Progressive Image Hotspot Navigation for Successful Security Evaluation

E.Nalina, Kotha Hari Chandana, B.Krishna Priya, K.Semmangai Selvi, R.Rashmi

Abstract—Password is a group of characters used to allow only authorized user to enter in to the computer system. Password protection is a security process that protects information from unauthorized user. This project is an integration of the password scheme in a graphical manner. Graphical password scheme includes usability, security evaluations and implementation considerations. An important usability goal for knowledge-based authentication systems is to support users in selecting passwords of very high security, in the sense of being from an expanded effective security space. Users were provided an option of selecting a stronger password (which is not comprised entirely of known hotspots or following a predictable pattern). The formation of hotspots across users is minimized since click- points are more randomly distributed.

Index Terms—Cued Click-Points, Authorization, Hot Spot, File Stream, Authentication, Clustering,graphical password authentication, security.

1 INTRODUCTION

IN this project it involves the persuasive cued click point's option where the user will be provided an option of selecting the hotspots in an image. The successive selection of the exact hot spots will enable the user to move the next successful images. For login into the system, the user will be provided an option of selecting the hotspot in the continuous 5 images. After reaching the successful login attempt the user will be allowed to access the application. Storing the images in a secure database through file stream data type is one of the options used to secure the images instead of storing the images in the server[1]. Users will be provided an option of selecting the images to create the authentication page which is not included in the existing system. Possibility of monitoring the hotspots by the nearby user is possible. To avoid the same the password with matrix formation is one of the complex password schemes in the world. This option will be added in our project. This paper classifies the image retrieval into text based and content based, including the newly growing ontology based image retrieval system as one focus [1]. In this project it overcome the drawback of emphasize the usage of jpeg file and it remains a major drawback if in case of using different image types. This paper didn't explain the impact of using other image types [2]. Real-time implementation of human detection [3] in video using the state-of-the-art histograms of oriented gradients method. Each image in the video sequence is tested at multiple scales using a sliding window. Security related drawback is overcome in this project. This paper focus towards Scale-invariant local descriptors method in which the individual objects will be grouped into basic parts. A classifier is then learned for each of these parts, and feature selection is used to determine the most discriminative ones [4]. Replacing the textual password with a graphical password is the core idea of the project. In the older ages, the passwords were materialized in the form of graphical passwords with X,Y as coordinates on the images. Randomization clicks on the images enable the user to access the system is one of the major drawback. To overcome this issue, Persuasive cued click points comes into the picture. A picture will be framed with multiple click points in turn, which will have successive cued clicks on the images. The core point is, the user should select a secure hotspot in the image. The viewport is positioned randomly rather than specifically to avoid known hotspots, since such information might allow attackers to improve guesses and could lead to the formation of new hotspots. Still, if there is a possibility of selecting the correct spot in the first image. The possibility of selecting the second hot spot becomes a complex end where the user will be deviated at various stages and possibility of access the application is not possible.

IJSER staff will edit and complete the final formatting of your paper.

E.Nalina is with the Computer Science Department, Sri Muthukumaran Institute of Technology, Chennai, India.Phone:9840999577;(email: nalinasmit@gmail.com)

Kotha Hari Chandana is with the Computer Science Department, Sri Muthukumaran Institute of Technology,Chennai,India..Phone:9566209974;(email:hari_7chandana@yahoo.com)

B.Krishna Priya is with the Computer Science Department, Sri Muthukumaran Institute of Technology,Chennai,India..Phone:9176331868;(email:priya.balakrishnan1992@gmail.com)

K.Semmangai Selvi is with the Computer Science Department, Sri Muthukumaran Institute of Technology, Chennai, India. Phone: 9094894535 ; (email: semmangaiselvi@gmail.com)

R. Rashmi is with the Computer Science Department, Sri Sairam Engineering College, Tambaram, Chennai, India. Phone:044 23612121; (email: rashmismit@gmail.com)

2 System Architecture

The architecture for image hot spot is used to avoid the unauthorized user assessing the system and it also prevent from hacking the password. Initially authorized user need to identify the exact hot spot from the image.In earlier algorithm nearly five hot spot is used. Since this process has high probability of finding the password, proposed system with one hot spot password is designed .The user is asked to click the exact point and to confuse the hackers for each hot spot clicked, a duplicate image is generated so that hackers found difficult for accessing the password. Second step is once hot spot is clicked a matrix with list of alphabet is displaced user need to choose the character with intersecting points. To make the process more difficult for hackers each time a new matrix is generated. In this method user created two passwords one is textual password and another one is graphical password. In graphical password particular hot spot is allowed to click by using segmentation algorithm spot from the image is compared and alpha numeric matrix algorithm used.

