International Journal of Technical Research and Applications e-ISSN: 2320-8163,
www.ijtra.com Volume 4, Issue 2 (March-April, 2016), PP. 334-337

GRAPHICAL AUTHENTICATION USING REGION BASED GRAPHICAL PASSWORD

Bhagyash Patil, Akshay Sable, Anurag Kadel, Devika Vernekar
COMPUTER DEPARTMENT
RAJIV GANDHI INSTITUTE OF TECHNOLOGY, MUMBAI
leobhagyash@gmail.com

Abstract— **Password authentication is failing as an authentication since it increases the user burden to remember the passwords. Graphical authentication is proposed as a alternative for textual passwords since it may be easy for users to remember. In this paper we propose a new image region selection based graphical password scheme. We are going to present a new technique for authentication which is based on the tracking of mouse motions on an image called mouse gestures for selecting regions in the image.A set of gestures may be stored in a database called gesture classes for each user. Users are allowed to select a set of random images and a gesture for each image. Some tolerance level is also given for each gesture. When logging in if the user draws the correct gesture using mouse the user will be treated as an authenticated user.Mouse gestures are captured through bounding box and corner detection algorithms.This method provides more security than cued click points where the user is allowed to click on a particular point called pass point for authentication which is more vulnerable to hackers.**

Index Terms: **Password, Graphical authentication, mouse gestures.**

I. INTRODUCTION

[1]Passwords are expected to comply with two fundamentally conflicting requirements:

Passwords should be easy to remember,

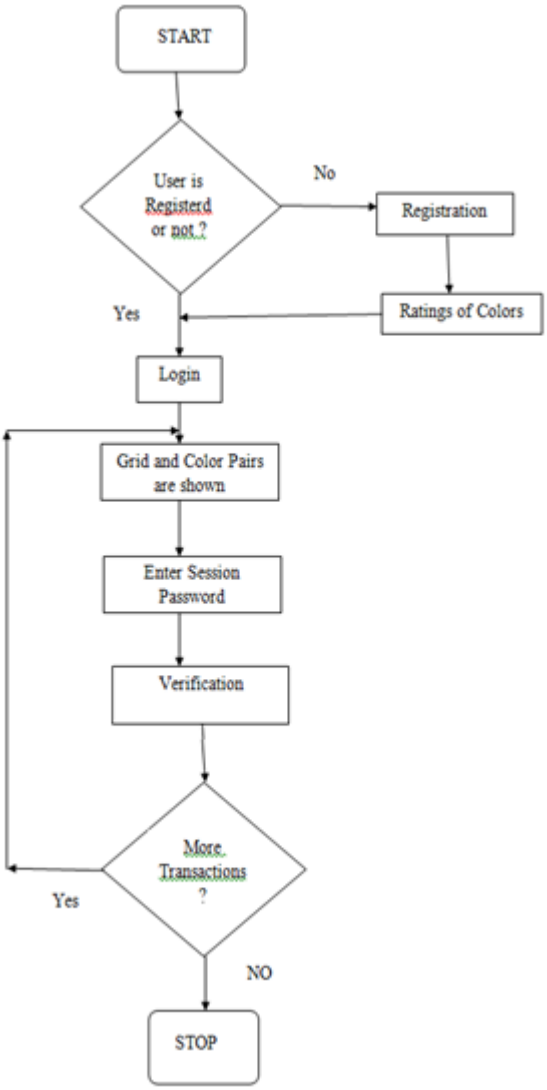
A. Passwords should be secure

Satisfying these requirements is virtually impossible for users [5]. Various graphical password schemes have been proposed as alternatives to text-based passwords. Research and experience have shown that text-based pass-words are fraught with both usability and security problems that make them less than desirable solutions [5]. Psychology studies have revealed that the human brain is better at recognizing and recalling images than text [3]; graphical pass-words are intended to capitalize on this human characteristic in hopes that by reducing the memory burden on users, coupled with a larger full password space offered by images, more secure passwords can be produced and users will not resort to unsafe practices in order to cope. Initially Cued Click Points (CCP) was used for authentication where the users are allowed to select a set of images and in each image one particular point is selected. This particular point is called the passpoint through which the user is authenticated [2]. A password consists of one click-point per image for a sequence of images. The next image displayed is based on the previous click point. Graphical authentication using CCP method has the drawback that the user has to remember the particular pass point in the given set of images and it should have high tolerance level. In this paper, we propose a new image region selection based graphical password scheme. It can be viewed as a combination of Pass Points and Cued Click Point (CCP).). A password consists of one region selection per image for a sequence of images. The next image displayed is based on the previous selected region so users receive immediate implicit feedback as to whether they are on the correct path when logging in. This scheme offers both improved usability and security. In the proposed method the user can just remember the region and its shape. No burden to human brains and also a security level may also be given for it.

II. EXISTING SYSTEM

Session passwords are being used lately.Session passwords are passwords that are used only once. Once the session is terminated, the session password is no longer useful. For every login process, users input different passwords.Every time the users enters a session he has to input different password. Once the session is over that password becomes is of no use for next session and the current session gets terminated. Session password provide more security as every time the session start a new password is created and they are not prone to dictionary attacks, brute force attacks and shoulder surfing attacks.

A FLOWCHART of the Existing system is as below :



III. LIMITATIONS

Although existing system has many strong points. But its main drawback is that it cannot be used by a colour blind person.

So to overcome this drawback we have come up with a new system.

IV. PROPOSED SYSTEM

REGION DETECTION ALGORITHM:

To detect region a very efficient way we have used two methods :

- Bounding box method.
- Corner detection method.

