Authentication for Session Password using Colour and Images

Jay Patel, Student, SNJB's COE Chandwad
Sagar Padol, Student, SNJB's COE Chandwad
Bhushan Kankariya, Student, SNJB's COE Chandwad
Kainjan Kotecha, Associate Professor, SNJB's COE Chandwad

ABSTRACT

Authentication is the first step in information security.It requires the user to memorize their password and remember at login time.textual passwords are the most traditional schemes that are used for providing security, but textual passwords are vulnerable to dictionary attacks, shouldersurfing. Graphical password schemes overcomed the shortcomings of textual passwords,but they were vulnerable to shoulder surfing attacks.to solve and overcome this problem,text and images are combined to generate passwords for providing higher security for password.A new technique called session password is introduced on the combination of text and images to solve the problem of security.Session password can be used everytime the password is created for authentication.Two techniques are used to generate session password which overcomes the attacks like shoulder surfing,dictionary attacks.

Keywords: Authentication, Security, Shoulder Surfing, Dictionary attacks.

I. INTRODUCTON

Recently there has been a great emphasis to provide more security for passwords.The 21st century is the more advancing age of internet and related contents, highly exposing data which innovated before a minute or say as to some seconds.The most traditional method for authentication is textual Password.Users first choice for authentication is textual passwords. Mostly users chooseshort and simple password so that they can be easily memorised and can be recalled at the login-time.In common it has been surveyed that an average users has to memoriseatleast 3 passwords.again in addition to this the user has to remember password for banking, e-commerce, social networking sites and also email accounts. Short and simple textual passwords are easy to remember, but can be easily hacked while random and lengthy passwords are secured but hard to remember.to overcome this problem graphical authentication schemes were proposed. But this schemes had many problem like they were easily prone to shoulder surfing attacks. Many others authentication schemes were proposed to overcome the shoulder surfing attacks but they had many drawbacks like they take more time to login,usability.In this paper there are two authentication schemes that are designed to provide more security than that of textual passwords and graphical passwords.The user is authenticated using session password.Session password are the password that is provided to authenticate the user for a session.Session passwords are used only once.Everytime the users enters a session he has to input different password.once the session is over that password becomes is of no use for next session and the current session gets terminated.Session password provide more security as everytime the session start a new password is created and they are not prone to dictionary attacks ,brute force attacks and shoulder surfing attacks.This paper is organized into four sections. The previous section covers the Introduction. Next section describes literature review & findings. Section III describes the details of the proposed scheme. Security analysis is included in Section IV.

II. LITERATURE SURVEY

Various comprehensive investigations on the existing authentication schemes have been accomplished. And it has been discerned that none of the recent authentication schemes can resist all sorts of attacks. With this outcome, this paper proposes an authentication schemes which overcomes all the existing authentication schemes. Literature review reveals all the studies that are done in past. Some of the authentication schemes are discussed as follows:

A. Dhamija and Perrig[1]

Proposed a graphical authentication scheme in which the user identifies the pre-defined images to prove the authentication of the user. In this scheme, during registration the user selects a set of images from a predefined set of images. Later on at the login time the user has to select the images that he had selected during the registration time to prove his authentication.
But this system is vulnerable to shoulder-surfing.

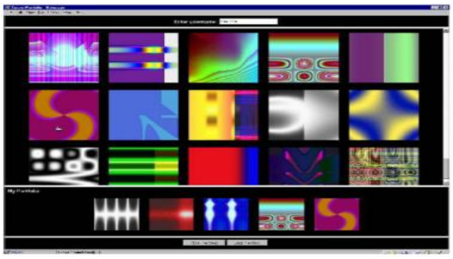


Fig. 1 Random images used by Dhamija and Perrig.

B. *Passfaces :*

Later on a new schemes was introduced known as Passfaces[2].In this scheme there is a grid of nine faces and the user to select on image from the grid.the user chooses four images of human as their password and have to select their pass image from the other eight images.since there are four user select images it is done four times.But this schemes was very easy to attacks by guessing or trying for number of time.

