ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2014

Authentication Using Images and Pattern

Mr. R. B. Sangore[1], Gaurav Patil[2], Sagar Ramani[3], Sunil Pasare[4]

Assistant professor, Dept. of Information Technology, SSBT College of Engineering, Jalgaon, Maharashtra, India [1]

BE Students, Dept. of Information Technology, SSBT College of Engineering, Jalgaon, Maharashtra, India [2, 3, 4]

ABSTRACT: Secrete code (password) provides the sanctuary mechanism for substantiation and protects user data or unauthorized access of information. Graphical password base hybrid authentication system is a new password scheme. New scheme is alternative to textual password. In that password is created from images and text password. Existing password scheme is easy but the problem in that when user give the small password then it is easy to guess through different attack i.e. dictionary attack and brute force attack. If the text password length is greater, then it is hard to remember and user can write our password in page or in computer file. If the page is damage or that computer file is corrupted then password is loss. Existing system consist only images for password or draw a secret pattern for password, but there was problem of shoulder surfing. Any person is easily seeing the other person password and accesses his secret information. New method of secret code is image password. Individual can easily remember picture as compare to alphanumeric secrete code. In this paper we have proposed a new image password scheme, in that user can give password in combination of images and secrete pattern. The system is a combination of recognition base technique and secrete code (alphanumeric) password, recall base technique and secrete code (alphanumeric) password or recognition base technique and recall base technique. Our system removes the problem of mouse logger and shoulder surfing problem in greater extent. Graphical password is use in PC, smart hand held device, ATM machine.

Keywords: brute force attack, dictionary, image password, fusion, sanctuary, secrete code, shoulders surfing, substantiation.

I.INTRODUCTION

Security provides the very important role in our daily life. Security is in the form of physical security, information security and our national border. In order to that computer system and the information associated to computer system should also be protected. Computer system considers the human factors such as ease of use, ease to remember etc [1]. Most of the computer system protected using the textual password and another is biometrics in some system [5]. But most common is textual password. The way to provide the security to computer system or our important data is first, give the username and second, give the text password. Some program user use the encryption technique for storing password in database for security purpose. The problem in that process is if the user gives the weak password then it is easily identify through different type of attack like dictionary attack and brute force attack. When we give strong password i.e. more combination of characters, symbols and numbers then our password is strong but hard to remember. This type of password is also useful in web application. The new type of password is graphical password. It is alternative to text password. The idea of graphical password was originally described by Greg Blonder in 1996 (Blonder 1995) [1]. Graphical password is easy to remember as compare to text password because human brain process picture better than the text. Human brain process the picture easily i.e. faces of people, place they visit and also process things they seen for the long duration [3]. Hence graphical password provides the means of for making more user-friendly passwords and making more security.

Graphical password is more strong than the text password but the disadvantages of GP is it suffers from shoulder surfing [2] [4]. Shoulder surfing is one of the drawback of GP because some people are stand around to the user, which give the graphical password then this people capture this session and identify the password of user. This way of observing password any can access the account of user which is not authorized person.

Literature Survey

Partha Pratim Ray et al. [1] implemented the Ray's Scheme: Graphical Password Based Hybrid Authentication System for Smart Hand Held Devices this scheme is proposed for smart hand held devices (like smart phones i.e. PDAs, ipod, iphone, etc) which are more handy and convenient to use than traditional desktop computer systems.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2014

