Volume 3, Issue 8, August 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Design, Implementation and Evaluation of Knowledge-Based Authentication Mechanism Using Persuasive Cued Click-Points

Prof. Anil Kulkarni*
Department of Computer Science and Engineering
Guru Nanak Dev Engineering College, India

Sangameshwar
Department of Computer Science and Engineering
Guru Nanak Dev Engineering College, India

Abstract—The most common computer authentication method is to use alphanumeric usernames and passwords .This method has been shown to have significant drawbacks. For example, users tend to pick passwords that can be easily guessed. On the other hand, if a password is hard to guess, then it is often hard to remember. To address this problem, some researchers have developed authentication methods that use pictures as passwords. In this work we conduct comprehensive analysis of the existing image based password techniques. We discuss strengths and limitations of each method. Our analysis suggest that most of the picture based authentication schemes are easily breakable as user tends to click on hotspots in the images. A hotspot is the area of the image which is easily recognized against all other images. Thus making such techniques vulnerable. We propose a unique solution to this problem by a Persuasive Cued Click based image authentication scheme. We use persuasion to influence user choice in click-based graphical passwords, encouraging users to select more random, and hence difficult to guess, click-points. We also prove through performance analysis that by using this system, randomness is increased and hotspots in the images are reduced.

Keywords— authentication, graphical passwords, guessing attacks, hotspots, usable security.

I. INTRODUCTION

Passwords are the most commonly used method for identifying users in computer and communication systems. Typically, the most commonly used passwords are strings of letters and digits (text based passwords). The problems of these knowledge-based authentication, typically text-based passwords are well known. Users often create memorable passwords that are easy for attackers to guess, but strong-system-assigned passwords are difficult for users to remember[5].

A password authentication system should encourage strong passwords while maintaining memorability [1]. So we are proposing that authentication scheme that allow user choice (persuasion) while influencing users towards stronger passwords (Persuasive Cued Click-Point(PCCP) based authentication scheme [2], [3]). In our system, the task of selecting weak passwords (which are easy for attackers to guess) is more tedious, discouraging users from making such choices that is rather than increasing burden on users, it is easier to follow system's suggestions for a secure password- a feature lacking in most existing schemes. So this proposed approach helped to conduct user studies evaluating usability and security. Through these user studies [1]-[4], [6], we compared PCCP to text passwords and two existing click-based graphical password systems. Results show that PCCP is effective at reducing hotspots (areas of the image which is easily recognized against all other images) and avoiding patterns formed by click-points within a password which are the major drawbacks in the existing click based graphical password systems respectively.

II. BACKGROUND

Text passwords are the most popular user authentication method but have some security and usability problems. Security problem is nothing but causing various attacks like shoulder surfing (looking over one's shoulder to get information) etc and usability problem refers to limited password space. So to overcome from these drawbacks, graphical passwords had been introduced by Greg Blonder in 1996 which offers another alternative and are the focus of this paper. The passwords which we are focussing are cued-recall click based graphical passwords(also known as locimetric [7]).In such systems, users identify and target previously selected locations within one or more images. The images act as memory cues [8] to aid recall. Examples of these systems include Pass Points (PP) [9] and Cued Click-Points(CCP) [6] which are the present or existing systems.

A. Pass Points (PP):

- User selects N random points in an image presented to user:

In this system an image is picked from set of images present in a gallery and user is shown the image. Task of user is to click N points as shown in Fig 1. As user clicks on the points, features from points are stored and not the point itself. Because storing points directly reduces the security of the technique. As it is very difficult to remember the random points, user chooses to select points on images that can be easily recognized in the image. It is called Hot Spot [10]-[13]. Advantage of this system is simplicity of implementation and drawback is low security. In another variant of this system, user himself picks the image which increases the security. However user has to always enter the same image and within

some system-defined tolerance region for each click point during authentication which means that image must be physically present in the client system.

