

Colour-Code Combination for Secured Login

Abhinandan P. Mangaonkar

Lect. Bharatesh College of Computer Applications, Belagavi, India

ABSTRACT

Article Info

Volume 7, Issue 2

Page Number : 47-51

Publication Issue :

March-April-2021

Article History

Accepted : 01 March 2021

Published : 08 March 2021

In earlier days there was no much use of computers. As developments took place in the field of computer science, every little and large industries or even every person started using computers. Computers are now in every field and in every little thing. Then there comes a part of internet for sharing information with each other. Internet is mainly used for social networking, online marketing, net banking, and online money transactions. With all this there comes the darker side of the internet that is: internet frauds, hackings, cracking etc. Whoever is using the internet first and foremost they wish their safety and security and this is done by using authentication. In most of the cases, the user is provided with USERNAMES and PASSWORDS for authentication. But hackers are now attacking authentication systems for doing online frauds and we need stronger solutions to avoid attacks, that will be possible using “colour-code combination for secured login” technique.

Keywords : Security, Password Attacks, Color-Codes Combination.

I. INTRODUCTION

If we are using any social media websites or any online transaction systems or any online shopping website then most commonly we will be told to set “username” and “password” for security purpose.

Even after setting-up the authentication in the form of Username-Password, most of the times we observe that there are many un-authorized accesses because these Usernames and Passwords are in the form of normal texts. And these textual passwords can easily be accessed or guessed. There are even many different attacks likes: Eves Dropping, Shoulder Surfing and Dictionary Attacks, by which it is very much possible

for attacker to hack or guess the password and gain the access on any user’s account.

We can’t even make our passwords complicated because now days we have so many different social media accounts, banking accounts or even online shopping accounts, Because of all these we will be confused if we chose complicated usernames or passwords. We can’t even use same username or password everywhere because if someone guesses the password for one account then there are chances that we may lose all the accounts.

Rather than using just simple textual passwords it is better to use some different technique which will provide us a better way of setting a password.

Password must be complicated to guess but at the same time it should be easy to remember.

II. LITERATURE SURVEY

Various studies and investigations on the existing schemes have been accomplished. Zheng et al. [1] studied a hybrid password method based on shapes and texts both. The shapes on the grid are used as the real passwords and allow users to log in with text passwords via normal devices. This scheme provides strong opposition to hidden-camera, attacks like shoulder surfing or brute force attacks. It also has differences in improving the security by changing the interface for login in the system.

Sreelatha et al. [2] and Joshi [3] introduced two methods to produce session passwords based on combinations of colours and texts which are pair-based authentication technique and hybrid textual authentication technique. These methods used grids to generate the session passwords generation which is resistant to dictionary attack, brute force attack, and shoulder surfing.

Mathur [4] on the other hand proposed the scheme of giving an option for the user to select the password with the colour. The passwords must contain at least 6 text or alphanumeric characters with coloured fonts to double protect the password.

Patel et al. [5] studied a new technique called session password based on a combination of text and images to resolve the problems related to security. This technique uses grid for the session password generations by which ratings must be given to colours and grid will be displayed based on these ratings.

These techniques are very complex and also some of these takes lots of time to process. So because of this

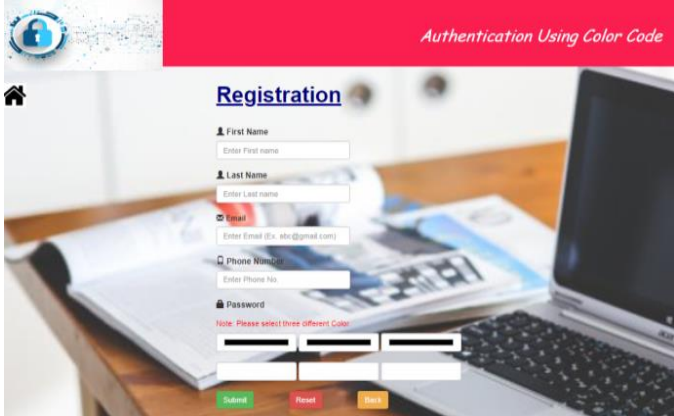
we need some technique which is simple and yet powerful against different attacks.

III. OBJECTIVE

Password in the form of text is the most common way used in user authentication. However, textual passwords are unsafe against eves dropping, shoulder surfing and dictionary attacks. Solution for this is Graphical passwords, which are used as an alternative technique for textual passwords. But Most of the graphical schemes are very complicated and require several rounds of verification, resulting usability issues and it takes lot of time for processing. In this paper, a hybrid and different user authentication technique which combines text and colors is proposed to generate passwords with improved security, usability and stability.

