International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 06 | June-2018 www.irjet.net p-ISSN: 2395-0072

# GRAPHICAL USER AUTHENTICATION FOR AN ALPHANUMERIC OTP

**Mrs. Suvarna. K. Kabadi[1], Mr. ZaheerAhmed Indikar[2]**

*[1]PG Student Secab Institute of Engineering and Technology Vijaypur, Karnataka*
*[2]Assistant Professor and PG Co-ordinator Secab Institute of Engineering And Technology Vijaypur, Karnataka*

---

**ABSTRACT-** *Today majority of computer systems or our day today activities are passwords. Passwords are used for authenticating users. The most widely and commonly used authentication is the traditional system "Username" and "Password", for such authentication generally text or alphanumeric is used. Alphanumeric passwords have been prone to a number of attacks. users tend to choose passwords that are easy to remember, on the other hand, if a password is hard, then it is often hard to remember. So text based passwords are easy to crack by intruders by using several techniques like, dictionary attack ,brute force attack, shoulder surfing and social engineering attack etc. Keeping these things in mind and to overcome these drawbacks it has been proposed innovative and more secure way of selecting passwords: Graphical Passwords for authenticating the users. As graphical passwords are vulnerable to shoulder surfing attack hence one-time generated password is sent to users mobile. Using the instant messaging service available in internet, user will obtain the One Time Password (OTP). The OTP gives the information of the items present in the image to be clicked by the user. The users can authenticate themselves by clicking on various items in the image based on the information sent to them.*

**Keywords:** Graphical password, Authentication, One Time Password(OTP), Token Based, Biometric, Knowledge Based, Recognition Based, Recall Based, Hybrid Based, Shoulder Surfing, Brute Force, Spyware, Social Engineering , Dictionary attack.

## 1. INTRODUCTION

Textual password is the most common method used for the Authentication purpose. Now use of internet is rapidly increasing day by day, So many transactions (Banks, College/Schools, Hospitals, online utility bill payment and online shopping sites) using internet are also increasing day by day. So password is a must for Security purposes for the users. Password are text based passwords or graphical passwords. Most of the user uses the common method i.e. the Text Based Password because that are easy to remember (weak passwords) but the lengthy passwords are hard to remember. But the main disadvantage of using Text Based Passwords are many attacks can happen like eavesdropping attack, dictionary attacks, denial of service attacks…etc. To overcome these disadvantages of Text Based Password new Graphical Passwords are used. Even Graphical Passwords(Graphical passwords consist of clicking or dragging activities on the pictures) are also susceptible to attacks such as Shoulder Surfing, So Graphical Password as an OTP and this OTP which gives the information about the items present in the image to be clicked by the user. One Time Password Authentication is proposed for enhancement in security and privacy. General Guidelines for the text based passwords are given below

1. The length of the password should be at least 8 characters long and alphanumeric.
2. Should not be easy to relate to the user Personal Information(e.g. First-Name, Last-Name, Phone-Number, Date-of-Birth, Home-Address).
3. Should not be a word that can be found in any of the dictionary.
4. Should combination of upper case letters, lower case letters and digits

Many problems and difficulties have been faced by the user because of the above mentioned guidelines of the Text based Passwords. Below mentioned are the difficulties faced by the user for using the Text based Password Scheme

1. User may forget the Password if it is too long or complicated
2. The Password remain unused for a long time.
3. Watching a user log on as they type their Password
4. Dictionary attacks

To overcome the above mentioned problems and difficulties, The Graphical Password is the better as well as alternative solution to the Text Based Password.