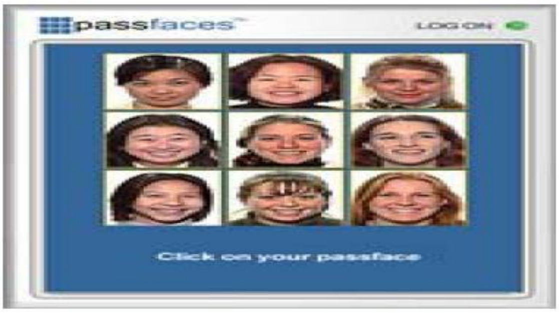
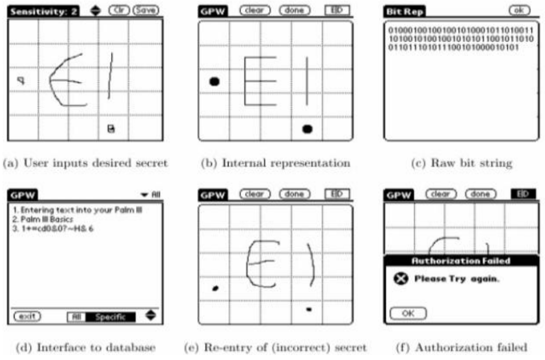


Fig. 2 Example of Passfaces

Futher studies were made on authentication schemes and a new scheme was proposed known as "Draw-a-Secret"(DAS) by Jermyn, et al. [3].The user has to draw a picture on the grid at the time of registration. The user has to draw the same picture on a 2D grid at the time of login. If the drawing of picture touches the same grid in same sequens.the users gets authenticated. But this scheme was prone to shoulder surfing attacks.

C. Draw –A-Secret

Similar to this a same scheme was introduced by Syukri [4].This authentication scheme was based on the principle that the user has to draw his signature by using mouse. This scheme had two stages of implementation viz.the registration phase and the verification phase. At the time of registration the user draws a signature that is extrated by the system.At the time od registration the signature is taken as an input and normalozation is done and then the parameters are extracted and cheking is done and the user is authenticated if the parameters gets matched.But drawing with mouse is not so easy and acutals parameters cannot be matched with the signature that was drawn at the registration time.this schemes is prone to forgery of signature.



(a) User inputs desired secret

(b) Internal representation

010001001001001010001011010011
101001010010010101011001011010
01101110101110010100001010 1

(c) Raw bit string

1. Entering text into your Palm III
2. Palm III Basics
3. 1+=cd0&07~H& 6

(d) Interface to database

(e) Re-entry of (incorrect) secret

Please Try again.

(f) Authorization failed

Fig. 4 DAS technique by Jermyn

D. Story-Scheme

To overcome this shoulder surfing attacks a scheme was proposed by Haichang et al [7].This schemes is the combination of DAS and Story schemes. The user has to draw a curve along the images to prove their authenticity.

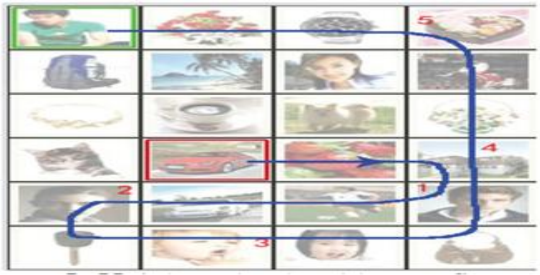


Fig. 4 Haichang's shoulder-surfing technique

E. I) Graphical Passwords.

To overcome shoulder surfing attacks a new graphical password scheme was introduced byWiedenback et al [8].the user has to recognise the pass objects and click in the convex hull formed of the pass objects. If the password had to be made large then it becomes crowded.

II) Graphical Passwords.

A new Graphical scheme was introduced by Jansen [9,10].This scheme had two phases one that is creation and the other is authentication.in the creation phase the user selects a theme that consist photos in a thumbnail size and a set of sequence of pictures as password. And then at the authentication phase the user has to recognise the images incorrect order. Each thumbnail is assigned a numeric value .Based on the thumbnails a numeric password is created. But the limit size of this password is 30.Hence Short password is created.

