Int.J.HIT.TRANSC:ECCN.Vol.7: Issue 2A (2021) Page 64-71 ISSN: 0973-6875

Available Online at www.hithaldia.in/locate/ECCN
All Rights Reserved

ORIGINAL CONTRIBUTION

Graphical Password Authentication System Using Modified Intuitive Approach

[1]Abhishek Narayan Shah, [2]Dipti Anand, [3]Sabyasachi Samanta and [4]Dipankar Dey

[1,2]B. Tech Student, Haldia Institute of Technology, Dept. of IT, Haldia, WB, India

[3]Haldia Institute of Technology, Dept. of IT, Haldia, WB, India

[4]Global Institute of Science and Technology, Haldia, WB, India

ABSTRACT

In today's world everything we use needs security, especially when we are using something on internet. For security purpose, we use text passwords as it is the most popular user authentication method, but have security and user friendly problems. To address this problem, some researchers have developed authentication methods that use pictures as passwords. Graphical passwords offer another alternative, and are the focus of this project. Graphical password authentication systems are a type of Image-based authentication that attempt to understand the human memory for visual information. In Pass Points, passwords consist of sequence pixel click-points on a given image. Users may choose one pixels in that image as click-points for their password. To log in process, they repeat the sequence of clicks in the same order. In this paper, we conduct a modified intuitive approach of the graphical password techniques.

KEYWORDS: Graphical Password Authentication, Intuitive Approach, Recognition-basedapproache, Recall-based approaches.

1. INTRODUCTION

A Pass Points password is a sequence of points, chosen by a user in an image that is displayed on the screen. Our work predicts probabilities of likely click points; this enables us to predict the entropy of a click point in a graphical password for a given image. It allows us to evaluate automatically whether a given image is well suited for the Pass Points system, and to analyze possible dictionary attacks against the system.

In order to improve the security of user authentication, alternatives to alphanumeric passwords have been proposed, e.g., token based authentication, biometrics, graphical passwords, or "multiple factors" based on the simultaneous use of two or more authentication mechanisms. This paper focuses on graphical password systems, as a "single factor" authentication. The main motivation for graphical passwords is the hypothesis that people are better at remembering images than artificial words. Visual objects seem to offer a much larger set of usable passwords. For example we can recognize the people we know from thousands of faces; this fact was used to implement an authentication system.

In the Pass Points graphical password scheme, a password consists of a sequence of click points that the user chooses in an image. The image is displayed on the screen by the system. The image is not secret and has no role other than helping the user remember the click points. Any pixel in the image is a candidate for a click point. We classify these techniques into two categories: recognition-based and recall-based approaches.

Corresponding Address: diptianand3@gmail.com

Recognition-Based Technique: In this type of technique, users will select pictures, logos or any symbols from restored image. For authentication process user need to recognize the image, which he choose as a password. Recognition based systems have been proposed using usability and security considerations, and offers usability. In some graphical password schemes, Knowledge of some details of the shared secret must be retained by the system.

Dhamija and Perrig Based Technique: Dhamija and Perrig proposed a graphical authentication scheme based on the Hash Visualization technique. In their system, the user is asked to select a certain number of images from a set of random pictures generated by a program (figure 1). Later, the user will be required to identify the preselected images in order to be authenticated.

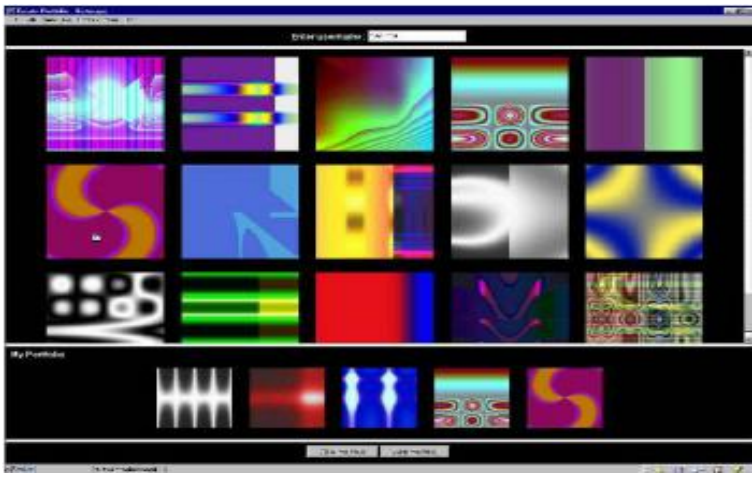


Figure 1: Random images used by Dhamija and Perrig.

