# Different Graphical Password Authentication Techniques

Dhanashree Kadu
M.E. Computer Department,
Shree L.R. Tiwari College of Engineering,
Mumbai University, India

Shanthi Therese
Assistant Professor,
Thadomal Shahani College of Engineering,
Mumbai University, India

Anil Chaturvedi
Assistant Professor,
Shree L.R. Tiwari College of Engineering,
Mumbai University, India

**Abstract**: In the field of information security user authentication is very important. To enforce security of information, passwords were introduced. User authentication is one of the important topics in information security. A strong text-based password scheme provides some degree of security. However, the fact that strong passwords are difficult to memorize often leads their owners to write them down on papers or even save them in a computer file.
Text based password is a popular authentication method used from ancient times. Text based passwords are tend to various attacks such as dictionary attacks, guessing attacks, brute force attacks and social engineering attacks etc. alternative solution to text-based authentication, is graphical password authentication.
In recent years, computer systems and Internet based environments used graphical authentication technique for their user's authentication. Numerous graphical password schemes have been proposed so far as it improves password usability and security. This paper proposed of the existing graphical password techniques, which is categorize into four techniques as recognition-based, pure recall-based, cued-recall based and hybrid based.

***Keywords:*** *Graphical password, Security, Alphanumeric Password.*

*****

## I. INTRODUCTION

In recent years, information security has been formulated as important problem. Main area of information security is authentication which the determination of whether user should be allowed access to given system or resource. In this context, password is a common and widely authentication method.
A password is a form of secret authentication that is used to control access to data. It is kept secret from unauthorized users, and these wishing to gain access are tested and are granted or denied the access based on the password according to that.
Passwords are used from ancient times itself as unique code to detect the malicious users. In modern times, passwords are used to limit access to protect computer operating systems, mobile phones, others etc. A computer user may need passwords for many uses such as log in to personal accounts, accessing e-mail from servers, retrieving files, databases, networks, web sites, etc.
Normal passwords have drawbacks such as hacked password, forgetting password and stolen password [1]. Therefore, strong authentication is needed to secure all our applications. Conventional passwords are been used for authentication but they are known to have problems in usability and security. Recent days, another method such as graphical authentication is introduced. Graphical password are been proposed as an alternative to alphanumeric password. Psychological studies have shown that people can remember images better than text. Images are generally easier to remember than alphabets and numbers, especially photos, which are even easier to remember than random pictures [2].

## II. GRAPHICAL PASSWORDS

Graphical password is an alternative option to alphanumeric passwords in which users click on images to authenticate themselves rather than typing alphanumeric words [3]. Graphical passwords are more memorable compared to alphanumeric passwords, because it is easier to remember an image of flower than a set of alphabets and numbers.
Several psychological studies have recognized human brains have apparently superior memory to recognize, recall visual information like photos as opposed to verbal or text based information [4]. Text mentally represented symbols which give meaning which is associated with the text, as opposed to a meaning perceived based on the form of the alphabets.
Using images instead of characters will help user improve the security as alphanumeric corpus size is limited. But in the case of graphical password, the size of the corpus is infinity if it is in the case multiple numbers of images or if it is in the case of multiple points in single image [5].

## III. GRAPHICAL PASSWORD METHODS

Some existing graphical password methods are as follows. Graphical based password techniques have been proposed to solve limitations of conventional text based password techniques, because pictures are easier to remember than texts. Graphical password techniques show that techniques can be categorized into four groups as follows.
A. Recognition-Based Technique: In this category, users select images, icons or symbols from a collection of images. At the time of authentication, the users need to recognize

their images, symbols, icons which are selected at the time of registration among a set of images.

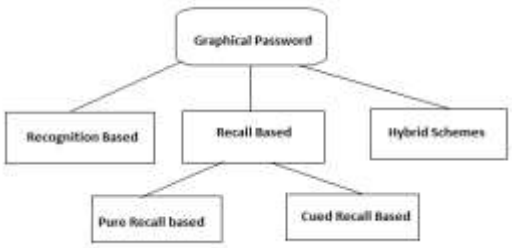


Fig.1.Categorization of Graphical password authentication techniques

B. Recall-Based Technique: This category is very easy and convenient, but it seems that users can hardly remember their passwords. Still it is more secure than the recognition based technique.
C. Cued Recall-Based Technique: In this category, users are provided with reminders or hints. Reminders help the users to reproduce their passwords or help users to reproduce the password more accurately. This is similar to recall based schemes but it is recall with cueing.
D. Hybrid Schemes: In this category, the authentication will be typically the combination of two or more schemes. These schemes are used to overcome drawbacks of single scheme, such as spyware, shoulder surfing.

