwords is graphical passwords. In this paper, the various techniques related to Graphical User Authentication namely Recall based, Recognition based and Hybrid techniques are discussed. The characteristic of each method in terms of authentication, memorability and possible attacks is also presented.*

*Keywords - Graphical User Authentication, Recall Based Authentication, Recognition based Authentication, Hybrid Based Authentication*

## 1. Introduction

User authentication is an important aspect in computer security. Authentication [1] is a process which provides and confirms the identity of a person. It is the basis for access control and user accountability. The most popular approach of authentication system is textual passwords, which is a combination of alphanumeric characters and consists of username and passwords. A password is a collection of characters or words utilized to gain access to a webpage, network resource or data. The usage of textual passwords is not secured, because people created passwords are memorable (names, birthdates, phone numbers are used as weak passwords) and these passwords can easily guessable by the attackers. On the other hand, strong passwords are hard to guess or break but it is hard to remember. When the user is not

using password frequently then there will be a chance to forget the password. Text passwords can easily guess by using the various techniques such as brute force attack, dictionary attack, social engineering, shoulder surfing, and spyware attacks.

To overcome the drawbacks of text passwords, graphical password authentication

scheme is introduced. People can recognize pictures and drawings easily than text, so graphical passwords are an alternative authentication scheme to textual passwords. Human brains can easily remember images and the text is generally harder to remember.

## 2. Graphical Password Authentication

In the graphical password [2] authentication, passwords are expected to have two basic requirements such as passwords should be easy to remember and passwords should be secured. Graphical password [3] techniques are classified into three main categories namely recall based, recognition based and Hybrid based techniques. A brief description of these techniques is described below.

### 2.1 Recall based

In recall based techniques, a user is asked to reproduce something that he or she created or selected earlier during the registration phase. Users need to produce their passwords without being given any hints or reminder. Some of the recall based techniques such as pass doodle, Draw a Secret (DAS) and pass point are presented below.

Goldberg et al. [4] proposed a technique called "Pass doodle". This technique comprised of handwritten designs or text, usually drawn with a stylus onto a sensitive touch screen. In this

scheme, users able to remember complete doodle images as accurately as alphanumeric passwords. Pass doodle allows the user to create a freehand drawing as a password. A doodle consists of at least two pen-strokes placed anywhere on the screen, also user can draw color doodles also. An example of pass doodles is shown in the Fig 1.



Fig 1: Pass doodle

The limitations of pass doodle are users were attracted by the doodles drawn by other users, and frequently entered other user's login details merely to see a different set of doodles from their own.

Draw a Secret (DAS) [5] is another recall based technique, in which user is allowed to draw a simple picture on a rectangular two-dimensional grid. Each cell in a grid is denoted by discrete rectangular coordinates(x, y). An example of DAS on 4X4 grid is shown in the Fig 2. User should redraw the picture by creating the stroke in the same sequence done in registration phase. If the drawing touches on the grid in the same sequence, then the user is authenticated.

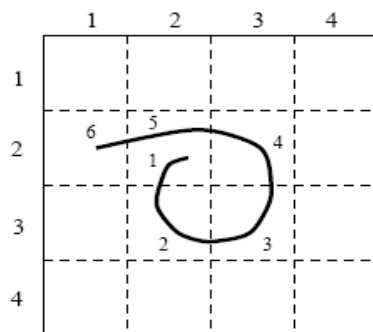


Fig 2: Draw a Secret

The limitation of DAS is user suffers difficulty in remembering and they forgot their stroke order.

Pass point [6] is one of the methods in recall based technique in which the user chooses multiple click points on a picture in some order. When login to the system, the user should select

click points that have been selected in the registration phase. An example of pass point is shown in the Fig 3, in which the user has to select the picture 1 to 5 in some sequence then the sequence of click points becomes the password.

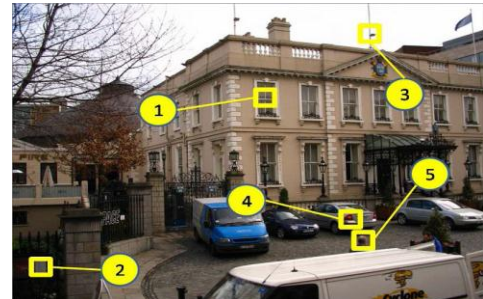


Fig 3: Pass point

The limitation of pass point method is user took more trials on the picture and he/she may guess the correct click points in the picture. Also, login time takes longer than usual alphanumeric method.

## 2.2 Recognition based

In recognition based schemes deal with identifying user images from a grid of images. Dhamija and Perrig [7] proposed a graphical authentication scheme based on the Hash Visualization technique. In this system, the user is asked to select a certain number of images from a set of random pictures generated by a program. In Fig 4, the output will be abstract random image. Later, the user will be required to identify the selected images in the order which they specified at the time of registration phase, and then the user is authenticated.

