Graphical Password Authentication System with Integrated Sound Signature

[1,] Anu Singh , [2,]Kiran Kshirsagar, [3,]Lipti Pradhan
[1](Department of Computer Engineering, Pune University, India

Abstract

We are proposing a system for graphical password authentication with the integration of sound signature. In this work, Cued Click Point scheme is used. Here a password is formed by a sequence of some images in which user can select one click-point per image. Also for further security user selects a sound signature corresponding to each click point, this sound signature will help the user in recalling the click points. The system showed better performance in terms of usability, accuracy and speed. Many users preferred this system over other authentication systems saying that selecting and remembering only one point per image was aided by sound signature recall.

Keywords: *Sound signature, Authentication, Cued Click points*

I. INTRODUCTION

Basically passwords are used for

[1] Authentication (verifying an imposter from actual user).
[2] Authorization (process to decide if the valid person is allowed to access the data)
[3] Access Control (Restricting the user to access the secured data).

Usually passwords are selected by the users are predictable. This happens with both graphical and text based passwords. Users tend to choose password which are easy to remember, unfortunately it means that the passwords tend to follow predictable patterns that are easier for attackers to hack. While the predictability problem can be solved by disallowing user choice and assigning passwords to the users, this usually leads to usability problems since it's difficult for the user to remember such passwords. Many graphical password systems have been developed; research shows that a text-based password suffers with both usability and security problems. According to a recently published article, a security team at a company ran a network password cracker and within 30 seconds and they identified about 80% of the passwords. According to the practical research, it is well known that the human brain is better at recognizing and recalling the pictorial content, graphical passwords exploit this human characteristic.

II. RELATED WORK

Considerable work has been done in this field, the best known of these systems are Pass faces [1][4]. Brostoff and Sasse (2000) carried out an empirical study of Pass faces, which demonstrate well how a graphical password recognition system typically works. Blonder-style passwords are based on cued click recalls. A user clicks on several previously chosen locations in a single image for logging in. As implemented by Passlogix. Corporation (Boroditsky, 2002), the user chooses some predefined regions in an image as a password. To log in the user has to click on the same regions selected at the time of creation of the password. The problem with this system is that the number of predefined regions is small for selecting, perhaps around 10-12 regions in a picture. The password may have to be up to 12 clicks for adequate security, which again tedious for the user to operate. Another problem of this system is the need for the predefined regions to be readily recognizable. In effect, this requires artificial, cartoon-like images rather than complex, real-world scenes [2][3]. Cued Click Points (CCP) is a proposed alternative to previous graphical authentication system. In the proposed system, users click one point on each of 5 images rather than on five points on one image.

III. PROPOSED WORK

In the proposed work along with the cued click point we have integrated sound signature to help in recalling the password easily. No system has been designed so far which uses sound signature in graphical password authentication. As per the research it has been said that sound effect or tone can be used to recall facts like images, text etc [3].Our idea is inspired by this novel human ability. Using this sound signature and click points the user can be intimated if he or she is going in a write direction. It also makes the task of the hackers

more challenging. As shown in Figure 1, each click is directing the user to the next image, in effect leading users down a "path" as they click on their sequence of points. A wrong click leads down an incorrect path, with an explicit indication of authentication failure only after the final click. In the proposed system, users click one point on each of 5 images rather than clicking on five points on one image. A wrong click leads down an incorrect path, with an explicit indication of authentication failure only after the final click. Users can choose their images only to the extent that their click-point dictates the next image. If they dislike the resulting images, they could create a new password involving different click-points to get different images.