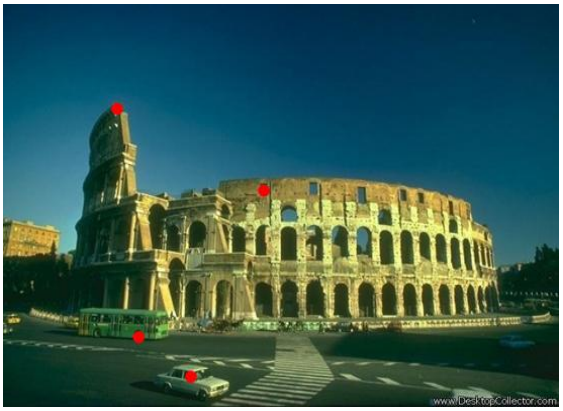


Fig.1. Pass Points(PP)

B. Cued Click-Point (CCP):

- User selects one point in each of N images presented to user randomly:

In order to increase the security loopholes mentioned in pass points system, password distribution scheme is developed. Here user is presented with N random different images and user has to click one point at every image. Based on selected click point of current image next image is displayed randomly by the system as shown in Fig 2.The complexity of this technique is high as user not only has to remember the images in proper order but also has to remember points in every image. This method therefore presents great challenge for the user to remember the password.

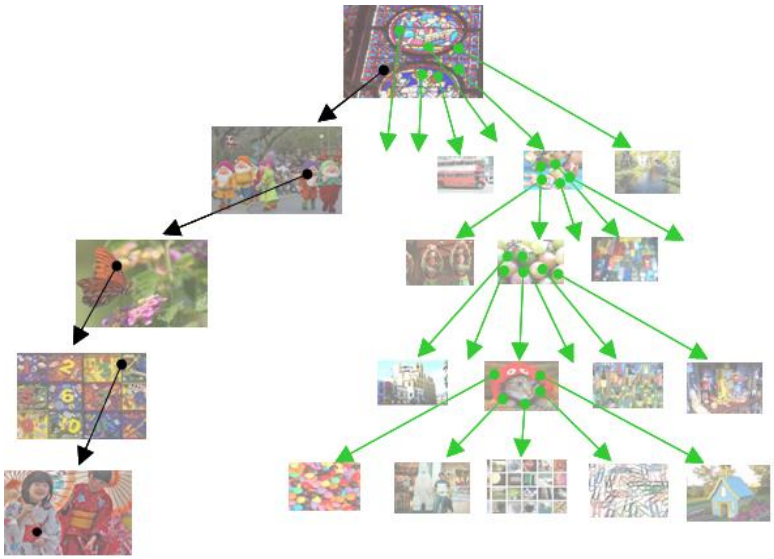


Fig.2. Cued Click-Points(CCP).Each click determines the next image.

- User selects one or N images and selects the points themselves manually:

In this technique user himself selects the number of images and number of points in every image. Further user selects the image manually. This has several limitations as most often user chooses to select an option that is easily rememberable. Hence number of selected images are low.

III. PROPOSED WORK

Persuasive Cued Click-Points(PCCP):

It is clear from above discussion that Image Based Passwords can be made more secured by increasing the randomness. Increase in randomness increases the complexity of remembering the passwords. Therefore methods are needed that can offer high security, low predictability and at the same time makes it easier for the user to remember the password points. Following proposed system solves this problem:

- First a Random Image is picked up from database. One random block of the image is selected as viewport and rest of the image is blurred. This viewport can be shuffled to desired position as per user choice. User just has to remember the image and the viewport point as shown in Fig 4.
- When user selects a point in the viewport, its features are extracted. Here, features are based upon color. Then compare its features with image features of all images. Closest image is shown next. Thus user does not have to remember the next image.

- Subsequently as user selects a point, its features are stored and at the same time next matching image is stored.

Fig 3 shows the complete block diagram of proposed PCCP graphical password system.

Thus system only stores one image for the user and features of click points. Therefore the password is automatically secured as it does not contain any physical location. User has to specifically remember the first image and the click point. Thus even though the system makes the password more random, it makes it easy for the user to remember the password. User can select hotspots from second image onwards. From an imposter point of view, he has to know the first image, the first click point and then he has to guess all the subsequent click points in subsequent images. A wrong guess alters the image itself, thereby eliminating the chance of misdetection.

As the first view port is purely random, chances of user clicking on hotspot is minimum.

By this proposed system, the drawbacks occurred in existing system (hotspots) can be easily identified and are reduced effectively using hotspot coverage graphs as shown in Fig 5.

