A SHOULDER SURFING RESISTANT IMAGE AUGMENTED MULTI PASSWORD AUTHENTICATION SYSTEM WITH KEY STORE TIME LOG IN & COORDINATION COMPARISON

Amit Kumar[1], Amit Sharma[2], Laxmi Narayan Balai[3]

[1]*M. Tech. Scholar (ECE), Yagyavalkya Institute of Technology, Jaipur, India*
[2]*Assistant Professor (ECE), Yagyavalkya Institute of Technology, Jaipur, India*
[3]*H.O.D (ECE), Yagyavalkya Institute of Technology, Jaipur, India*

Abstract - *In this work we propose a unique system to provide a text password based authentication that is shoulder surfacing resistant. We propose a multi password scheme, where each password is associated to a particular image & the system randomly selects the image at login & the user has to enter the associated password with that image. To make the matters worse for shoulder surfer, the time difference between keystrokes is recorded while password creation & its correlation is compared to the user input key stroke timing using 2-D correlation matching, if the user is not entering password with the same rhythm as done in password creation, these correlation value will drop than a predefined threshold, login will be denied & the user will be prevented the new image. The idea of key storage time correlation matching & requirement of new password associated with new image totally complicates the matters for shoulder surfer. After a predefined log-in attempts, the system sends a warning e-mail & allow for back up password entry, which user is trained to enter covering the keypad thus completing last discuss for shoulder surfacing attack.*

Key words: Shoulder Surfing, Graphical Password, Authentication System, Randomized Image, Augmented Password, Key Logging

1. INTRODUCTION

Graphical password schemes have been proposed as a possible alternative to text-based schemes, the psychological studies which supports the fact that humans can remember pictures better than text. Pictures are generally easier to be remembered or recognized than text. Input devices such as mouse, stylus and touch screen that permit make the appearance of graphical user technique possible. Graphical passwords are applied to workstations, web log-in applications, TM machines and mobile devices. Shoulder surfing refers to using direct observation techniques, such as looking over someone's shoulder, to get information. Shoulder surfing is effective in public places because standing near someone and watch them entering a PIN number at ATM machine is nearly very easy. This attack is also possible at long distance using binoculars or vision enhancing devices like miniature closed circuit cameras which can be concealed in ceilings, walls or fixtures to observe data entry. The users have been more prone to password thefts because of such kind of sneaking. To prevent shoulder surfing attack it is advised to shield paperwork or the keypad from view by using one's body or cupping ones hand.

Graphical passwords are introduced as alternative techniques to textual passwords. Most of the graphical schemes are vulnerable to shoulder surfing. The main intention of this project is Data Security using the Text-based Graphical pass-word Sachems using color Combination for E-mail system. It secures users data from shoulder surfing attack. Since conventional password schemes are vulnerable to shoulder surfing, many shoulder surfing resistant graphical password schemes have been proposed. However, as most users are more familiar with textual passwords instead of pure graphical password. Unfortunately, none of existing text-based shoulder surfing resistant graphical password schemes is both secure and efficient enough. In this paper, we propose an improved text-based shoulder surfing resistant graphical password scheme by using colors for Data Security. Access to computer systems is most often based on the use of alphanumeric passwords. However, users have interested on graphical password, therefore we have been proposed text based graphical password scheme for application. In this project we have to use the Authentication purpose password Sachems using the Texts Based Graphical password for the data security.

