



# **Innovative Color Band Security System to Avoid Shoulder Surfing**

**Milind Jamnekar<sup>1</sup>, Asif Shaikh<sup>2</sup>, Aakash Ombase<sup>3</sup>, Prof. Sneha Deshmukh<sup>4</sup>**

Students, Department of Computer Engineering<sup>1,2,3</sup>

Professor, Department of Computer Engineering<sup>4</sup>

Dhole Patil College of Engineering, Pune, Maharashtra, India

**Abstract:** Conventional password schemes are greatly at risk of shoulder surfing, many shoulder surfing graphical way schemes are created. But, end users are more acquainted with textual password than pure graphical password, text-based graphical password schemes are proposed. Sadly, none of the text-based shoulder surfing resistant graphical password schemes is both secure and efficient enough right now. In this paper, it proposed an enhanced version of text-based shoulder surfing resistant graphical password using your favourite color. In this proposed scheme, the user can easily and efficiently login in the system. Next, we analyze the protection and usefulness of the proposed scheme, and show the resistance of the proposed scheme to shoulder surfing and accidental login. The shoulder surfing attack is an attack in which attacker try get the user's password by watching over the user's shoulder as he enters his password. As conventional password schemes are prone to shoulder surfing, Bravado and Biretta proposed three shoulder surfing resistant graphical password schemes. Since then, many graphical password schemes with different degrees of resistance to shoulder surfing are proposed and every has its pros and cons. The alphabet utilized in the proposes scheme contains 16 characters, including 8 small letter alphabets from a to h & 8 numerical from 1-8.

**Keywords:** Shoulder Surfing; Color band security; Graphical Password; web security; login security

## **I. INTRODUCTION**

Net surfing is often based on the use of alphanumeric password. However, end users always have difficulty to remember password which is long, random and they opt out long, difficult, and secure passwords. Graphical passwords are the idea in which password become more memorable and easier for people to use and, therefore, more secure. Using a graphical password, users click on graphical media which could be images or SVG's, rather than typing characters. A most important factor in security is authentication, the determination of whether a end-user should be allowed access to a system or resource. Normally, alphanumeric passwords have been used for authentication and authorization, but they are known to have bad user experience . Nowadays, including graphical passwords, are best alternatives. This paper reports on research aimed to make a graphical password system, practical usability, and compare it to traditional alphanumeric passwords. In this system an image would show up on the screen, and the user would click on a few chosen regions of it. If the correct buttons were clicked in, and correct password were put in, then the user would be authenticated.

Zhao et al. [4] introduced S3APS, a text-based shoulder surfing resistant graphical password scheme because it appears that most users are more familiar with textual passwords than pure graphical passwords. To retrieve the session password in S3PAS, the user must mix his textual password on the login screen. However, Zhao et al's login scheme process is complicated and time-consuming. Then there were numerous text-based shoulder surfing resistant graphical password systems proposed, e.g. [5][6][7] but they always has complication and difficult to implementation.

To perform data protection the user is prompted with password input and has to fill using color band. The data is encoded and made unreadable. After successfully entering password through color band, site is then prompted to further site which is secure for authorize and authenticated users.

## II. RELATED WORK

In 2002, in order to reduce shoulder surfing attack, Sobrado and Birget [1] proposed three password schemes that show shoulder surfing avoidance, the Movable Frame scheme, the Intersection scheme, and the Triangle scheme. But in all of these systems, the Movable Frame system and the Intersection system often fail in the Verification process. In the Triangle program, the user must select and memorize a few passing icons as his or her password. To log in to the system, the user must correctly pass a predetermined number of challenges and for each challenge, the user must find three icon pass symbols in a set of randomly selected icons displayed on the login screen, and then click inside the invisible triangle created caused by those three passing icons.

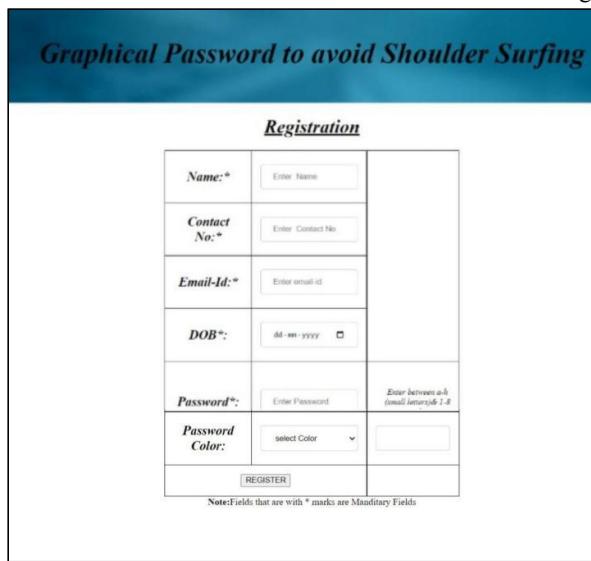
In 2011, a text-based shoulder surfing graphical image password scheme, use an analytical approach to counterfeit entry and shoulder surfing resistance to analyze the security of their system proposed by Kim et al. [2]. Unfortunately, the resistance of the program by Kim et al is very poor which is login by mistake and it failed to show satisfactory result.

