



## Enhancement of Password Authentication System Using Recognition based Graphical password for web Application

Ms. Dipti H. Dhandha  
Student of M.Tech in Cyber Security  
Raksha Shakti University  
Ahmedabad, Gujarat, India

Mr. Chandresh Parekh  
Assistant Professor (Telecommunication)  
Raksha Shakti University  
Ahmedabad, Gujarat, India

**Abstract:** Authentication is most important topic in information security. Currently web applications are using text based password for authentication, but text based passwords are suffered to security and usability issues. Text passwords are vulnerable to spyware, brute force and dictionary attacks. Graphical based password is proposed to overcome vulnerabilities of text based passwords. Graphical based password authentication technique use images as a password. Psychological studies says that human mind remember images better than text. Graphical passwords are more secure than text. In this paper, we will propose recognition based graphical password scheme to provide security against spyware and shoulder surfing attacks as well as this scheme provide the two factor authentication in order to resist unauthorized users. In this scheme, at time of sign up user has to choose images from set of images given by server and at time of signing user has to recognize that images from set of images for authentication. We are using random character set generation for each image to resist shoulder surfing as well as spyware attacks. We also fetch user's password images randomly from database to resist spyware attack.

**Keywords:** graphical password, recognition based password, shoulder surfing, spyware, text passwords.

### I. INTRODUCTION

One of the most important topics in information security today is user authentication [2]. Authentication is the process to allow users to confirm his or her identity to a Web application [1]. Password authentication is most widely used authentication mechanism for web applications. Most of authentication systems are used text based password. Major issues in text based passwords are forgetting password, stolen password, weak password. Text based passwords are vulnerable to various kind of attacks like as brute force, spyware, and dictionary. So we required strong authentication method. To overcome vulnerabilities of text password, graphical based password scheme is proposed [6]. In graphical password techniques, images are use as passwords. Reason behind for choosing that method is psychology study says that human mind remember thousands of images with detail. Graphical based passwords are also categories into two categories, Recognition based and recall based. In this paper we will propose recognition based graphical password scheme for web application to resist spyware and shoulder surfing attacks. In recognition based method, at the time of signup user has to select images from set of images given by server and at the time of login user has to remember or recognize that images for authentication.

### II. RELATED WORK

Techniques	Login interface	Drawbacks
Graphical Password Authentication System in an Implicit Manner[3]	Users have to give their answer in implicitly way by choosing image [3].	Authentication process is time consuming.

Graphical Password Authentication Cloud Securing Scheme[4]	Users have to select two images from set of image given by server. Those sets of images are given by based on username [4].	Access can be given if Anyone knows sequence With username
Intrusion Prevention by Image Based Authentication Techniques[5] (1) PIA based	Users have to selects eight pairs of images from a set of images in the system [5].	Hard to remember eight pairs of image. Logging process is time consuming.
(2) TIA based[5]	Users have to selects six images and assign a character to each image [5].	Shoulder surfing attack is possible.
A Graphical Password against Spyware and Shoulder-surfing Attacks[7]	The user selects 10 images from 50 images that are shown to her/him and assigns a character to each image [7].	User has phase difficulty to remember 10 images.

### III. PROPOSED SCHEME

In this paper, we are proposing new scheme on recognition based graphical password authentication for web applications to resist shoulder surfing and spyware attacks. We have created webpage for signup and signing which are based on recognition based graphical password. In this scheme, during signup user has to choose images as password by entering

appropriate string of selected images and at the time of signing user recognize that images for authentication. In following we are explain in detail.

### A) Sign up

In signup page 20 images are display on screen that images are randomly fetched from database. Show in figure we are attaching unique string on each image for resisting shoulder surfing as well as spyware attacks. Length of each string is three characters long. These strings are combination of lowercase, uppercase character, numbers and special symbols. When user has refresh the page that time all images and string of each images are change. User has to select minimum three and maximum six images from 20 images by entering appropriate string (which display on below right corner of each image) in password field.

Fig. 1 signup page

### B) Signing

At the time of signing, user has to enter his name that he or she used at the time of signup. If user name valid then by pressing tab key, user's password images along with other images are fetching randomly from database. Total 12 images are display on screen. In 12 images some of images are user's password images. Suppose, at the time of sign up user has select three images as password. During signing process user's password images are fetching randomly from database. So here total selected images as password is three then three conditions are occurring.



Fig. 2 user selects images as password

**Condition 1:** If one password image is display along with other 11 images then user has to select only one password

image out of 12 by entering **Pv^** string in password field shown in fig. 3

Fig. 3 one image is fetch out of three password images

**Condition 2:** If two password images are display along with other 10 images then user has to select two password images out of 12 by entering **Go)Om5** string in password field shown in fig. 4





**Condition 3:** If three password images are display along with other 9 images then user has to select three password images out of 12 by entering **Ho!Un2Zq%** string in password field shown in fig. 5





Fig. 4 two images are fetched out of three password images





**Sign In**

Username

dipti

Passwords

...

submit

Fig. 5 all (3) password images are fetch from database

User has to correctly recognize password images from set of images. In this scheme user's password images are fetching randomly from database to resisting spyware attack.

