Abstract — many password authentication schemes have been proposed. Most of the shoulder-surfing resistant password schemes proposed is based on textual authentication and many users are still not familiar with the graphical password scheme. Text based password scheme has many security issues, so unfortunately none of exiting text-based shoulder surfing resistant graphical password schemes is both efficient and secure enough. In this scheme, we propose an improved text-based shoulder surfing resistant graphical password scheme by using colors. In the proposed scheme, the user can easily and efficiently login system. Next, we analyze the security and usability of the proposed scheme, and show the ability of the system to tackle shoulder-surfing and accident login.

Keywords — Graphical, Shoulder-surfing,

I. INTRODUCTION

In recent times the use of internet has increased to a greater extent for different purposes such as Banking, social media, sending messages etc. and for the same the need of proving a secure way to login into the system has also increased. For the same many password authentication systems exist for the user accounts, But using that system gives rise to different security issues such as shoulder-surfing, brute-force attack etc. Shoulder-surfing means adversary to obtain the user’s password by watching over the user’s shoulder as he enters his password. As conventional password schemes are unprotected to shoulder surfing. Observing that most users are more familiar with textual passwords than pure graphical passwords, so Zhao et al proposed a text-based shoulder surfing resistant graphical password scheme, In S3PAS, the user has to mix his textual password on the login screen to get the session password. However, this login process scheme is complex and tedious. And then, several text based shoulder surfing resistant graphical password schemes have been proposed.

Unfortunately, none of existing text based shoulder surfing resistant graphical password schemes is both secure and efficient enough. In this paper, we will propose an improved text-based shoulder surfing resistant Graphical password scheme by using colors. The operation of the proposed scheme is simple and easy to learn for users familiar with textual passwords. The user can easily and efficiently to login the system without using any physical keyboard or on-screen keyboard.

II. LITERATURE REVIEW

The first three Graphical password schemes were proposed by Sobardo and Birget in 2002. These were named as The Moveable Scheme, The Intersection Scheme and The Triangle Scheme. But, both the Movable Frame scheme and the Intersection scheme have high failure rate. In the Triangle scheme, the user has to choose and memorize several pass-icons as his password. In every time whenever login the
user has to find three pass-icons among a set of randomly chosen icons displayed on the login screen, and then click inside the invisible triangle created by those three pass-icons. To overcome the drawbacks of Triangle Scheme, in 2006, Widenbeck et al, proposed a Convex Hull Click Scheme possessing a superior security and usability. To login the system, the user has to correctly respond several challenges. In each challenge, the user has to find any three pass-icons displayed on the login screen, and then click inside the invisible convex hull formed by all the displayed pass-icons. However, the login time of Convex-Hull Click scheme may be too long and more tedious. To reduce the login time, in 2009, Gao et al proposed a Shoulder Surfing Resistant Graphical Password Scheme, with alphabet characters and colors, where background colors are a usable factor. However, the probability of accidental login of Color Login is too high and the password space is too small. As most users are familiar with textual passwords and conventional textual password authentication schemes have no shoulder surfing resistance, Zhao et al. in 2007, proposed a text-based shoulder surfing resistant graphical password scheme, S3PAS, in which the user has to find his textual password and then follow a special rule to mix his textual password to get a session password to login the system. However, the login process of Zhao et al.’s scheme is complex and tedious. In 2011, Sreelatha et al. also proposed a text-based shoulder surfing resistant graphical password scheme by using colors. Clearly, as the user has to additionally memorize the order of several colors, the memory burden of the user is high. In 2012, Rao et al. proposed a text-based shoulder surfing resistant graphical password scheme, PPC. To login the system, the user has to mix his textual password to produce several pass-pairs, and then follow four predefined rules to get his session password on the login screen. However, the login process of PPC is too complicated and tedious.

III. PROPOSED SYSTEM
We will see a simple and efficient shoulder surfing resistant graphical password scheme based on texts and colors in this section. The alphabet used in this propose scheme is a 64 characters, including 26 lower case letters, 26 upper case letters, 10 decimal digits, and symbols “.” and “/”. This proposed scheme includes two phases; one is registration phase and second is login phase.

1. Registration phase
The user has to set his textual password K of length $L$ $(8 \leq L \leq 15)$ characters, and choose one color as his pass color from eight colors assigned by the system. The remaining seven colors not chosen by the user are his decoy colors. In addition, the user has to register an e-mail address for re-enabling his disabled account. The registration phase should proceed in an environment free of shoulder surfing. In addition, a secure channel will be established between the system and the user during the registration phase by using SSL/TLS or any other secure transmission mechanism. The system stores the user’s textual password in the user’s entry in the password table, which should be encrypted by the system.

2. Login Phase
When user requests to login the system, then the system displays a circle composed of eight equally sized sectors. That is our project login screen. In that login screen colors of the arcs of the eight sectors are different, and each sector is identified by the color of its arc, example- the blue sector is the sector of blue arc. Initially, 64 characters are placed averagely and randomly among these sectors. All the displayed characters can be simultaneously rotated into either the adjacent sector clockwise by using the clockwise button once or the adjacent sector anticlockwise by clicking the anticlockwise button once,
and the rotation operations can also be performed by scrolling the mouse wheel. The login screen of the proposed scheme can be illustrated by an example shown in Fig. 1.