Pass Face Scheme: Generally during setting a password the user selects a set of human faces. A panel of candidate faces is presented during his/her login. Among the given set of decoys the user must select the faces he/she selected during setting the password.



Figure 2: An example of Passfaces

Sobrado And Birget Scheme: Sobardo and Birget developed a method to prevent shoulder surfing attack. System displayed number of pass object among many other object ,user click inside the convex hull bounded by pass-object.



Figure 3: Convex hull shoulder surfing.

Recall-Based Technique: Recall-based graphical password systems are occasionally referred as draw metric systems since a secret drawing is recalled and reproduced by the user. In these systems, users typically draw their password either on a blank canvas or on a grid. You can secure your password using various techniques in graphical authentication.

Draw-A-Secret Scheme (DAS): This technique in which the user is allowed to draw a simple picture onto a 2D rectangular grid of size G * G which is denoted by discrete rectangular coordinates (x, y) without a pen up event a shown in the figure.

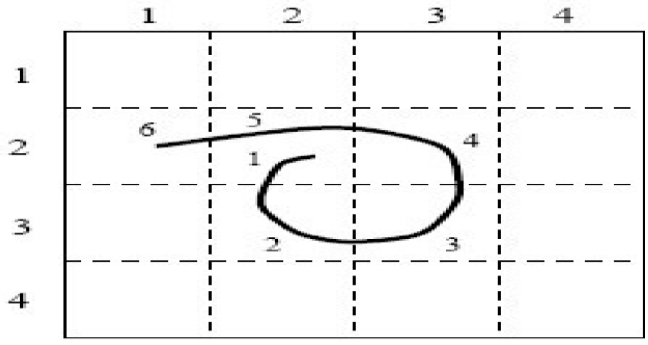


Figure 4: Draw a Secret (DAS) method on a 4*4 Grid.

Signature Scheme: Here authentication is conducted by having the user drawing the signature using mouse.

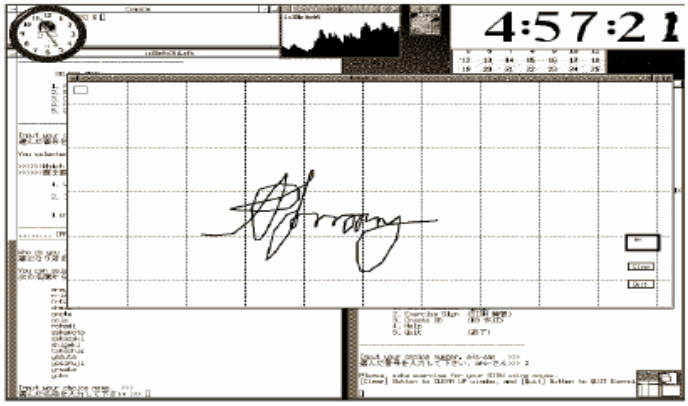


Figure 5: A signature is drawn by mouse.

Pass Point Scheme: User click on any place on an image to create password. A tolerance around each chosen pixel is calculated. In order to be authenticated, user must click within the tolerance in correct sequence.

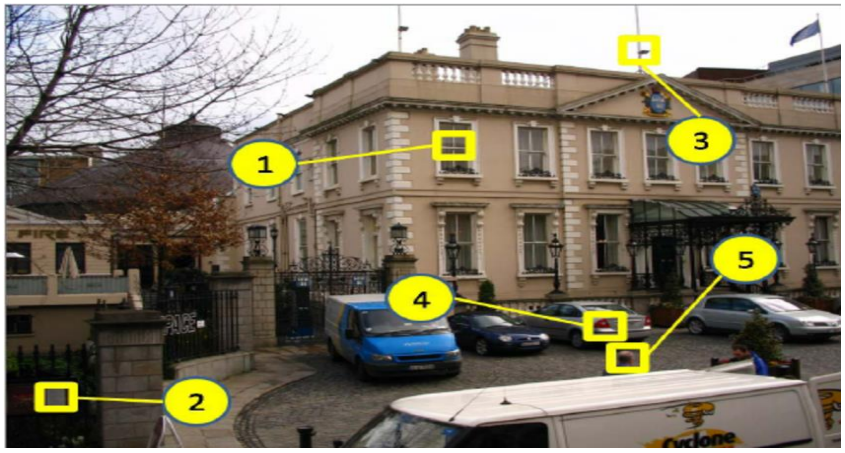


Figure 6: A sample of Pass Point method.

