Integration of Sound Signature in Graphical Password Authentication System

Saurabh Singh
Invertis University
Bareilly, India

Gaurav Agarwal
Invertis University
Bareilly, India

ABSTRACT
Here a graphical password system with a supportive sound signature to increase the remembrance of the password is discussed. 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. 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.

Keywords: Sound signature, Authentication

1. Introduction
Passwords are used for –

(a) Authentication (Establishes that the user is who they say they are).

(b) Authorization (The process used to decide if the authenticated person is allowed to access specific information or functions) and

(c) Access Control (Restriction of access-includes authentication & authorization).

Mostly user select password that is predictable. This happens with both graphical and text based passwords. Users tend to choose memorable password, unfortunately it means that the passwords tend to follow predictable patterns that are easier for attackers to guess. While the predictability problem can be solved by disallowing user choice and assigning passwords to users, this usually leads to usability issues since users cannot easily remember such random passwords. Number of graphical password systems have been developed, Study shows that text-based passwords suffers with both security and usability problems[1][8]. According to a recent news article, a security team at a company ran a network password cracker and within 30 seconds and they identified about 80% of the passwords [2]. It is well know that the human brain is better at recognizing and recalling images than text[3][7], graphical passwords exploit this human characteristic.

2. PREVIOUS WORK
Considerable work has been done in this area,The best known of these systems are Passfaces [4][7]. Brostoff and Sasse (2000) carried out an empirical study of Passfaces, which illustrates well how a graphical password recognition system typically operates. Blonder-style passwords are based on cued recall. A user clicks on several previously chosen locations in a single image to log in. As implemented by Passlogix Corporation (Boroditsky, 2002), the user chooses several predefined regions in an image as his or her password. To log in the user has to click on the same regions. The problem with this scheme is that the number of predefined regions is small, perhaps a few dozens in a picture. The password may have to be up to 12 clicks for adequate security, again tedious for the user. Another problem of this system is the need for the predefined regions to be readily identifiable. In effect, this requires artificial, cartoon-like images rather than complex, real-world scenes[5][6]. Cued Click Points (CCP) is a proposed alternative to PassPoints. In CCP, users click one point 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 hotspot analysis more challenging. As shown in Figure 1, each click results in showing a 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. 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.

3. PROPOSED WORK
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. Study says that sound signature or tone can be used to recall facts like images, text etc[6]. In daily life we see various examples of recalling an object by the sound related to that object [6]. Our idea is inspired by this novel human ability.

3.1. Profile Vectors-
The proposed system creates user profile as follows-

Master vector -

(User ID, Sound Signature frequency, Tolerance)

Detailed Vector - (Image, Click Points)