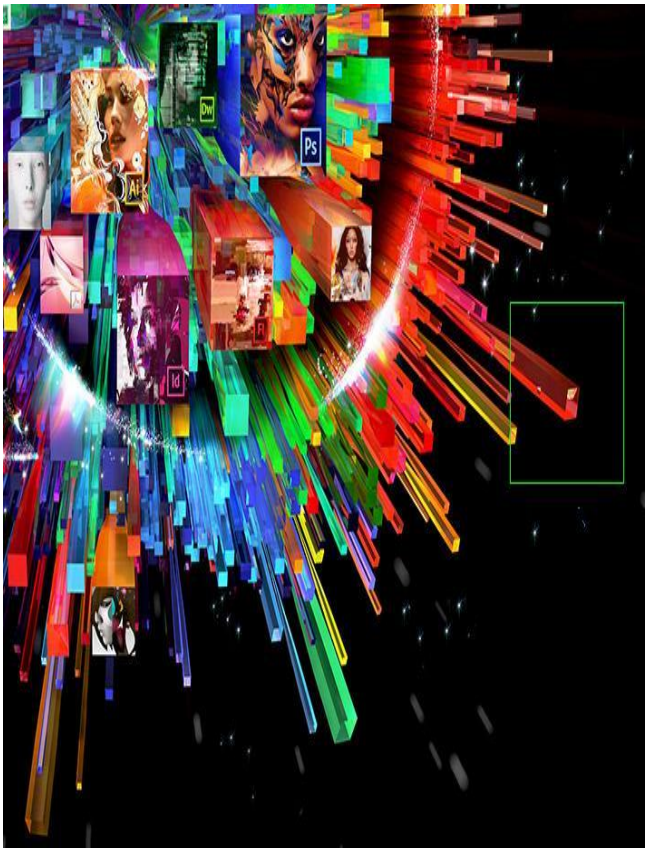

Fig 1.Click Point per image

Two vectors are created for in this system:

3.1. Profile Vectors

The proposed system creates user profile as follows-

3.2 Master vector

(User ID, Sound Signature frequency, Tolerance)

3.3 Detailed Vector (Image, Click Points)

As an example of vectors – Master vector (Smith, 2689, 50)

Detailed Vector

Image	Click points
I_1	(123,678)
I_2	(176,134)
I_3	(450,297)
I_4	(761,164)

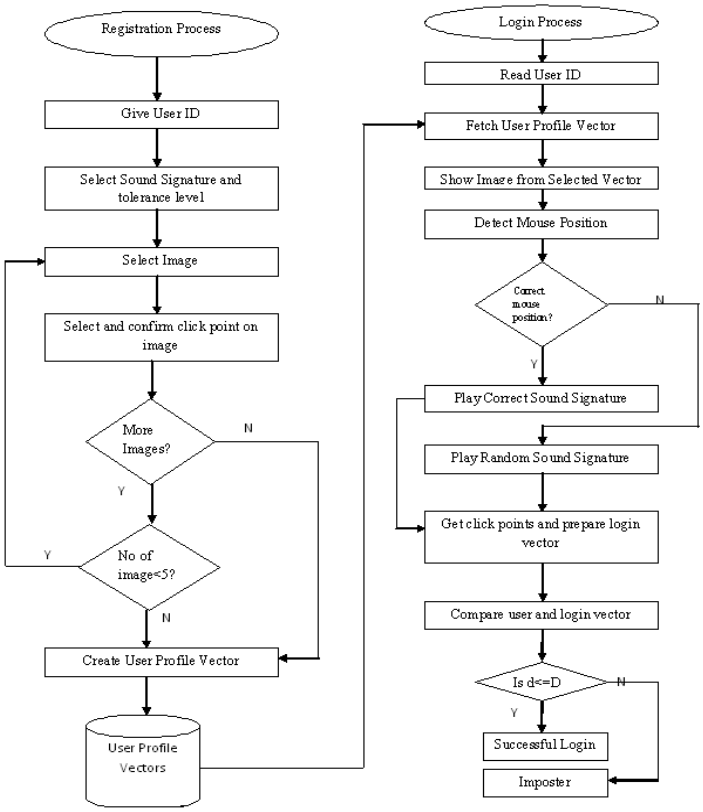

Fig.2 System Flow

3.4 System Tolerance

After creation of the login vector, system calculates the Euclidian distance between login vector and profile vectors stored. Euclidian distance between two vectors **p** and **q** is given by-

$$d(p\ q)=\sqrt{(p_1-q_1)^2+(p_2-q_2)^2+\ldots.+(p_n-q_n)^2}=\sqrt{\sum_{i=1\ to\ n}(p_1-q_1)^2}$$

Above **distance is calculated for each image** if this distance comes out less than a tolerance value D. The value of D is decided according to the application. In our system this value is selected by the user.

This is the registration form which shows that the userID is given by the system itself.

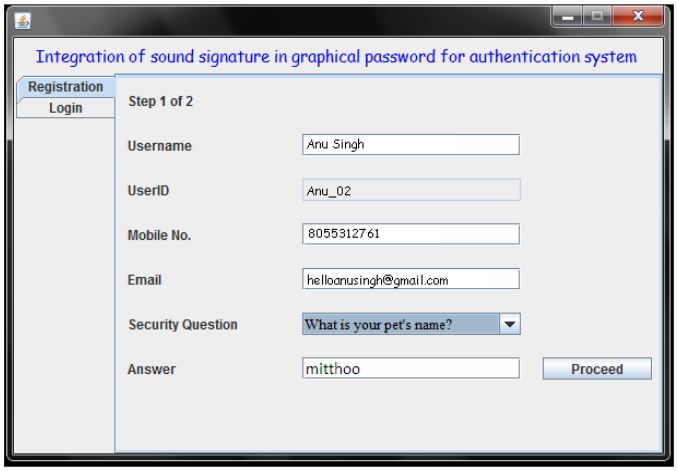

Fig 3.Registration Step 1

This is the selection of sound signature and the click points for creating the password.

