Volume No:4, Issue No:11 (April-2019) ISSN No : 2454-423X (Online)

International Journal of Research in Advanced Computer Science Engineering

A Peer Reviewed Open Access International Journal

www.ijracse.com

Session Passwords Authentication Using Colors and Images

Gangu Vijay Kumar
Assistant Professor,
Department of Computer Science& Engineering,
Aditya Institute of Technology and Management, Tekkali, Srikakulam District, Andhra Pradesh 532201, India.

Manchala Yugandhar
Assistant Professor,
Department of Computer Science & Engineering,
Aditya Institute of Technology and Management, Tekkali, Srikakulam District, Andhra Pradesh 532201, India.

Bandaru Ramesh
Assistant Professor,
Department of Computer Science & Engineering,
Aditya Institute of Technology and Management, Tekkali, Srikakulam District, Andhra Pradesh 532201, India.

ABSTRACT:

Generally text passwords are the most common method used for authentication. But text passwords are vulnerable to eves dropping, dictionary attacks and shoulder surfing. So, Graphical passwords are introduced as an alternative technique to text passwords. Graphical passwords are said to be more secure than traditional text passwords. Most of the existing graphical password schemes rare unsafe to spyware and shoulder surfing. A novel graphical password scheme color login is implemented to make the user to feel more interesting and to avoid the baring feelings to a user. In color login concept multiple colors are used to confuse the people but it does not leads to any kind of burden to the authorized users. But the graphical schemes are also being attacked or harmed by shoulder surfing. In order to solve the problem text can be combined with images or colors to generate session passwords for authentication. By this password is used only once and each time a new password is generated. Two methods are proposed to generate session passwords.

Keywords:
Authentication, session passwords, shoulder surfing.

1. INTRODUCTION

Authentication is a key concept in security. Authentication is used to determine whether a user should be allowed to access a given system. Sufficient Authentication can be said as a defence for protecting resources.

Textual password is a very simple password scheme. It was used in old days. Random and lengthy passwords can make system secure but it is difficult to remember. Mostly we use passwords that are short and these can be easily guessed or cracked. Because user give the passwords like petname, birth date, mobile number etc. So this is unreliable. For this problem a new technology is invented that is “Graphical password”. Security and protection of personal accounts in social media is a major issue in these days lack of security is a major problem and becoming an issue. These security issues are rising because of cyber attacks due to attackers, hackers, crackers, scammers. Generally an existing Authentication processes are carried out by user ID and password, with the Authentication schemes alphanumeric-based, biometric-based or increasingly graphical-based. Alphanumeric passwords are the most usual method for user authentication. The use of alphanumeric passwords has several limitations such as Passwords have low entropy in practice and somewhat difficult to remember. The alternative techniques are graphical passwords and biometrics. Every technique has their own disadvantages. Biometric systems uses the physiological characteristics like finger prints, retina pattern, iris, voice print and face pattern and these are also used as an alternative to alphanumeric passwords, but it is not

Cite this article as: Gangu Vijay Kumar, Manchala Yugandhar & Bandaru Ramesh, "Session Passwords Authentication Using Colors and Images", International Journal of Research in Advanced Computer Science Engineering, Volume 4, Issue 11, 2019, Page 1-8.

yet adopted. The major drawback of biometrics is that the systems may be expensive and it handle the physical characters of users, and also the identification process takes some amount of time. Also the identification feature for biometric of a human is physically changed through an accident, then the authentication becomes invalid. Anyhow, biometric-based passwords are said to be a high level secure system. The graphical password is most commonly used in authentication purpose; here the user selects a certain number of images from a set of random pictures during registration later during login the user has to identify the preselected images for authentication from a set of images. Researchers have developed several authentication processes based on graphical passwords, it is initially proposed by “Blonder” in 1996. Images are more memorable than words. Various graphical password schemes have been expressed as suitable alternatives to alphanumeric based or biometric-based authentications.

