ijecs open access www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 6 Issue 4 April 2017, Page No. 20809-20812
Index Copernicus value (2015): 58.10 DOI: 10.18535/ijecs/v6i4.02

Color Scheme Authentication for Session Password

Indhu D, Surya G, Abirami A

[#]Computer Science Department, Velammal Engineering College
Chennai
[1]indhu5dilli@gmail.com
[2]suri5gandhi@gmail.com
[3]*Abiramiaaru21@gmail.com*

***Abstract*— In this paper we are dealing with the new scheme to provide authentication for files and folders using colours in which the password are generated for every session, that is we have our new password every time you login hence we called it as color scheme authentication for session password. The main purpose for this method is to stricter the authentication, to provide security to our documents in folders and PDF. We have implemented and it proved to be a better technique in providing authentication when compared to textual passwords and other existing techniques.**

***Keywords* — Authentication, session, folders and PDF.**

I. INTRODUCTION

The main objective of this idea is to generate passwords for sessions in digital application using colors and pictures. Textual passwords are the most common method used for authentication. The existing system passwords can be easily guessed or cracked. The alternative techniques are graphical passwords and biometrics. But these two techniques have their own disadvantages. Biometrics, such as finger prints, iris scan or facial recognition have been introduced but not yet widely adopted. The main disadvantage is systems can be expensive, the identification process can be slow, and it is difficult to remember long and random passwords.

The Session passwords are passwords that are used only once. Once the session is terminated, the session password is no longer in use. The users input different passwords every time they login. The session passwords provide better security against dictionary and brute force attacks as password changes for every session. It also avoids eves dropping and shoulder surfing. Hence we provide authentication.

In this technique colours will be used, user will give rating to color which will be used as his password. User just needs to remember his colour rating. During authentication a grid with random numbers will be displayed along with colors appearing in pair on top of grid. In a pair of a colour 1stcolour represent row and second the column. Based on the rating of colour that user gave user will find intersection of row and column and get the first digit of his session password. Similarly he will find the rest digit for password. Every time numbers in grid change and also the pairing of colour and so the password changes

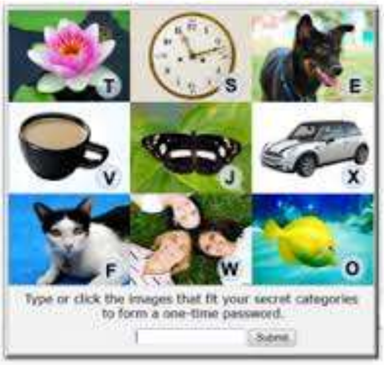
So we have come up with this paper as a result of our mini project where we have used colors for generating session passwords.

II. EXISTING SYSTEM

1. GRAPHICAL SYSTEM

In the graphical authentication scheme the user has to identify the pre-defined images in correct order to prove the authentication . In this scheme , during registration the user selects a set of images from a predefined set of images. During login the user has to select the image in same order he had given during registration.

But this system is vulnerable to shoulder surfing.



Type or click the images that fit your secret categories to form a one-time password.

Figure 1: Random images used by Dhamija andPerrig

2. DAS TECHNIQUE

Jermyn, et al proposed a graphical based technique called “Draw-a-secret”(DAS).In this scheme the user has to re-draw the predefined picture on a 2D grid . If the drawing touches the same grids in the same sequence , then the user is authenticated. But this system also vulnerable to shoulder surfing.

DOI: 10.18535/ijecs/v6i4.02

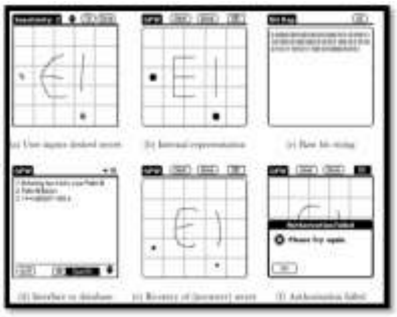


Figure 2: DAS technique by Jermyn

3. CONVEX HULL

To overcome shoulder surfing Wiedenback et al Proposed a graphical password scheme using convex hull method .A user needs to recognize pass-objects and click inside the convex hull formed by all the pass-objects. In order to make the password hard to guess large number of objects can be used but it will make the display very crowded , but using fewer objects may lead to a smaller password space , since the resulting convex hull can be large.