## 2. GRAPHICAL PASSWORD

A graphical password is a secret that a user inputs to a computer with the help of the computers' graphical input (e.g., mouse, stylus or touch screen) and output

devices. Graphical Password can be formed in the combination of Image Icons or Pictures. In other words, graphical password is an authentication system that works by having the user select from images, in a specific order, presented in a graphical user interface (GUI). Because of this reason, the graphical password approach is sometimes called graphical user authentication (GUA). Computer and Information security is very much dependent on password for the authentication of the users and are common in practice. The password design methods include Text method, Biometrics. Text method is most widely used, since it is easy to implement and use. Three basic features of Password are as follows 1. Passwords should be easy to remember. 2. User authentication protocol should be executed quickly and easily. 3. Passwords should be secure (random, hard to guess and not in plain text). One of the main pitfalls in Text-based Password is the difficulty of remembering it but these passwords can be easily guessed or broken. So Graphical Password is the alternative solution to Text based passwords.

It has the following advantages:

1. Pictures are generally easier to be remembered than text.

2. If the number of pictures is sufficiently large, the possible password space of a graphical password scheme may exceed that of text based schemes and hence may prove to offer better resistance to dictionary attacks.

3. Examples include places we visited, faces of people and things we have seen which are easy to reframe.

So it is difficult to implement automated attacks (such as dictionary attacks) against Graphical Passwords.

## 3. GRAPHICAL AUTHENTICATION TECHNIQUE

Current Authentication methods can be classified as follows:

### 3.1 Token based authentication

It is based on "Something You Possess". For example Smart Cards, ATM cards with a PIN number, a driver's license, credit card, a university ID card etc. It allows users to enter their username and password in order to obtain a token which allows them to fetch a specific resource. Once their token has been obtained, the user can offer the token - which offers access to a specific resource for a time period - to the remote site . Many token based authentication systems also use knowledge based techniques to enhance security

### 3.2 Biometric based authentication

Biometrics (ancient Greek: bios ="life", metron ="measure") is the study of automated methods for uniquely recognizing humans based upon one or more intrinsic physical or behavioral traits. It uses physiological or behavioral characteristics like fingerprint or facial scans and iris or voice recognition to identify users. A biometric scanning device takes a user's biometric data, such as an iris pattern or fingerprint scan, and converts it into digital information a computer can interpret and verify. A biometric-based authentication system may deploy one or more of the biometric technologies: voice recognition, fingerprints, face recognition, iris scan, infrared facial and hand vein thermo grams, retinal scan, hand and finger geometry, signature, gait, and keystroke dynamics. The major drawback of this approach is that such systems are expensive, and the identification process can be slow and often unreliable. However, this type of technique provides the highest level of security.

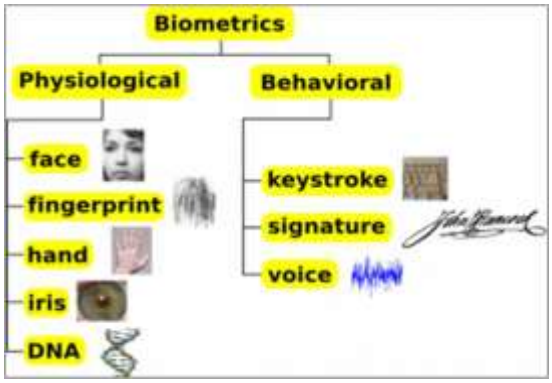


**Figure 1: Biometrics**

### 3.3 Knowledge based authentication

Knowledge based techniques are the most widely used authentication techniques and include both **text-based** and **picture-based** passwords.

The picture-based techniques can be further divided into

1. Recognition–based System

2. Recall-based System (Pure and Cued)

3. Hybrid-based System

## 4. CLASSIFICATION OF GRAPHICAL BASED PASSWORD SYSTEMS

Graphical based passwords schemes can be broadly classified into four main categories:

1. Recognition based Systems(Click, Choice, Typing)
2. Recall based Systems(Draw, Click,Typing)
    a. Pure Recall based systems
    b. Cued Recall based Systems
3. Hybrid systems

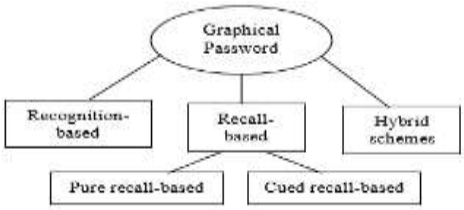


**Figure 2: Graphical Password Authentication Techniques.**

### 4.1 Recognition based Systems

Recognition based Systems which are also known as Cognometric Systems or Searchmetric Systems. Using recognition-based techniques, a user is presented with a set of images and the user passes the authentication by recognizing and identifying the images he or she selected during the registration stage.