Color login is expressed and evaluated as a promising recognition-based graphical password scheme; image background color is used as a safety factor. The main advantage of color login is providing an attractive authentication method, with resistance to shoulder surfing. The major disadvantage of graphical password schemes is mouse-click. Color login depend on mouse click. Such actions make color login resistant to shoulder surfing. The new Authentication schemes are proposed for PDA’s. These authenticate the user by session passwords. Session passwords are passwords that are used only once. Once the session is completed, there is no more use of that password. For every login we use different passwords. This provides a better security. These authentication schemes use text and colors.

2. RELATED WORKS

Graphical password schemes based on choosing multiple images as pass objects usually require users to recognize the preselected pictures. Multiple images can be chosen as pass objects scheme, based on flash visualization technique, Deja Vu Authenticates a user through his ability to identify previously registered images. As a result of random generation of candidate pictures, it is not forceful to conclude that passwords can be remembered easily than text-based passwords. Real user employs facial photographs in graphical password system pass faces. It is a technique of using human face as a password; it is implemented and developed because people can be recognized by their faces. However, only limited candidate faces are given on the screens. The security of pass faces is unsafe as it is also may lead to attacks. The above mentioned graphical password schemes have not given a suitable answer for usability and security, these two are major design and implementation issues of a graphical passwords.Color login is a recognition-based graphical password scheme, choosing multiple images as pass-icons which can be used in logging into the system or unlocking the screen.

In this system, the user selects a set of images/pictures from random pictures at the time of registration. Later at the time of login, we have to select the preselected images from the random set of images. It is vulnerable to shoulder surfing. Pass face is a technique, where the user selects four faces from grid of nine faces. They choose four faces as their password. At the time of login they have to select their pre-selected image from eight other images.Since, earlier we selected four faces. This can be done for four times.Jermyn, et al. Proposed a new technique called Draw-a-secret.

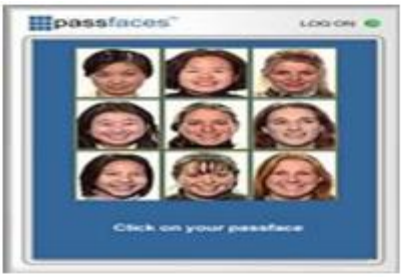


Figure : Examples of pass faces

In this technique, the user has to re-draw the picture that he/she earlier drawn. At the time of re-drawing, if it touches the same grids in same sequence, the user is authenticated. This scheme is vulnerable to shoulder surfing.Syakri developed a technique where authentication is done by drawing user signature with mouse. It includes 2 stages.

1) Registration
2) Verification

At the time of registration, the user has to draw signature with mouse. The system extracts the signature area. In verification stage, it takes the user signature as input and there extracts the parameter of signature. The disadvantage is forgery of signature. Drawing with mouse is difficult are many of them are not familiar with this and one can't draw the signature in the same perimeters as at the time of registration. Blonder designed a graphical password scheme. In this scheme the user have to click on the areas, where he/she has selected at the time of registration. Pass logic has extended the graphical password scheme. In this scheme, the user has to click an various items in the correct sequence as he/she selected before. By this he/she can prove their authenticity.Haichang et al proposed new shoulder surfing resistant scheme.

In this scheme instead of clicking on the images in sequence. The user has to draw across their password images orderly. This graphical scheme combines DAS story schemes to provide authenticity to the user. Many techniques are proposed to overcome shoulder-surfing problem. Zhao and li proposed a shoulder-surfing resistant scheme 'SZPAS'. As like all the schemes at the time of recognition we give a password. The password might be in different forms according to the schemes. In this scheme, we give a textual password and at the time of login we must have to find the password i. e the password at the time login image and click inside the invisible triangle region. Then the system integrates both graphical and textual password scheme and has high level security.Man et al proposed another technique for shoulder-surfing problem resistant. In this scheme, the user selects many images as the pass object and each pass-object have variants and is assigned to a unique code. At authentication stage, the user must type the unique codes of pass objects variants in the scenes provided by the system. Even though the scheme shows perfect results in resisting hidden camera, but it might be difficult to users they have to remind the code with pass-object variants.More graphical password schemes have been summarized in a recent survey paper.

