Authentication for the System by using Graphical Region and Alphanumeric Password

C. S. Saharkar
Student of M.E, Information Technology
P.R.M.I.T&R, Badnera
Amravati, India
chetansaharkar@gmail.com

Prof. S. V. Dhopte
Associate Professor, Information Technology
P.R.M.I.T&R, Badnera
Amravati, India

Abstract— Security in the computer is largely supported by the passwords for authentication process. The common computer authentication method is to use alphanumerical usernames and passwords. However, users have complexity remembering a password that is long and random appearing. Instead, they create short, simple, and insecure passwords. Graphical passwords have been designed to try to make passwords more memorable and easier for people to use and more secure. The graphical password provides a promising alternative to traditional alphanumeric passwords.

In this paper, graphical passwords have been introduced as an alternative to authentication schemes. Though the graphical password scheme helps in generating more user friendly passwords, they are still weak to shoulder surfing. To address this issue, text along with image can be combined to generate more secure password. In this paper we developed a design of graphical region and alphanumeric password system as to click on image along with text and select the region rather than type only alphanumeric characters.

Keywords: *Graphical Password, Authentication, Security, Recognition.*

*****

I. Introduction

Authentication is a basic component in most computer security contexts. It provides the access to control and user responsibility. While there are various types of user authentication systems, alphanumerical passwords are the most common type of authentication system. They are flexible and easy to implement and use [1].

In the 21st century is the more advancing mature of internet and related contents, highly sensational data which innovated. The most traditional method for authentication is textual Password. User's first choice for authentication is textual passwords. Mostly users choose short and simple password so that they can be easily memorized and can be recalled at the login-time. In common it has been surveyed that an average users has to memories at least 3 passwords. Again in addition to this the user has to remember password for Banking, e-commerce, and social networking sites and also email accounts. Short and simple textual passwords are easy to remember, but can be easily hacked [2].

While random and lengthy passwords are secured but hard to remember. To overcome this problem graphical authentication schemes were proposed. But these schemes had many problems like they were easily prone to shoulder surfing attacks. Many others authentication schemes were proposed to overcome the shoulder surfing attacks but they had many drawbacks like they take more time to login, usability. In this work there are two authentication schemes that are designed to provide more security than that of textual passwords and graphical passwords [3].

Textual passwords are the most common authentication techniques used in the computer world. Textual password has two conflicting requirements: passwords should be easy to remember and hard to guess. Many graphical passwords schemes have been proposed. The strength of graphical passwords comes from the fact that users can recall and recognize pictures more than words. Most graphical passwords are weak for shoulder surfing attacks, where an attacker can observe or record the legitimate user's graphical password by camera. The graphical password combines all existing authentication schemes into one image. Graphical passwords provide a talented alternative to traditional alphanumeric passwords. [4]

II. System Anlysis And Design

A. System Analysis

This project is basically based on the graphical region based password to expansion the authentication structure which is working based on graphical password along with alphanumeric password. That is very much typical for us to remember instead of recall only character, numbers and alphanumeric password and present the situation in which user will upload one image based on its expediency, then user select an area in that image and assign name to that selected image. This is similar to like setting a name on the area of an image and that person will be fixed for all time whenever user is going to arrangement.

The authentication system working at the time of registration, a user creates a graphical password by entering a picture chooses. The user then chooses regions in the image. For every region, the user types a word or phrase that would be associated with that region. The user can choose either to enforce the order of selecting region or to make the order insignificant.

B. *System Design*

The system designed consists of the four modules such as.

- Admin module
- Password generation module
- Password verification module
- Manager module

- Admin module

In Admin module admin enter the manager name in name field and also remaining details when user entered the all user details in registration phase, then user password generation will be carried out depending on the email address of manger, then admin will generate password. Admin is only single person which is going to register new manger.

- Password generation module

First of all user is going to select one image on which user is going to select region. Once image is uploaded then user will going to select one or more region based on user interest. Then for each selected region on the image user has to type numeric password for more security.

- Password verification module

In very first step presorted image is retrieved which is stored at the time of password generation then user will going to select the same regions which is selected at the time of registration then after selection each region user has to type password should be same as that of registration time. If password does not match then user will not able to login.

- Manager module

Manager has to pass through authentication process if manager is successfully login then manger has right to create new account of users then able to make transaction in which user can able to deposit or withdraw money from their account.

III. IMPLEMENTATION

A. *Password Generation Flowchart*

Below flowchart shows the password generation procedure. The process flow starts from select image and the region and set the value. Once user completes all the user details then precede to next stage, Finally stored the details about password. After done with all these above procedure, user profile vector will be created.