2. PURPOSE AND SCOPE

Studies on visual attention and eye movements show that most images contain a few portions that most humans focus on. When asked to create a graphical password a user would probably not click with the same frequency on all available pixels, but focus on some specific areas. In the Pass Points scheme the clustering of the users' click points reduces the entropy of these click points. In this section we develop a model of user choice of a click point in the Pass Points system and give an algorithm that predicts the most likely click locations, along with their probability values.

In future it has great scope. It can be used everywhere instead of text-based password .We can increase the security of this system by increasing the number of levels used, the number of tolerance squares used. The software should be developed according to the system. The user interface module should be developed in such a

way that the user can easily operate the system. The most important responsibility of developer is maintenance. He is responsible to give support to the customer when they are getting problem related to the software.

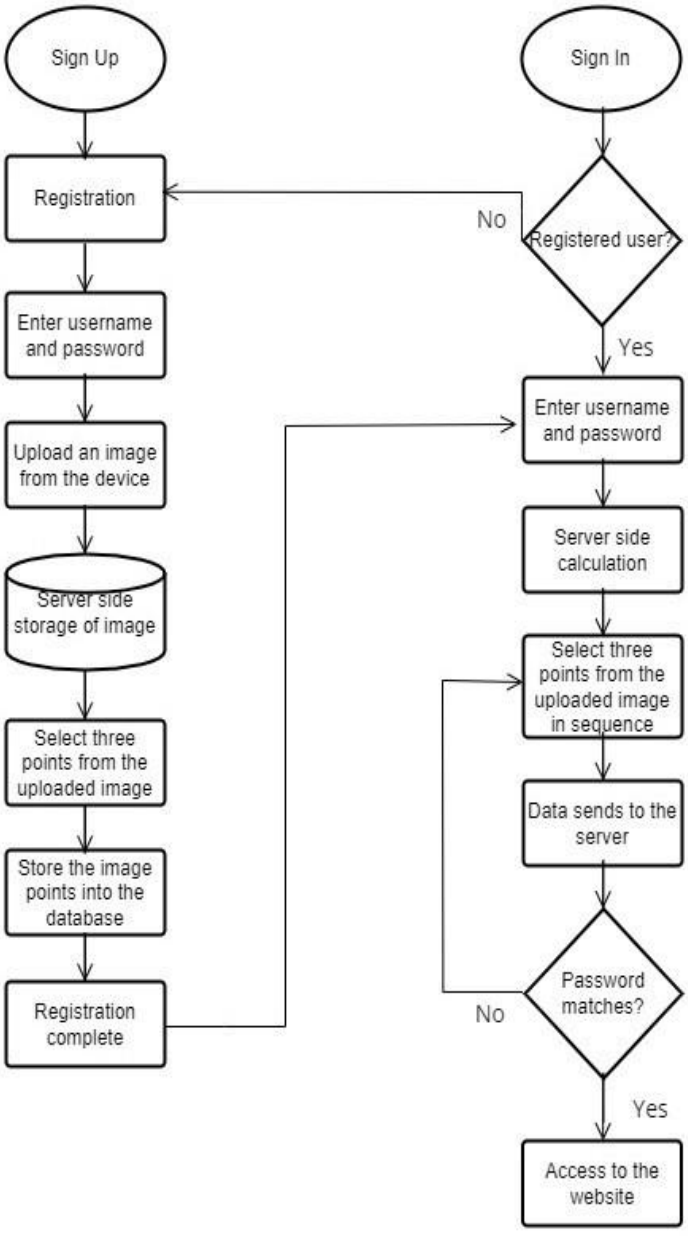


Figure 7: Flowchart for Modified Intuitive Approach

3. RESULT AND DISCUSSION

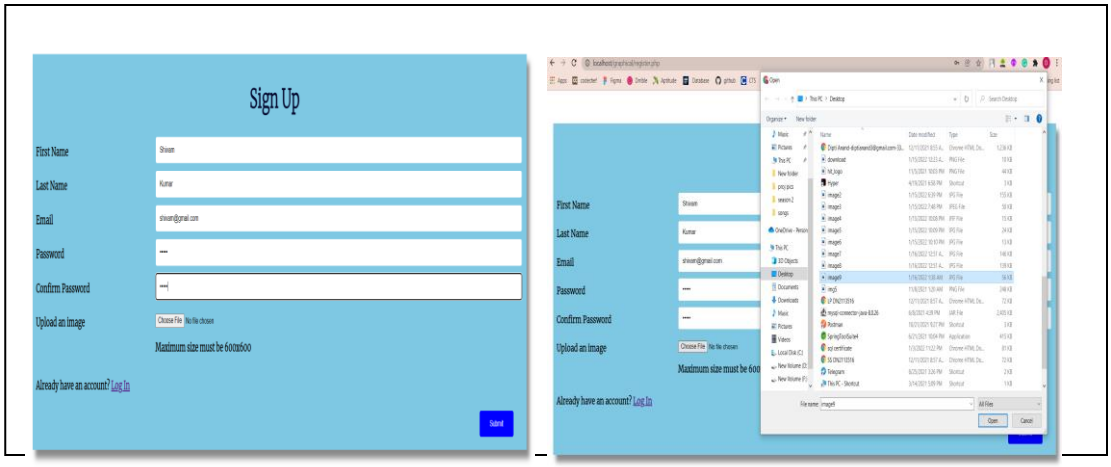


Figure 8: New Registration page

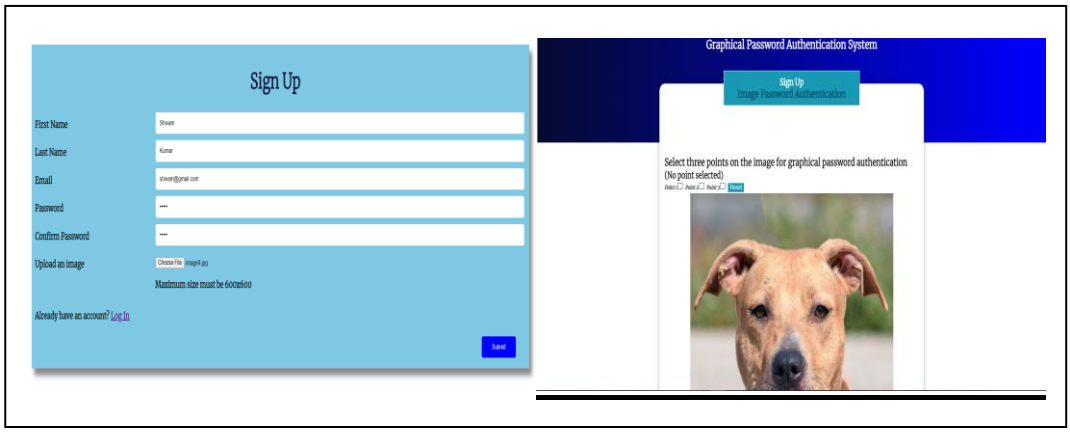


Figure 9: Image insertion



Figure 10: Pass Point selection for password verification

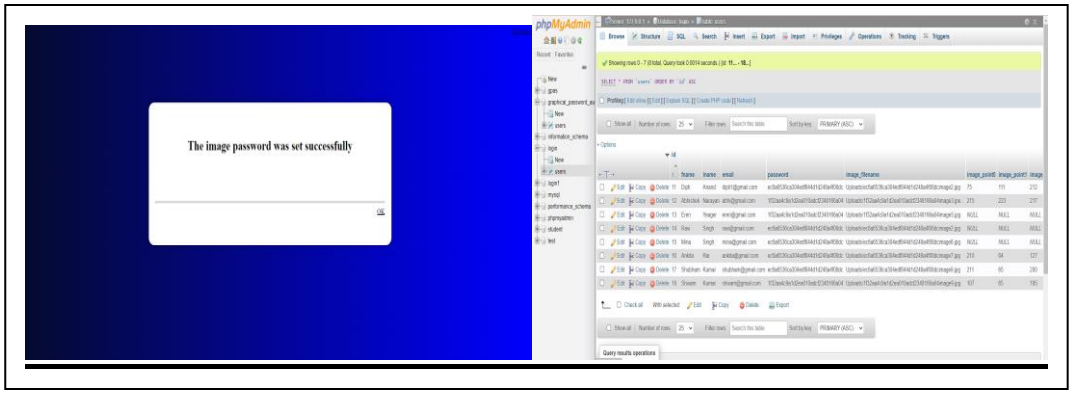


Figure 11:Database for user authentication details

4. CONCLUSION