Dhamija and Perrig proposed a graphical authentication scheme based on the Hash Visualization technique. In their system, the user is asked to select a certain number of images from a set of random pictures generated by a program. Later, the user will be required to identify the preselected images in order to be authenticated. The average log-in time, however, is longer than the traditional approach. A weakness of this system is that the server needs to store the seeds of the portfolio images of each user in plain text. Also, the process of selecting a set of pictures from the picture database can be tedious and time consuming for the user. This system is vulnerable to shoulder-surfing

**Figure 3: Random images used by Dhamija and Perrig**

"Passface" was proposed by Brostoff. Here the user will be asked to choose four images of human faces from a face database as their future password. In the authentication stage, the user sees a grid of nine (3x3) faces, consisting of one face previously chosen by the user and eight decoy faces shown in below figure. The user recognizes and clicks anywhere on the known face. This procedure is repeated for several rounds. The user is authenticated if he/she correctly identifies the four faces. The technique is based on the assumption that people can recall human faces easier than other pictures.

**Figure 4: Passfaces**

### 4.2 Recall based Systems

### 4.2(a) Pure Recall based Systems

Pure Recall based systems which are also known as Drwanmetric Systems. In pure recall-based methods the user has to reproduce their password that he or she created or selected earlier during the registration stage without being given any reminder, hints or gesture.

Jermyn et al. launched an authentication mechanism called "**Draw-A-Secret**" (DAS), which gives the user the ability to draw their desired password. Put simply, the user is required to draw a secret shape on a grid. The system then records the coordinates on the grid occupied by the drawn shape in the drawing sequence. During authentication, the user must re-draw the secret shape closely enough to the pre-stored input. The authors claim that the full password space of DAS when using an adequate length on a 5x5 grid is larger than that of the full textual password space. However showed that forgetting the stroke order or marking adjacent cells in accurately are considered to be the main reasons for incorrect match of the original password redrawing.

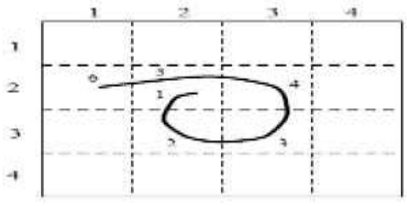

**Figure 5: Draw-A-Secret (DAS)**

The "PassPoint" system by Wiedenbeck, et al. allowing arbitrary images to be used., and the password consists of a sequence of PassPoints on a single image. Users may select n pixels in an image as click points and create their own password.. To login they select their click points again within a system defined tolerance band of the original click points (A tolerance around each chosen pixel is calculated. In order to be authenticated, the user must click within the tolerance of their chosen pixels and also in the correct sequence). Although, PassPoints is usable, it makes security a weakness and makes passwords easier for hacker to guess. It may be obvious that some areas of in an image are more attractive to users to choose as click-points.

**Figure 6: Passpoint Scheme.**

### 4.2(b) Cued Recall based Systems

Cued Recall based systems which are also called Iconmetric Systems. In cued recall-based methods, a user is provided with a hint so that he or she can recall his his/her password.

Oorschot, and Robert Biddle proposed clued click point. In preference to five click-points on one single image, CCP uses one clickable region on five distinct images. The next new image presented is based on the location of the previously entered click-point; it creates a path through an image set. Each click shows a next-image, in leads the user down a "path" as they click on their sequence of points. A wrong click leads down to an incorrect path, with an explicit indication of authentication failure only after the final click.