3. DESIGN OF COLOR LOGIN AND SESSION PASSWORD:

3.1 Color Login:

There are four security levels in color login. They are: low,medium,high and self-define. There are six parameters R,C,K,Nc,h,and n. R,C,K,n are determined by level.

1) R is the number of rounds for authentication, ranging from 1 to 3 respectively to define low, medium and high security levels.
2) C is the number of colors used, ranging from 3 to 5.
3) K is the number of pass icons.
4) Nc is the number of total icons per color in the database for different value of C. N3 = 40 , N4 = 72and N5 = 112.
5) h is the number of pass icons shown on each screen and h=2 is used in this paper.
6) n is the number of rows or columns, and n=9,12 or 15.

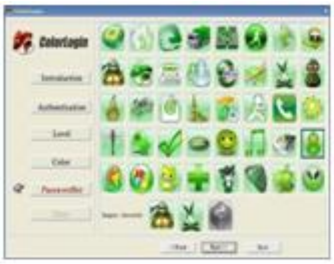


Figure 1. A group of chosen-color icons are displayed for the user to set as his pass-icons. Here the user chooses red icons as his passwords.

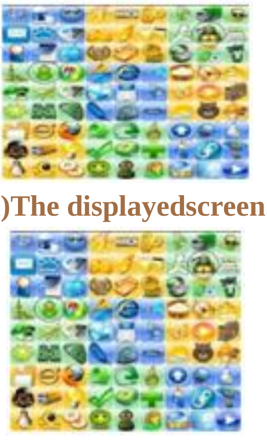
Volume No:4, Issue No:11 (April-2019) ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

In registration phase, shown in figure 1, the user operations can be divided into three steps:

1) Choose a security level needed.
2) Choose one color from colors random provided by system.
3) Choose K images from the sets of the chosen color as pass-icons.

The generation process in the authentication phase can be described below:

1) Randomly generate i th round screen, where the icon group are distributed by a sliding color sequence.
   In each group,icons are chosen in random from database form a single color icon square.
   On the entire screen, there would be such color square filling in the coarse grid. And each icon is different on the screen.
2) When the icons are distributed, h of K pass-icons must be displayed randomly are h different lines.
   For example, in figure 2(a), there are two of three pass-icons lying in two different lines in authentication round.
3) Wait for the user to click on pass-icons lines and replace all icons on line with substituted icons.
4) Gather input information to authenticate the user.



(a)The displayedscreen.

(b)A completedround.

Figure 2. A completed authentication round is shown here (R=1,C=3,n=a,h=2).It has two pass-icons in two lines.When the user clicks on a line,the icons in that line are replaced by substituted icons.

In each login, the system tests a user who want to be authenticated. It is by conducting in R rounds and each round provides random icons displayed on the screen. An example of a challenge round is shown in figure 2; in which red is the focused color while blue and green are inducing ones. A pass-icon will be chosen when the user clicks on the row, that row contains all the pass-icons. And these icons will be replaced by substituted lock icon which is used to resist shoulder-surfing. whenever all h hiding pass-icons are correctly chosen, then the round can be considered as a successfull.

Generally, we may forget our passwords, so for this reason, the user need not to choose icons in a particular order. The login screen is divided into C x C background color squares. After the user chooses his color, both colors and their positions will be displayed on the screen. And moreover, the icons of each color are randomly chosen from database. H pass-icons which are randomly chosen, will be displayed on different rows. At the point of security and usability h is set as 2 i.e.h=2.If h is set as 1,the probability of successful login will be greater. And if h>=3,the time period for finding pass-icons will be longer for legal users.