Textual Password allow the user to select password from the matrix this is more advantageous since each time a new matrix is generated. There are three types of password evaluation technique

2.1 Text Only Authentication

The regular text password interface are used. The main reasons for choosing this system; (1) users are already familiar with it, (2) there does not appear to be a significant difference between the different parts of text passwords.

2.2 Graphics Only Authentication

Persuasive Cued Click Points is the best graphical password system developed so far.

2.3 Combination

Cued Click Points is used. This is because cued click points offers reasonable security and high usability. Though we believe that PCCP is a better graphical password system, it is our opinion that the combination should have a system with better usability. We believe that when combined with text passwords, this may help to bridge the gap between security and usability.

3 Related Works

3.1 Genuine Image Hot Point Check Module

In this module, the users were provided an option of selecting the hotspots in the hierarchy of the images. Once the hotspot is identified, the relevant point boundary of the hotspot is identified with the help of fast segmentation algorithm. Appropriate pixel values of box shaped were taken to avoid discrepancy in identifying the hotspot during authentication page. Once the first level of images was identified for the hotspot, the second levels of images were placed for the hotspot. A similar algorithm is implemented to scale up the exact location of the hotspot. After that, based on the image ranking for the user, the hotspot on the next level of hierarchical images was identified. This process becomes a recursive process for the successive images.

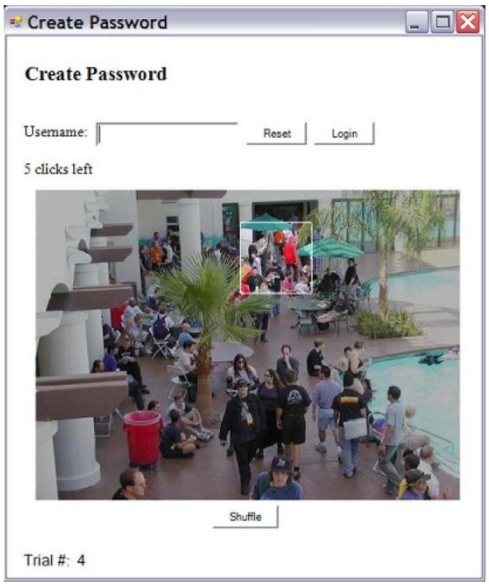
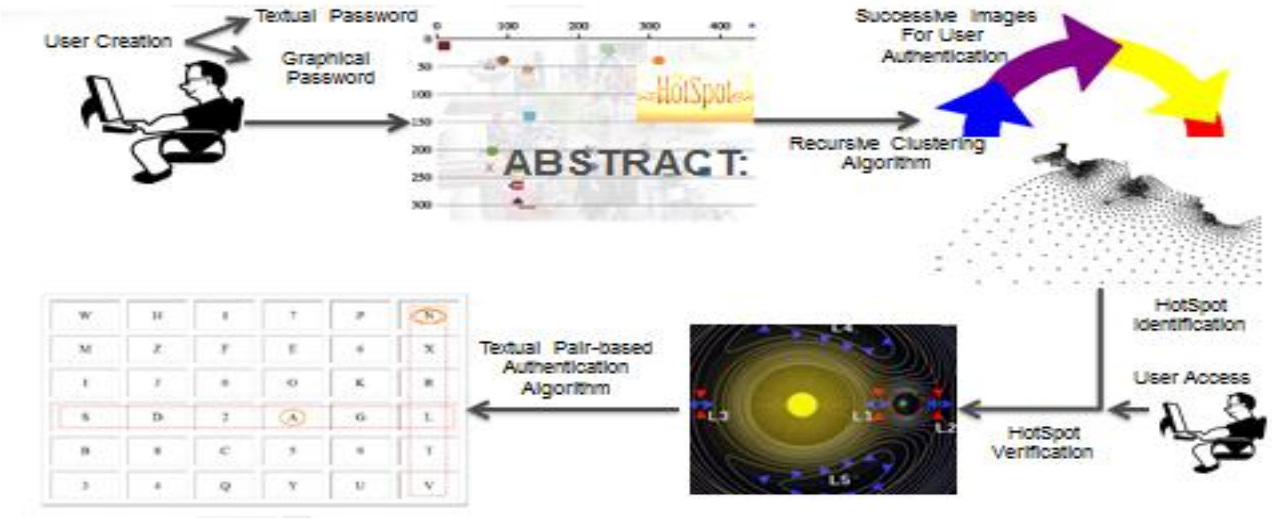


Fig 2: Hot Point Check Module

Fig 1 System Architecture



3.2 Fake Image Hot Point Check Module

In this module, to make the fake users to deviate from the original image. Fake hotspots on the fake images were placed in a hierarchical manner. The hotspots will be placed with the help of segmentation algorithm. Appropriate pixel values of box shaped were taken to avoid discrepancy in identifying the hotspot during authentication page The fake images with fake hotspot on the images will increase the complexity of the authentication scheme. The process will be followed as specified in the previous modules