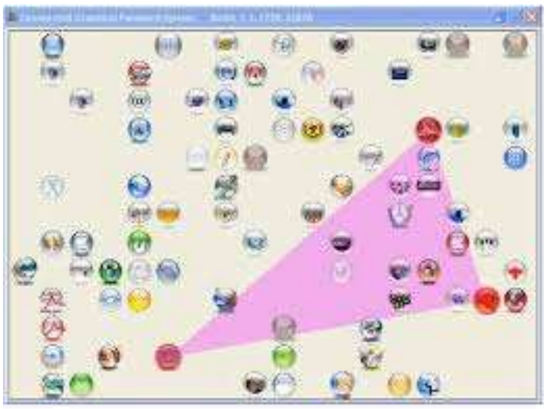


Figure 3: Example of a Convex hull

III.PROPOSED SYSTEM

1. COLOR BASED AUTHENTICATION SCHEME

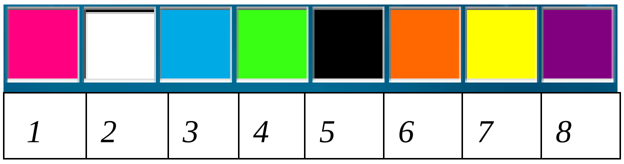
We propose a new authentication scheme “Color Scheme Authentication” .Instead of just words we propose a system in which authentication is done using colors and numbers.

The proposed system using new Authentication technique consists of 3 phases:

- registration phase
- login phase and
- verification phase

During registration, user enters his password by rating the colors. User can give values from 1 to 9 for the given 8 colors. Users can even give same value for two different colors this makes the authentication method risk free of shoulder attack, dictionary attack, eves dropping etc. The only the thing the user has to keep in mind is the random rating for the colors which is the password (fig1).

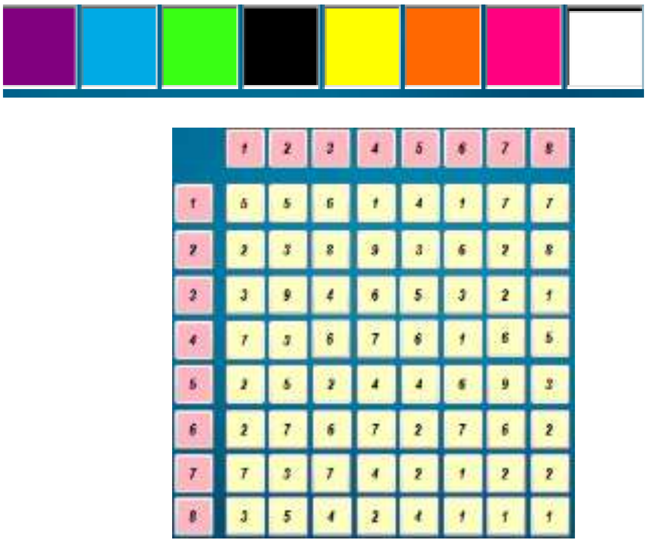
During registration, user should rate colors. The user should rate colors from 1 to 9.



1	2	3	4	5	6	7	8

Figure 4: colour rating in register phase.

During the login phase, when the user enters his user name an interface is displayed based on the colors selected by the user. The login interphase consists of grid of size 8x8. This contains digit 1-9 placed randomly in grid cells. The interface also contains strips of colors. The color grid consists of 4 pairs of colors. Each pair of color represents the row and the column of the grid. Depending on the ratings given to colors, we get these session passwords. As discussed above, the first color of every pair in color grid represents row and second represents column of the number grid. The number in the intersection of the row and column of the grid is part of the session password. Likewise we generate password from 4 pair of colours (fig 2).