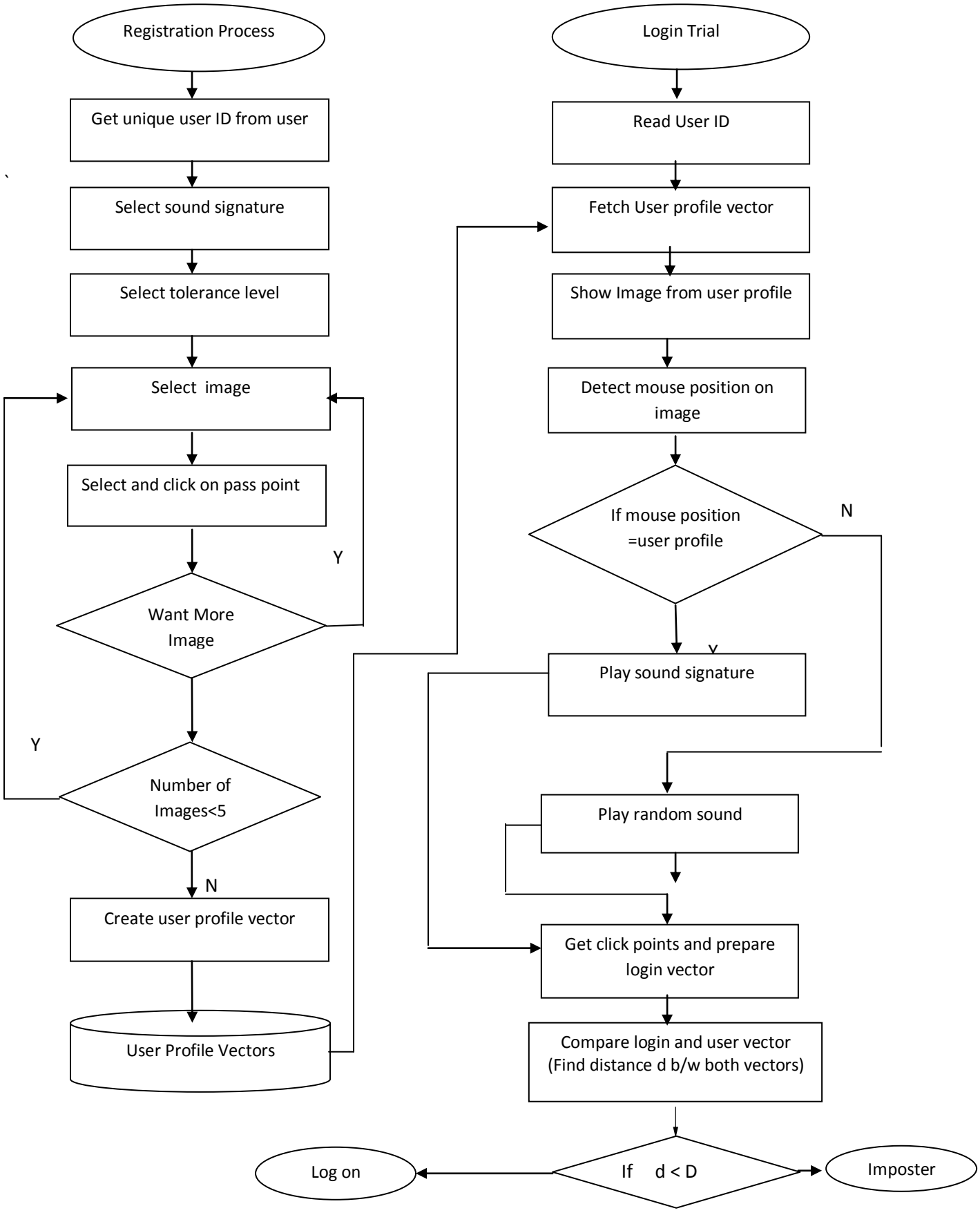
As an example of vectors -

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)

Figure 1. System Flow Chart



enters User ID and select one sound frequency which he want to be played at login time, a tolerance value is also selected with will decide that the user is legitimate or an imposter. To create detailed vector user has to select sequence of images and clicks on each image at click points of his choice. Profile vector is created.

No.	Login ID	Login Trails	Times Accepted	Times Rejected
1	U1	5	5	0
2	U2	5	4	1
3	U3	5	5	0
4	U4	5	5	0
5	U5	5	5	0
6	U6	5	3	2
7	U7	5	5	0
8	U8	5	5	0
9	U9	5	5	0
10	U10	5	4	1
11	U11	5	5	0
12	U12	5	5	0
13	U14	5	5	0
14	U14	5	5	0
15	U15	5	5	0
16	U16	5	5	0
17	U17	5	5	0
18	U18	5	5	0
19	U19	5	5	0
20	U20	5	5	0

Table 1. Attempts by legitimate users
(5 attempts per login ID)

3.3 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-

$$d(\mathbf{p},\mathbf{q}) = \sqrt{(p_1-q_1)^2+(p_2-q_2)^2+\cdots+(p_n-q_n)^2} = \sqrt{\sum_{i=1}^{n}(p_i-q_i)^2}.$$

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.

No.	Login ID	Login Trails	Times Accepted	Times Rejected
1	U1	5	0	5
2	U2	5	0	5
3	U3	5	0	5
4	U4	5	1	4
5	U5	5	0	5
6	U6	5	0	5
7	U7	5	0	5
8	U8	5	0	5
9	U9	5	0	5
10	U10	5	0	5
11	U11	5	1	4
12	U12	5	0	5
13	U14	5	0	5
14	U14	5	0	5
15	U15	5	0	5
16	U16	5	0	5
17	U17	5	0	5
18	U18	5	0	5
19	U19	5	0	5
20	U20	5	0	5

Table 2. Attempts by Imposters (5 attempts per login ID by randomly selected imposters)

4. EXPERIMENTAL RESULTS

Data collected from 20 participants. Each participant was asked to register himself/herself and then each was invited to for login trail 5 times as legitimate user and 5 times as impostor randomly. Participants were final year engineering students of age group 20-28 Y. Table 1 shows the detail of the data generated by legitimate users and Table 2 contains the data generated by imposters. According to the data generated FRR is 4.0 and FAR is 2.0 which are very good for Graphical password authentication system.

5. 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.

6. REFERANCES

[1] Birget, J.C., D. Hong, and N. Memon. Graphical Passwords Based on Robust Discretization. IEEE Trans. Info. Forensics and Security, 1(3), September 2006.

[2] Blonder, G.E. Graphical Passwords. United States Patent 5,559,961, 1996.

[3] Chiasson, S., R. Biddle, R., and P.C. van Oorschot. A Second Look at the Usability of Click-based Graphical Passwords. ACM SOUPS, 2007.

[4] Cranor, L.F., S. Garfinkel. Security and Usability. O'Reilly Media, 2005.

[5] Davis, D., F. Monrose, and M.K. Reiter. On User Choice in Graphical Password Schemes. 13th USENIX Security Symposium, 2004.

[6] R. N. Shepard, "Recognition memory for words, sentences, and pictures," Journal of Verbal Learning and Verbal Behavior, vol. 6, pp. 156-163, 1967.

[7] 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.

[9] D. Weinshall and S. Kirkpatrick, "Passwords You'll Never Forget, but Can't Recall," in Proceedings of Conference on Human Factors in Computing Systems (CHI). Vienna, Austria: ACM, 2004, pp. 1399-1402.