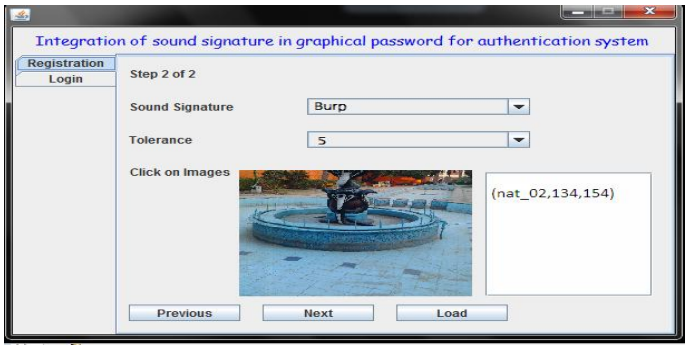

Fig 3.Registration Step 2

IV. PROJECT SCOPE

In proposed work a click-based graphical password scheme called Cued Click Points (CCP) is presented. In this system a password consists of sequence of some images in which user can select one click-point per image. Cued Click Points (CCP) is a proposed alternative to Pass Points. In CCP, users click one point hotspot analysis more challenging. Each click results in showing a next-image, in effect leading users down on each of 5 images rather than on five points on one image. It offers cued-recall and introduces visual cues that instantly alert valid users if they have made a mistake when entering their latest click-point (at which point they can cancel their attempt and retry from the beginning). It also makes attacks based on a "path" as they click on their sequence of points. A wrong click leads down an incorrect path, with an explicit indication of authentication failure only after the final click. Users can choose their images only to the extent that their click-point dictates the next image. If they dislike the resulting images, they could create a new password involving different click-points to get different images.In addition user is asked to select a sound signature corresponding to each click point this sound signature will be used to help the user in recalling the click point on an image.

System showed very good Performance in terms of speed, accuracy, and ease of use. Users preferred CCP to Pass Points, saying that selecting and remembering only one point per image was easier and sound signature helps considerably in recalling the click points.In the proposed work we have integrated sound signature to help in recalling the password. No system has been devolved so far which uses sound signature in graphical password authentication.

4.1 Authentication:

The only significant user study on the security of graphical passwords for authentication was performed by Davis[2] and the present authors[3] in that work; we studied the security of two schemes based on image recognition, denoted "Face" and "Story," which are described shortly. This study focused specifically on the impact of user selection of passwords in these schemes, and the security of the passwords that resulted. We recount some of the notable results from this study, and the methodologies used to reach them, as an illustration of some of the challenges that graphical passwords can face. In particular, this study demonstrated that graphical password schemes can be far weaker than textual passwords when users are permitted to choose their password.

V. CONCLUSION AND FUTURE WORK

We have proposed a novel approach which uses sound signature to recall graphical password click points. No previously developed system used this approach this system is helpful when user is logging after a long time. In future systems other patterns may be used for recalling purpose like touch of smells, study shows that these patterns are very useful in recalling the associated objects like images or text.

REFERENCES

[1] Cranor, L.F., S. Garfinkel. Security and Usability. O'Reilly Media, 2005.
[2] Davis, D., F. Monrose, and M.K. Reiter. On User Choice in Graphical Password Schemes. 13th USENIX Security Symposium, 2004.
[3] R. N. Shepard, "Recognition memory for words, sentences, and pictures," Journal of Verbal Learning and Verbal Behavior, vol. 6, pp. 156-163, 1967.
4] A. Perrig and D. Song, "Hash Visualization: A New Technique to Improve Real-World Security," in Proceedings of the 1999 International Workshop on Cryptographic Techniques and E-Commerce, 1999.

AUTHOR PROFILES

[1] **Anu Singh** pursuing the bachelor degree in computer science from Pune University, in 2013.

[2] **Kiran Kshirsagar** pursuing the bachelor degree in computer science from Pune University, in 2013.

[3] **Lipti Pradhan** pursuing the bachelor degree in computer science from Pune University, in 2013.