III PROPOSED SYSTEM

General

First it will be checked that the user is already registerd or not. If yes, then it will go for the step of login, but if user is not registered then first he will go through registration and then to the login step. Then at the time of transaction the color pairs and grid will be shown and from that the user will enter the session password. This password will be verified at the verification phase. If the user wants another session then a new session will be generated and the grid and color pair will be shown to the user again.

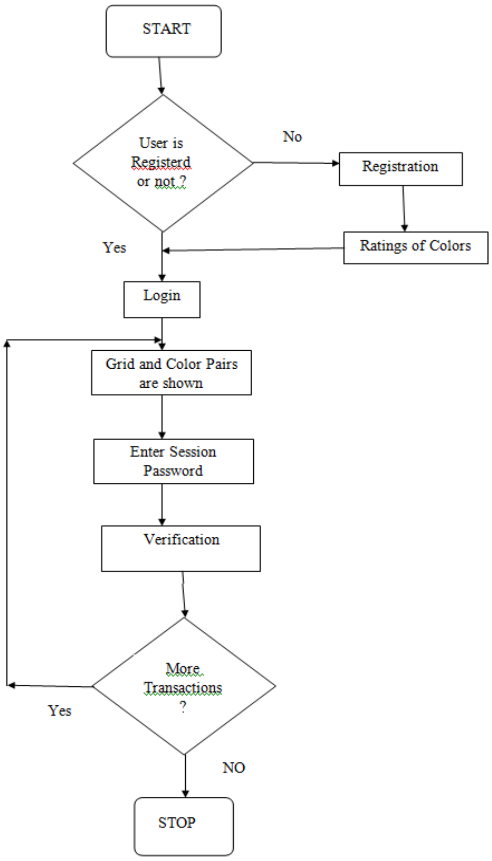
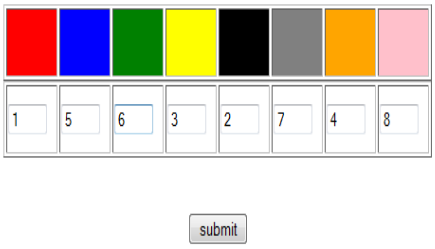


Fig. 5Working of Proposed system

Hybrid Textual Authentication Scheme

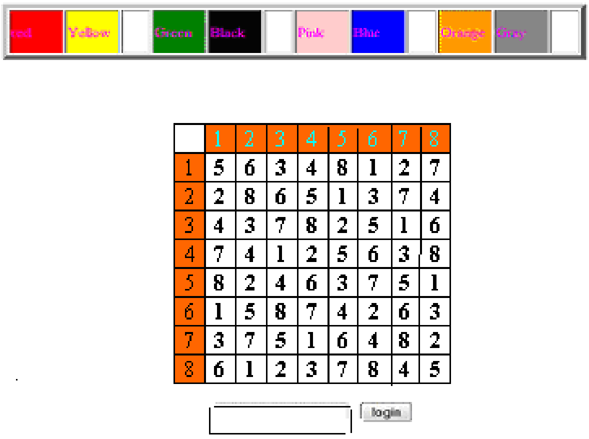
a) During registration, user should rate colors as shown in figure 6. The User should rate colors from 1 to 8 and he can remember it as “RLYOBGIP”. Same rating can be given to different colors.



🟥	🟦	🟩	🟨	⬛	▨	🟧	▨
1	5	6	3	2	7	4	8

Figure 6 : Rating of colors by the user

b) During the login phase, when the user enters his username an interface is displayed based on the colors selected by the user. The login interface consists of grid of size 8×8. This grid contains digits 1-8 placed randomly in grid cells. The interface also contains strips of colors as shown in figure 7.. The color grid consists of 4 pairs of colors. Each pair of color represents the row and the column of the grid.