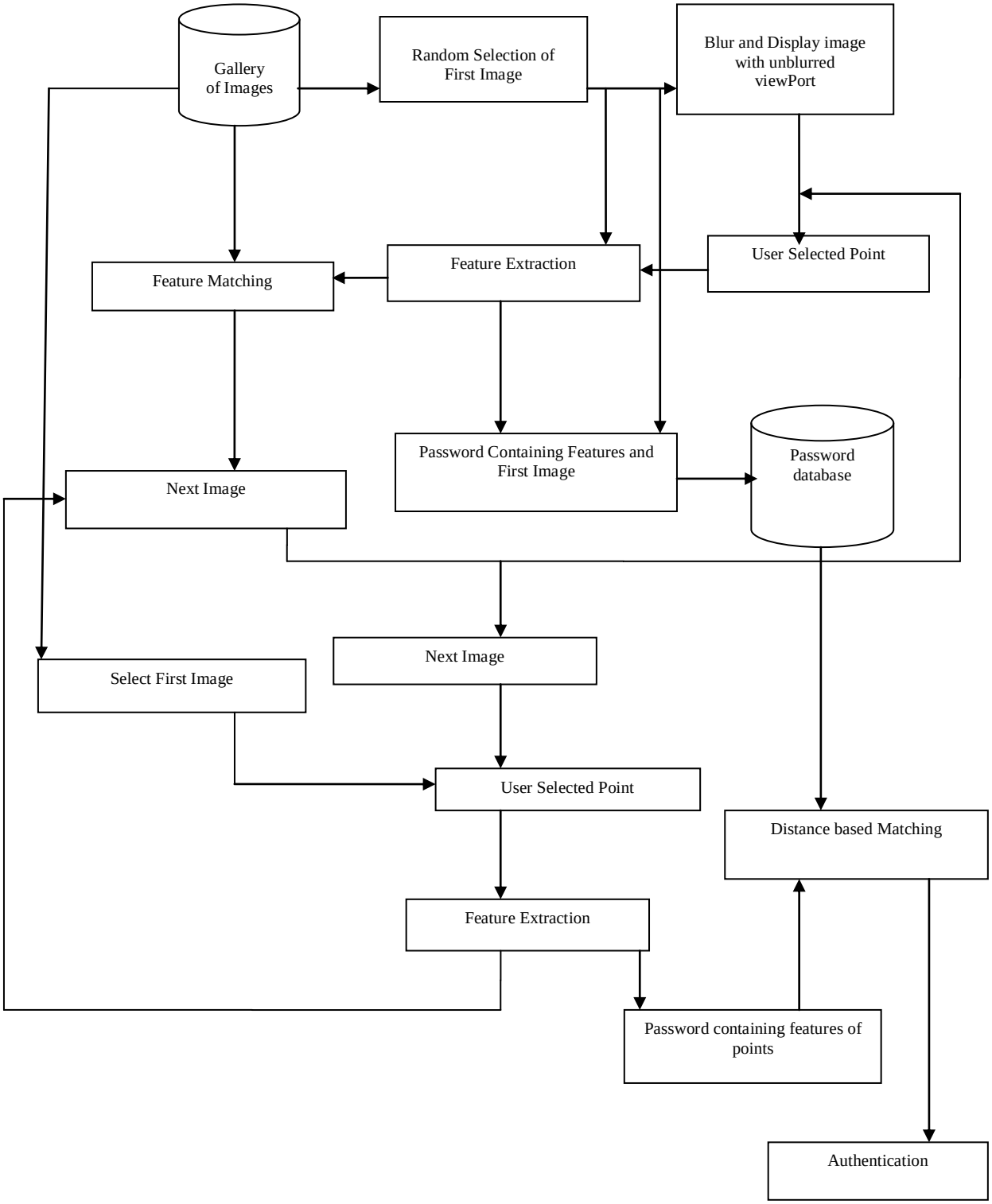


Fig.3. Block diagram of proposed system

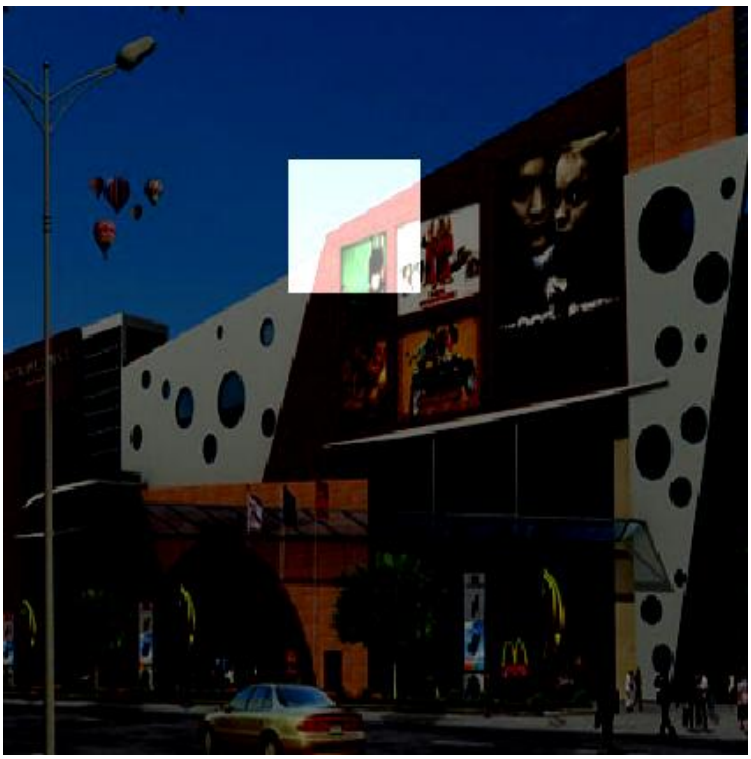
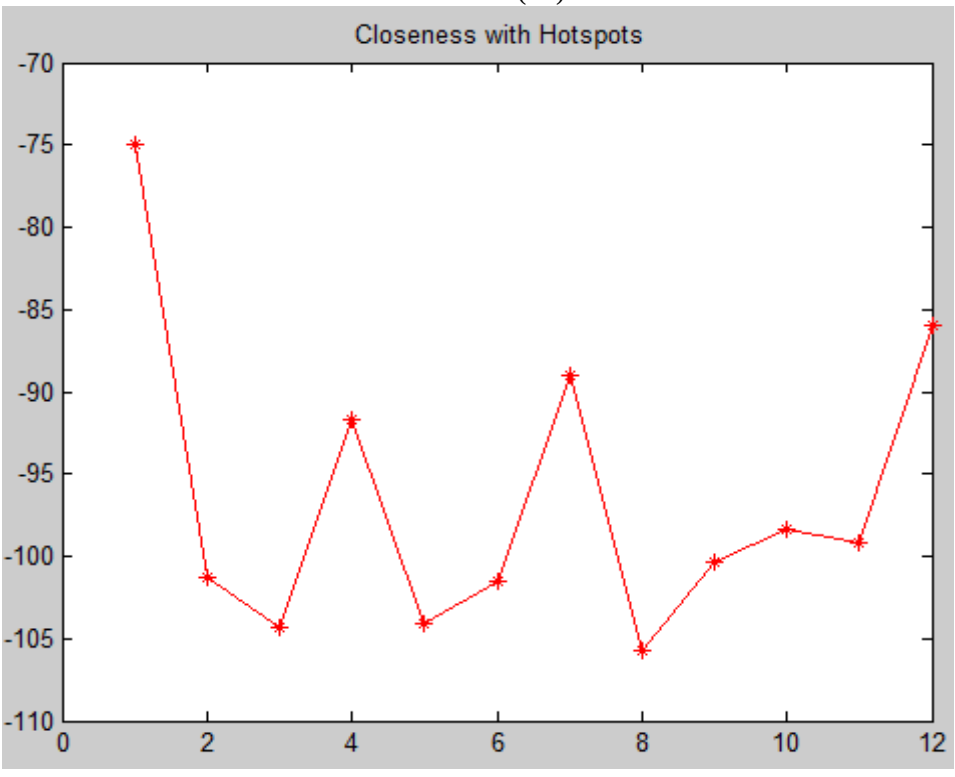


Fig.4. Simple PCCP. The viewport highlights part of the image.

Hotspots coverage graphs for PP, CCP and PCCP:

Using graph shown in Fig 5, we conclude that hotspots are reduced effectively in proposed system compared to existing systems. The distance of actual click point entered by user with hotspot in PP (-75) is greater compared to CCP(-110) which in turn is greater compared to PCCP (-132). So less closeness or distance of actual click point with hotspots will reduce in number of hotspots for that particular image for legitimate users to authenticate respectively.

