Color Scheme Password Encryption & Storage

Alwin K Thomas
Department of computer science & Engineering
College of Engineering, Chengannur, India

Haripriya Rajan
Department of computer science & Engineering
College Engineering, Chengannur, India

Lintu Liz Thomas
Asst. Professor
Department of computer science & Engineering
College Engineering, Chengannur, India

Mohammed Farize
Department of computer science & Engineering
College of Engineering, Chengannur, India

Sachu Shylan
Department of computer science & Engineering
College of Engineering, Chengannur, India

Abstract— **One of the most important password protection issues is to secure encrypted passwords on server's database. In cryptanalysis, a dictionary attack or brute force attack are the most common ways of guessing passwords. In order to augment the security aspect regarding passwords, we are devising this algorithm which will be responsible for preventing dictionary or brute force attacks on the passwords. In this Color Scheme Password Encryption method, it will allow the users to create a two layer password system; the first one deals with the colors and on further encryption a single color will be stored on the database, and the second one deals with the ordinary character password but it will be converted to a color based on several algorithms. This application provides a better way for securing various online systems by encrypting the password to generate a color, and as a second phase, the color password encryption scheme will add up the security to a higher level**

Keywords—Color Password, Color Password Encryption

I. INTRODUCTION

Authentication is a process by which system verifies the identity of a user. Authentication is the main step of any security system. Text passwords remain the most common method for several reasons [11-12]. This method is susceptible to various predominant attacks like phishing, spyware attacks etc. To address the problem with conventional models alternative authentication models such as biometrics were used. A very high level of security can be achieved with the help of biometrics [2-3]. But this authentication system involves a lot of expense. In the recent times there has been a great deal of hype for the graphical passwords.

With the rapid advance of science and technology, more and more people rely on modern computers and networks to communicate with each other, and to store and process information. One side effect of this trend is that the availability of electronically stored information to illegitimate users has also increased. Due to the distributed nature of the network architecture and the increased demands of sharing resources and exchanging data among users, protection mechanisms residing within each individual computer become inadequate to insure the security of communications across the network. Hence a security enforcement mechanism for the network is required to prevent information from being destroyed, altered, disclosed or

copied. Various kinds of protection schemes have been employed so far. Among them, the password authentication schemes draw special attention because of their inexpensiveness, ease of implementation and user friendliness. The security of conventional password authentication schemes depends on the following: (a) strong and effective protection schemes for the system's password file; (b) high degree of difficulty for an intruder to compromise users' passwords by exhaustive search and (c) users taking precautions to prevent their passwords from being lost. In a distributed environment, it is possible to implement network security functions on top of the transport or presentation layer. Such implementations ease the task of modifying existing operating systems, whereas they lack the capability of providing full protection of security-relevant secret information, such as password files, from being disclosed. To solve this problem, new schemes have been proposed such that even if the password file is compromised, the system security is still retained. This goal can be achieved if a scheme ensures that (a) no passwords are stored in clear text form in the password file; (b) an intruder is unable to derive users' passwords from any information he could possibly obtain in the password file and (c) no alteration or modification of the password file could help an intruder to get into the system.

In the proposed system, the Color scheme will allow users to create a two layer password system; the first one deals with the colors and on further encryption a single color will be stored on the database, and the second one deals with the ordinary character password but it will be converted to a color based on several algorithms.

EXISTING SYSTEM

The idea of graphical passwords was initially developed by Greg Blonder [1] in the year 1996. Though Graphical passwords are much easier to remember, they provide high level of security. Graphical passwords are classified into two types i.e. recognition based graphical passwords and recall based graphical passwords [8]. Recognition-based systems, also known as cognometric systems [9] or search metric systems [10]. Recall bases systems are further classified into 2 types i.e. a pure recall based graphical passwords and cued recall based graphical passwords. In Recognition based schemes, user will be shown a set of images. In the authentication step user selects a couple of images which were chosen at the registration phase. In Recall based schemes, user is supposed to reproduce something which he/she created or selected during the registration phase. In Pure recall based schemes the user has to reproduce the password without any help from the system. Draw-A-Secret technique [6], grid selection [1] and Passdoodle [4] are some of the examples of this method. In recall based schemes the user will have some assistance from the system to reproduce their passwords. User has to click on some points at the registration phase to set them as his password and has to click on the same points during the authentication. Passpoints [5] scheme, cued click points [7] scheme are the examples of this method.