IV. PROPOSED SYSTEM.

First user has to register him/her self with the system. In registration process user will be asked to enter the details as shown in following figure.



The image shows a registration form on a laptop screen. The form is titled "Registration" and is part of a system called "Authentication Using Color Code". It contains the following fields: "First Name" (with a sub-label "Enter First name"), "Last Name" (with a sub-label "Enter Last name"), "Email" (with a sub-label "Enter Email (E.g., abc@gmail.com)"), "Phone Number" (with a sub-label "Enter Phone No."), and "Password". Below the password field, there is a red note that says "Note: Please select three different Color". At the bottom of the form, there are three buttons: "Submit", "Reset", and "Start". The background of the laptop screen shows a desk with papers and a pen.

Figure 1: User registration.

In normal systems we just have an option of selecting passwords in the form of text, numbers or few symbols. These types of passwords can easily be guessed and hacked, in proposed system as we can see in above Figure 1; we can select a password which is

the combination of color and codes. During the registration phase, the user should fill up all of the information required in the registration form and selects three different colours and rate them individually. The user should rate each of the colours uniquely from 0 to 9 as a password. Selected colours and their ratings are stored in the database. See the following Figure to get the clear idea about color-code combination.

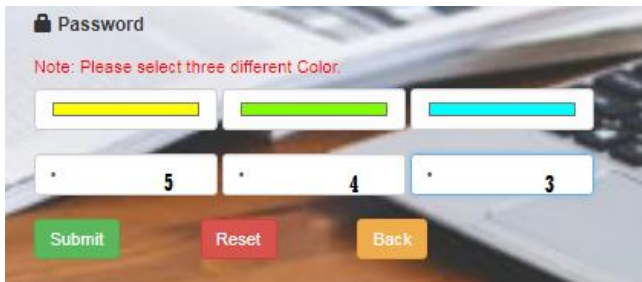


Figure 2: color-code combination.

As we can see in above diagram, user has selected three different colors as Yellow, Green and Blue and with that also selected the codes as: 5, 4, 3. Now this color-code combination will be stored as Yellow-5, Green-4, Blue-3. After user is done with selecting the color-code combination user needs to click on submit to complete the registration process, if the registration is successful then a notification message will be displayed.

During the login phase, the user has to enter a registered email address to continue the login process. The system will verify from the database whether that user is an existing user or not. The colors selected by the user during the registration phase will be displayed automatically and randomly and then the user needs to rate them correctly for a successful login. Then, the user needs to click on the login button for successful authentication. Then the system will verify from the database whether that username and password matches or no. Consider the following figures to understand the login process.

User Abhi registered himself with email abhi@gmail.com and colors Green, Black and Red.

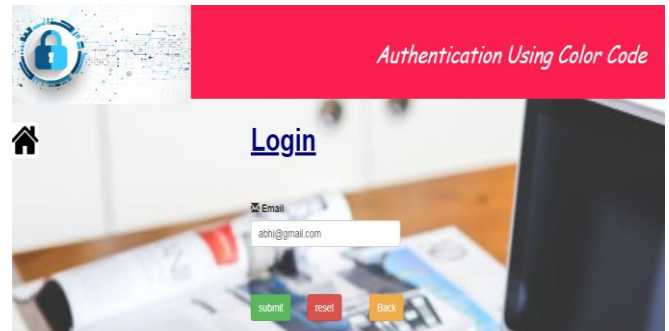


Figure 3: user login (Part 1).

Now the system will check this E-mail in the database, if the user is registered then he will be directed to the next phase to enter the password as shown in the following figure.

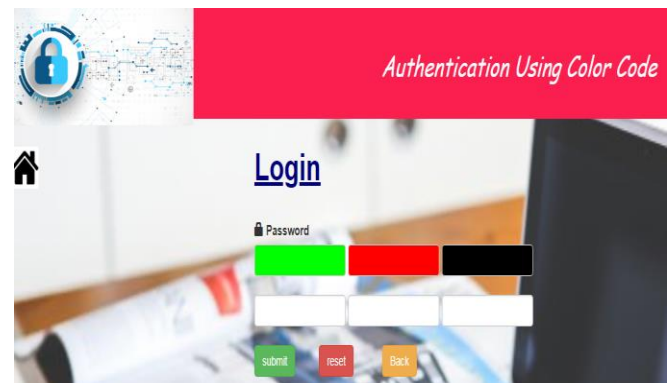


Figure 3: User login, password entering (Part 2).

If the user logs in next time then the color will be displayed in different combinations each time randomly as shown in the following figures.