1.1 Types of Authentication System

The most frequent types of authentication available in use for authenticating online users differ in the level of security provided by combining factors from the one or more of the four categories of factors for authentication:

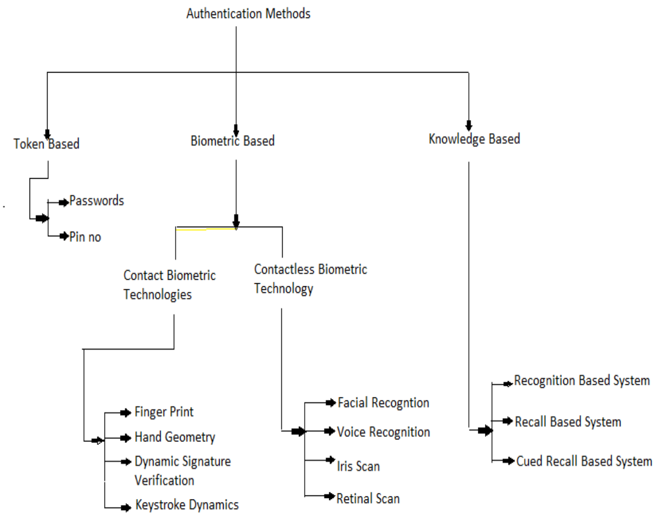


Fig.1: Classification of Authentication Methods

1.2 Token Based Authentication

Many token-based authentication systems use knowledge based techniques to enhance security. For example, ATM cards are generally used together with a PIN number. Token based techniques, such as key cards, bank cards and smart cards are widely used.

The general concept behind a token-based authentication system is simple. Allow users to enter their user name and password in order to obtain a token which allows them to fetch a specific resource without using their user name and password. Once their token has been obtained, the user can offer the token which offers access to a specific resource for a time period to the remote site. Method of Loci. It also uses recall based technique. IBA is based on a user's successful identification of his image password set. After the user name is sent to the authentication module, it responds by displaying an image set, which consists of images from the user's password set mixed with other images. The user is authenticated by correctly identifying the password images. The human brain is more adept in recalling a previously seen image than a previously seen text.

1.3 Knowledge Based Authentication

The knowledge based authentication is the most commonly used authentication systems. They are two types: Text based password and picture based passwords. Although there are different type of authentication techniques available alphanumeric passwords are the widely used because they are versatile and it is easy to implemented use. The text based passwords need to satisfy two contradictory requirements. That is it should be easily remembered by user and it should be hard to guess by an attacker. So these text passwords are vulnerable to dictionary attacks brute force attacks.

1.4 Biometric Based Authentication

Biometric authentication system uses physiological or behavioral characteristics of a person for authentication. It is based on "Something You Are". Some of the biometric authentication systems use. Password or pass phrase. It is an authentication scheme in which the user is asked to answer at least one "secret" question (Knowledge 2011). KBA is often used as a component in multifactor authentication (MFA) and for self-service password retrieval and offers several advantages to traditional (conventional) forms of e-authentication like passwords, PKI and biometrics (Kba 2011).

1.5 Objective of Thesis

1. Design & Development of a Shoulder Surfing Prevention algorithm using hybrid multi domain techniques.

2. Implementation of touch characteristics sensing to sense touch type, touch duration, etc to determine user touch pattern to prevent password cracking.

3. Use of intuitive visual based curing techniques to the user to input multi password, multi rotation password that user has provided.

4. Implementation of Eye Gaze detection, & store detection while password entering to corroborate User behavior.

5. Use of key speed mapping logging technique to learn user input patterns, & authenticate user accordingly.

6. Development of a Graphical Scene/ Image based Interactive password system for shoulder surfing prevention.

7. Integration of our hybrid shoulder surfing algorithm with existing biometric technology such as

Face/finger print etc, in event of doubtful entry, to save authentic user from accesses denial, save time &be a deterrent to password crackers

2. LITERATURE REVIEW

Users may have various login ids that will be hard to remember. Graphical passwords are easier to remember than alphanumeric passwords. Some threats of Internet security are spyware and shoulder-surfing attacks. The purpose of the current paper is to offer a graphical password against spyware largely and shoulder-surfing attacks. In this scheme assuming that adversaries know which key is struck, need several login phases to understand images accordance with the character, which is time consuming and costly. Therefore, the scheme is resistant to spyware largely. Shoulder-surfing attacks include mouse clicks, touch screens or stylus pens. Using keyboard is more secure than mouse. The proposed scheme in this paper is secure against shoulder surfing attack because it is not clicked or touched directly on Images and is used keyboard. To avoid the guess ability, observation and record ability, we showed 50 images of 70 images in registration phase and also chose images that are hard to describe and colorful and do not have especial color. Also we used asterisk star that prevent password from being seen. The proposed scheme is practical and we plan to extend our work and concentrate on how to reduce overall total number of images.