3.2 Session Password:

Authentication technique consists of 3 phases:

1.Registration phase.
2.Login phase.
3. Validation phase

In Registration phase the user enters the password in first method or rates colors in the second method. In Login phase the user has to enter the password that he/she given in the registration phase. In the verification phase, the system verifies and compares the password that is entered in login phase with the password that is entered in the registration phase.

3.2.1 Pair based Authentication scheme:

During registration phase the user submits a password.The minimum length of the password is 8 and is called as a secret pass. Secret password should contain even number or characters .Based on the secret pass session password is generated.In the login phase, user enters username and a grid is displayed on the screen.The grid is of the size 6X6 and consists of alphabets and numbers. These alphabets and numbers are randomly placed in the grid. The Interface of grid changes every time.User enters the password based on secret pass.This session password consists of both numbers and alphabets.

Password is based on the secret pass and pass has to be considered in pairs.The first letter in the pair is used to select row and the second letter is used to select column. The intersection of the row and column we will get a letter (i. e common for both row and column). And that letter is the part of session password.This process is repeated for all the pairs of secret pass. The password entered by the user is verified by the server to authenticate the user. If the password is correct then the user can enter into the system. Grid size can be increased to include special characters in the password.

3.2.2 Hybrid textual Authentication scheme:

During registration, users should rate colors. The user should rate colors from 1 to 8 and he/she can remember it as “RLYOBGIP” same rating need to give the other colors i. e if the rate 3 for yellow, we can rate Green with 3.During login phase, the user enters his/her username and an interface is displayed based on the colors selected by user. The login interface consists of grid of size 8X8. And this grid contains 1-8 digits placed randomly in the cells.This interface also contains the strip of colors. The color of grid consists of 4 pairs of colors. In each pair, the first color represent the row and the second color represents the column.

Before we have to rate the colors in registration phase. Based on that rating we have to select rows and columns. Firstly, in the login phase, we have color grid and take the first pair, for example, the pair may red and yellow. As we already know that 1st color represent row and second color represents columns. In registration phase, we rated red, so we have to select the 1st row from the grid of size 8X8. And we rated yellow with 3. So we should select 3rd column. The intersection of the first row and 3rd column is the part of the password (I. e digit from 1st row and 3rd column). In the similar manner we have to select the rows and columns according to the pair of colors.This is followed for the other 3 pairs also. So we will get the session password.Instead of digits we may use alphabets also. For every login, the number grid and color grid changes and so the password also changes.

4.ANALYSIS OF SCHEME:

4.1 Contribution Of Background Color:

When users log into the schemes, which choose multiple images as pass-icons, the pass-icons take more time in locality itself from large number of icons which are randomly placed.Color is one of the most important features of images. But it is not considered as much as important in previous multiple image choice schemes.The background color of images is first proposed and used in color login. In color login,the icons appears very clearly on the screen. When users want to recognize the pass-icons in the authentication, we should give priority to icons of predefined color rather than all the icons displayed.As shown in the figure 2,users only need to search for the pass-icons from 27 red icons,while 81 are presented. Thus,introduction of colors can cut workload 2/3 relative to similar schemes with out background color. This is just an instance at lowest level.In higher levels,more colors are introduced with a decreased workload. Atmost, 5 colors can be used in color login and 4/5 of the workload is reduced.Hence,we can say that login time will be reduced greatly.

In addition to that,if the authentication procedure is too slow,it may create memorization difficulties and sometimes irritate the users.Background colors are the user interface friendly,which helps users escape from the irritation of large number of confusing icons.