The existing graphical passwords are seen as complex and time consuming for the users and existing system like DES has several loop poles that can be easily decrypted and hacked easily. An Authentication system should force the user to select strong password while not affecting the memorability. We applied this approach to propose a novel two step authentication graphical password scheme.

II. PROPOSED SYSTEM

- This application provides a better way for securing various online systems by encrypting the password to generate a color, and as a second phase, the color password encryption scheme will add up the security to a higher level. This scheme will allow users to create a two layer password system.
- The first one deals with the colors and on further encryption a single color will be stored on the database, and the second one deals with the ordinary character password but it will be converted to a color based on several algorithms.
- User defines the encryption key.
- Even if two users select same combination, their color preference values will be different. So the problem of redundancy of password is omitted.

The main objective of the application is to encrypt the password assigned with the help of various color schemes. Currently the ordinary password creation mechanisms have various loop holes and are easy to hack. This project is aimed at developing a better password encryption mechanism so that it will be difficult for the hackers to gain access to the system.

The objective of this project is to create and implement a new method of password encryption mechanism. This system of new encryption will be used primarily by those who need more security to their application or any other online systems. This scheme will allow users to create a two layer password system; the first one deals with the colors and on further encryption a single color will be stored on the database, and the second one deals with the ordinary character password but it will be converted to a color based on several algorithms.

A. *OVERALL DESCRIPTION*

Product Perspective

This product is an entirely new product. It is not a component of a larger system. The main objective of the application is to provide a better way for securing various online systems by encrypting the password to generate a color, and as a second phase, the color password encryption scheme will add up the security to a higher level.

Product Functions

The following list of function descriptions explains the major features of the Color Scheme Password Encryption and Storing.

Account Creation

The registration function shall allow users to create secure accounts the account will track the user's name, e-mail address, mobile phone number, username and password.

This provides security to the account member by setting up an account that is password protected. Before choosing the password, first the user will be asked to rate 10 different colors, and then the user has to choose 3 pairs of colors where each pair is used for selecting a random number from the matrix created. Then these numbers will again be processed so that these three numbers will be in the range 0-255.Then the corresponding colors will be chosen from these numbers with the help of different color models. The color models itself are selected with the help of an algorithm. Then these three colors are processed (if it is RGB, color addition will take place, CYMK, color subtraction will take place) to form a single color and will be stored in the database as password.

Then in the second phase, user can choose another ordinary password consisting of characters, numbers or special symbols. And then the password will be divided into three. And the corresponding ASCII numbers are generated, then the resulting number is processed with the help of another encryption algorithm to generate numbers in the range 0-255.And the same process is repeated for phase 1, and a single color is generated and stored in the database. And after choosing the username, the username itself will be encrypted by an algorithm and will be stored in the database. This also offers convenience so the user only has to enter the information listed above once and then it is stored in the account.

Account Login

The account login function shall allow account members to enter their username and password. Once verified, users will be able to access the account. During login, the encrypted username in the database will be decrypted, and will be checked with the entered username. Here also, the user will be provided with colors to rate them, and allowed to enter the color password combination. These sets of colors entered by the user are encrypted by the same process, and the resultant color is checked with the color in the database, if it matches user will be able to access the account.

Account Logout

The account logout function shall allow account members to exit their account for security purposes. This allows account members to exit their accounts, and prevent others from accessing it.

Reset Password

Here the user will be asked to enter his email address, and the reset link will be send to the user's email address. The email will contain necessary information's and links for resetting the password.

Contact

This function will help the user to send their queries to the admin. The user has to enter the name, email address and his query. Once submitted it will be send to the admin's email.