Suchita Sawla et al. [2] implemented the Graphical Password Authentication System in an Implicit Manner. It is a variation to the login/password scheme using graphical passwords used in an implicit manner. This Graphical Password Authentication System in an Implicit Manner is immune to the common attacks suffered by other authenticati+++on schemes.
Xiaoyuan Suo et al.[3] discussed on the topic Graphical Passwords: A Survey and conducted a brief study on comprehensive survey of the existing graphical password techniques .This topic will be useful for information security researchers and practitioners who are interested in finding an alternative to text-based authentication methods.
Sonia Chiasson et al.[4] carried a brief study on Graphical Password Authentication Using Cued Click Points i.e. proposed a new click-based graphical password scheme called Cued Click Points (CCP). It can be viewed as a combination of Pass Points, Pass faces, and Story. A password consists of one click-point per image
Khan w. z. et al. [16] proposed A Graphical Password Based System for Small Mobile Devices i.e. proposed a hybrid system which is a combination of recognition and recall based techniques. This graphical password removes the problem of shoulder surfing and many more problem regarding to graphical password.
Haichang Gao et al. [19] proposed the Graphical password scheme resistant to shoulder surfing i.e. proposed system work on draw a curve around the password images orderly rather than click.
Wells Jason et al. [18] discussed on the topic Enhanced Security for Preventing Man-in-the-Middle Attacks in Authentication. This scheme discussed on refinement of the image generation format, size and layout and facilities.
This scheme prevents the shoulder surfing attack.

Now a day's textual password use every where. But it is very easy to break through different type of attack like brute force, dictionary attack, key logger etc. so we can develop new system i.e. Authentication using images and pattern. In Graphical password three techniques are found. Current authentication methods can be divided into three main areas:

a. Token based authentication
b. Biometric based authentication
c. Knowledge based authentication

a. Token based techniques

Token based techniques, such as key cards, bank cards and smart cards are widely used. Many token-based authentication systems also use knowledge based techniques to enhance security. For example, ATM cards are generally used together with a PIN number [1] [4].

b. Biometric based authentication

Biometric based authentication techniques, such as fingerprints, iris scan, or facial recognition, are not yet widely adopted. The major drawback of this approach is that such systems can be expensive, and the identification process can be slow and often unreliable. However, this type of technique provides the highest level of security [1] [7].

c. Knowledge based authentication

Knowledge based techniques are the most widely used authentication techniques and include both text-based and picture-based passwords. The picture-based techniques can be further divided into two categories: recognition-based and recall-based graphical techniques. Using recognition-based techniques, a user is presented with a set of images and the user passes the authentication by recognizing and identifying the images he or she selected during the registration stage. Using recall-based techniques, a user is asked to reproduce something that he or she created or selected earlier during the registration stage [5] [11].

II.EXISTING SYSTEM

Graphical password first found in 1995 by Greg Blonder [1]. Graphical password has three types there are as follows: A. Recognition Base Technique B. Recall Base Technique C. Cued Recall Base Technique.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2014

A. Recognition Base Technique

Recognition base technique contain group of images. User can select images from that group for password. Figure 1 show the recognition base technique. Using recognition base technique user set our password at the time of registration and selects same images at the time of authentication [2] [5].

Fig. 1 Recognition Base Technique

B. Recall Base Technique

Using recall base technique user can draw a secrete pattern or generate a shape over the 2D grid at the time of registration and generate a same shape at the time of authentication. This 2D grid is provided by the system [5].

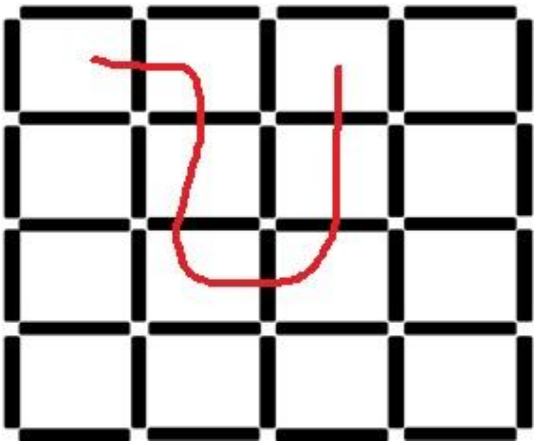

Fig. 2 Recall Base Technique

C. Cued Recall Base Technique

In this technique, system gives some hints which helps user to reproduce their password with high accuracy. These hints will be presented as hot spots within image. The user has chosen some of these regions to register their password. But this technique is not easy to use; because the click position is not on specific point then user cannot access his information [6] [8].