4.2 Resistance To Shoulder Surfing

Some proposed password schemes have proved to be shoulder surfing resistant.But they are alphanumeric-based,which requires users to remember and input text characters,not a good user experience,such as CHC proposed in[10],which results in facing difficulties for users in clicking icons.Color login provides a shoulder surfing resistant scheme which can overcome the drawbacks noted above. In color login,there are different icons on screen in each login round.Neither icons nor pass-icons displayed are fixed.When the user finds one pass-icon,he need to click on the line where pass-icon lies,after this action,it will be replaced by substituted icons.Although such replacement is no use in resisting shoulder surfing when the process is recorded by video tape,it is very helpful to resist shoulder watches,where the peepers cannot remember the icons in a short time.

4.3 Password Space

System security depends on having large password space, the main defence against a brute force search.Alphanumeric based passwords have a password space of 94^n,where n is the password length,94 is the number of printable characters excluding SPACE.One major faced by graphical passwords is protecting that the password space is comparable to that of alphanumeric passwords. In color login,the password space S can be determined by equation(1). N_c -it denotes the combination of number of choosing any K icons among N_c icons of same color.Then,for all C colors,the password space S can be obtained. The password space varies with CN_c and k.According to value of $CN_c$and K,the password space of color login can be obtained.

The system can also extend the password space by increasing the number of colors and as well as number of pass-icons. When C=5 the password space is approximately 1112≈6.7e8 which is smaller than text-based passwords with a length of 5.So,it is more difficult to carry out a brute force attack against graphical passwords than text-based passwords.As a graphical password scheme,the password space of color login is sufficient.Mostly recognition based graphical passwords have a small password space.Picture passwords are used for mobile devices,thus the total number of pictures is small due to size limit of mobile devices and password space must be limited. Deja Vu and CHC printed out that the password space can be enlarged by increasing the number of total icon and pass-icons,but it is not realistic for users.

C, k, N_C	**3, 3, 40**	**4, 4, 72**	**5, 5, 112**
space	3e+5	4e+7	6e+9

Table1. The password space of Color Login

- **Security Analysis:**

Session password changes every time as the interface changes. This is resistant to shoulder surfing. With the use of dynamic passwords, dictionary attack is not applicable.

- **Dictionary Attacks:**

These attacks are directed towards textual passwords. In this attack, the hacker uses a set of dictionary words and try to authenticate. These Dictionary attacks fails towards authentication systems why because for every login the session password changes.

- **Shoulder surfing :**

These are shoulder surfing resistant techniques:In pair scheme,session secret pass created in registration phase cannot be known as it is hidden. So by the session password cannot find the secret pass. Hence resistance is provided.In hybrid textual scheme, random colors hide the password.

In this scheme, rating decide password. But with password we can't find rating. Even if we know password, the complexity is 8^4. And in every login colors are changed and the numbers in the grid are also changed. So these two are shoulder surfing resistant schemes.

- **Guessing:**

Guessing can't be possible on pair based because it's hard to guess secret pass and it is 36^4.The hybrid textual scheme is based on user selection of colors and ratings. So,it would be difficult guess. If the user selects in general order then is a possibility of breaking the system.

- **Brute force attack:**

These techniques are particularly resistant to brute force because of the use of session passwords. The use of these i. e session passwords will take out the traditional brute force attack out of the possibility.

- **Complexity:**

Complexity for pair-based Authentication scheme is to be carried over the secret pass. Complexity for a secret pass of length 8 is 36^8. Complexity depends on colors and ratings for hybrid textual authentication scheme. The complexity is 8! If ratings are unique otherwise it is 8^8.

5. USABILITY EXPERIMENTS:

The proposed color login is implemented in C++.The tool can be used as a password login scheme replacing that Windows XP's. Before the experiments, the experimenter explained the needs of the system and it's working used to tutorial materials. In first session 30 participants repeatedly attempted to authenticate themselves until ten successful logins were achieved. The mean times to log into color login is shown in figure 3,which indicates that there is a slight downward trend in the time taken for the user to be authenticated.