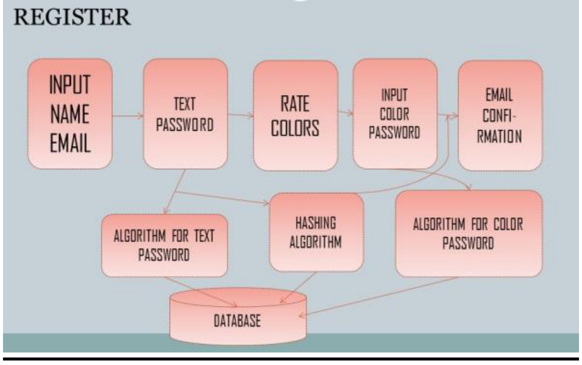
Help

The help function shall give the user an overview of how to use the different functions listed above. This allows the user to get answers to immediate questions on using the website.

*1) **User Interfaces:***

The system will provide the ability for users to access the application via the Internet. There will be two different user interfaces that will accompany this scheme: one for the users and the administrators.

Users will be allowed to create, login and logout from the account.

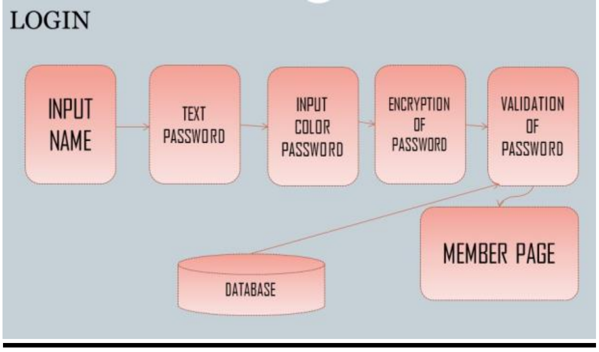


1) Account Registration

- The system shall allow a non-registered user to create a secure account.
- The system shall require the following information from the user:
- Name, e-mail id.
- The system shall ask the user for a username and password.
- The system shall confirm the username and then should display 10 different colors to rate them.
- The system should check whether the username and password are acceptable and it should be encrypted by using different algorithms.
- The system shall store the information in the database.

2) Account Login

- The system shall allow a registered user to log-in to their account.
- The system shall require a username and password from the user.
- The system will verify the username and password, and the user will be considered "logged-in"



3) Reset Password

- The system shall allow a user to enter his email address.
- The system will send the necessary instructions and reset link to the user's email address.

4) Account Logout

- The system shall allow the registered and logged-in user to exit his/her account, so that accesses to operations requiring a user to be logged in are now disabled.

Logical Structure of the Data

The two sections below show the different types of information used by various functions and the overall data model, respectively.

Types of Information Used

The types of information used by various functions of the website:

Function	**Types of Information Used**
Account Registration	User information (name, mailing address, phone number, and user name, and password)
Account login	User information (user name, and password)

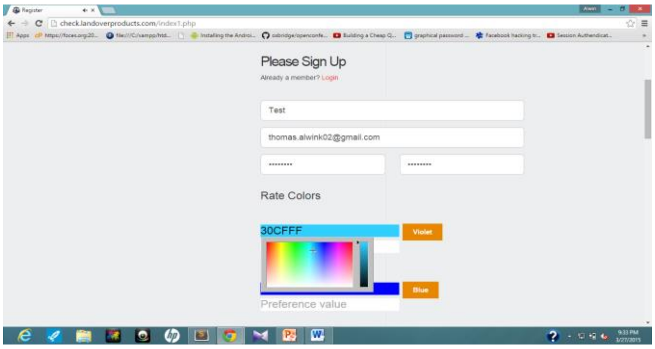
DATA MODEL
USER:

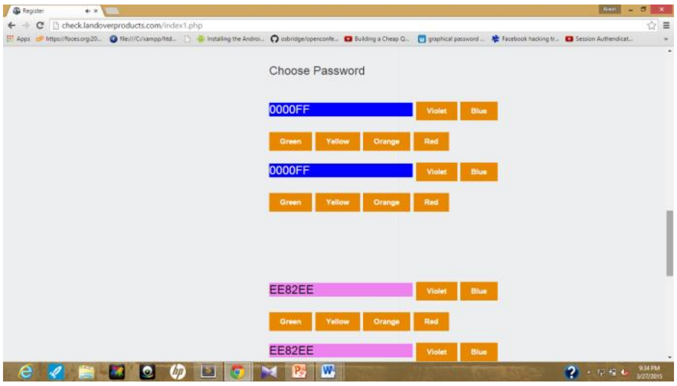
B. IMPLEMENTATION

ALGORITHM FOR COLOR SCHEME PASSWORD ENCRYPTION

Algorithm for color code encryption of selected colors from a palette

Step 1: Select 6 colors from a palette of a million colors.
Step 2: Order the 6 colors in any preference.
Step 3: Pair the 6 colors into three groups.
Step 4: The first pair denotes the value of red in the RGB scale.
The second one green and third one blue.
Step 5: The red generate function is used to generate the red value in RGB. The green generate function is used to generate the green value in RGB. The blue generate function is used to generate the blue value in RGB.All values generated are integers below 256.
Step 6: Convert the respective values below 256 to their hex representation. Thus blue, green and red integer values will have their Hex equivalent which is combined together.
Step 7: This represents the unique color code value.


Register
check.landoverproducts.com/index1.php
Please Sign Up
Already a member? Login
Test
thomas.alwink02@gmail.com
•••••••••
•••••••••
Rate Colors
30CFFF
Preference value


Register
check.landoverproducts.com/index1.php
Choose Password
0000FF
0000FF
EE82EE
EE82EE

Algorithm for color code encryption of the given password.

Step 1: Enter the password and determine its length.
Step 2: For a password with length of multiples of 3 divide the password in to three pairs in order.

In case if the password is not a multiple of three, specific characters are added to make it into multiples of three.

Step 3: Encrypt the password using the following scheme

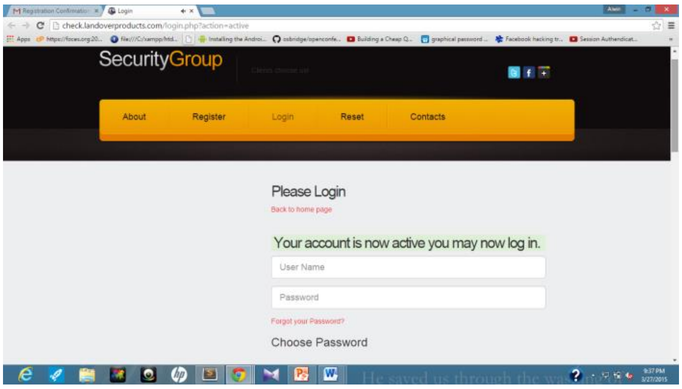
.If the character is an alphabet; the value of character= Alphabetical order of character jumbled to spaces defined by adding the overall length.

Username	3 digits + / + maximum 3 digits
Password	At least 8 letters+digits,1 cap
Password	6 colors(3 pairs each)
Name	First : String Middle : String Last : String
Phone number	10 digits

Else if the character is number: The value of character= one obtained by sequentially performing a queue operation on 0-9 till the total length of password.

Else if the character is a special character: The character is replaced with another character defined by the programmer.

Step 4: The total value of the characters in ASCII of the individual characters in a group is added and finally provided to red generate, green generate and blue generate functions.
Step 5: The three pairs are then converted to their HEX value to generate a color code.


Registration Confirmation
Login
check.landoverproducts.com/login.php?action=active
SecurityGroup
Please Login
Back to home page
Your account is now active you may now log in.
User Name
Password
Forgot your Password?
Choose Password

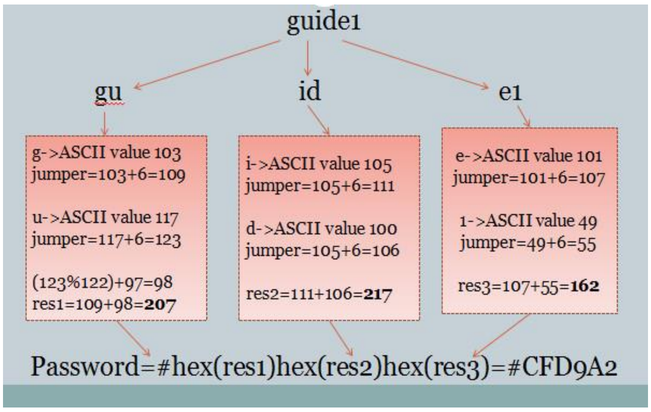
Algorithm for final comparison and encryption.