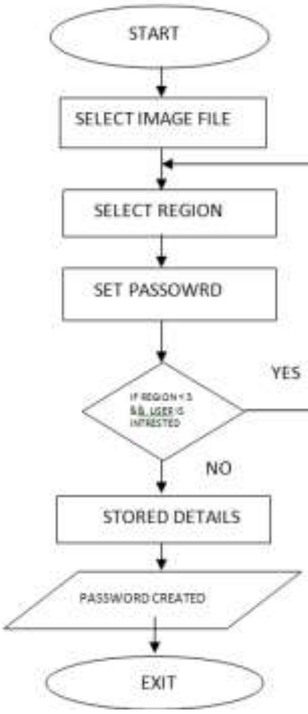


Figure 1 : Flow chart for Password generation

B. *Password Checking Flowchart*

In this login procedure, first user enters the unique user ID as same as entered during registration. Then images are displayed normally, without shading or the viewport, and repeat the sequence of clicks in the correct order, within a system-defined tolerance square of the original click-points. After done with all these above procedure, user profile vector will be opened.

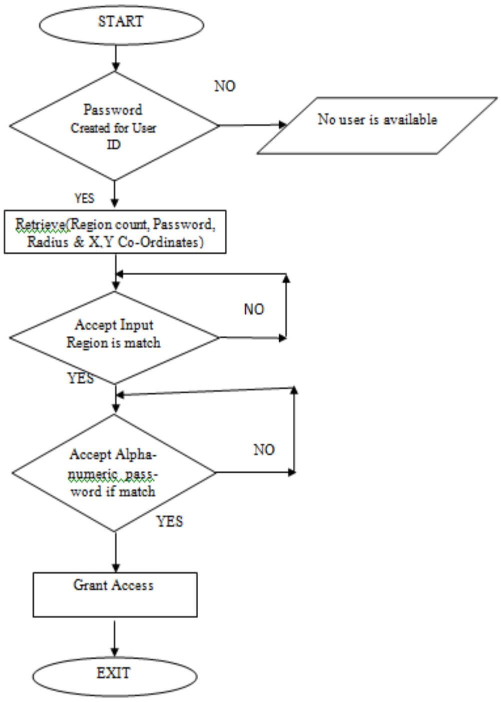

START
Password Created for User ID
NO
No user is available
YES
Retrieve(Region count, Password, Radius & X,Y Co-Ordinates)
Accept Input Region is match
NO
YES
Accept Alpha-numeric pass-word if match
NO
YES
Grant Access
EXIT

Figure 2: Flow chart for Password checker

IV. Result and Discussion

A. *Home Page*

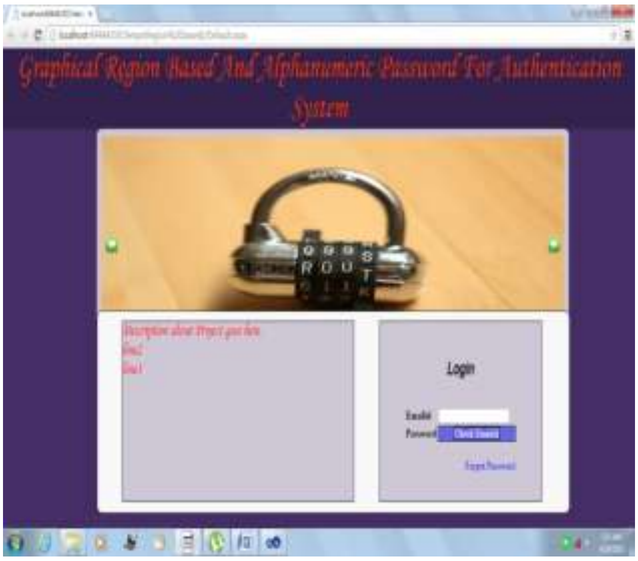

Graphical Region Based And Alphanumeric Password For Authentication System
Login
Email
Password
Forgot Password

Figure 3: Home Page

This is the home page of the web application which is the log in page for the admin. Email id and password are required at the time of login along with Graphical password. After the log in then admin can registered to Manager as well as Branch for exciting system. User can go to forgot password page by clicking on link of “Forgot password”