	1	2	3	4	5	6	7	8
1	5	5	6	1	4	1	7	7
2	2	3	8	9	3	6	2	8
3	3	9	4	6	5	3	2	1
4	7	3	6	7	6	1	6	5
5	2	5	2	4	4	6	9	3
6	2	7	6	7	2	7	6	2
7	7	3	7	4	2	1	2	2
8	3	5	4	2	4	1	1	1

Figure 5: login phase

Consider the Figure 4 rating and figure 5 login interface for demonstration . The first pair contains violet and blue colours. The violet colour rating is 8 therefore select 8 in the row and blue colour rating is 3therefore select 3 in the column. So the first number of session password is 8th row and 3nd column intersecting element i.e., 4 will be generated automatically. The same procedure is followed for other pairs of colours.

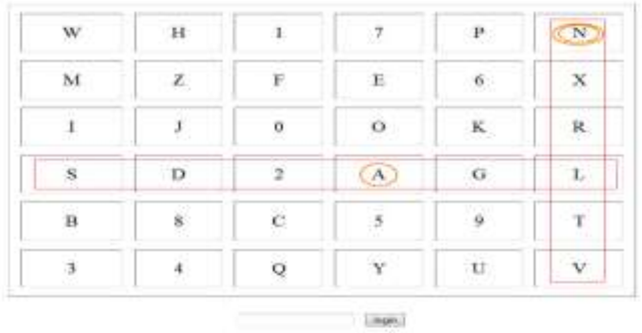
Each time when we login the pairs of colours and the numbers in the 8X8 grid will randomize. So for each session we will get a new password.

2.PAIR-BASED TEXTUAL AUTHENTICATION SCHEME

DOI: 10.18535/ijecs/v6i4.02

In this scheme during registration user submits his password. The maximum length of the password can be 8 and it is called as secret pass. The secret pas should contain even number of characters. Session passwords are created based on the secret pass. When user enters login an interface consisting of 8x8 grid will be displayed. It consist of alphabets and numbers randomly placed int the grid.

The grid will appear as shown in below figure 5. Depending upon the password which is submitted during the registration phase ,the user has to enter the password. User have to consider in terms of pairs



W	H	1	7	P	N
M	Z	F	E	6	X
I	J	0	O	K	R
S	D	2	A	G	L
B	8	C	5	9	T
3	4	Q	Y	U	V

Figure 6: Intersection letter for pair ‘AN'

The first letter in pair is used to select the row and second letter is used to select the column. The intersection letter is part of session password. This is repeated for all pairs of secret pass.

3. PICTURES-BASED AUTHENTICATION SCHEME

We propose another authentication scheme called “Picture-based Authentication scheme”. This method is similar to colour based scheme for authentication In this scheme we use pictures instead of colours .Since pictures are used it will be easy for us to remember what rating we had given to each picture. This authentication technique also consist of 4 phases:

Registration phase
Login phase
Verification phase
Recovery phase.

.In this scheme the user has to register his password by rating the pictures .User should rate the picture from 1 to 9. During login phase an 8x8 grid will be displayed. This grid contains digits 1-9and also alphabets. These are randomly placed on grid and the interface changes every time. The login interface also contains 4 pairs of pictures.

User has to enter the password depending upon the rating given to the pictures. As the 8x8 grid and pictures changes for every login each time a new password will be generated. Here figure 4 shows the login interface having picture grid and grid of 8x8 with numbers and alphabets randomly placed in the grid.

