# Authentication using Images as Password for Providing High Security in Networks

**Kavya H C**

PG Student, Department of Computer Science, SJBIT, Bengaluru, India

**Abstract:** Graphical Password Authentication has been accepted and there is a significant increase in usage of it. As using Text based password is common throughout all the domain areas, it creates the situation where incase if a user selects a password that he can easily remember then an attacker is provided with an oppurtunity to easily guess. If user selects a password that an attacker could not guess, then it becomes hard to remember for the user. So, Graphical password scheme is used as humans can easily remember images compared to alphabets or numbers. The focus here is to replace the static images used in graphical password system with the tokens. Usually the server would store the images and display it for the user while log in. But this would provide an option for an attacker to easily know the password by using some hacking techniques. Here, the user is responsible to get the image that which he wants to make it as a password. Moreover, the image that he gives it as a password is not at all stored in the server. User has to give in his own image which he has selected and then choose some five locations in that. It is converted to some value and then stored in the server. In this way an attacker is restricted a little as he would never know which image the user has uploaded during registration and he would not have it as it would be the personal image of the user. Even though if an attacker somehow got to know what is been stored in server by using some attacks, he can get only converted value not full data about it. Usability, reliability, and security against observation is provided. The study shows that there would be a threshold set, only when the password items match with the originals it is said to be equivalent. Resistance to observation attack is increased by using this approach.

**Keywords:** Graphical password, Security, Shoulder surfing, Authentication.

## I. INTRODUCTION

Internet can connect many people throughout the world at the same time and acts as boon to the society but also it creates security problems along with it. For an organization it is necessary to protect internet resources from all the security threats. Security has become the most important concern in all the fields including military, bank sectors and educational institutions. The measures could be like providing access to only limited number of users who are authorized. It is called as confidentiality. Integrity is protecting our resources from being changed by an unauthorized user. Availability is the service must be available to an authorized user at any time, the service should not go down.

Authentication is to check the identity of the user. Passwords are used for authentication. Passwords are the secret keys used for authentication. There are three methods in authentication. They are:

(a) Token based: Here the user needs to have some token of proof for his identity. Like having a smartcard or bankcard

(b) Biometric based: This method uses unique characteristic feature of an individual for authentication like fingerprint or iris scan.

(c) Knowledge based: The user has to remember the password. This approach is based on users knowledge.

Knowledge based technique is used more throughout all the areas. To prove the identity of an user usernames and passwords must be provided. By using such a type of authentication many drawbacks may incur. Passwords have limitations like security and memorability. Usually a user will generate a text password that he can easily remember. So this becomes easy for an attacker to guess the password. It goes on like – if a password is easy to remember for an user then it will be easier to guess for an attacker and if a password is hard to guess for an attacker then surely it will be difficult for an user to remember.

To solve this issue, one of the authentication method is used which use picture as passwords. Graphical password technique is an alternative to alphanumeric authentication scheme. Motivation is that it is proved that a human can easily remember pictures compared to numbers or texts. Graphical passwords can be used in web login applications, workstations and also ATM machines.

Attack is someone who is not related gaining access to the resources and making use of it. There are many attacks like: Brute force attack, shoulder surfing and dictionary attack. Brute force attack is a method where application programs are designed to use trial and error method to decode the data which is encrypted. Dictionary attack is described as a person attempting to gain access to a system by using a large set of words which are previously stored to generate passwords while authenticating. Shoulder surfing is knowing others password by directly observing the user entering his password standing next to him. Graphical passwords shows high resistance to brute force attack but it is susceptible to shoulder surfing attacks.

This paper aims at solving the issue of shoulder surfing attack during graphical password authentication. It is easy to carry on this attack as the images are stored in server and attacker can get more details about this when he tries to gain access using his username and password. Here, we use new point click graphical password system and user has to carry his own image mean he has to upload the exact image that he had selected during registration.

## II. RELATED WORK

Various source information is collected to get detailed understanding about the graphical authentication system.
Joseph et.al, describes Based on the proposals that are given to replace the text passwords, it shows texts provide all the basic necessities in providing security to the system. But there is a requirement to new security proving system to improve security. There was a very little hope to replace the system as it could provide only marginal increase in providing security. But analyzed that sometimes even that marginal increase becomes more important in securing the systems. Long term security system is required to avoid all the transition related costs those may occur. [1]
Daniel et.al, says that the click based passwords are creating a password after clicking on a particular locations on the image. The discussion is about observing the eye gaze of a user while choosing the location when he is entering his password. Eye tracker may be used to record the whole scenario and later analyze to get details of his gazing at the particular location for fewer more seconds. Then on a random basis he could choose the exact locations and hack the password. But it is not as simple as it is said. It takes more attempts to guess but the security can be provided by locking the system if a user enters wrong password thrice. [2]
Sayed and Fadi et.al, described about two factor authentication. That is sending a OTP message to the mobile of the user and that OTP life would be of shorter span. Hence it becomes a waste later after the deadline time given for that OTP which is sent. The user can gain access after entering the OTP and also he has to enter the password in next step. This way security can be provided twice. Once while the OTP message and later entering the password. The application can be in banks and ATM's. The OTP would be unique for both the user and device so that it is not repeated and provide any chance to attacks. It also shows the success of the proposed method. [3]
Sonia et.al, says about the advantages and disadvantages about the knowledge based system. Moving on to graphical passwords there is more probability in selecting hot spots of the image as password. It makes an attacker to guess the favourite spots of all the users and make an attack easily. The paper discusses about the authentication system itself providing information about the mostly selected areas and suggesting it to user while registration. As an example if the ratio of users selecting the nose as a password then the nose part would be shaded to indicate it to the user not to select it as it is most selected part. This is a better idea where user could know the hot spots and avoid them in early scenes.[4]
Nitesh et.al, describes about the pairing technique that could be used for obtaining higher security in the system. The popularity of WLAN and Bluetooth could be used over for betterment in securing the system. As all the phones would have these features in it, by making use of it the improvement could be made. It is a key agreement between the two of the devices over a wireless channel. The basic pairing operation can be done at the starting level and then other techniques can be used for providing greater security. And also by using unidirectional channel the privacy would be much more increased. Mutually the two devices exchange the keys through a unidirectional channel. [5]