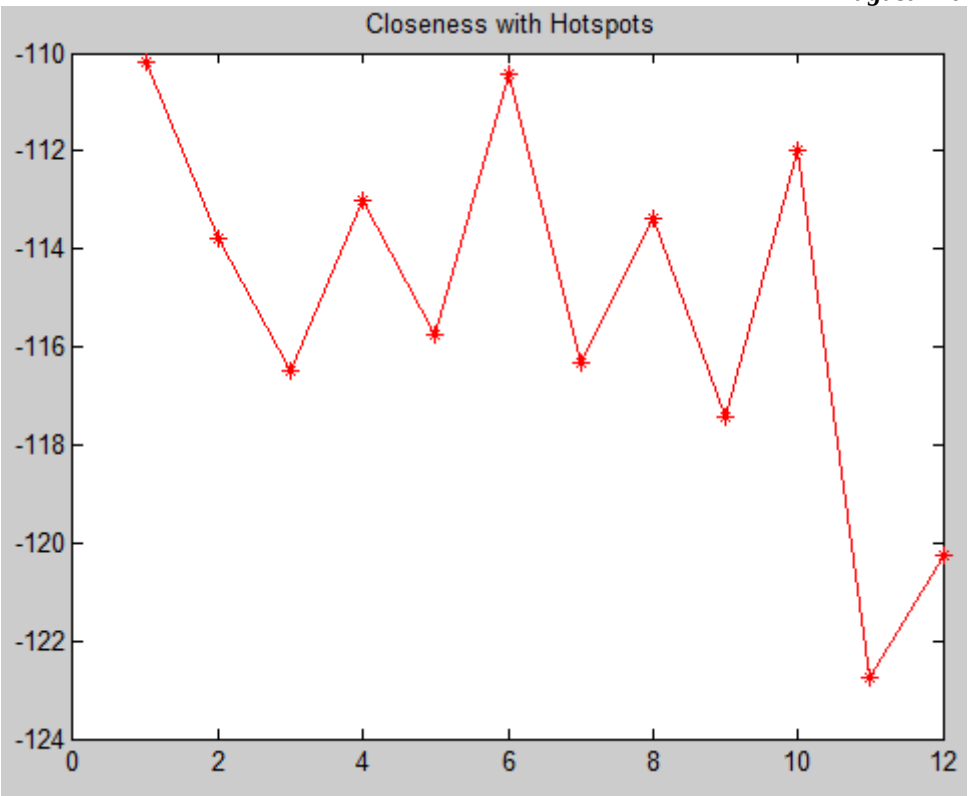
Pass Points (PP)



X-axis represents number of hotspots per image.

Y-axis represents distance between hotspot and actual click point entered by the user of that particular image.

Cued Click-Points (CCP)



X-axis represents number of hotspots per image.
Y-axis represents distance between hotspot and actual click point entered by the user of that particular image.

Persuasive Cued Click-Points (PCCP)