To provide more security we use OTP in order to resist unauthorized users. If user enter wrong password more than three times then user account will be deactivated till user enter correct OTP. One OTP will send to user's registered mail address. User has to enter that OTP for activate account.

Your account has been deactivated. [Please click here to activate.](#)

Steps for SignUp and SignIn process

**Sign In**

Email Address

Enter Email Address

Passwords

...

submit

Cancel

Don't have an account?

Fig. 6 user account deactivated

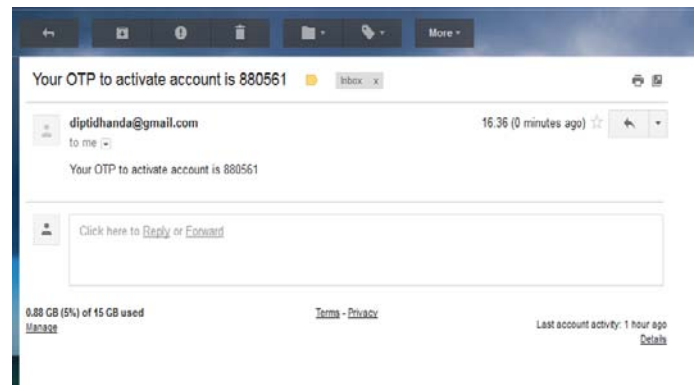


Fig. 7 OTP will send to user's registered mail address

A security code has been sent to your registered email address (dhandhadipti13@gmail.com)

**Activate your account**

Enter OTP

880561

submit

Your account has been activated. [View your account](#)

**Activate your account**

Enter OTP

Enter OTP

submit

Fig. 8 users account activate after entering valid OTP

#### IV. IMLEMENTATION ENVIRONMENT

Table 1

<b>Operating System</b>	Windows 7 operating system
<b>Server</b>	XAMPP
<b>Database</b>	MySQL
<b>Programming Language</b>	PHP,JavaScript, Ajax

#### V. SECURITY

##### A) Shoulder surfing attack:

In this attack passwords are stolen by observing the user. Attacker spies the user by using closed circuit camera or by standing back side of the user. In our proposed scheme it is difficult to do this attack because user has to select images by using keyboard instead mouse click, touch screen. We are

using random string for each image. User has to select images by entering appropriate string of selected images as password.

#### B) Spyware attack:

Spyware attacks are most common and easy to perform on text based password compared to graphical password. If system affected by key logger then all keystrokes get by attacker. In proposed scheme user's password images are fetching randomly from database to resisting spyware attack. Also we are using random string for each image so if attacker gets the string then he or she does not know which images are selected as password because every time that string and number of password images are change.

### VI. CONCLUSION

Interests of using graphical or picture passwords are growing at the faster pace as to provide more security than text based password. In recognition based graphical password scheme user has to select images as password. We strongly consider that the core reason for using recognition based graphical password is that remembering the images are much easier than a long text password and more secure than text password. Some threats of web application security are spyware and shoulder-surfing attacks. In proposed scheme, we are providing security against these two attacks as well as we are using two factor authentications in order to resist unauthorized users activities. We have created signup and signing page which are based on graphical password. We are using the random character set generation for each image to resisting shoulder surfing as well as spyware attack. We also resist spyware attack by fetching user's password images randomly from database.

### VII. REFERENCES

- [1] M.ArunPrakash, T.R.Gokul, "Network Security-Overcome Password Hacking Through Graphical Password Authentication", Proceedings of the National Conference on Innovations in Emerging Technology-2011, pp.43-48.
- [2] Arash Habibi Lashkari, Azizah Abdul Manaf, Maslin Masrom, "A Secure Recognition Based Graphical Password by Watermarking", 11th IEEE International Conference on Computer and Information Technology-2011, pp. 164-170.
- [3] Suchita Sawla, Ashvini Fulkar, Zubin Khan And Sarang Solanki, "Graphical Password Authentication System In An Implicit Manner", International Journal of Cryptography and Security, 2012, pp.-27-31.
- [4] Sh. Gurav, L. Gawade, P. Rane, N. Khochare, "Graphical Password Authentication Cloud securing scheme", International Conference on Electronic Systems, Signal Processing and Computing Technologies, pp. 479-483, 2014.
- [5] M Sreelatha, M Shashi, M Roop Teja, M Rajashekar, K Sasank, "Intrusion Prevention by Image Based Authentication Techniques", IEEE-International Conference on Recent Trends in Information Technology, ICRTIT 2011, pp. 1239-1244.
- [6] Harsh Kumar Sarohi, Farhat Ullah Khan, "Graphical Password Authentication Schemes: Current Status and Key Issues", IJCSI International Journal of Computer Science, March 2013, pp.437-443.
- [7] Elham Darbianian, Gh. Dastghaiby fard, "A Graphical Password against Spyware and Shoulder-surfing Attacks", IEEE, 2015.