**Figure 7: Cued Click Points**

### 4.3 HYBRID SYSTEMS

Hybrid Systems which are typically the combination of two or more schemes. Like recognition and recall based or textual with graphical password schemes.

Zhao and Li proposed a graphical scheme known as S3PAS (Scalable Shoulder-Surfing Resistant Textual-Graphical Password Authentication Scheme), combining both textual and graphical images . Users of this scheme have two types of passwords; one fixed password which only they know (e.g. Staff number, Library ID) and one random password which is created during the login. To login, users will be displayed with the login screen which consists of the image of characters 45 displayed randomly for every round and two text boxes for inserting fixed and random password. First, users need to input the fixed passwords. To get the random password, first they need to find their fixed textual passwords represented in a graphic. Here, users‟ random passwords are actually obtained in the triangle area formed by the three of their fixed passwords. After identifying their random password, users have to insert it in the text box provided. The process would continue for several rounds and if users correctly enter both of their passwords, they would be allowed to login. To simplify the above explanation, suppose Alice enters ABCD as her fixed password. Therefore, her random passwords would be any characters in the triangle area formed by ABC, BCD, CDA and DAB (the lengths of random password will be determined by the length of fixed password).

**Figure 8: S3PAS graphical scheme**

## 5. EXISTING SYSTEM

Generation of secure one-time password based on image authentication. Here, The user will be asked to enter his user name, previously selected images (for authentication) and his email address. An one Time Password (OTP) will be generated following the submission and will be sent to the email id. The user has to

enter the particular OTP communicated through email. If OTP get verified then he will be directed to the home page.

### 5.1 VARIOUS ATTACKS

**Brute Force Attack**

The main defense against brute force search is to have a sufficiently large password space. Text-based passwords have a password space of 94^N, where N is the length of the password, 94 is the number of printable characters excluding SPACE. Some graphical password techniques have been shown to provide a password space similar to or larger than that of text-based passwords. Recognition based graphical passwords tend to have a smaller password spaces than the recall based methods. It is more difficult to carry out a brute force attack against graphical passwords than text based passwords

**Dictionary Attack**

Since recognition based graphical passwords involve mouse input instead of keyboard input, it will be impractical to carry out dictionary attacks against this type of graphical passwords. Overall, graphical passwords are less vulnerable to dictionary attacks than text-based passwords.

**Guessing Attack**

Unfortunately, it seems that graphical passwords are often predictable, a serious problem typically associated with text-based passwords. For example, studies on the Passface technique have shown that people often choose weak and predictable graphical passwords. Nali and Thorpe's study revealed similar predictability among the graphical passwords created with the DAS technique. More research efforts are needed to understand the nature of graphical passwords created by real world users.

**Spyware Attack**

Except for a few exceptions, key logging or key listening spyware cannot be used to break graphical passwords. It is not clear whether "mouse tracking" spyware will be an effective tool against graphical passwords. However, mouse motion alone is not enough to break graphical passwords. Such information has to be correlated with application information, such as window position and size, as well as timing information.

**Shoulder Surfing Attack**

Like text based passwords, most of the graphical passwords are vulnerable to shoulder surfing. At this point, only a few recognition-based techniques are designed to resist shoulder-surfing. None of the recall-based based techniques are considered should-surfing resistant.

**Social Engineering Attack**

Comparing to text based password, it is less convenient for a user to give away graphical passwords to another person. For example, it is very difficult to give away graphical passwords over the phone. Setting up a phishing web site to obtain graphical passwords would be more time consuming.

## 6. PROPOSED SYSTEM

Graphical Password as an OTP is based on Passlogix graphical password scheme (Passlogix Inc is a security company in New York city. This method repeats sequence of action, it means create a password by chronological situation. User selects the image based on the environment) which is a recall based graphical system. This system is an approach towards more reliable, secure, user-friendly, and robust authentication. It also tries to reduce the various attacks on graphical password and aims to provide a secure authentication.