## IV. RECOGNITION BASED ALGORITHMS

Recognition-based systems are also known as cognometric systems. These systems generally require that users must memorize portfolio of images during the process of password creation, and when logged in, users must recognize images from decoys. Exceptional ability of humans to recognize the images previously seen made the recognition based algorithms more popular. Various recognition based systems have proposed using different types of images, mostly like faces, icons, everyday objects, random arts etc.
The user has to identify the password pictures from the challenge set of password images and decoy images. It is easy to store and transmit random art images generated by small initial seeds and also art images make it inconvenient to record or share with others. This system having drawbacks as it is hard to remember an obscure picture and corpus size is much smaller than that of text based passwords.
Cognitive Authentication is recognition based algorithm designed to resist shoulder-surfing. If a user stands on an image belonging to the portfolio, then the user will move right or move down until the bottom or right edge of the panel is reached. Cognitive authentication system computes cumulative probability of the correct answer to ensure that was not entered by chance after each round. When probability is above a certain threshold, authentication is success.

## V. PURE RECALL BASED ALGORITHMS

Pure recall-based graphical password systems are also referred to as draw metric systems because users recall an outline drawing on a grid that they created or selected during registration phase. In these types of systems, users usually draw their password either on grid or on blank canvas. Memorability is difficult in case of recall is a difficult as retrieval is done without any reminders or cues.

A) Passdoodle: This graphical password technique is made up of handwritten design or text drawn on user screen using some input device. For authentication, user has to record a very similar doodle. So in terms of security it is much more secure from the attackers and it will be very difficult for them to guess [3].

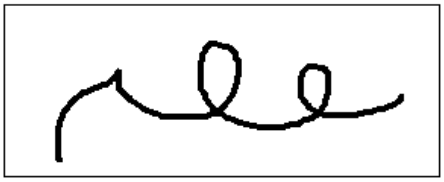

Fig.2.Example of passdoodle

B) Draw A Secret (DAS): This technique in which the user is allowed to draw a simple picture onto a 2D rectangular grid of size G * G which is denoted by discrete rectangular coordinates (x, y) without a pen up event as shown in Figure 2. For the given example, the sequence generated is (2,2), (3,2), (3,3), (2,3), (2,2), (2,1). For authentication, the user is supposed to re-draw the picture by creating stroke in the exact sequence that was used in registration phase [3][4].

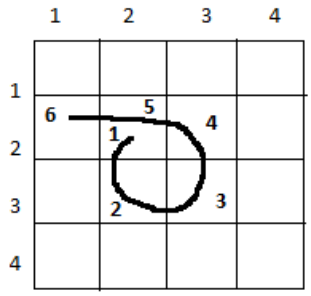


Fig.3. Draw a Secret (DAS) method on a 4*4 Grid.

C) Qualitative DAS (QDAS): It is the improved method of DAS technique in which each stroke is encoded was designed. This model is implemented using dynamic grid transformation. This method provides much more password space than DAS method and it also reduces the problem of shoulder surfing, however, it is found that it is even more difficult for the user to recall the sequence than the original DAS method [3].

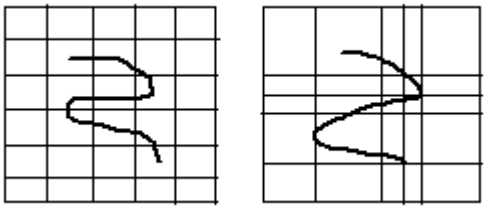

Fig.4.Example of qualitative DAS algorithm

D) Syukri: According to this algorithm user has to draw his/her signature using a mouse. Benefit of this approach is there is no requirement of memorization of signature for the user and it will be difficult for the attackers to counterfeit the same. The drawback of this scheme is that most users do not find it convenient to use the mouse for writing their signature. Pen-Tablets are useful to implement this technique but then pen-tablets are not widely available or integrated into the computing devices [3][4].