3. METHODOLOGY

Today's various accounts holder is suffering from various type of attacks so, we have proposed a system that start from creation of password and display parameter and password entry authentication.

We can classify its operations into three categories.

The existing system is a graphical password authentication system. It is a combination of Recognition and Recall based approach. The user authentication is verified in two steps.

1. A user creates his profile by entering personal details and user name.

2. Then the P set of pool of images from local database are presented to the user. These images are common to all the users. The user has to select an images to set as a password cue & later enter the password.. The user can repeat any image. This process is repeated until N number of Image-Password Pairs is recorded as Main Password(s).

3. After this, again the same P set of pool of images from local database are presented to the user. The user has to select images to set as a password cue & later enter the password. This process is repeated until M number of Image-Password Pairs is recorded as Auxiliary Password.

4. As, the password has been setup, for the user, the user can now login the system by authenticating himself.

5. For authentication, the user is presented a random image from the N image – password, pairs selected by him, to cue him, and the user has to enter the password associated with that image, if the password entered is correct, its keyboard key logging time is compared to previously recorded time while password creation, if the threshold of correlation is above a particular value, say 70%, access is granted.

6. In case of wrong entry or mismatch of time correlation, the user is denied access, and is again presented with a random image from N image-password pool, and is again required to enter the password associated to the image displayed. This process can be repeated till allowed number of login attempts K, say 3, gets exhausted.

7. If the user is not able to login, in predefined number of login attempts, the system goes into secure mode & send an warning E-Mail to the user of "Unauthorized Access Attempt", and presents the user with a random image from M image-password pool of auxiliary or backup passwords.

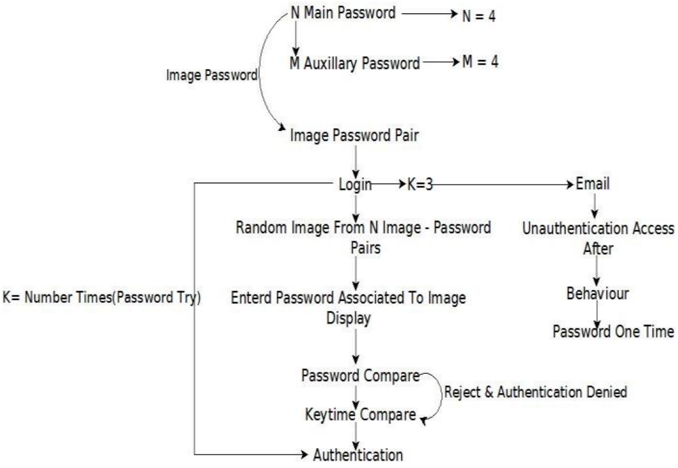
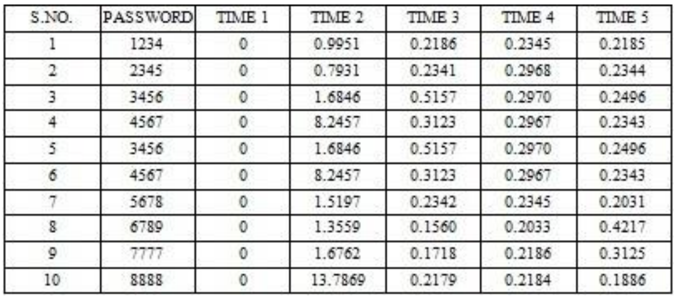