In 2009, In order to overcome shoulder surfing attacks, a password system that uses color penetration and provides resistance to shoulder surfing attacks is proposed by Gao et al. [3]. In this program background color is a useful feature to reduce logging time. This program has problems such as, the chance of accidental logging in color is too high and the password space is too small.

## III. METHODOLOGY

This section discusses in detail the architecture of Innovative Color Band Security System Figure 1 and Figure 2. As shown here there are two modules i.e. Registration phase and Login Phase and admin is responsible for managing and updating both modules. Innovative color band.

**Registration phase:** Here in the Registration phase we accept the data from the user and here we get the security color code from the user and we store all the data in here and we verify that the email address mention at the time of registration is valid or not of if the user is already login or not so we have to tell the user that you had already created a account. After verifying the correct email address we take the password from user that he needs to enter at login time with the help of color band and also we took the secret color band the he needs to remember at the time of login.



The form is titled "Graphical Password to avoid Shoulder Surfing" and "Registration". It contains the following fields:

Name:*	Enter Name
Contact No:*	Enter Contact No
Email-Id:*	Enter email id
DOB*: dd-mm-yyyy	<input type="text"/>
Password*: Enter Password	Enter between 6-15 (email between 1-8)
Password Color: select Color	<input type="text"/>
<input type="button" value="REGISTER"/>	

Note: Fields that are with \* marks are Mandatory Fields

**Figure 1:** Registration Phase with password color property

With this number of parameter provided by color band we can choose minimum length of Password is 6 Characters and the maximum length of password is 15 characters i.e password length is between 8 to 15 Characters, and we have to choose one color as our pass color from 8 colors assigned by the system.

The remaining 7 colors that the user has not selected are his deceptive colors. Also, the user must register an email address to re-open their account when they enter the wrong password because entering wrong password for 3 consecutive time will disabled account. In this case, the registration process should be done in a place where there is no possibility of shoulder

surfing attempt and this might could be your home. In addition, a secure channel should be established between the system and the user during the registration phase using SSL / TLS or any other secure transfer method. The system stores the user's text password in the user entry in the password table, which must be encrypted with the system key. So briefly in the registration section of the user set a text password and select 1 Color from 8 Colors

**Login Phase:** The user requests to login the system, and the system displays a circle composed of 8 equally sized sectors. The colors of the arcs of the 8 sectors are different, and each sector is identified by the color of its arc, e.g., the red sector is the sector of red arc. Initially, 16 characters are placed averagely and randomly among these sectors. All the displayed characters can be simultaneously rotated into either the adjacent sector clockwise by clicking the "clockwise" button once or the adjacent sector counter clockwise by clicking

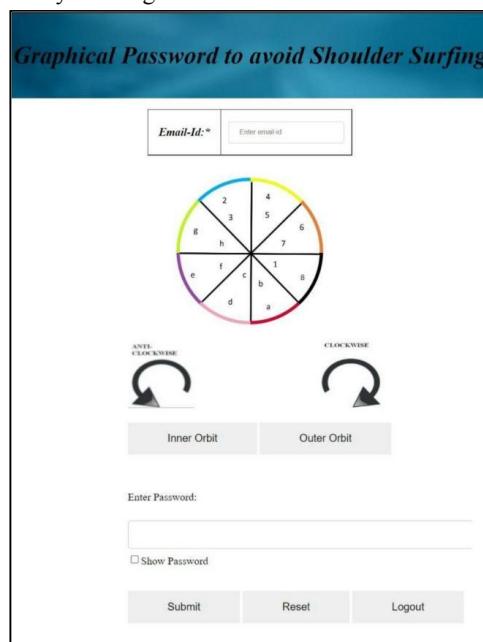


Figure 2: Login phase with color band display

All the characters shown can be rotated simultaneously in the clockwise field by clicking the button which symbolizes clockwise direction and at the anticlockwise counter by clicking the button which symbolizes anticlockwise direction once, and rotation functions can be done by scrolling the mouse. The login screen of the proposed system can be displayed with the example shown in Figure 2. To sign in to the system, the user must complete the following steps:

- Step 1: The Login Screen is appear in front of end-user.
- Step 2: After login screen appear, the system displays a circle consists of 8 sectors of equal size and each sector contain 2 characters randomly distributed among the sectors. also there is a button for rotating the circle clockwise and the button for rotating the Circle anti clockwise. After successfully entering password user can proceed to press "Confirm" button. The feature is, mouse wheel can also be used to move the color band in clockwise or anticlockwise direction. Supposed, at the very first of current session we assume one variable i , and Let i = 1.
- Step 3: In this step user has to rotate the field containing the password characters, and he has to move that color band to the character arc, which his character from password reside in, for that purpose system will have button that we rotate clockwise or anticlockwise color band easily. After bringing color arc the desired character, user has to check whether the character is appear on inner loop or outer loop and click accordingly. After rotating and filling desired and appropriate password using color band, click the confirmation button, and after confirmation, increase the value of i by 1.
- Step 4: System will check if the value of i is less than L, where L means the length of the password, then do step 3 repeatedly until the value of i becomes L, then press the enter button and the login process ends. To provide more

security, the user can enter the wrong password only 3 times in a row. If the account is not successfully authorized within 3 times in a row, account will be disabled and the system will send a link to a registered email address that can be used by the authorized end-user. and correct person to log in and re-enable a blocked account.