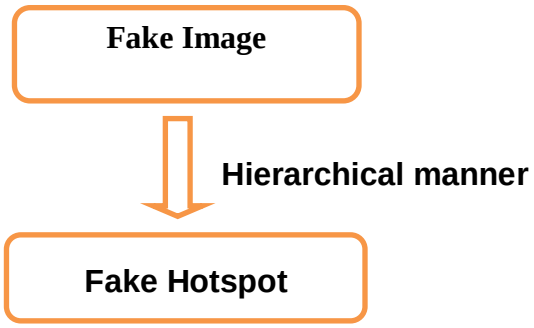


Fig 3:Fake Image

3.3 Matrix Formation Module

A most complicated algorithm concept which provides one of the world's strongest algorithm in the place of authenticating the user. Registering the user involves, Minimum length of the password should be 8 and it can be called as secret passcode. The secret passcode should contain even number of characters. In our case, we made this one mandatory as 8. Session password will be generated based on this secret pass code. During the login phase of the project, the user will enter his username an interface consisting of a complex grid which is displayed. The Alphanumeric grid is of size 6 x 6 and it consists of numbers and alphabets. These were randomly placed on the data grid and the interface will change every time during user login.

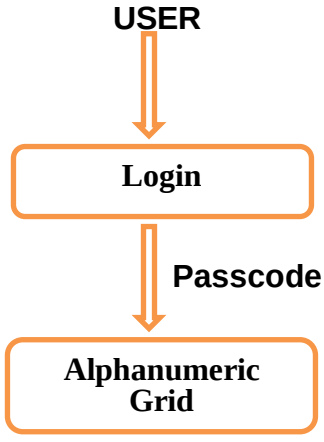


Fig 4: Matrix Formation Module

3.4 Authentication Scheme Module

The user will be permitted to provide their valid credentials to login into the system. Before finalizing the validation of the user, they need to cross two level of boundaries. The users will be checked for the valid hotspot of the images. Once the user crossed the exact boundaries of valid checks. The second check with be the matrix validations. Once the user provides valid data. He will be permitted to view his profile page. If more than a stipulated time, the user have tried the login. In that case, the user will be blocked permanently and it can be overcome by the Admin. The users were provided with permissible number of access on the authentication page. If they couldn't access the content, in that case the user's IP Address and MAC address will be blocked by the system to prevent future access on the system. Once the user needs to access the data, a special request to the admin followed by the admin unlocking the system

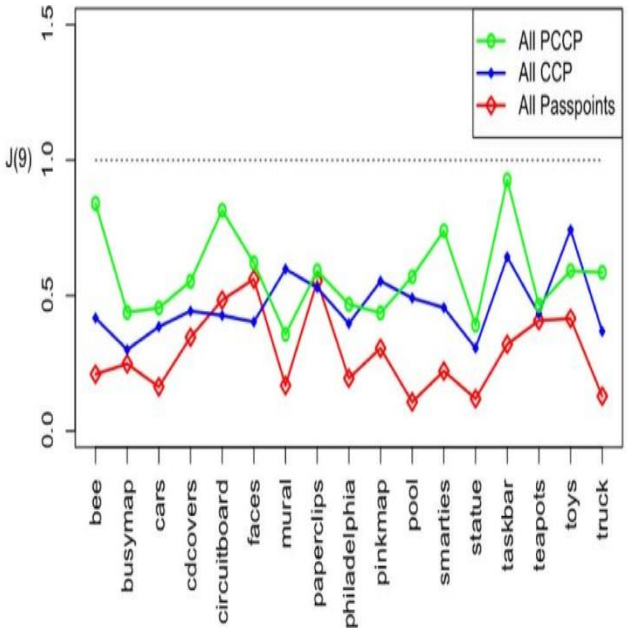


Fig 5: Comparison of Hot Spot

4 Algorithm Specification

Alphanumeric Matrix Algorithm and Fast image segmentation Algorithm is used for security evaluation. Alphanumeric Matrix Algorithm can provide a password input system and method that can defend against key logging attacks and shoulder surfing attacks, by having the final password inputted by way of certain alphanumeric matrix letters which are separated by a particular distance from the letters forming the password in the alphanumeric matrix rotated every time a letter is inputted.