B. *Sign in Page*

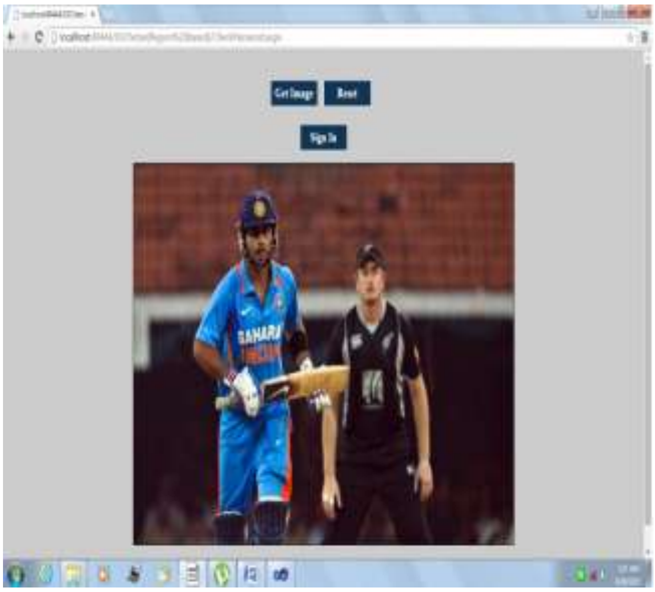


Figure 4 : Screenshot of Sign In Page

After clicking on generate password at the time of sign in this window will be generated, then click on the get Image and the select accurate region for the password which can be selected at the time of registration. After selecting an accurate region the pop will generate. Now enter the password and repeat this step 3 times then click on sign in.

C. *Branch Registration Page*

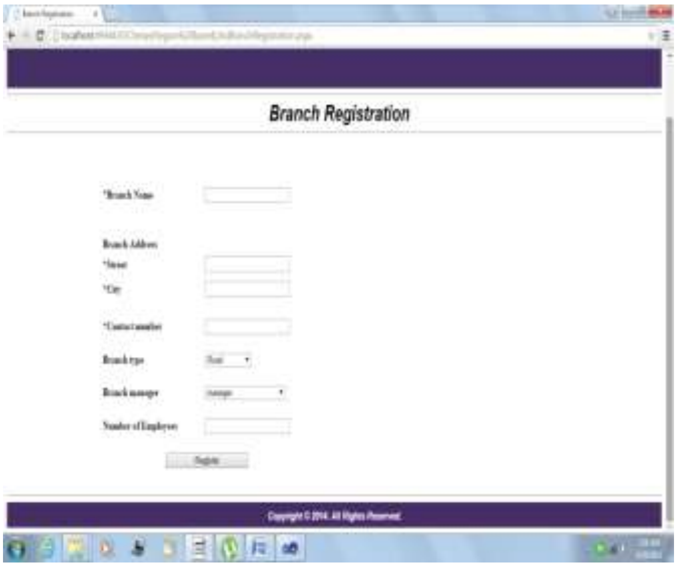


Figure 5: Branch Registration Page

This is the Branch Registration page which can be allow to register the Branch in to the exciting system. The registration page comprises of the user information and brief detail about the user along with the email id and password required for login procedure. This page also comprise of the recovery questions required if any user forgets his password.

D. *Manager Registration Page*

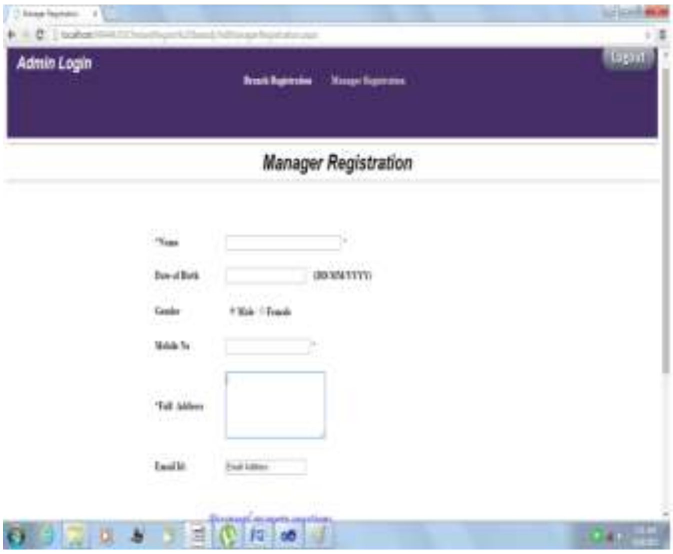
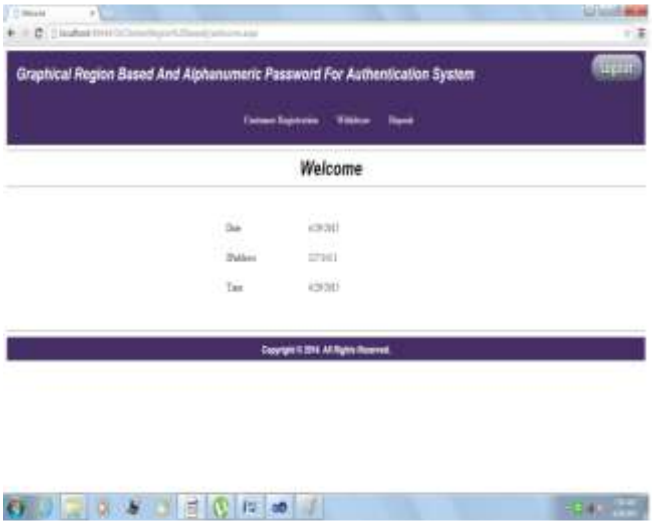


