# ANALYSIS ON GRAPHICAL PASSWORD AUTHENTICATION TECHNIQUES

**M.SRIVIDYA**
Asst. Prof, Dept of CSE,
Mahaveer Institute of Science and Technology
reddy.srividya @gmail.com

**G .MANASA**
Asst. Prof, Dept of CSE,
Mahaveer Institute of Science and Technology
manasa.587@gmail.com

***Abstract:*** *Nowadays, user authentication is one of the important topics in information security. Passwords are the most commonly used method for identifying users in computer and communication systems. Authentication is process of determining whether someone or something is, in fact who or what to be declared. For authentication mostly textual passwords are used. Strong text-based password schemes could provide with certain degree of security. Mostly passwords are strings of letters and digits, i.e., they are alpha-numeric. Such strong passwords are difficult to memorize often leads their owners to write them down on papers or even save them in a computer file, emails. Graphical passwords have emerged over the past decade as a technology that may change the way we authenticate to systems; it is a potential technology to replace typing passwords and remembering sophisticated password strategies Graphical passwords utilize the human ability to remember images and thus have the potential to increase security since longer pass-words can be used, and will be remembered for a longer period of time. However graphical password is also vulnerable to various types of attacks. In this paper we present few trending techniques in graphical passwords and its advantages and disadvantages.*

*Keywords: textual passwords, authentication, graphical passwords, information security*

## INTRODUCTION

With increase speed, evolution of systems and applications, the push for a strong computer security is growing. The majority of the computer systems and applications are preserved with user identification, authentication and confidentiality. Main area of information security is authentication, which the determination of whether user should be allowed access to given system or resource. Authentication is a process which provides and confirms the identity of a person. It is the basis for access control and user accountability. In this context, password is a common and widely authentication method. **Password** is a secure identifier that enables a user to access a secured resource. It is kept secret from unauthorized users, and those wish to gain access are tested and are approved or denied the access based on the password. 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..A password is a basic security mechanism that consists of a secret pass phrase created using alphabetic, numeric, alphanumeric and symbolic characters, or a combination, these type of passwords are called textual passwords. The usage of textual passwords is not secured, because people created passwords are memorable (birthdates, phone numbers, repeated characters, choosing names of family members are used as weak passwords) and these passwords can easily guessable by the attackers. 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, in which graphics (images) are used. The selection of regions from an image can be done rather than typing characters as in alphanumeric password approaches. Graphical passwords are better choice than the traditional alphanumeric passwords as memorization of pictures is easier than words. Human beings have the capability to recognize places they visit, other people's faces, and things. Therefore, graphical password system paves a path by presenting a lot easier to use passwords thus enhancing the security level .

## LITERATURE SURVEY

Graphical images are easily memorized then text. In this section graphical password system based on recognition, recall and captcha graphical password are discussed.

R.Biddle,S.Chiasson presents three types of graphical password. Recognition based Graphical password, cued recall graphical password, and recall based graphical password. In recognition based graphical password user need to recognize password for authentication from the set of images, users will select pictures, logos or any symbols from prestored image as password. in cued recall graphical password some sign is provided to identify password from the image. This technique is based on a framework of reminders, hints and gestures that are meant to support the user to reproduce their password or to make a reproduction more accurate. In recall based graphical password user need to recall password without any indication. Generally during password creation the users are required to memorize a series of images, and then must recognize their images from among decoys to log in.

A new technology is built over the CAPTCHA called graphical CAPTCHA which is resilient to dictionary attack and hence more secure with the hybrid use of CAPTCHA and graphical password one can address a number of security problems such as relay attacks, CARP does not act as a cure all technique but it stipulates security and usability to legitimate use in real time applications

## GRAPHICAL PASSWORD METHODS

Graphical password techniques show that techniques can be categorized as per the task to be performed in recollecting and entering the passwords. Many graphical password types have been proposed in security.User would click on a few chosen regions of it. If the correct regions were clicked in, the user would be authenticated. Memorize ability of password and efficiency of their inputs is two key human factors criteria

Mainly used graphical password techniques are

- Recognition-Based Technique
  1. Visualization
  2. Interaction
- Recall-Based Technique
  1.Pure Recall Based Techniques
  2. Cued Recall Based Techniques