N Main Password
N = 4
M Auxillary Password
M = 4
Image Password
Image Password Pair
Login
K=3
Email
Random Image From N Image - Password Pairs
Unauthentication Access After
K= Number Times(Password Try)
Enterd Password Associated To Image Display
Behaviour
Password One Time
Password Compare
Reject & Authentication Denied
Keytime Compare
Authentication

Fig 2.1 Password Entry of Authentication System

3. RESULTS

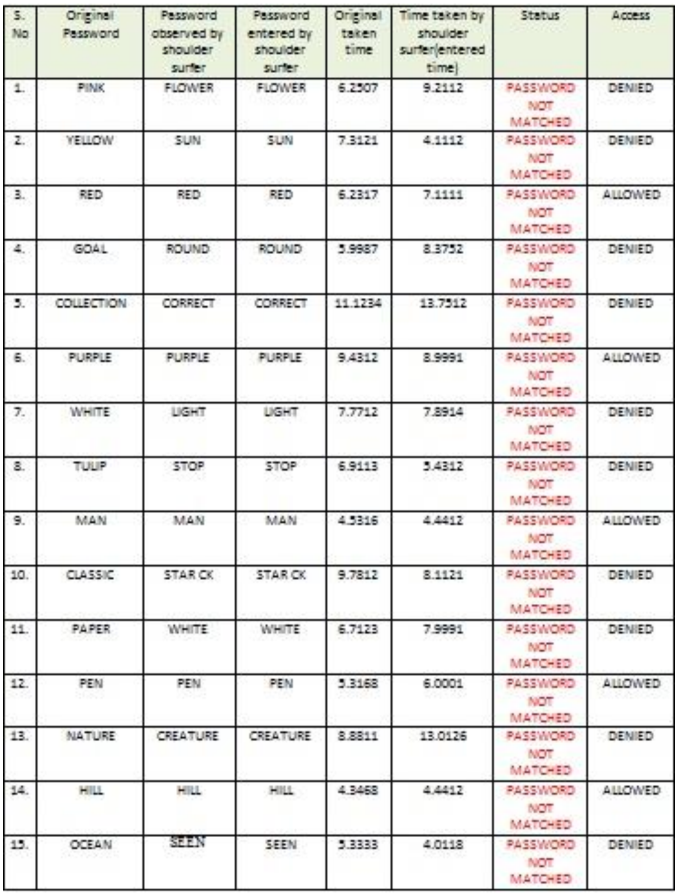
Program Start up, Operation Menus & Password Creation

This topic, depicts the, process of software startup, its loading, the menu's provided to the user for operation of the system. Process of screenshot, is used to depict the operation of entire software, with authenticity. Tables & Graphs have been provided as and where required. Both positive & negative test cases have been evaluated



S.NO.	PASSWORD	TIME 1	TIME 2	TIME 3	TIME 4	TIME 5
1	1234	0	0.9951	0.2186	0.2345	0.2185
2	2345	0	0.7931	0.2341	0.2968	0.2344
3	3456	0	1.6846	0.5157	0.2970	0.2496
4	4567	0	8.2457	0.3123	0.2967	0.2343
5	3456	0	1.6846	0.5157	0.2970	0.2496
6	4567	0	8.2457	0.3123	0.2967	0.2343
7	5678	0	1.5197	0.2342	0.2345	0.2031
8	6789	0	1.3559	0.1560	0.2033	0.4217
9	7777	0	1.6762	0.1718	0.2186	0.3125
10	8888	0	13.7869	0.2179	0.2184	0.1886