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2014

Fig. 3 Cued Recall Base Technique

The main disadvantage of above three technique is shoulder surfing. Other disadvantage of graphical password is mouse logger. Mouse logger is one of the major problems of graphical password.

III.PROPOSED SYSTEM

Our proposed system contains combination of two password schemes they are recall based technique and recognition base technique and text password. Hence our system is also called hybrid password system. Our password scheme provide the security in greater extend. Our password scheme removes the problem of shoulder surfing and mouse logger. In system, there are three phases first is, user information second is, username and text password and third is, graphical password. User fill two fields and then give graphical password from two schemes i.e. recall based technique or recognition base technique or both.

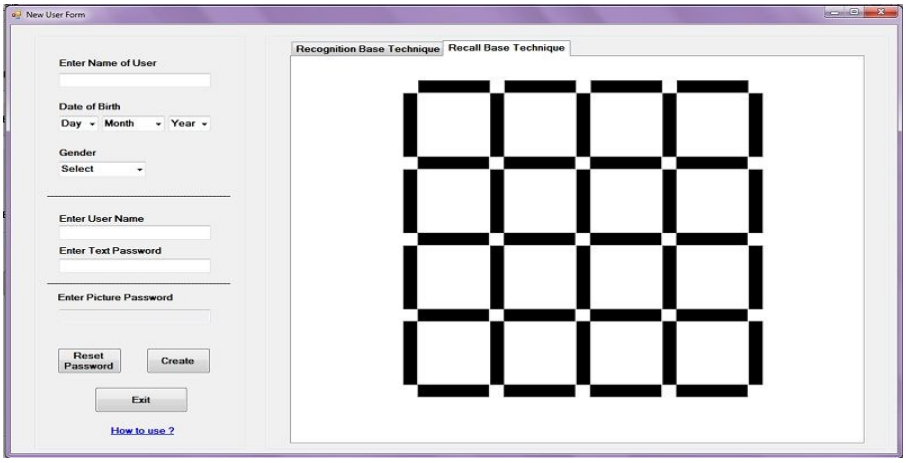

Fig. 4 Recall Base Technique

Our system provides choices to user for giving graphical password. Fig. 4 shows recall base technique user can draw a secrete pattern over the 2D grid at the time of registration. But our system doesn't show the pattern which is drawn by user only mouse over on that grid in particular pattern is possible then our secrete pattern is produced. Same pattern should be drawn at the time of authentication.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2014

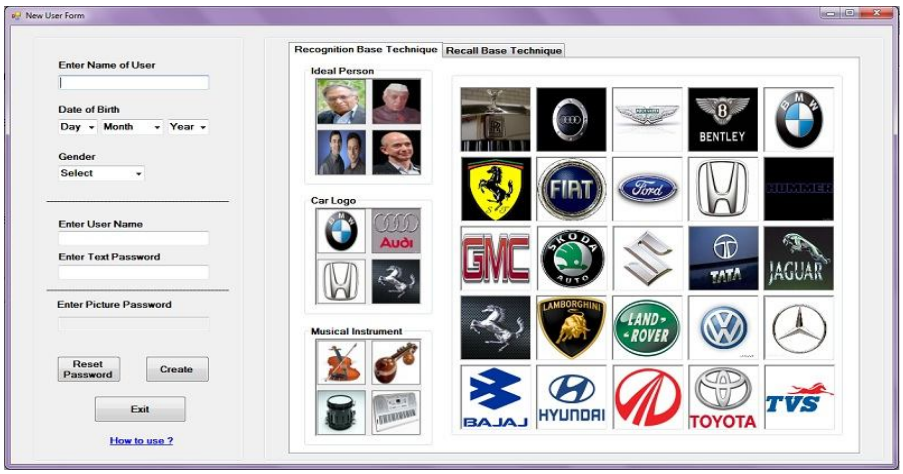

Fig. 5 Recognition Base Technique

Fig. 5 and Fig. 6 shows recognition base technique user first selects one particular group of images from three different groups i.e. Ideal Person, Car logo, or Musical instrument, after selecting a group, user select number of images from that group then selects another group from above three group and select images from that group and set password. This process is performing one to two times or repeatedly as per user choice. User can also give the password from both recognition base technique and recall base technique at same time. Architecture diagram of our system shows detail of process.