	1	2	3	4	5	6	7	8
1	5	6	3	4	8	1	2	7
2	2	8	6	5	1	3	7	4
3	4	3	7	8	2	5	1	6
4	7	4	1	2	5	6	3	8
5	8	2	4	6	3	7	5	1
6	1	5	8	7	4	2	6	3
7	3	7	5	1	6	4	8	2
8	6	1	2	3	7	8	4	5

Figure 7: Login interface

Figure 7 shows the login interface having the color grid and number grid of 8 x 8 havingnumbers 1 to 8 randomly placed in the grid. Depending on the ratings given to colors, we getthe session password. As discussed above, the first color of every pair in color grid representsrow and second represents column of the number grid. The number in the intersection of therow and column of the grid is part of the session password. Consider the figure 9 ratings andfigure 10 login interface for demonstration. The first pair has red and yellow colors. The redcolor rating is 1 and yellow color rating is 3. So the first letter of session password is 1st rowand 3rd column intersecting element i.e **3**. The same method is followed for other pairs ofcolors. For figure 10 the password is “ **3573**”. Instead of digits, alphabets can be used. Forevery login, both the number grid and the color grid get randomizes so the session passwordchanges for every session.

IV SECURITY ANALYSIS

As the interface changes every time, the session password changes. This technique is resistant toshoulder surfing. Due to dynamic passwords, dictionary attack is not applicable. Hidden cameraattacks are not applicable to PDAs because it is difficult to capture the interface in the PDAs.

Dictionary Attack: [12]These are attacks directed towards textual passwords. Here in this attack,hacker uses the set of dictionary words and authenticate by trying one word after one. TheDictionary attacks fails towards our authentication systems because session passwords are usedfor every login.

Shoulder Surfing:[13] These techniques are Shoulder Surfing Resistant. In Pair based scheme,resistance is provided by the fact that secret pass created during registration phase remainshidden so the session password can’t be enough to find secret pass in one session. In hybridtextual scheme, the randomized colors hide the password. In this scheme, the ratings decide thesession password. But with session password you can’t find the ratings of colors. Even byknowing session password, the complexity is 84 .So these are resistant to shoulder surfing .

Guessing:[11] Guessing can’t be a threat to the pair based because it is hard to guess secret pass and it is 364.The hybrid textual scheme is dependent on user selection of the colors and the ratings. If the general order is followed for the colors by the user , then there is a possibility of breaking the system.

Brute force attack:[12] These techniques are particularly resistant to brute force due to use of thesession passwords. The use of these will take out the traditional brute force attack out of thepossibility.

Complexity : The Complexity for Pair-Based Authentication Scheme is to be carried over thesecret pass. For a secret pass of length 8, the complexity is 368. In the case of the HybridTextual Authentication Scheme the complexity depends on colors and ratings. The complexityis 8! if ratings are unique ,otherwise it is 8.

V MATHEMATICAL MODEL

The system M is mathematically represented as follows :

$M = \{\sum, \delta, O, T\}$

Where $\sum = \{C_1, C_2, C_3, C_4, C_5, C_6, C_7, C_8\}$

C_1 = Red, C_2 = Blue, C_3 = Green, C_4 = Yellow, C_5 = Black, C_6 = Grey, C_7 = Brown,

C_8 = Pink

$(CR_i)_{i=1 \text{ to } 8} = \delta\{C_j \mid 1 \le j \le 8 \text{ and } 1 \le i \le 8\}$

;where CR_i = Color rating of color C_j

O = {Display message “Registration successful”, Entry to “Authenticated area”, Display message “Password incorrect”, Display message “Contact developer”}

T = {CP,G}
;Where CP = Color Pair
G = Grid

$G = \{\sum_{i=1}^{8}\sum_{j=1}^{8} x(i, j)\}$

;where G = Matrix Array of 8 × 8
x = values among Color Ratings

$CP = \{CP_1, CP_2, CP_3, CP_4\}$
; where CP_1 = Color Pair 1
CP_2 = Color Pair 2
CP_3 = Color Pair 3
CP_4 = Color Pair 4

$CP_i = x , y$
; where x,y can be colors from $C_1, C_2, C_3, C_4, C_5, C_6, C_7, C_8$

$G = \{\text{rand}(i, j) \mid 0 < i < 9 \text{ and } 0 < j < 9\}$
; where G = Grid