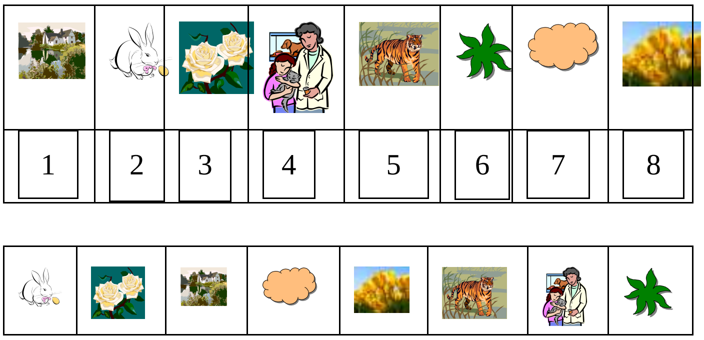
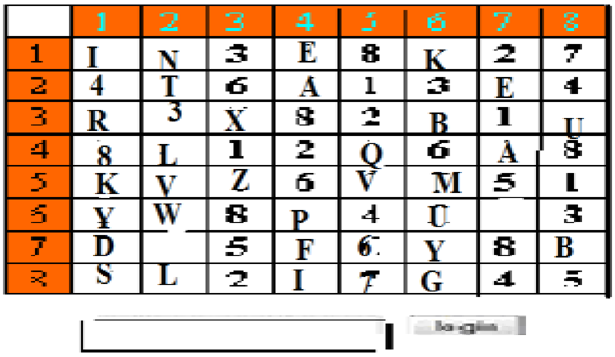


Figure7: pictures rating in register phase

Consider figure 7 and figure 8 for demonstration. The first pair contains the picture of rabbit and roses. The rating given to these were 2 and 3 respectively. Therefore the session password will be the intersection of 2nd row and 3 rd column i.e.,6.The same procedure is repeated for other pairs of colours. For figure 4 the password will be “6276”.

This system provides better security against dictionary and brute force attacks.



	1	2	3	4	5	6	7	8
1	I	N	3	E	8	K	2	7
2	4	T	6	A	1	3	E	4
3	R	3	X	8	2	B	1	U
4	8	L	1	2	Q	6	A	8
5	K	V	Z	6	V	M	5	I
6	Y	W	8	P	4	U		3
7	D		5	F	6	Y	8	B
8	S	L	2	I	7	G	4	5

Figure 8: login phase

IV.RESULT ANALYSIS

Here we have discussed about 3 authentication schemes. These techniques are resistant to shoulder surfing. Due to dynamic password, the dictionary attacks is not applicable. Hidden camera attacks are not applicable to PDA’s because it is difficult to capture the interface in PDA’s.

By studying these techniques we came to know that according to ‘time to login’ the pair based authentication scheme is better than the other two authentication schemes. But according to security Pictures-Based authentication and colour-based authentication are preferred to pair-based authentication scheme.

The following table shows the comparison with the existing system

Authentication Schemes	**Textual password scheme**	**Graphical Password Scheme**	**Pair-Based Authentication**	**Color-Based Authentication**
Usability	High	Less	Very high	Very high
Implementation	Easy	Complicated	Easy	Less complicated
Time to login	Low	High	Low	Moderate
Security	Very Low	Low	High	Very High
Password Space	More	Quite less	less	less
Attacks	Brute force, dictionary, guessing	Shoulder surfing , guessing	Sometimes shoulder surfing	Sometimes shoulder surfing

V. CONCLUSION

The general methods of providing authentication such as textual password, graphical passwords has its own disadvantage such as shoulder surfing, dictionary attacks. So we provide this effective technique Color based authentication and Picture based authentication for sessions which provides stricter authentication and protects your files and folders from being pirated. These techniques can be used for external authentication to connect the application to database. Also it can be used to provide security to any windows applications.

VI. REFERENCE

[1] N. Kumar, "Bhumi12," Mandar Sonawane, 2013. http://www.slideshare.net/niteshkrsah/authentication-scheme-for-session-password-using-images-and-color.

[2] http://www.ijetmas.com/admin/resources/project/paper/f201505121431406716.pdf.

[3] http://ijcsit.com/docs/Volume%206/vol6issue02/ijcsit2015060268.pdf.

[4]. http://airccse.org/journal/nsa/0511ijnsa08.pdf.

[5]http://www.academicscience.co.in/admin/resources/project/../f201404171397746848.pdf.

[6] M. S. T. Miss Nagama Khan and Miss. Swati Balpande, "Password Authentication Using Text and Colors,". http://www.ijsret.org/pdf/121048.pdf.