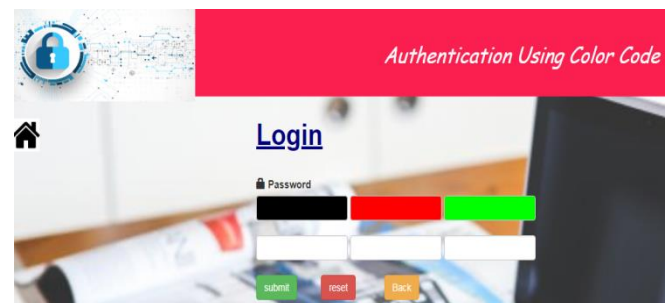


Figure 4: other combination of color.

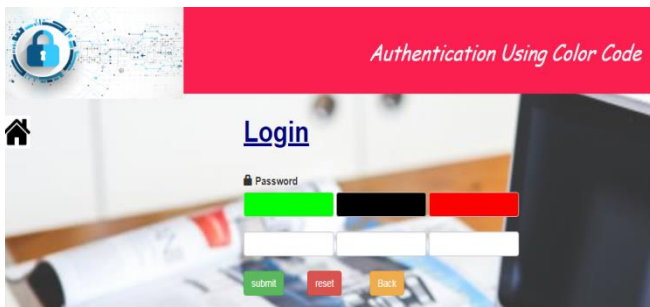


Figure 5: Another combination of color.

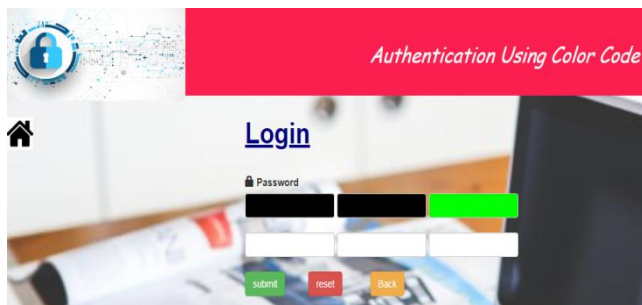


Figure 6: sometimes combination of color may appear as shown in figure.

This has very good advantages over a conventional method of password setting using only text.

V. MEHODOLOGY

The idea used is to save the username and password in database. Password will be the combination of COLOR-TEXT. When username is matched successfully in database, the color which was selected will appear randomly. We used only 3 colors here so there are totally $3*3*3=27$ possible combinations of the colors. In short that means you will set you password once but it is as good as setting 27 passwords at a time. Each time when you login you will get any one combination out of 27. We just have to remember the colors and associated ratings or text. If we are setting ratings then we have to only remember three colors and three numbers, which is easy but it is very complicated for the hackers because of its randomness.

VI. CONCLUSION

Password is in the form of color and text combination, and at the time of login the colors will appear randomly.

Because of this randomness code which is used as password will also have to be entered accordingly. So all the time order will differ which makes it hard for the attacker to guess the password. This method gives a very good security against different attacks like Eves Dropping, Shoulder Surfing and Dictionary Attacks. In above mentioned attacks hackers try to guess the passwords and crack the passwords but because of the randomness in this system it makes it very hard and difficult for hackers to the passwords. We can increase the complexity of the system by increasing number of colors in password field.

VII. REFERENCES

- [1]. Zheng, Z., X. Liu, L. Yin and Z. Liu, 2010. A hybrid password authentication scheme based on shape and text. *Journal of Computers*, 5: 765-772.
- [2]. Sreelatha, M., M. Shashi, M. Anirudh, M.D.S. Ahamer and V.M. Kumar, 2011. Authentication schemes for session passwords using color and images. *International Journal of Network Security & Its Application*, 3: 111-119.
- [3]. Joshi, N.S., 2013. Session password using grids and colors for web applications and PDA. *International Journal of Emerging Technology and Advanced Engineering*, 3: 248-253.
- [4]. Mathur, A., 2011. Improved password selection method to prevent data thefts. *International Journal of Scientific & Engineering Research*, 2: 1-2.
- [5]. Patel, J., S. Padol, B. Kankariya and K. Kotecha, 2013. Authentication for session password using

colour and images. International Journal of Computer Applications, pp: 5-10.

- [6]. Lokhande, K.P. and V.M. Gajbhiye, 2014. Extended text and color based session password security against shoulder surfing and spyware. Journal of Emerging Technologies and Innovative Research, 1: 665-669.
- [7]. Tidke, S., N. Khan and S. Balpande, 2015. Password authentication using text and color. International Journal of Scientific Research Engineering & Technology, 4: 278-281.

Cite this article as :

Abhinandan P. Mangaonkar, "Colour-Code Combination for Secured Login", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 7 Issue 2, pp. 47-51, March-April 2021. Available at doi : <https://doi.org/10.32628/CSEIT217211>



Journal URL : <https://ijsrcseit.com/CSEIT217211>