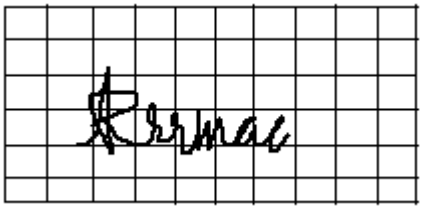

Fig.5.A sample of Syukri algorithm

## VI. CUED-RECALL BASED TECHNIQUES

A) Blonder: The first graphical password, in which a pre-determined image is presented to the user and the user is supposed to click on pre-determined regions/locations. As the area of predefined click regions was relatively small so password had to be quite long in order for it to be secure, so it may be difficult for the user to remember long password [2][3].

B) PassPoint: In this method the image could be any complex, real-world scene and there was no predetermined region, which were the shortcomings of Blonder algorithm. For registration, user has to click on the images at some locations. For authentication the user needs to click close to the selected points within some tolerance distance. With this feature the user can easily recall the password with a little bit of practice, however, the password space will be reduced if the tolerance distance is large. The problem of shoulder surfing is also not completely eliminated [3][4].

C) Passlogix v-Go: In this technique a password is created with a specific chronological order. The user can choose her preferred background image based on the surroundings, such as the living room, kitchen, or bedroom. Consecutive clicks onto the items in the scene allow the user to input her password. The action may be the replication of actions usually done in a room e.g. in a kitchen a number of items may be clicked to follow a certain recipe of the meal [3].

D) Drawing Geometry: In this scheme there are m x n grids and each grid is further divide into four parts by diagonal lines. Depending on screen size it can be changed with justifiable number of rows and columns.

## VII. HYBRID SCHEMES

Hybrid schemes are the combination of two or more graphical password schemes. These schemes are introduced to overcome the limitations of a single scheme, such as hotspot problem, shoulder surfing, spyware etc. Many single schemes on recognition-based and recall-based schemes are discussed and some of these schemes are combined to develop the hybrid schemes.

In this scheme, based on the color, templates are given to the users that contain several holes. First, the user chooses an image, then selects a colored template, then clicks on a specific location inside the image, and then selects the position to place the template and stores the password. At the time of login, the users have to choose the right template, place it on the correct location on the image then enter the characters visible through the holes from top to bottom. Memorability of the passwords in this scheme is higher than text based password as this scheme only requires users to remember the correct location of template on the image.

## VIII. CONCLUSION AND FUTURE ASPECTS

A novel Graphical Password scheme is proposed in this paper which tries to meet the criteria of ease of use and the security at the same time. The scheme has large password space and the simple implementation makes it easy for the user to create password and memorize it too. The main reason for using graphical password is they are more secure and can be recalled easily. Graphical password techniques achieve better security than conventional textual passwords. They are more accurate and reliable than textual passwords. Different algorithms from recognition-based, pure recall-based, cued recall-based, and hybrid schemes of graphical password authentication are reviewed. In this paper, we identify several advantages of graphical password authentication. Therefore, it can be concluded that it is more difficult to break graphical passwords than to break alphanumeric passwords.

## REFERENCES

[1] Eluard, M.; Maetz, Y.; Alessio, D., “Action-based graphical password: Click-a-Secret”, 2011 IEEE International Conference on Consumer Electronics, 2011, pp.265-266.

[2] P. C. van Oorschot, A. Salehi-Abari, and J. Thorpe, “Purely automated attacks on pass points-style graphical passwords,” IEEE Trans. Inf. Forensics Security, vol. 5, no. 3, pp. 393–405, Sep. 2010.

[3] Umar, M.S.; Rafiq M.Q. Ansari J.A.,”Graphical user authentication: A time interval based approach"; Signal Processing Computing and Control (ISPCC), 2012 IEEE International Conferencettsburgh, Pennsylvania, USA, ACM

[4] X. Suo, Y. Zhu, and G. S. Owen, "Graphical Passwords: A Survey", in Proceedings of the 21st Annual Computer Security Applications Conference (ACSAC 2005), IEEE Computer Society, pp. 463-472, 2005.

[5] Muhammad Daniel Hafiz, Abdul Hanan Abdullah, NorafidaIthnin, Hazinah K. Mammi; 2008, "Towards Identifying Usability and Security Features of Graphical Password in Knowledge Based Authentication Technique"; IEEE Explore.