- Hybrid Schemes
  1.captcha
  2.passhands

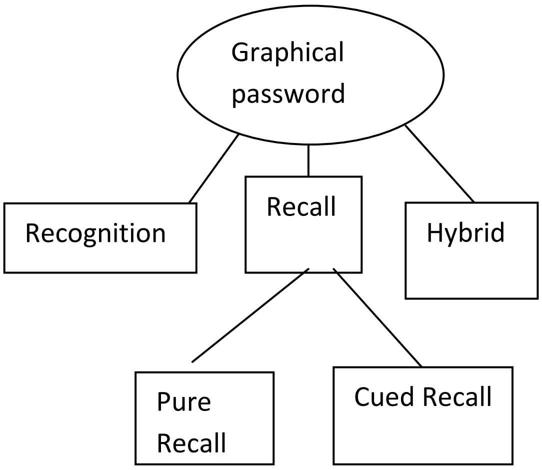

**Figure 1: classification of graphical passwords methods**

## RECOGNITION-BASED TECHNIQUES

In this technique, user is provided with set of images from which he is supposed to select the correct image which he has selected during registration phase.

There are two important factors for designing recognition based graphical passwords: visualization and interaction.

**Visualization:** Visualization has three main parameters: content, spatial layout, and distraction images. The content of the visualization is a set of images, which can be random pictures, human faces, or users' favorite images.

Spatial layout is an important factor that affects usability. In most graphical password techniques, images are presented in a matrix. But in some schemes, images are randomly placed in a 2D space. When there are too many images on the screen, the display gets overly crowded and the usability will be severely decreased – finding a target image becomes difficult. In many cases, images are grouped in pages and users would need to "page down" during the authentication process. This often makes entering graphical passwords slower than text-based ones. During the authentication stage, the user is asked to choose from a set of images, which contains a few pass-images and many distraction images. The ratio greatly affects the size of the password space.

**Interaction:** During the authentication stage, the user can interact with the system either with a mouse, keyboard, or stylus pen. With mouse, there are two options. The user can either use the mouse to select a target image, or the target image is not visually selected. For example, the program can animate the image and when the target image hits an object, the user would click the mouse button. The interaction technique also greatly affects the security aspect of the password scheme. For example, key loggers are often used to secretly record users' passwords. The sound of keyboard typing can also be used to identify the keys being typed.

**Distraction images:** Distracters are the regions of an **image** that draw attention away from the main subjects and reduce the overall **image** quality.

**Figure 1: distraction image**

## RECALL-BASED TECHNIQUES

In these techniques, a user is asked to repeat (recall) something that he/she created or selected earlier during the registration stage.

It has two categories:

- Pure Recall Based Techniques
- Cued Recall Based Techniques

**Pure Recall Based Techniques**: In this user is not provided a clue, any reminder, hints or gesture to recall a password.

Pass doodle: Pass doodle is a graphical password comprised of handwritten designs or text, usually drawn with a stylus onto a touch sensitive screen.

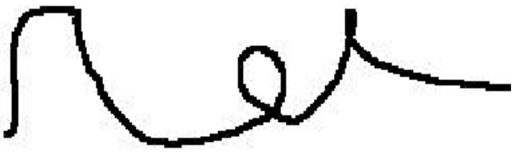

**Figure 2: Hand Written Design**

**Cued-Recall Based:** In the cued recall based technique, the image cues the user.

For example to click a set of option a set of point on an image means hint and reminder help user to reproduce their passwords.

## HYBRID TECHNIQUES

Hybrid schemes are the combination of two or more graphical password schemes.

**Captcha:** (Completed Automated Public training Turing tests to tell Computer and Humans Apart). Thus, it provides features of both Graphical Password scheme as well as CAPTCHA technology. During registration, user selects the image as their password. At the time of authentication, users choose the password image from trick of images and type the password CAPTCHA below every password image.

**Pass hands:** is a combination of recognition based and palm based biometric technique. This scheme uses image of palm of human. During the login phase, nine images are placed in 3x3 grid in which one of image is chosen as a password image. At the time of login, the Users have to compare left or right hand to that particular region which is generated by the system image and click on password image.

## ENHANCED SECURITY USING CAPTCHA AS GRAPHICAL PASSWORD

captchatrusts on the gap of capacities between individuals and bots. There are two forms of picture Captcha: textCaptcha and Image-Recognition Captcha(IRC). The previous relies on character recognition while the second relies on identification of non-character objects. safety of text Captchas has been expansively read. The following rule has been launched: text Captcha had better rely on the fight of character partitioning, which is computationally pricy and combinatorial tough. The example of captcha is shown in figure.