In addition to the normal way of authentication that is user id and password this system uses graphical password scheme to provide more secured authentication. Here the user needs to provide textual password first and then the user needs to click on few items from an image. The items to be clicked are a one-time password (OTP) which will be sent to the user‟s mobile number by a text message from a database. The user must click on the sent items on the image provided in order to be authenticated. In addition this system also tries to authenticate the visually impaired people. This system consists of two phase Registration phase and Login phase to authenticate the user. Graphical Password as an OTP is Resistant to all the above mentioned possible attacks.

### 6.1 Registration Phase

In Registration phase user is going to register with the system by providing user id, password, email id and Mobile Number. This information will be then stored in a database which will be used to authenticate the user during next phase i.e Login Phase.

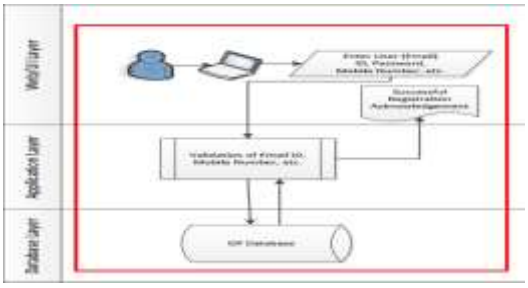

**Figure 9: Registration Phase**

### 6.2 Login Phase

In Login phase the user is asked to enter user id and password and an image with several items is displayed to the user. The system then validates the user id and password in the database. If the data matches then the system sends some items from the image to be clicked to the user‟s mobile number as an OTP. Then the user must click the items in the image in proper sequence. If the user doesn‟t click the image in some speculated time then the OTP expires. Then a new image is loaded and a new OTP will be send to the user. If the user clicks on time then the system verifies whether the user has correctly identified and clicked the items in correct sequence. If it matches the user is authenticated. Otherwise, whole process will be repeated.

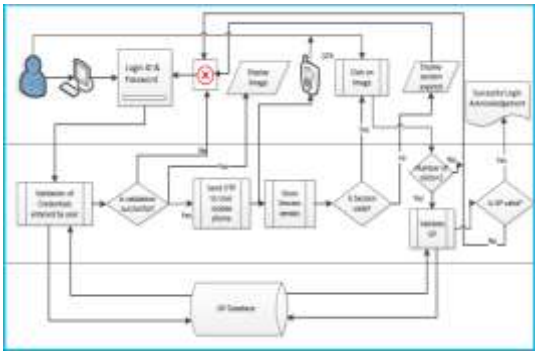

**Figure 10: Login Phase**

## 7. SECURITY ANALYSIS

Here the system selected image and system generated OTP reduces the the task for users to remember the images they selected. As this system provides multilevel authentication i.e text based password as well graphical password it overcomes the potential attack that may exploit the password space size and dictionary attack. This system tries to overcome guess ability, observe ability, and rememberance of the user's password by generating one time password as OTP expires after certain time. This system tries to avoid shoulder surfing attack. As items to be clicked is directly sent to user's personal mobile number and other person cannot overlook the password and cannot copy and re-enter the password because the password expires after certain period.

### 7.1 Comparison of Authentication Techniques

| Authentication Schemes | Cost | Protection Level | Processing Time | Additional H/W Required |
|---|---|---|---|---|
| Textual password | Low | Medium | Low | No |
| Graphical Password | High | Medium | High | Yes |
| Boimetric | High | High | High | Yes |

**TableI. Comparison of Authentication technique**

## 8. CONCLUSION AND FUTURE WORK

This system tries to avoid shoulder surfing attack, dictionary attack, brute force attack, guessing attack, Phishing attack by generating Graphical password as an OTP. The one time password is sent to user's mobile number by a text message from a database. The user must click on the sent items on the image provided in order to be authenticated. It requires large number of images in order to be secure and this will actually slow down the user authentication process.