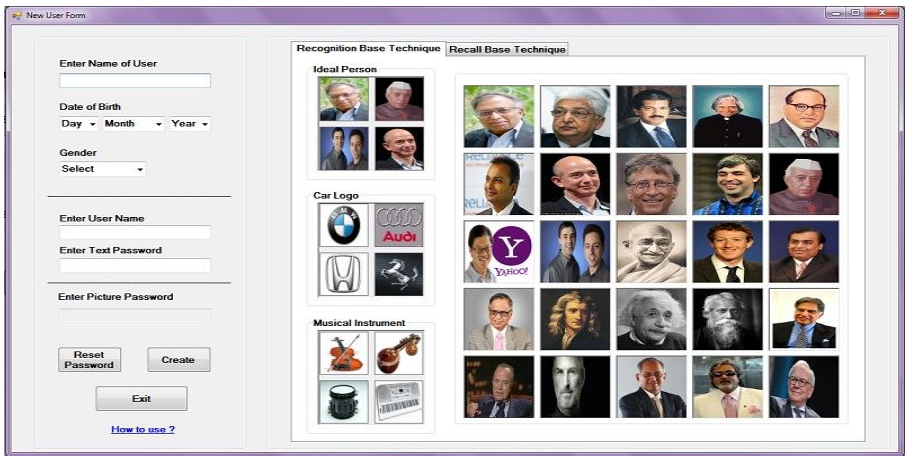

Fig. 6 Recognition Base Technique

Fig.5 and Fig. 6 shows how to implement the recognition base password. E.g. suppose user can create hybrid password using our technique, in that first user select any one group of images, after selecting any particular group user select images from that group shown in above Fig. 5, after selecting images user can change the group shown in above Fig. 6. If user has to add pattern in his password then user move to recall base technique and draw a secrete pattern over the 2D grid shown in Fig.4 and save the password.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2014