The past decade has seen a growing interest in using graphical passwords as an alternative to the traditional text-based passwords. In this paper, we have conducted a comprehensive survey of existing graphical password techniques. The current graphical password techniques can be classified into two categories: recognition-based and recall-based techniques. Although the main argument for graphical passwords is that people are better at memorizing graphical passwords than text-based passwords, the existing user studies are very limited and there is not yet convincing evidence to support this argument.

Our preliminary analysis suggests that it is more difficult to break graphical passwords using the traditional attack methods such as brute force search, dictionary attack, or spyware. However, since there is not yet wide deployment of graphical password systems, the vulnerabilities of graphical passwords are still not fully understood.

Overall, the current graphical password techniques are still immature. Much more research and user studies are needed for graphical password techniques to achieve higher levels of maturity and usefulness.

5. FUTURE SCOPE OF THE PROJECT

The deliverable product is named as “Graphical Password Authentication System Using Intuitive Approach” I have designed the given proposed in the PHP, JAVASCRIPT, CSS, HTML to make the user login more secure and reliable. The given system is used for the different product where text password is not more reliable and also it is generating report is called “Graphical Password Authentication System Using Intuitive Approach” My project gives a brief idea regarding the type of password verification beside the text password.

REFERENCES

[1] L. Sobrado and J. C.Birget,”Graphical passwords,” The Rutgers Scholar, An Electronic Bulletin for Undergraduate Research, vol. 4, 2002.

[2] S. Akula, V. Devisetty, “Image based registration and authentication system,” Midwest Instruction and Computing Symposium (2004).

[3] D. Davis, F. Monrose, M. Reiter, “On user choice in graphical password schemes”, 13th Usenix Security Symposium (2004) 1-14.