Step 1: The color code generated for password and selected colors are fed into a comparator function.
Step 2: The Red value of the color code of password and selected colors is compared with red values of the color pair that denotes Red color. If both of them are at a higher value or equal to Red color code of password is taken else that of selected colors is taken.
Step 3: Similarly the Green and Blue values are obtained. Thus a new color code is generated which is the final color code that represents the encryption of the password.

Algorithm for hashing password.

Step 1: Take 6 colors from user as input & provide them with a preference value.
Step 2: A particular key is generated using the six colors & preference value & is employed on a new encryption technique called as color peppering.
Step 3: The six colors are used to form a combination of three pairs.
Step 4: The first combination is used to generate the red color value using red_generate()

Step 5: Similar process is done for generating blue & green color



III. CONCLUSION

A better user interface can increase the ease of use of our software. The FASH algorithm can be modified for higher level of encryption. EVSSL (Extended Validation –SSL) can be implemented. The encrypted code of FASH algorithm cannot be decrypted even by the coder. The Brute Force combinations needed are above 256^6 * $256^{6\,*}99^{6\,=}7.45*10^{40}$ (approx.). Brute force attacks will take years to hack the code. Comparator can be used to merge the encrypted color and text password so that it increases more security.

IV. ACKNOWLEDGEMENT

We are indebted to our project co-coordinator **Mrs. Renu George,** Assistant Professor and guide and mentor **Ms. Lintu Liz Thomas,** Assistant Professor at College of Engineering, Chengannur for their timely help and advice throughout the project. And we would also like to thank Department of Computer Engineering of College of Engineering, Chengannur for the technical guidance for this research work.

V. REFERENCES

[1] G. Blonder. Graphical passwords. United States Patent 5559961, 1996.

[2] K. Gilhooly, "Biometrics: Getting Back to Business," in Computerworld, May 09, 2005.

[3] A. Jain, L. Hong, and S. Pankanti, "Biometric identification," Communications of the ACM, vol. 33, pp. 168-176, 2000.

[4] Real User Corporation (2007) PassfacesTM, http//:www.realuser.com.

[5] Brostoff S. and Sasse M.A. In People and Computers XIV – Usability or Else: Proceedings of HCI. Sunderland, U.K, 2000.

[6] Sobrado L. and Birget J. (2007) http://rutgersscholar.rutgers.edu/volume04/sobrbirg/sobrbi rg.htm.

[7] S. Chiasson, P. van Oorschot, and R. Biddle, "Graphical password authentication using Cued Click Points," in European Symposium on Research in Computer Security (ESORICS), LNCS 4734, September 2007, pp. 359–374.

[8] I. Jermyn, A. Mayer, F. Monrose, M. K. Reiter, and A.D. Rubin, "The Design and Analysis of Graphical Passwords," in Proceedings of the 8th USENIX Security Symposium, 1999.

[9] A. De Angeli, L. Coventry, G. Johnson, and K. Renaud, "Is a picture really worth a thousand words? Exploring the feasibility of graphical authentication systems," International Journal of Human-Computer Studies, vol. 63, no. 1-2, pp. 128–152, 2005.

[10] K. Renaud, "Guidelines for designing graphical authentication mechanism interfaces," International Journal of Information and Computer Security, vol. 3, no. 1, pp. 60–85, June 2009.

[11] K. Renaud, "Evaluating authentication mechanisms," in Security and Usability: Designing Secure Systems That People Can Use, L. Cranor and S. Garfinkel, Eds. O'Reilly Media, 2005, ch. 6, pp. 103–128.

[12] C. Herley, P. van Oorschot, and A. Patrick, "Passwords: If Were So Smart, Why Are We Still Using Them?" in Financial Cryptography and Data Security, LNCS 5628, Springer, 2009 Financial Cryptography and Data Security, LNCS 5628, Springer, 2009.