$P2 = \{G(i, j) \mid \text{where } i = CR(CP_{i1}), j = CR(CP_{i2})\}$
;where P2 = New password
CR = Color Ratings of Color from Color Pair CP_i

TABLE I

COMPARISONS OF VARIOUS AUTHENTICATION SCHEM

Authentication schemes	**Textual passwords**	**Graphical passwords**	**Token based passwords**	**Biometric passwords**
Usability	very high	High	Less	very less
Implementation	Easy	Complicated	more complicated	highly complicated
Attacks	Bruteforce, dictionary, guessing	shoulder surfing, guessing	Forgery	Forgery
Password space	quite less	Less	no matter	no matter
Cost of attacks	Low	Moderate	High	Very High
Time to login	Low	Moderate	Moderate	High
Flexibility	Moderate	High	Low	very low
Recovery	Easy	Easy	Hard	Difficult
Class	what user remember	what user remember/ recognize	what user possess	what user is
Sharing of password	very easy	Easy	Hard	very difficult
Hardware	not required	not required	Required	Required
Features	easy to remember : easy to guess, hard to remember :hard to guess	easy to remember: hard to guess	maintaining tokens	maintain same physical properties
Varies acc. to time	No	No	No	Yes

VI CONCLUSION

These techniques generate session passwords and are resistant to dictionary attack, brute forceattack and shoulder-surfing. This technique use grid for session passwords generation.For hybrid textual scheme, ratings should be given to colors, based on these ratings and the grid displayed during login, session passwords are generated. However this scheme is completely new to the users and the proposedauthenticationtechniques should be verified extensive.

References

[1] R. Dhamija, and A. Perrig. “Déjà Vu: A User Study Using Images for Authentication”. In 9th USENIX Security Symposium, 2000.

[2] Real User Corporation: Passfaces. www.passfaces.com

[3] 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.

[4] A. F. Syukri, E. Okamoto, and M. Mambo, "A User Identification System Using Signature Written with Mouse," in *Third Australasian Conference on Information Security and Privacy (ACISP)*: Springer-Verlag Lecture Notes in Computer Science (1438), 1998, pp. 403-441.

[5] G. E. Blonder, "Graphical passwords," in *Lucent Technologies, Inc., Murray Hill, NJ*, U. S. Patent, Ed. United States, 1996.

[6] Passlogix, site http://www.passlogix.com.

[7] HaichangGao, ZhongjieRen, Xiuling Chang, Xiyang Liu UweAickelin, “A New Graphical Password Scheme Resistant to Shoulder-Surfing

[8] S. Wiedenbeck, J. Waters, J.C. Birget, A. Brodskiy, N. Memon, “Design and longitudinal evaluation of a graphical password system”. International J. of Human-Computer Studies 63 (2005) 102-127. [9] W. Jansen, "Authenticating Mobile Device User through Image Selection," in *Data Security*, 2004.

[10] W. Jansen, "Authenticating Users on Handheld Devices “in *Proceedings of Canadian Information Technology Security Symposium*, 2003.

[11] 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.

[12] J. Goldberg, J. Hagman, V. Sazawal, "Doodling Our Way To Better Authentication", CHI '02 extended abstracts on Human Factors in Computer Systems, 2002.

[13] H. Zhao and X. Li, "S3PAS: A Scalable Shoulder-Surfing Resistant Textual-Graphical Password Authentication Scheme," in *21st International Conference on Advanced Information Networking and Applications Workshops (AINAW 07)*, vol. 2. Canada, 2007, pp. 467-472.

[14] S. Man, D. Hong, and M. Mathews, "A shoulder surfing resistant graphical password scheme," in *Proceedings of International conference on security and management*. Las Vegas, NV, 2003.

[15] X. Suo, Y. Zhu and G. Owen, “Graphical Passwords: A Survey”. In Proc. ACSAC'05.

[16] Z. Zheng, X. Liu, L. Yin, Z. Liu “A Hybrid password authentication scheme based on shape and text” Journal of Computers, vol.5, no.5 May 2010