To login the system, the user has to finish the following steps:

Step 1: The user requests to login the system.

Step 2: Application will display the login screen, which consists a circle composed of eight equally sized sectors, and places 64 characters among the 8 sectors averagely and randomly so that each sector contains 8 characters. The 64 characters are in three typefaces and different three colour in that the 26 upper case letters are in bold typeface, the 26 lower case letters and the two symbols “.” and “/” are in regular typeface, and the 10 decimal digits are in italic typeface. In addition, the button for rotating clockwise, the button for rotating anticlockwise, the “Confirm” button, and the “Login” button are also displayed on the login screen. All the displayed characters can be simultaneously rotated into either the adjacent sector clockwise by clicking the clockwise button once or the adjacent sector anticlockwise by clicking the anticlockwise button once, and the rotation operations can also be performed by scrolling the mouse wheel. Let I= 1.

Step 3: The user has to rotate the sector containing the i\(^{th}\) pass character of his password K, denoted by Ki, into his pass-color sector, and then clicks the “Confirm” button. Let i = i + 1.

Step 4: If i < L, the system random Permuted all the 64 displayed characters, and then go to step 3. Otherwise, the user has to click the “Login” button to complete the login process.

If the account is not successfully authenticated for three consecutive times, this account will be disabled and the system will send to the user’s registered e-mail address an e-mail containing the secret link that can be used by the legitimate user to re-enable his disabled account. The login process of the proposed scheme can be illustrated by an example shown in. The user has to rotate the sector (marked with brown dotted line for illustration only) containing Ki (marked with small red circle for illustration only) into his pass-color sector (marked with brown dotted line for illustration).

IV. RANDOM NUMBER GENERATION ALGORITHM

Input: 64 character a to z=26, A to Z=26, 0 to 9=10, and ". /"=2 Output: Random Printing Algorithm:

1. To generate the matrix wit row and column 8*8.
2. Put 0 to 63 numbers into matrix.
3. Select one random number from 0 to 63.
4. For putting number into matrix system check number is already parent or not.
5. If number present, then perform Step 3. If not present, then put into a matrix and go to step3.
6. Do step 5 repeatedly up to 0 to 63 inserted into matrix.
7. Print The Matrix.
8. Now get string which have 64 character " a to z=26, A to Z=26, 0 to 9=10, and . /=".
9. Get number present into matrix sequentially [0][0] to [8][8] i.e., total 64 character.
10. Select index of string from 64 char. put into that current location.
11. Do step 9 and 10 repeatedly up-to [8][8] number.
12. Print Current Matrix with String Char.
13. Display a matrix with Random Printing
14. Stop

V. ANALYSIS
In this section, we will describe analysis of our project. The security and the usability, which is most important part of system, is analyzed in this section for our project.

A. Password space:
The total number of all possible passwords with length L is $8 \times 64^L$.

B. Resistance to accidental login:
Our system is more resistance of accidental login since the probability of correctly responding to password (Ki) is $8/64$, that is $1/8$, the success probability of accidental login with the password (ki) with length L, denote by Pal (L), is
$$
\text{Pal} (L) = (1/8)^L
$$

However, since the password length is a more secret, if hackers want to hack the system he will first guess the user password. He will then try to hack but as the probability distribution of the lengths of the passwords to be used is assumed uniform between 8 and 15, the probability that the hacker correctly guesses the password length is $1/8$. Thus, the probability of accidental login is very less and if the attacker fails to login system consecutively for three times, then that account will be disabled and the system will send e-mail to the user’s registered email-id with a secret link that can be used by the legitimate user to change the password re-enable his disabled account. Thus, accidental login cannot be performed easily and efficiently is to be complicated.

AKNOWLEDGEMENT
We have taken efforts in this project. However, it would not have been possible without the kind support and help of many individuals and organization. I would like to extend my sincere thanks to all of them. I am highly indebted to my college for their guidance and constant supervision as well as for providing necessary information regarding the project & for their support in completing the project. I would like to express my gratitude towards my parents & members of my project for their kind co-operation and encouragement, which helped me in completion of this project.
REFERENCES


2. HUANYU ZHAO AND XIAOLIN LI, S3PAS:”A SCALABLE SHOULDERSURING RESISTANT TEXTUALGRAPHICAL PASSWORD AUTHENTICATION SCHEME” ,SCALABLE SOFTWARE SYSTEMS LABORATORY DEPARTMENT OF COMPUTER SCIENCE,OKLAHOMA STATE UNIVERSITY, STILLWATER, OK 74078, USA,2006.


6. JAY PATEL,SAGAR PADOL, BHUSHAN KANKARIYA,KAINJAN KOTECHA ,” AUTHENTICATION FOR SESSION PASSWORD USING COLOUR AND IMAGES”,INTERNATIONAL CONFERENCE ON RECENT TRENDS IN ENGINEERING AND TECHNOLOGY - 2013(ICRTET’2013)