Table 1: Listing of Main Password & Aux Password Along With Key Logging Times



S. No	Original Password	Password observed by shoulder surfer	Password entered by shoulder surfer	Original taken time	Time taken by shoulder surfer(entered time)	Status	Access
1.	PINK	FLOWER	FLOWER	6.2507	9.2112	PASSWORD NOT MATCHED	DENIED
2.	YELLOW	SUN	SUN	7.3121	4.1112	PASSWORD NOT MATCHED	DENIED
3.	RED	RED	RED	6.2317	7.1111	PASSWORD NOT MATCHED	ALLOWED
4.	GOAL	ROUND	ROUND	5.9987	8.3752	PASSWORD NOT MATCHED	DENIED
5.	COLLECTION	CORRECT	CORRECT	11.1234	13.7512	PASSWORD NOT MATCHED	DENIED
6.	PURPLE	PURPLE	PURPLE	9.4312	8.9991	PASSWORD NOT MATCHED	ALLOWED
7.	WHITE	LIGHT	LIGHT	7.7712	7.8914	PASSWORD NOT MATCHED	DENIED
8.	TULIP	STOP	STOP	6.9113	5.4312	PASSWORD NOT MATCHED	DENIED
9.	MAN	MAN	MAN	4.5316	4.4412	PASSWORD NOT MATCHED	ALLOWED
10.	CLASSIC	STAR CK	STAR CK	9.7812	8.1121	PASSWORD NOT MATCHED	DENIED
11.	PAPER	WHITE	WHITE	6.7123	7.9991	PASSWORD NOT MATCHED	DENIED
12.	PEN	PEN	PEN	5.3168	6.0001	PASSWORD NOT MATCHED	ALLOWED
13.	NATURE	CREATURE	CREATURE	8.8811	13.0126	PASSWORD NOT MATCHED	DENIED
14.	HILL	HILL	HILL	4.3468	4.4412	PASSWORD NOT MATCHED	ALLOWED
15.	OCEAN	SEEN	SEEN	5.3333	4.0118	PASSWORD NOT MATCHED	DENIED

Table 2: Shoulder surfing time by surfer and status and access

4. CONCLUSION

In this work, we have proposed on random image augmented text password authentication system. That is highly resistant to shoulder surfing attacks. As the textual password randomly, this makes shoulder surfing difficult. Also keystroke time logging & comparison, makes attacks such as shoulder surfing, brute force & dictionary attacks highly improbable. Our system combines the best of the two prominent techniques namely text based password(s) & image based password(s), as text password are hard to memorize, & short password are vulnerable to various attack. Also image based passwords are very easy to remember, but are highly susceptible to attack such as shoulder surfing. Here, in this system, we have combined the desirable characteristics of the two schemes such as high memorability of the image related data, & better security of textual password for shoulder surfing attacks, to create a highly resistant authentication system. As image is only used for cueing the user for enter a specific text password & the text password(s) are randomly warranted, out of a pool on N password - image pairs

5. FUTURE SCOPE

Our system is a combination of recognition and recall based approach. It is more usable and secure as compare to previous graphical password authentication systems. As password space is very large it provides the security against brute force attack. It is easy to use. Passwords can be created and memorized easily. Randomization in both the authentication steps provides strong security against shoulder surfing. Overall our system is resistant to all other possible attacks also. This system can be used for highly secure systems. In future, one more addition possible to our system is, if the user forgets any password that password is mailed to user's registered mail id and such a message will be sent to user's registered mobile number also. So user can get the system updates although he is offline. Thus, in future, our system can be made more secure and easy to access.

6. REFERNCES

[1] A graphical password against spyware and shoulder-surfing attacks elham darbanian, gh. dastghaiby fard, 2015 ieee

[2] Secure graphical password authentication system
rajguru dipali, j walunj jyoti, jadhav jayashree , handereshma 4 computer engineering, sgoi coe, maharastra, india vol-2 issue-2 2016 ijariie

[3] Text based shoulder surfing resistant using graphical password (captcha) navina bokariya, pooja gawali, snehal magar, prof. kothari s.b. student, dept. of computer, g.h. raisoni college of engineering ahmednagar, maharashtra, india ijircce.2016