This system can be extended by sending the one time password to user's whatsapp account for authentication. This system can be used with Visually impaired users with the inclusion of Audio Clips.

## REFERENCES

[1]. Caryn Savia Vaz, Sonia Fernendes, Razia Sardinha, Authentication Technique for Security using Ensemble Graphical Password , IJESC April 2017.

[2]. D. D. Walanjkar, Prof. Vaishali Nandedkar, User Authentication Using Graphical Password Scheme: A More Secure Approach Using Mobile Interface, IJIRCCE December 2014.

[3]. Anagha Gaikwad, Bharti Gadkar, Bhagyahri Jadhav, Kanchan Bobade, Prof. Rohit Bamne, A Survey on Shoulder

Surfing Resistant Graphical Authentication System, IJETCS May 2017.

[4]. S. Eswaran, A. Ashok, R. Hari Krishnan, Graphical passwords effects of tolerance password, image choice and OTP Login, IJRE January 2017.

[5]. Ankesh Khandelwal ,Shashank Singh , Niraj Satnalika , User Authentication by Secured Graphical Password Implementation.

[6]. Brajesh Kumar Kushwaha, An Approach for the user Authentcation One Time Password(Numeric and Graphical) Scheme. JGRCS November 2012.

[7]. Wazir Zada Khan, Mohammed Y Aalsalem and Yang Xiang, A Graphical Password Based System for Small Mobile Devices, IJCSI September 2011.

[8]. Sirisha.G, V.Suryanarayana garu, Dynamic Authentication over Graphical Passwords using Visual Cryptography, IJRCCT, August 2015.

[9]. Veena Rathanavel, Swati Mali, Graphical Password as an OTP, IJECS January 2017.

[10]. A Study of Graphical Alternatives for the User Authentication by Mohd. Zalisham Jali. 2011.

[11]. Graphical One-Time Password Authentication , Hussain. S. Alsaiari 2016.

[12]. Shritika Waykar, Tejaswini Barhate, Nidhi Iche, Survey of Various Password Authentication Schemes, IJSRSET 2018.

[13]. Sourav Kumar Dandapat,Bivas Mitra,Romit Roy Choudhury,Niloy Ganguly, ActivPass: Your Daily Activity is Your Password ,April 2015.

[14]. Neha Vishwakarma, Kopal Gangrade, Secure Image Based One Time Password, IJSR November 2016.

[15]. Saranya Ramanan, Bindhu J S, A Survey on Different Graphical PasswordAuthentication Techniques, IJIRCCE December 2014.

[16]. Himika Parmar, Nancy Nainan and Sumaiya Thaseen, Generation of Secure One Time Password Based on Image Authentication, CSIT.

[17]. V. Bhusari, Graphical Authentication Based Techniques, IJSRP July 2013.

[18]. Rebeiro Caroline Leontia Carlton Christopher1, Huda Noordean, A Survey on Graphical Password Authentication System and their Security Issues, IJIRSET June 2017

[19]. Priti S. Katkade 1, Dr. Shubhas K. Shinde, Secured Hybrid Authentication Schemes using Session Password and Steganography, IJIRCCE April 2016

[20]. Yash Khandelwal1, Jay Shah2, Shaunak Shah3,, Neha Katre, Hybrid Authentication Technique, IJARCCE September 2015.

[21] Ejike Ekeke Kingsley Ugochukwu, Yusmadi Yah Jusoh, A Review on the Graphical User Authentication Algorithm: Recognition-based and Recall-based, International Journal of Information Processing and Management · May 2013

[22] Aishwarya N. Sonar, Purva D. Suryavanshi, Pratiksha R. Navarkle, Prof. Vijay N. Kukre , Survey on Graphical Password Authentication Techniques, IRJET February 2018