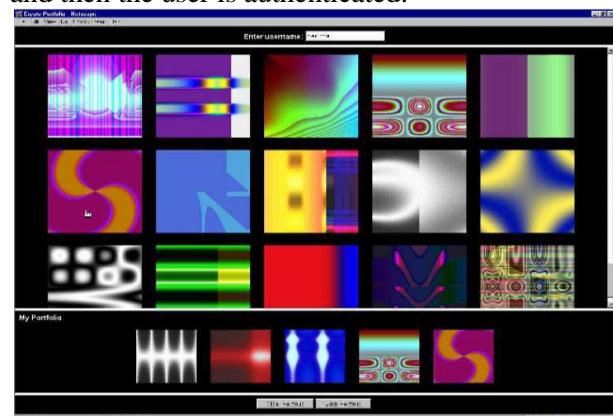


Fig 4: Random images used by Dhamija & Perrig

The drawback of this method is the server needs to store the sets of the portfolio images of each user in plain text. The process of selecting a set of pictures from the database takes time consuming for the user.

“Passface scheme is developed by Real User Corporation [8]. In this scheme, user has to select four face images from a database as a password. During authentication phase, user has a grid of size 3x3; he/she recognizes only one face among nine faces and clicks anywhere on the face. This process repeated for several rounds until he/she identifies four faces. A grid of pass face images is shown in the Fig5.

There are several limitations in the pass face, there is a chance of guessing attack and also this scheme takes longer time to process than textual passwords and also this method is uncertain.



Fig 5: Pass faces

Sobrado and Birget Scheme [9], the system displays a number of pass-object images. Among these objects, user has to click inside the convex hull bounded by pass objects. This scheme is called triangle scheme and is shown in the Fig 6.

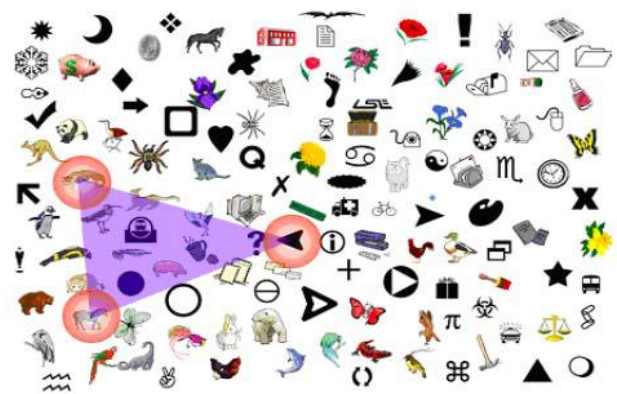


Fig 6: Triangle scheme

The main drawback of this scheme is login time takes too long and also the lots of crowded objects in the image.

### 2.3 Hybrid

Hybrid based systems are typically a combination of two or more schemes, recognition with recall based and textual with graphical password schemes.

One of the hybrid techniques is text based shoulder Surfing Resistant scheme [11]. This scheme contains sixty-four characters, including twenty six uppercase, twenty six lowercase letters and two special symbols “.” and “/”. All the sixty four characters displayed on the wheel and can be rotated either by “clockwise” button or “counter clock wise” button once and the rotation operations performed by scrolling the mouse wheel. The user needs to rotate the sector into pass-color sector. In the Fig7 & Fig 8, shows the text based shoulder surfing scheme and its rotating image.

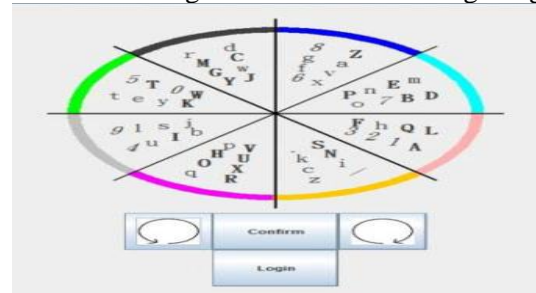


Fig 7: Text based shoulder Surfing Resistant scheme.

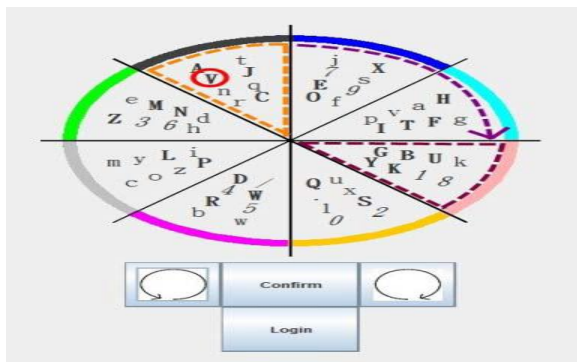


Fig8: Rotated sector image

Another hybrid [10] technique is proposed in which strings are assigned to image; user has to remember the order of the selected images and also to remember the string corresponding to the image which is assigned by the user during registration phase. User has to select the order of images from a grid and also user has to enter password at the time of login. An example of this technique is shown in the Fig9. In this figure, the user has to assign strings to each image i.e. Image1, Image2, and Image3.