## III. WORK FLOW

The modules that are involved in the project are: User Registration, Upload image, Hash code generation and GLCM process, User Login process and Admin part.

### 3.1 User registration.

In this module, the user will have to register by giving his details like user name, user id, email address, password etc. After providing all these information, he has to upload the image which he chooses to keep it as a password. After uploading the image he has to select five locations from that image to set it a s a password.

### 3.2 Upload image.

During log in process the user has to upload the same image which he has given it during registration process. Splits are made in the image to form a coordinate blocks and store it. When the user chooses the location, that location particular block hash code would be stored in the database.

### 3.3 Hash code generation and GLCM process.

The abbreviation of GLCM is Grey level Co-occurrence Matrices. After the location selections are made from the image the details are stored in the database. It stores after concatenating all the image locations, and it generates a hash code for that and stores it accordingly to the specific user.
In the GLCM process, conversion is made from the chunk images to the grey scale , then feature vector of those chunks are obtained. Then the distance from histogram of

feature vectors and selected chunks, only if the distance is zero then password will be accepted successfully.

### 3.4 User Login process.

User will have to enter his user id and password during log in process. He has to upload the same image that he has given it while registering. If it is correct, he has to upload the image and select the same locations which he selected before. Hash code is generated for that and then it is matched with the previously selected hash code. If it matches Home page is displayed for him or else he has to login again.

### 3.5 Admin part.

Admin has to login by the authenticated user name and password. Admin can be able to view all the users details, who are successfully registered.

## IV. EXPERIMENTAL EVALUATION

Two algorithms are used in this project namely GLCM (Grey level Co-occurrence Matrices) and RANSAC (Random Sample consensus) algorithm. GLCM considers the relationship between neighboring pixels. First pixel is considered to be a reference and second pixel is known as neighbor pixel. GLCM is a square matrix with Ng dimension, where Ng is the number of gray levels in the image. Each element of the matrix is the numbers of occurrence of the pair of pixel with value i and a pixels with value j. A co-occurrence matrix is a two dimensional array in which both columns and rows would represent a set of possible image values.

RANSAC is an iterative method to estimate parameters of a mathematical model from a group or set of observed data. It can also be interpreted as an outlier detection method.

## V. CONCLUSION

The main intent of this paper is to improve the security of the graphical password authentication system. It is done by integrating the token system i.e, user has to get his own picture while giving the password. Resistance to observation attack is been relatively increased. It also increases the resistance to shoulder surfing attacks compared to existing graphical password techniques.

## REFERENCES

[1] Joseph Bonneau, Cormac Herley, Paul C. van Oorschot, Frank Stajano,"The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes",IEEE Symposium on Security and Privacy, 2012.

[2] Daniel LeBlanc, Alian Forget and Robert Biddle,"Guessing Click-Based Graphical Passwords by Eye Tracking", Eighth Annual International Conference on Privacy, Security and Trust, 2010.

[3] Fadi Aloul, Syed Zahidi, Wassim El-Hajj,"Two Factor Authentication Using Mobile Phones", Proc. Comput. Surveys,2009.

[4] Sonia Chiasson, Elizabeth Stobert, Alian Forget, Robert Biddle, Paul C. van Oorschot, "Persuasive Cued Click-Points: Design, Implementation, and Evaluation of a Knowledge Based Authentication Mechanism", IEEE Transactions on Dependable and Secure Computing, March/April 2012.

[5] Nitesh Saxena, Jan-Eric Ekberg, Kari Kostiainen and N.Asokan "Secure Device Pairing Based on a Visual Channel: Design and Usability study", IEEE Transactions on Information Forensics and Security,March 2011.

[6] Mr. Amit Kashnath Barate, Mrs. Sunita Sunil Shinde,"Graphical Password System using Different Techniques-A Review", International Journal of Engineering Trends and Technology(IJETT), November11, Mar 2014

[7] Arti Bhanushali, Bhavika Mange, Harshika Vyas, Hetal Bhanushali , Poonam Bhogle,"Comparison of Graphical Password Authentication Techniques", International Journal of Computer Applications, April 2015

[8] Jonathan M. McCune, Adrian Perrig, Michael K. Reiter,"Seeing-Is-Believing: Using Camera Phones for Human-Verifiable Authentication", International J. Security Networks,Feb 2009.

[9] Anjitha K, Rijin I K, "Captcha As Graphical Passwords-Enhanced with Video-based Captcha for Secure Services",International Conference on Applied and Theoretical Computing and Communication Technology,2015

[10] John V. Monaco, Ned Bakelman, Sung-Hyuk Cha and Charles C. Tappert"Recent Advances in the Development of a Long- Text-Input Keystroke Biometric Authentication System for Arbitary Text Input", European Intelligence and Security Informatics Conference.