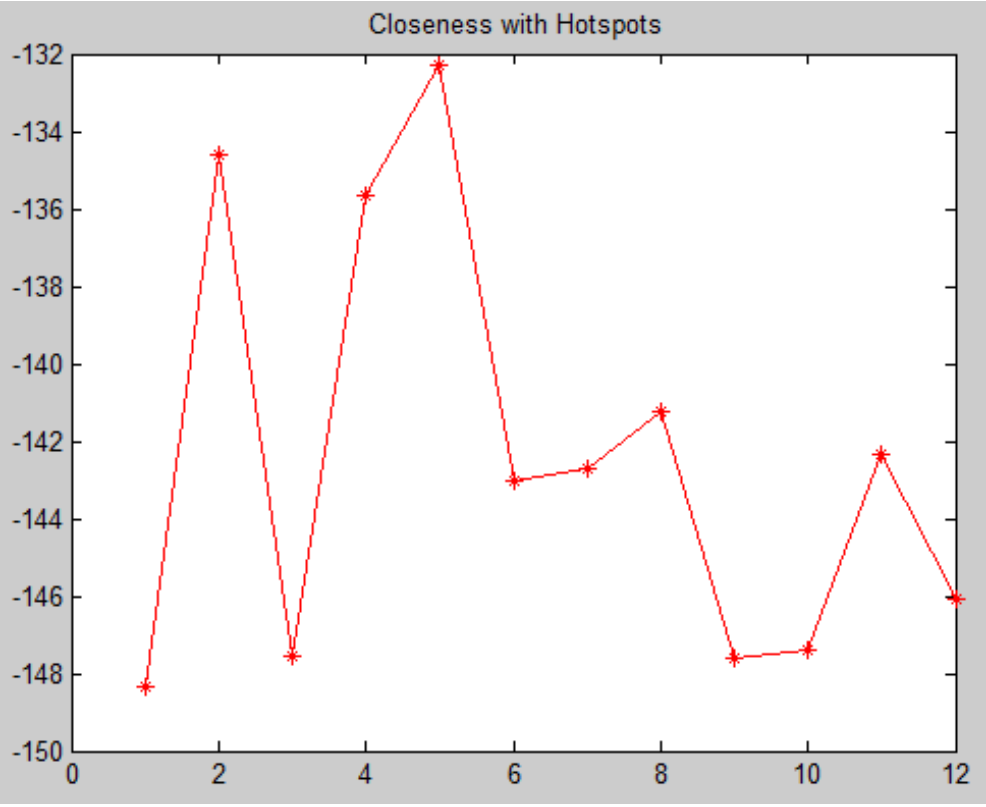


Fig.5. Hotspots coverage graphs

X-axis represents number of hotspots per image.
Y-axis represents distance between hotspot and actual click point entered by the user of that particular image.

IV. CONCLUSIONS AND FUTURE WORK

The major advantage of persuasive cued click point scheme is its large password space since entire image is used for generating the password and it helps in reducing number of hotspots in the image compared to existing click based graphical password systems. Therefore it provides better security. Randomness of the system is very high in comparison to both single-image multi-point based technique and multi-image single-point based techniques. The system offers features based matching instead of point based matching. Thus physical password does not store the image points. There by securing the password to a great deal. The system allows user to select first image at the time of authentication, thereby eliminating the need of exposing the gallery for every images. It is tough for the imposters to remember the first image and view port. Thus system is better equipped to deal with false acceptance and shoulder surfing attacks.

This method can be further improved by incorporating better image features than color features. Texture descriptor could be used for complex images.

REFERENCES

[1] S. Chiasson, R. Biddle, and P.van Oorschot, "A second look at the usability of click-based graphical passwords," in ***ACM*** *Symposium on Usable Privacy and Security (SOUPS),* July 2007.

[2] S. Chiasson, A. Forget, R. Biddle, and P. van Oorschot, "Influencing users towards better passwords: Persuasive Cued Click-Points," in *Human Computer Interaction (HCI), The British Computer Society*, September 2008.

[3] S. Chiasson, A. Forget, E. Stobert, P. van Oorschot, and R. Biddle, "Multiple password interference in text and click-based graphical passwords." in *ACM Computer and Communications Security (CCS)*, November 2009.

[4] E. Stobert, A. Forget, S. Chiasson, P. van Oorschot, and R. Biddle, "Exploring usability effects of increasing security in click-based graphical passwords," in *Annual Computer Security Applications Conference (ACSAC)*, 2010.

[5] J. Yan, A. Blackwell, R. Anderson, and A. Grant, "The memorability and security of passwords," in *Security and Usability: Designing Secure Systems That People Can Use*, L. Cranor and S. Garfinkel, Eds. O'Reilly Media, 2005, ch. 7,pp. 129–142.

[6] S. Chiasson, P. van Oorschot, and R. Biddle, "Graphical password authentication using Cued Click Points," in *European Symposium On Research In Computer Security (ESORICS), LNCS 4734*, September 2007, pp. 359–374.

[7] A. De Angeli, L. Coventry, G. Johnson, and K. Renaud, "Is a picture really worth a thousand words? Exploring the feasibility of graphical authentication systems*," International Journal of Human-Computer Studies,* vol. 63, no. 1-2, pp. 128–152, 2005.

[8] E. Tulving and Z. Pearlstone, "Availability versus accessibility of information in memory for words," *Journal of Verbal Learning and Verbal Behavior*, vol. 5, pp. 381–391, 1966.

[9] S.Wiedenbeck, J.Waters, J. Birget, A. Brodskiy, and N. Memon, "PassPoints: Design and longitudinal evaluation of a graphical password system," *International Journal of Human-Computer Studies*, vol. 63, no. 1-2, pp. 102–127, 2005.

[10] K. Golofit, "Click passwords under investigation," in *12th European Symposium On Research In Computer Security (ESORICS), LNCS 4734*, September 2007.

[11] A. Dirik, N. Menon, and J. Birget, "Modeling user choice in the Passpoints graphical password scheme," in *3rd ACM Symposium on Usable Privacy and Security (SOUPS),* July 2007.

[12] J. Thorpe and P. C. van Oorschot, "Human seeded attacks and exploiting hot-spots in graphical passwords," in *16th USENIX Security Symposium*, August 2007.

[13] A. Salehi-Abari, J. Thorpe, and P. van Oorschot, "On purely automated attacks and click based graphical passwords," in *Annual Computer Security Applications Conf. (ACSAC),* 2008.