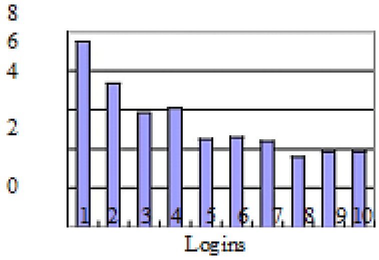


Figure 3. Mean times of 30 participants for 10 correct logins in ColorLogin with a 9×9 grid screen，R=1.

The results in table 2 are encouraging with proper grid density authentication challenge rounds, color login reveal good performance. Even though it takes a long time to log into color login than in text-based schemes, nearly 85% participants thought that the time of login was acceptable according to post test questionnaire. The reason may be that an appealing login process can shorten the perception of time taken.

	Grid size of Color Login		
	9×9	12×12	15×15
R = 1	3.4	5.2	5.5
R = 2	8.2	9.6	11.2
R = 3	11.3	13.6	15.2

Table 2. Mean times (seconds) of 30 participants for 5 correct logins.

The mean time of Convex Hull Click Scheme (CHC) for one round is 10.97 seconds and for five rounds is 71.66 seconds[10].The mean time of Deja Vu for one round is 32 seconds[5] compared to these similar schemes color login takes less time for users to be authenticated.

6. CONCLUSIONS:

Color login is a graphical passwords method to develop more effective user-friendly and secure.In this project,image background color is introduced which helps in reducing the legal user's login time,considered to be crucial to the usability of password scheme .It aims to motivate the user with a fun, friendly interface designed to improve user experience and provide acceptable login time.Color login is a promising technique which can developed by furher studies.Further work should consider high security mechanisms, and reducing time consumption.Users can choose their color and icons and some icons are chosen as pass-icons,creating so-called hotspots.Color-blind users will be taken into accounted.In the near future,Color login is expected be further tested in actual projects.

Two authentication techniques are proposed for PDA's based on text and colors. These techniques generate session passwords and are dictionary attack, brute force attack and shoulder surfing resistant. In both the techniques session passwords are generated using grids.In both the techniques there is no need of registration why because session password is generated on the grid at the time of login.In hybrid textual scheme, rating are given to colors. Session passwords are generated based on the ratings on the grid during login. But these schemes are new to the users and these schemes should be verified deeply for usability and effectiveness.

7. REFERENCES

[1] Jermyn, I., Mayer A., Monrose, F., Reiter, M.,and Rubin., "The design and analysis of graphical passwords" in Proceedings of USENIX Security Symposium, August 1999.

[2] Haichang Gao, Zhongjie Ren, Xiuling Chang,Xiyang Liu Uwe Aickelin, "A New Graphical Password Scheme Resistant To Shoulder Surfing.

[3] S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy and N. Memon, "PassPoints: Design and longitudinal valuation of a graphical password system", International Journal of Human-Computer Studies, vol. 63, **(2005)**, pp. 102-127.

[4] D. Weinshall, "Cognitive Authentication Schemes Safe against Spyware", (Short Paper), IEEE Symposium on Security and Privacy, **(2006)**.

[5] S. Chiasson, R. Biddle and P. C. van Oorschot, "A Second Look at the Usability of Click-based Graphical Passwords", ACM SOUPS, **(2007)**.

[6] L. F. Cranor and S. Garfinkel, "Security and Usability", O'Reilly Media, **(2005)**.

[7] R. N. Shepard, "Recognition memory for words, sentences, and pictures", Journal of Verbal Learning and Verbal Behavior, vol. 6, **(1967)**, pp. 156-163.

[8] A. Perrig and D. Song, "Hash Visualization: A New Technique to Improve Real-World Security", in Proceedings of the 1999 International Workshop on Cryptographic Techniques and E-Commerce, **(1999)**.

[9] D. Weinshall and S. Kirkpatrick, "Passwords You'll Never Forget, but Can't Recall", in Proceedings of Conference on Human Factors in Computing Systems (CHI). Vienna, Austria: ACM, **(2004)**, pp. 1399-1402.