Algorithm LI (linear iterative methods).

input: A = M + N 2 Cnn, b 2 Cn, x0 2 Cn

output: xk 2 Cn with Axk b

1: for k = 1; 2; 3; : : : do
2: compute yk = b . Nxk.1
3: solve Mxk = yk
4: end for

5 Conclusion

The proposed Cued Click Points scheme shows promise as a usable and memorable authentication mechanism. By taking advantage of users ability to recognize images and the memory trigger associated with seeing a new image, CCP has advantages over Pass Points in terms of usability. Being cued as each image is shown and having to remember only one click-point per image appears easier than having to remember an ordered series of clicks on one image.

References

[1] Alemu, Y.; Jong-bin Koh; Ikram, M.; Dong-Kyoo Kim; , "Image Retrieval in Multimedia Databases: A Survey," Intelligent Information Hiding and Multimedia Signal Processing, 2009. IIH-MSP '09. Fifth International Conference on , vol., no., pp.681-689, 12-14 Sept. 2009.

[2] Marwaha, P.; Marwaha, P.,"Visual cryptographic steganography in images," Computing Communication and Networking Technologies (ICCCNT), 2010 International Conference on , vol., no., pp.1-6, 29-31 July 2010

[3] Lillywhite, K.; Dah-Jye Lee; Dong Zhang; , "Real- time human detection using histograms of oriented gradients on a GPU," Applications of Computer Vision (WACV), 2009 Workshop on , vol., no., pp.1-6, 7-8 Dec. 2009

[4] Dorko, G.; Schmid, C.;, "Selection of scale-invariant parts for object class recognition," Computer Vision, 2003. Proceedings. Ninth IEEE International Conference on , vol., no., pp.634-639 vol.1, 13-16 Oct. 2003

[5] Sonia Chiasson1, Alain Forget1, Elizabeth Stobert, P.C. van Oorschot1, Robert Biddle" Multiple Password Interference in Text and Click-Based Graphical Passwords" September 25, 2008.

[6] Chippy.T, R.Nagendran "Defenses Against Large Scale Online Password Guessing Attacks By Using Persuasive Click Points" International Journal of Communications and Engineering Volume 03– No.3, Issue: 01 March2012.

[7]C Singh,L Singh,Chandrashekar Singh,Lenandlar Singh Lecturer, University of Guyana "Investigating the Combination of Text and Graphical Passwords for a more secure and usable experience" International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.2, March 2011.

[8] Joseph Bonneau, Cormac Herley, Paul C. van Oorschot, Frank Stajanoy" The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes" 2012 IEEE Symposium on Security and Privacy.

[9] Shuhaib K P , Sobin C," An Efficient Method for Graphic Password Authentication" MES Journal of Technology and Management

[10] Alain Forget, Sonia Chiasson, P.C. van Oorschot1, Robert Biddle" Improving Text Passwords Through Persuasion, Symposium on Usable Privacy and Security (SOUPS) 2008, July 23–25,2008, Pittsburgh, PA USA

[11] S. Chiasson, E. Stobert, A. Forget, R. Biddle, and P. van Oorschot,"Persuasive Cued Click-Points: Design, Implementation, and Evaluation of a Knowledge-Based Authentication Mechanism," Technical Report TR-11-03, School of Computer Science, Carleton Univ., Feb. 2011.

[12] P.C. van Oorschot and J. Thorpe, "Exploiting Predictability in Click-Based Graphical Passwords," J. Computer Security, vol. 19, no. 4, pp. 669-702, 2011.

[13] A. Forget, S. Chiasson, and R. Biddle, "Shoulder-Surfing Resistance with Eye-Gaze Entry in Click-Based Graphical Passwords," Proc. ACM SIGCHI Conf. Human Factors in Computing Systems (CHI), 2010.

[14] P. Dunphy, J. Nicholson, and P. Olivier, "Securing Passfaces for Description," Proc. Fourth ACM Symp. Usable Privacy and Security (SOUPS), July 2008.

K.Semmangai Selvi received B.E degree in Electronic and Instrumentation from Annamalai University,India,2004 and received M.E degree in Computer Science and Engineering in Annamalai University,India,2007
She is working as Asst.Professor in sri Muthukumaran Institute of Technology,India

R. Rashmi (M'12) received B.E degree in Computer Science Engineering from Sri Muthukumaran Institute of Technology, Chennai,Tamilnadu, India , 2011.
She is pursuing her M.E , Computer Science in Sri Sairam Engineering College, Chennai, Tamil nadu, India in the year 2011-2013

E.Nalina pursuing B.E, Computer Science Engineering from Sri Muthukumaran Institute of Technology, Chennai,Tamilnadu, India , 2013.

B.Krishna Priya pursuing B.E, Computer Science Engineering from Sri Muthukumaran Institute of Technology, Chennai,Tamilnadu, India , 2013.

Kotha Hari Chandana pursuing B.E, Computer Science Engineering from Sri Muthukumaran Institute of Technology, Chennai,Tamilnadu, India , 2013.