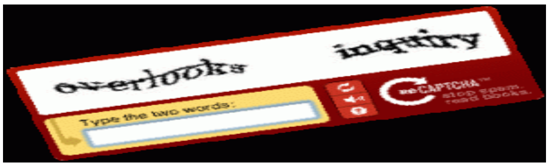

**Figure3:example of captcha**

Captcha is utilized to assist weak customer inputs on an untrusted client. This scheme shelters the communication channel between customer and Net server from key loggers and spyware, while CaRP is a family of graphical password systems for user authentication. User requests to register or login to specific pages request is sent to server and server generates the CaRP (Captcha as graphical Passwords) images. This step consists of converting the Captcha to CaRP and generating graphical images. Multiple types of images are generated like text images, 2D and 3D images. Generated CaRP images are displayed to user and user clicks on displayed images. Those resulting images are acts as user ID. Server matches the result obtained by the user. If the block matches then user logged in to specified page. Otherwise login or register attempt will failure.

Unlike other click-based graphical passwords, images used in CaRP are Captcha challenges, and a new CaRP image is generated for every login attempt. Carp offers safety against online dictionary attacks on passwords, which have been for long time a major security threat for various online services.This threat is extensive and measured as a top cyber security risk.

## LITERATURE SURVEY

Graphical images are easily memorized then text. In this section graphical password system based on recognition, recall and captcha graphical password are discussed.

R.Biddle,S.Chiasson presents three types of graphical password. Recognition based Graphical password, cued recall graphical password, and recall based graphical password. In recognition based graphical password user need to recognize password for authentication from the set of images, users will select pictures, logos or any symbols from prestored image as password. in cued recall graphical password some sign is provided to identify password from the image. This technique is based on a framework of reminders, hints and gestures that are meant to support the user to reproduce their password or to make a reproduction more accurate.In recall based graphical password user need to recall password without any indication. Generally during password creation the users are required to memorize a series of images, and then must recognize their images from among decoys to log in.

A new technology is built over the CAPTCHA called graphical CAPTCHA which is resilient to dictionary attack and hence more secure with the hybrid use of CAPTCHA and graphical password one can address a number of security problems such as relay attacks, CARP does not act as a cure all technique but it stipulates security and usability to legitimate use in real time applications

## CONCLUSION

Analysis has shown a growing interest in using graphical passwords as an alternative to the traditional text based passwords. In this paper we presented categories of graphical password techniques and focused on captcha as graphical password technique.

CAPTCHA(Completely Automatic Public Turing Test to Tell Computers and Humans Apart), are the graphical passwords which are used to generate test that only human can solve. In many online applications CAPTCHAs are used to protect from various attacks. Our groundwork analysis suggests that it is more difficult to break graphical passwords using the traditional attack methods such as brute force search, cipher text attack, dictionary attack, or spyware.

On the whole, the current graphical password techniques are still undeveloped. Much more research and user studies are needed for graphical password techniques to achieve higher levels of maturity and usefulness.

## REFERENCES

*1Jermyn, A. Mayer, F. Monrose, M. Reiter, and A. Rubin, "The designand analysis of graphical passwords," in Proc. 8th USENIX Security Symp., 1999, pp. 1–15.*

*2. Captcha as Graphical Passwords—ANew SecurityPrimitive Based on Hard AI Problems*
*Bin B. Zhu, Jeff Yan, Guanbo Bao, Maowei Yang, and Ning Xu*

*3.T. S. Ravi Kiran, and Y. Rama Krishna, ―Combining captcha and graphical passwords for user authentication‖ International Journal of Research in IT & Management, Volume 2, Issue 4 (April 2012).*

*4.Literature Survey on Data Security using Carp Two Step Authentication based on Human and Hard AI Problems .*

*5.Shubhangi G.Hande, M.S. Ali "enhancing the security using CAPTCHA as a Graphical Password" IJARCSMS, April, 2015.*

*6. R.Biddle, S. Chiasson "Graphical Password: learning from the first twelve years" ACM, 2012.*

*7.Ali Mohamed E (2008). Study and Develop a New Graphical Password System", University Technology Malaysia, Master Dissertation.*

*8.Arash HL, Rosli S, Samaneh F, Omar BZ (2009). A wide-range survey on Recall-Based Graphical User Authentications algorithms based on ISO and Attack Patterns, IJCSIS, 6: 3*

*8.H. Tao and C. Adams, "Pass-Go: A proposal to improve the usability of graphical passwords," Int. J. Netw. Security, vol. 7, no. 2, pp. 273–292, 2008*