Figure 6: Manager Registration Page

This is the Manager Registration page which can be allow to register the Manager in to the exciting system. The registration page comprises of the user information and brief detail about the user along with the email id and password required for login procedure. This page also comprise of the recovery questions required if any user forgets his password.

E. *Welcome Page for Manger*



Graphical Region Based And Alphanumeric Password For Authentication System

Welcome

Date [illegible]

IPaddress [illegible]

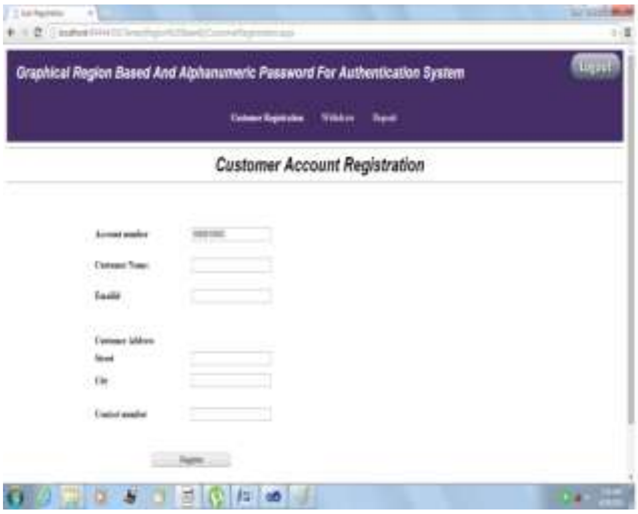
Time [illegible]

Copyright © 2014. All Rights Reserved.

Figure 7: Welcome Page

This is the welcome page in the manager log in. After the sin up by Manager then this page will appeared. It allow to manager to create a new customer and also provide the withdraw and deposit facility.

F. *Customer Account Registration Page*



Graphical Region Based And Alphanumeric Password For Authentication System

Customer Account Registration

Account number [illegible]

Customer Name

EmailId

Customer Address

Street

City

Contact number

Figure 8: Customer Account Registration

This is the Customer registration Page. The registration page comprises of the user information and brief detail about the user along with the email id and password required for login procedure. This page also comprise of the recovery questions required if any user forgets his password.

V. CONCULSION

In this study, fundamental concept of recognition based and recalls based graphical password authentication are studied. The main concept for graphical passwords is that people are better at memorizing graphical passwords than text based passwords. The system combines graphical and text based passwords trying to full resistant password.

Thus primary analysis suggests that it is more difficult to break graphical passwords using the traditional attack methods such as brute force search, dictionary attack, or spyware. We described the system operation with some examples, and highlighted main aspects of the graphical password system.

ACKNOWLEDGMENT

I would like to wish to the Head of the Department of Information Technology and my guide Prof. S. V. Dhopte for the encouragement and support, which lead to enhancement of the paper work.

REFERENCES

[1] Ahmad Almulhen”A Graphical Password Authentication System”,2011/IEEE,978-0-9564263-7/6.

[2] S. Chiasson, P. van Oorschot, and R. Biddle, “Graphical Password Authentication Using Cued Click Points,” Proc. European Symp. Research in Computer Security (ESORICS), pp. 359-374, Sept. 2007.Sigmund N. Porter. A password extension for improved human factors. Computers & Security,1(1):54 – 56, 1982.

[3] Wiedenbeck, S., Waters, J., Birget, J.C., Broditskiy, A., & Memon. (2005). PassPoints: Design and evaluation of a graphical password system. Submitted International Journal of Human-Computer Studies, 63:102–127, July 2005.Phen-Lan Lin, Li-Tung Weng and Po-Whei Huang. “Graphical passwords using images with random tracks of geometric shapes,” 2008 Congress on Images and Signal Processing. 2008.

[4] Ali Mohamed Eljetlawi, Norafida Ithnin. “Graphical password: comprehensive study of the usability features of the recognition base graphical password methods,” Third 2008 International Conference on Convergence and Hybrid Information Tech. 1137-1143.2008