IV.ARCHITECTURE DIAGRAM

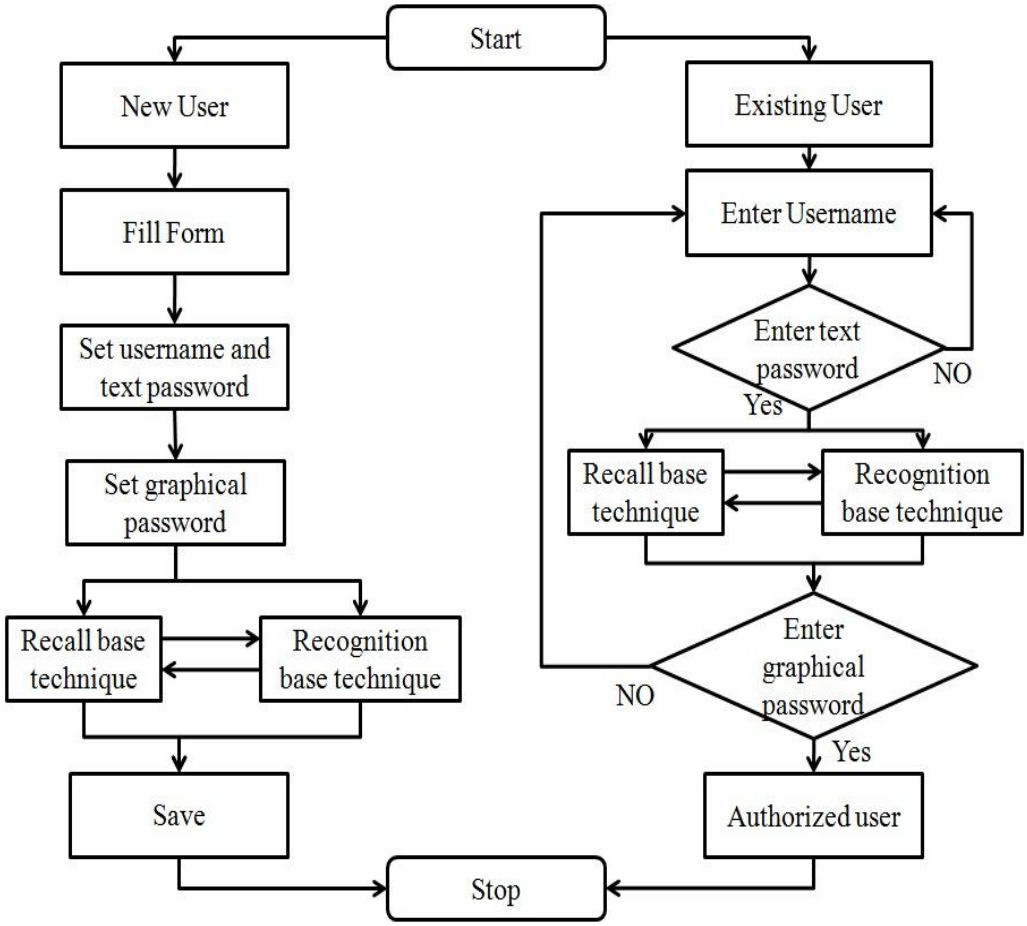

Fig. 7 Architecture diagram of system

Architecture diagram has two parts new user and existing user. First phase is new user fill the form (i.e. registration form) which contains three sections. First is their personal detail, second is username and text password and third is graphical password. In graphical password section there are two choices are provided to users which is shown in Fig. 7. Two password schemes are recall based technique and recognition based technique. In that user can give password in both ways (i.e. recall base technique or recognition base technique) and use both the technique alternative way. That alternative way remove the shoulder surfing problem in a little extend. In that user first draw a secrete pattern using recall base technique then select images for password. Figure-7 shows the detail working of creating password. Second phase is existing user, in that first user give username and text password. If text password is true then user can give images as a password. If the text password is not correct then system does not display the images as password. We can use text password, because text password remove the problem of shoulder surfing in greater extent. When user give graphical password then shoulder surfing problem is occur in that process, hence we provide text password suppose another person can see the images of particular user then the graphical password is known to that another person but text password is not see that another person and if the text password is true then the user can give graphical password and hence the problem of shoulder surfing is remove in greater extend.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2014

V.RESULT AND DISCUSSION

Our system removes the problem of shoulder surfing to greater extent. Because our system uses both text password and graphical password. We can use text password for removing the problem of shoulder surfing. When the user sets the image password then the person standing behind the user can observe the user's password. At that time the textual password is used to protect the image password. Our system also removes the problem of mouse logger because mouse logger captures the click points and scroll event of cursor. For that purpose we can provide the group of images. We are providing three groups of images. In that, suppose user select the ideal person group and select first two images of first row then user select second group that is car logo group in that user again select first two images of first row then mouse logger capture the same location on screen. But images are different and hence the hackers cannot understand the password of users.

VI.CONCLUSION

Our graphical password scheme provides better security to data and reduces the risk of breaking the user's password from different types of attacks. Our password scheme is based on images, pattern and text (i.e. numbers, alphabets and symbols) i.e. after clicking on a particular image or after drawing a pattern over the grid then it adds the code in text box which is alphanumeric and user can also provide the textual password according to his needs. It provides better security than existing system.