[4] Advance text and color based session password security resistant to shoulder surfing, key logger and mouse tracker spyware ms. kiran p.lokhande, prof.sonal honale pg scholar, aabha gaikwad patil college of engineering, mohagaon, nagpur, (india) assistant professor, dept of cse, aabha gaikwad patil college of engineering,mohagaon, nagpur, (india) 2015 ijarse, vol. no.4,

[5] A simple text based graphical password scheme to overcome shoulder surfing attacks monali bendale, neeta singh, sujata baid , aman maurya be (comp), department of computer engineering, ssbt's coet bambhori, jalgaon (m.s.), india international journal of advanced research in computer and communication engineering vol. 4, issue 3, 2015

[6] Textual graphical password scheme against shoulder surfing attack international journal of engineering and computer science issn:2319-7242 volume 4 issue 3 march 2015, page no. 10988-10991 saurabh saoji, swapnali bhadale, harshada wagh. professor computer engineering, savitribai phule pune university/isb&m school of technology.

[7] Shoulder surfing resistance using graphical password authentication in atm systems pooja k s, prajna venkatramana dhooli, prathvi, prof. ashwini n department of ise, bms institute of technology & mgmt., bengaluru, karanataka volume 6, issue 1, january - june (2015), pp. 01-10 © iaeme: http://www.iaeme.com/ijitmis.asp

[8] Shoulder surfing resistant graphical password kruthi k, kumuda b g, nandhini n v, mrs. r.anitha (associate professor) department of computer science and engineering, the national institute of engineering, autonomous under vtu mysore – 570008, karnataka, india international journal of modern trends in engineering and research (ijmter) volume 02, issue 06, [june – 2015] issn (online):2349–9745; issn (print):2393-8161

[9] A comprehensive survey on graphical passwords and shoulder surfing resistant technique analysis j. thirupathi associate professor, dept of computer science and engineering. ijiset - international journal of innovative science, engineering & technology, vol. 2 issue 4, april 2015. www.ijiset.com issn 2348 – 7968

[10] A simple text-based shoulder surfing resistant graphical password scheme international journal of advance foundation and research in computer (ijafrc) volume 2, special issue (ncrtit 2015), january 2015. issn 2348 – 4853 811 | © 2015, ijafrc and ncrtit-2015 all rights reserved www.ijafrc.org. nikam archana, bhujbal tejshri, warpe santosh. Department of computer engineering, mitaoe, alandi(d),pune-412 105

[11] Shoulder surfing resistant text-based graphical password scheme sumit h. wagh student me (computer) ytcem, bhivpuri road, karjat, mumbai aarti g. ambekar assistant professor d.j.sanghavi college of engg mumbai international journal of computer applications (0975 – 8887) international conference on computer technology (icct 2015) 17

[12] Defending shoulder surfing attacks in secure transactions using session key method m. r.divya, a.p.janani, international journal of science, engineering and technology research (ijsetr), volume 4, issue 2, february 2015

[13] Locker based graphical password authentication for data security uday gobbur, dr. suhas raut computer science and engineering, nk orchid college of engineering & technology, solapur,maharashtra, india 2015 (ijsetr)

[14] Graphical and pair based scheme for authentication using session password International journal of advance foundation and research in science & engineering (ijafrse) Volume 1, special issue, march 2015. impact factor: 1.036, science central value: 26.541 | © 2015, ijafrse and jcon 2015 all rights reserved www.ijafrse.org 1a.a.doke, 2d.b.wagh, 3s.h.shaikh, prof. s.s.gawali department of computer engg, jaihind college of engg, kuran savitribai phule pune university,pune,india,ashvinidoke41@gmail.com, dhanuwagh92@gmail.com, saddamshaikh1605@gmail.com

[15]Research article a graphical password based authentication based system for mobile devicesijcsmc, vol. 3, issue. 4, april 2014, pg.744 – 754 er.aman kumar1, er.naveen bilandi 21 department of computer science and engineering, dav university, jalandhar, punjab, india