#### **IV. RESULT ANALYSIS**

The security and the usability of the given system will be as follows,

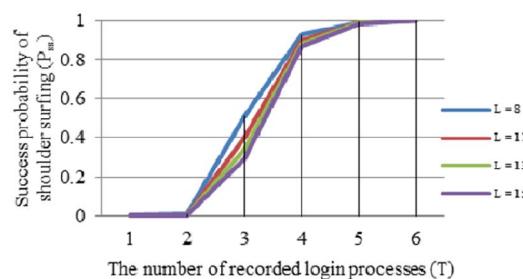
##### **4.1 Password Space**

Assume that the length of password is L and take parameter which is less than 15 and greater than 8 ( $8 < L < 15$ ) so now there are  $8 * 16^L$  password can be generated for use, Therefore, the scheme proposed, allow the number of password is

$$\sum_{L=8}^{15} 8 * 16^L \approx 9.8 * 10^{18}$$

##### **4.2 Resistance to Shoulder Surfing**

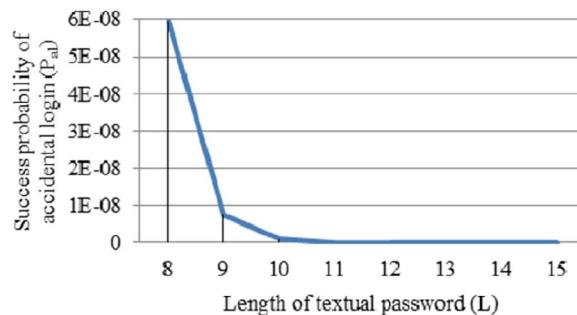
Because the user has only three chances to enter the password, and if he enters the wrong password, the account will be disabled, to log in to the account, the user must first select a specific colour, and then transfer all of the password characters to that color's sector. Shoulder surfing resistance is thus supplied.



**Figure 3:** Graph of resistance to shoulder surfing

##### **4.3 Resistance to Accidental Login**

Accidental Login refers to the possibility of typing a password incorrectly. Because the chance of typing a password is  $8/16$ , or  $1/2$ , the chance of an accidental login is  $(1/2)L$ . Consider the various L values presented in the graph.



**Figure 4:** Graph of resistance to accidental login

To ensure security, the user can only enter the incorrect password three times in a row. If the account is not successfully authenticated three times in a row, the account will be disabled, and the system will send a link to the registered email address that can be used by authorized and correct persons to login and re-enable the disabled account. As a result, the likelihood of an accidental login is quite minimal.

**V. CONCLUSION AND FUTURE WORK**

In this research, we present a solution for reducing shoulder surfing attacks that uses text and color-based graphical passwords. This authentication mechanism allows the user to log in to the system without worrying about shoulder surfing and without requiring a physical keyboard to enter the password. This method use both textual and color-based graphical passwords, and because the user is familiar with both, the system may be accessed quickly and easily. We can use this system in applications that require high security in the future.

**REFERENCES**

- [1]. L. Sobrado "Graphical passwords," The Rutgers Scholar, An Electronic Bulletin for Undergraduate Research, vol. 4,2002 .
- [2]. M. Sreelatha, M. Anirudh, Md. Sultan Ahamer, and V. Manoj Kumar. "Authentication schemes for session passwords using color and images," International Journal of Network Security & Its Applications, vol. 3, no. 3, May 2011..
- [3]. H. Gao, X. Liu and R. Dai, "Design and analysis of a graphical password scheme," Proc. of 4th Int. Conf. on Innovative Computing, Information and Control, Dec. 2009, pp. 675-678.
- [4]. H. Zhao and X. Li, "S3PAS: A scalable shoulder-surfing resistant textual-graphical password authentication scheme," Proc. of 21st Int. Conf. on Advanced Information Networking and Applications Workshops, vol. 2, May 2007, pp. 467-472
- [5]. Schemes using text-graphical passwords," International Journal of Information & Network Security, vol. 1, no. 3, pp. 163-170, Aug. 2012.
- [6]. B. R. Cheng, and W. P. Chen, "An efficient login recording attack resistant graphical password scheme Sector Login," Proc. of 2010 Conf. on Innovative Applications of Information Security Technology, Dec. 2010, pp. 204-210.
- [7]. S. H. Kim, S. Y. Kim, and H.G. Cho. "A new shoulder surfing resistant password for mobile environments," Proc.of 5th Int. Conf. on Ubiquitous Information Management and Communication, Feb. 2011.