REFERENCES

[1] P. P. Ray, "Ray's scheme: Graphical password based hybrid authentication system for smart hand held device," *Journal of Information Engineering and Application*, vol. 2, no. 2, 2012.
[2] Z. K. Suchita Sawla, Ashvini Fulkar and S. Solanki, "Graphical password authentication system in an implicit manner," *International Journal of Cryptography and Security*, vol. 2, no. 2249-7019, pp. 27-29, 2012.
[3] F. Towhidi, M. Masrom and A. A. Manaf, "An enhancement on Passface graphical password authentication," *Journal of Basic and Applied Scientific Research*, vol. 2, no. 2, 2013..
[4] Dhamija, R., Perrig, A. (2000), Deja Vu: A User Study. Using Images for Authentication. 9th USENIX Security Symposium..
[5] X. Suo, Y. Z. G. and S. Owen, "Graphical passwords: A survey."
[6] Sonia Chiasson, P.C. van Oorschot, and Robert Biddle, " Graphical Password Authentication Using Cued Click Points," *School of Computer Science, Carleton University, Ottawa, Canada.*
[7] Iranna A M, Pankaja Patil, "GRAPHICAL PASSWORD AUTHENTICATION USING PERSUASIVE CUED CLICK POINT," *International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering*, Vol. 2, Issue 7, July 2013.
[8] A Aswathy Nair, Theresa Rani Joseph, Jenny Maria Johny, "A Proficient Multilevel Graphical Authentication System," *International Journal of Science, Engineering and Technology Research (IJSETR)*, Volume 2, No 6, June 2013.
[9] Sonkar S.K., Paikrao R.L., Awadesh Kumar, "Graphical Password Authentication Scheme Based On Color Image Gallery," *International Journal of Engineering and Innovative Technology (IJEIT)*, Volume 2, Issue 4, October 2012.
[10] Arash Habibi Lashkari, Abdullah Gani, Leila Ghasemi Sabet and Samaneh Farmand, " A new algorithm on Graphical User Authentication (GUA) based on multi-line grids," *Scientific Research and Essays*, Vol. 5 (24), pp. 3865-3875, 18 December, 2010.
[11] S. Chiasson, A. Forget, R. Biddle, and P.C. van Oorschot, "User Interface Design Affects Security: Patterns in Click-Based Graphical Passwords," Int"l J. Information Security, vol. 8, no. 6, pp. 387- 398, 2009.
[12] Golofit, K. Click Passwords Under Investigation. ESORICS 2007. LNCS 4734, 343-358, 2007.
[13] P. Dunphy, J. Nicholson, and P. Olivier, "Securing Passfaces for Description," Proc. Fourth ACM Symp. Usable Privacy and Security (SOUPS), July 2008.
[14] Thorpe, J. and P.C. van Oorschot. Human-Seeded Attacks and Exploiting HotSpots in Graphical Passwords. 16th USENIX Security Symposium, 2007.
[15] Blonder, G.E, "Graphical Passwords", United States Patent 5,559,961, 1996.
[16] Khan. W. Z., Aalsalem. A. Y., Xiang. Y. (2011), A graphical password based systems for mobile devices. Internation Journal of Computer Science and Issues, Vol. 8, Issue 5, No. 2, 145-154.
[17] Wiedenbeck, S., Waters, J., Sobrado, L., and Birget, J. (2006), Design and evaluation of a shoulder-surfing resistant graphical password scheme, International Working Conference on Advanced Visual Interfaces.
[18] Wells Jason, Hutchinson Damien and Pierce Justin En-hanced Security for Preventing Man-in-the-Middle Attacks in Authentication, formation Security Management Conference. 58.
[19] Haichang Gao, Zhongjie Ren, Xiuling Chang, Xiyang Liu "A New Graphical Password Scheme Resistant to Shoulder-Surfing".
[20] S. L. Smith. Authenticating users by word association. Comput. Secur., 6:464{470, 1987.
M. Zviran and W. J. Haga. A comparison of password techniques for multilevel authentication mechanisms. The Computer Journal, 3(3), 1993.