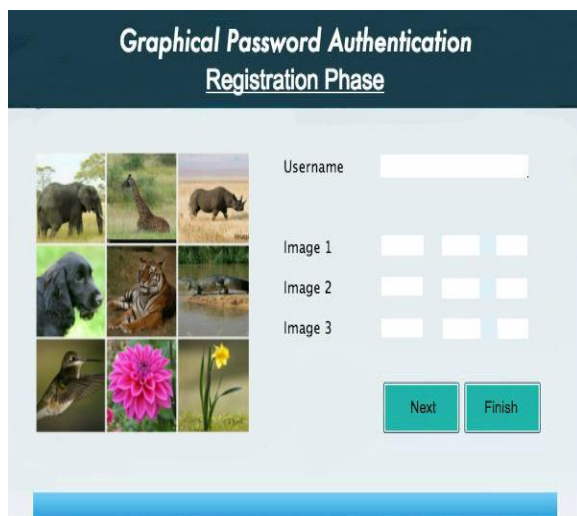


Fig 9: Combination of images with text using graphical password

The characteristics of recall, recognition and hybrid techniques in terms of authentication, memorability, possible attacks are discussed below.

Authentication:

- ❖ Recall Based- Every time signature or pictures are drawn using mouse and so the process of authentication is slow.

- ❖ Recognition Based- Recognizes registered images, so the process of authentication is fast.
- ❖ Hybrid Based- Remembering the images or text or both according to the scheme.

Memorability:

- ❖ Recall Based- Depends on what the user draw and sequence is difficult.
- ❖ Recognition Based- User can choose their own images and it is easy to remember and also easy to recognize preselected images.
- ❖ Hybrid Based- Easy to remember.

Possible Attacks:

- ❖ Recall Based- Attacks are possible and not so easy to break the password
- ❖ Recognition Based- Brute force attack, guessing, dictionary and shoulder surfing attacks is easy.
- ❖ Hybrid Based- Provides better security and not so easy for attacks.

### 3. Conclusion

This paper presents a brief description of graphical password authentication scheme. The three techniques related to graphical user authentication (GUA) namely, recognition based, recall based and hybrid based are discussed. The limitations and advantages of each method such as recall based, recognition based and hybrid based also presented. The earlier work specifies the characteristics of authentication, memorability and possible attacks in terms of security issue, hybrid technique is more effective than the other two techniques such as recall based and recognition based. Hybrid technique provides protection against attacks such as shoulder surfing, dictionary attacks, etc.

### References

- [1] Priti Jadhao, Lalit Dole, "Survey on Authentication Password Techniques", International journal of soft computing and Engineering (IJSCE), May 2013.
- [2] Graphical Passwords: A Survey Xiaoyuan Suo Ying Zhu G. Scott. Owen Department of Computer Science Georgia State University [xsuo@student.gsu.edu](mailto:xsuo@student.gsu.edu), [yzyhu@cs.gsu.edu](mailto:yzyhu@cs.gsu.edu), [owen@siggraph.org](mailto:owen@siggraph.org)
- [3] Shraddham. Gurav, leena s. Gawade, prathamey k. Rane, Nilesh r. Khochare, "graphical password authentication-a cloud securing scheme", 2014

international conference on electronic systems, signal processing and computing technologies

[4] J. Goldberg, J. Hagman, and V. Sazawal, "Doodling our way to better authentication," in *Proc. Extended Abstracts Human Factors Comput.Syst.*, 2002, pp. 868–869.

[5] I. Jermyn, A. Mayer, F. Monrose, M. K. Reiter, and A. D. Rubin, "The design and analysis of graphical passwords," in *Proc. 8th USENIX Security Symp.*, 1999, p. 1.

[6] Susan Wiedenbecka, Jim Watersa, Jean-Camille Birgetb and Alex Brodskiyc, Nasir Memon. PassPoints, "Design and longitudinal evaluation of a graphical password system", Academic Press, Inc. 102- 127, July 2005

[7] R. Dhamija and A. Perrig. "Déjà vu: A User Study Using Images for Authentication", In Proceedings of the USENIX Security Symposium, 2000.

[8] Pass faces <http://www.realuser.com>.

[9] Sobrado, J. C. Birget, Graphical passwords, <http://rutgersscholar.rutgers.edu/volume04/sobrbirg/sobrbirg.htm>.

[10] Z. Zheng, X. Liu, L. Yin, Z. Liu "A Hybrid password authentication scheme based on shape and text", *Journal of Computers*, vol.5, no.5, 2010.

[11]L. Sobrado and J.C. Birget, "Shoulder-surfing resistant graphical passwords," *Draft*, 2005.  
(<http://clam.rutgers.edu/~birget/grPsw/srgp.pdf>)