[4] Xiaoyuan Suo, Ying Zhu, G. Scott. “Graphical passwords: a survey”, Computer Security Applications Conference, 21st Annual Owen 2005.

[5] X. Suo, Y. Zhu, G.S. Owen, “Graphical passwords: A survey”, 21st Annual Computer Security Applications Conference (ACSAC’05) (2005) 463-472.

[6] Farnaz Towhidi, Maslin Masrom, (IJCSIS) International Journal of Computer Science and Information Security, Vol. 6, No. 2, 2009.

[7] D. Davis, F. Monrose and M.K Reiter, “On User Choice in Graphical Password Schemes”, In Proceesings of the USENIX Security Symposium, California, 2004.

[8] R. Dhamija and A. Perrig. “Déjà vu: A User Study Using Images for Authentication”, In Proceedings of the USENIX Security Symposium, 2000.

[9] S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy, and N. Memon, “Authentication Using Graphical Passwords: Basic Results”, In Human-Computer Interaction International (HCII 2005), Las Vegas, NV, 2005.

[10] S. Akula and V. Devisetty, "Image Based Registration and Authentication System," in Proceedings of Midwest Instruction and Computing Symposium, 2004.

[11] T. Valentine, "An evaluation of the Passface personal authentication system," Technical Report, Goldsmiths College, University of London 1998.

[12] Javatpoint “https://www.javatpoint.com/”.

[13] Sonia Chiasson, Alain Forget, Elizabeth Stobert, P.C. van Oorschot, Robert Biddle, Multiple Password Interference in Text Passwords and Click-Based Graphical Passwords, School of Computer Science, Department of Psychology Carleton University, Ottawa, Canada, ACM CCS’09, November 9–13, 2009.

[14] Eluard, M.; Maetz, Y.; Alessio, D., “Action-based graphical password: Click-a-Secret”, 2011 IEEE International Conference on Consumer Electronics, 2011, pp.265-266.

[15] 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): SpringerVerlag Lecture Notes in Computer Science (1438), 1998, pp.