A. BOUNDING BOX METHOD:

The first method we will discuss is the bounding box method. This involves drawing a box around the gesture and dividing it up into a grid. The gesture is then defined by the areas that it passes through.

B. CORNER DETECTION METHOD:

It figures out which points are the corners, and then looking at the relationships of those corners. The advantage of this is that it would be very accurate, provided the algorithm detects the corners properly. This method also takes into account the proportions of each part of the gesture.

V. EXPERIMENTAL RESULTS AND ANALYSIS:

At the time of registration the user selects a specific region on the given image of his interest which he can remember easily. A set of random and unique images are fetched from the database for registration. For the set of images given to the user,

user selects regions in every image and remembers its position and size in that sequence and this information is stored in the database for future login purpose. At the time of login the sequence of images given to the user one by one which was saved at the time of the registration. Now the user selects the region with the gesture that was used at the time of registration. For every image, our algorithm calculates the parameter's and matches with the previously stored parameter's for that image with some tolerance value. If the match is a success then next image is fetched from the database and the process is repeated and if the match is unsuccessful then the user is not notified until the end and at the next sequence a random image is given to the user and login fail flag is activated.

Fig (a). Cited from Ref no [1]

Fig (b)

Fig (c). Cited from Ref no [1]

Now figure(a) & figure(b) shows the original images. Figure (c) shows the user selected gestures.

Table 1. Actual data stored for user

Img Id	Seq No	Top X	Top Y	Bottom X	Bottom Y	Grid Pixel Count
84	1	59	3	73	30	71
165	2	85	15	115	59	135
169	3	12	46	79	78	151

Table 2. Data collected at the time of login

Imgid	SeqNo	Top X	Top Y	Botto m X	Bottom Y	Grid Pixel Count
84	1	59	6	73	31	74
165	2	86	18	118	60	121
169	3	11	43	81	73	179

Table 3. Test Cases:

Calculated Difference among the Stored Data & Login Data

Seqence Number	Top X Difference	Top Y Difference	Botto m X Difference	Botto m Y Difference	Grid Pixel Count Difference	Result
Login Attempt 1 / Authenticated / Tolerance [C.T=10] , [G.P.T=50]						
1	0	3	0	1	3	Pass
2	1	3	3	1	14	Pass
3	1	3	3	1	28	Pass
Login Attempt 2 / Login Fail / Tolerance [C.T=5] , [G.P.T=50]						
1	2	1	2	3	4	Pass
2	6	2	1	0	12	Fail
3	-	-	-	-	-	Fail
Login Attempt 3 / Login Fail / Tolerance [C.T=10] , [G.P.T=10]						
1	2	1	2	3	4	Pass
2	6	2	1	0	12	Fail
3	-	-	-	-	-	Fail
Login Attempt 4 / Success / Tolerance [C.T=8] , [G.P.T=20]						
1	2	1	2	3	4	pass
2	6	2	1	0	12	pass
3	1	7	3	8	18	pass

Table 4. Test Cases result on different tolerance level

No	C.T	G.P.T	Success/Correct Data	Total Attempt	Success Rate
1	2	2	**2**	20	10%
2	2	4	**1**	20	5%
3	2	8	**2**	20	10%
4	2	12	**3**	20	15%
5	2	16	**5**	20	25%
6	4	2	**9**	20	45%
7	4	4	**11**	20	55%
8	4	8	**10**	20	50%
9	4	12	**13**	20	65%
10	4	16	**13**	20	65%
11	8	2	**1**	20	10%
12	8	4	**3**	20	15%
13	8	8	**17**	20	85%
14	8	12	**17**	20	85%
15	8	16	**18**	20	90%
16	12	2	**3**	20	15%
17	12	4	**7**	20	35%
18	12	8	**15**	20	75%
19	12	12	**19**	20	95%
20	12	16	**20**	20	100%
21	16	2	**4**	20	20%
22	16	4	**6**	20	30%
23	16	8	**15**	20	75%
24	16	12	**18**	20	90%
25	16	16	**20**	20	100%

The above tables have been cited from ref no [1].

VI. ADVANTAGES

- Graphical authentication is more efficient and more securable.
- A graphical password authentication system encourages strong passwords while maintaining memorability.
- Psychology studies have revealed that the human brain is better at recognizing and recalling images than text so graphical passwords are intended to capitalize on this human characteristic in hopes that by reducing the memory burden on users.
- Graphical passwords provide enough security against common threats such as brute force attacks by dictionary means or OCR types, as well as shoulder-surfing attacks.
- To make passwords more secure without compromising their meaning and remembrance.

VII. DISADVANTAGES

- Graphical authentication using CCP method has the drawbackthat the user has to remember the particular pass point in the given set of images and it should have high tolerance level.
- Users rarely chose points that were within the tolerance around the click point of another participant.
- Shoulder surfing attack is possible.
- The problem with this model is that the Hotspots remain a problem that clicks can be predicted automatically with a significant probability.

REFERENCES

1. "Graphical authentication using region based graphical password", G. Niranjan & Kunal Dawn.
2. Sonia Chiasson, P.C. van Oorschot1, and Robert Biddle "A second look at the usability of click based graphical passwords" .
3. Wiedenbeck, S., Waters, J., Birget, J.C., Broditskiy, A., & Memon, N. (2005). PassPoints: Design and evaluation of a graphical password system. Submitted.
4. Rundus, D. J. (1971). Analysis of rehearsal processes in free recall.. Journal of Experimental Psychology, 89, 63-77.
5. E.H. Spafford, "Observing reusable password choices", In Proceedings of the 3rd SecuritySymposium.Usenix, 1992, pp. 299–312.