

A New System of Integrating Sound Signature in Graphical Password Authentication

Anita Rout ^{#1}, Mogali Madhu Babu ^{*2}

^{1#} M.Tech Scholar, ^{2*} Assistant Professor
Department of Computer Science & Engineering,
Gokul Institute of Technology and Science Engineering College,
Bobbili ,Andhra Pradesh,India.

Abstract

Graphical passwords (GP's) are the password which consists mainly of click or drag activities on the pictures or images rather than typing textual characters on it. So with this new type of authenticated passwords, it is the new option to overcome the problems that arise while using text-based passwords system. In this paper, we propose a new click-based graphical password system called Cued Click Points (CCP), where a password consists of collective sequence of some different images in which user can select at a time one click-point per individual image, this will be continued for about selecting five different click points from five different images. Along with this procedure ,the user is also asked to select a sound signature corresponding to each click point as this sound signature will be used for an user in recalling the click point on an image whenever he/she forget that clicks on a image. The proposed new system clearly tells us that it has very good performance in terms of speed, accuracy, integrity and ease of use. Users after their lot of research work preferred CCP to Pass Points, saying that by selecting and able to remember only one point per image was easier and sound signature also helps mostly in recalling the click points when needed.

Keywords

Sound Signature, Authentication, Human Factors, Textual Passwords, Graphical Passwords.

1. Introduction

Human factors are very often considered as the weakest relation link in a computer security system. As per the research work ,it clearly tells that there was mainly three important areas where human computer interaction is important. They are as follows

- 1) Authentication,
- 2) Security Operations, and
- 3) Developing secure systems.

In the field of information security (IS) the primary element for any user is nothing but authentication of user. For a vast majority of users, to provide authentication for their computer systems, password based authentication is the best choice. Authentication is the process of allowing /accepting or denying/restricting access to an individual's who claim with their identity. Authentication process asks users to memorize/remember the valid login passwords and recall them during log-in time process.

Most of the users select text based passwords for authentication of their computer systems which was maximum predictable in nature. This also happens with graphical password authentication process also. Users each and every time try to choose rememberable password which are mostly memorable and easy to remember, unfortunately this is the easy way where hackers are easily attacking the systems by breaking the predictable passwords. While this predictability problem can be solved by not allowing users choice

of giving his/her own passwords. This was replaced now a days by assigning passwords to users automatically by the system, this usually leads to usability issues since users cannot easily remember such random passwords. As the passwords which was given by system is mostly generated in random fashion it is not easy for the end users or attackers to remember or identify those random passwords, so this leads some level of security against attackers.

Till to date several number of graphical password systems has been developed. But our research study shows that text-based passwords suffer with both security problem and usability problems [1], [2]. According to a recent news channel article , a security team at a MNC company ran a network password cracker and within 30 seconds and they identified about 80% of the passwords [3]. It is well know principle to all of us, that the human brain is better at recognizing and recalling images than text [4], [5], graphical passwords exploit this human characteristic.

Passwords are majorly used for:

- (a) **Authentication** (Establishes that the user is who they say they are).
- (b) **Authorization** (This process used to decide if the authenticated person is allowed to access specific information or functions) and
- (c) **Access Control** (Providing restriction of access-includes authentication & authorization).

2. Related Work

There was a tremendous research work has been under gone in this password authentication process, among them the best known research work systems are Passfaces [8], [5]. Brostoff and Sasse (2000) where they carried out an empirical study of Passfaces, which clearly illustrates very well how a graphical password recognition system typically works and how they are well operated. Blonder-style passwords are also undergone with research work and they conclude that they were based on cued recall mechanism. In this effect, this process requires mainly artificial images, cartoon-like

images, easy to remember rather than complex images, real-world scenes [6], [7] which are hard to remember.

Cued Click Points (CCP) is a proposed alternative to Pass Points. In CCP, the users use the techniques in very different and new way when compared with existing graphical password methodology. Here in this new proposed technique users click one point on each of 5 individual images rather than like clicking on five points on one image. During this process, the attack that was based on hotspot analysis is also a more challenging task for this method implementation. Figure 1, clearly shows that each click results in showing a next-image, in effect leading users down a “path” as they click on their sequence of points until last point is reached in last image.

3. Proposed Work

In our current proposed work we have integrated sound signature into graphical password authentication method to help in recalling the password. As sound signature is also integrated in this authentication it gives utmost more security for the computer systems. In our daily life we will see various examples of recalling an object by the sound related to that object [7]. Our idea is inspired by this novel human ability.

3.1. User Profile Vectors

The Proposed System initially creates user profile in the form of vectors as follows

Master vector

The master vector values of user image are taken as follow, they are three parameters

(User ID, Sound Signature frequency, Tolerance)

3.2 Detailed Vector

Based on the master vector data, the detailed vector with the following parameters is converted and displayed as

(Image, Click Points)

As an example of vectors

Master vector (Smith, 2689, 50)

Detailed Vector for the user Profile is

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

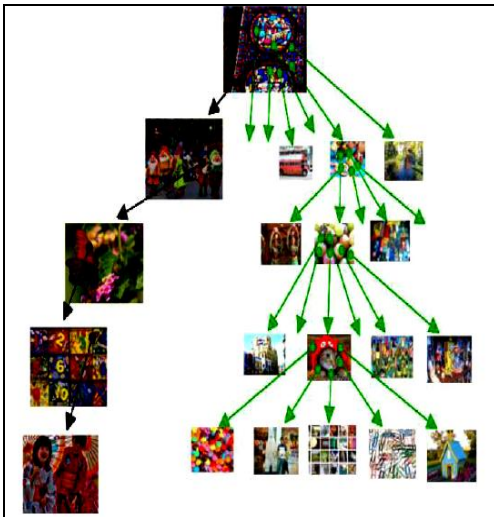


Fig. 1 each click point in the same image leads to different next image

4. Implementation Modules

The implementation of this paper has mainly four modules:

- 1) Create User profile Vector (master)
- 2) Create Detailed Vector
- 3) Compare User Profile/login Vector

4) Upload/Download Module

1) Create User Profile Vector (Master):

In this module, we mainly discuss creating of Master Vector, for that while registration of user information, the user id, sound frequency or time and tolerance are needed for generating.

Master vector – (User ID, Sound Signature frequency, Tolerance).

2) Create Detailed Vector:

In this module for creating a detailed vector user has to select sequence of images and clicks on each image at click points of his choice. Profile vector is created.

Detailed Vector - (Image, Click Points)

3) Compare User Profile/login Vector:

In this module user enters User ID and select one sound frequency or time 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. Users preferred CCP to Pass Points, saying that selecting and remembering only one point per image and sound signature helps considerably for login.

4) Upload / Download Module:

This module is mainly used for admin, defence, navy and air force are going to upload secret file between them. They can share the uploaded files. User (defence, air force and navy) uses sound signature for download files. System showed very good Performance in terms of speed, accuracy, and ease of use

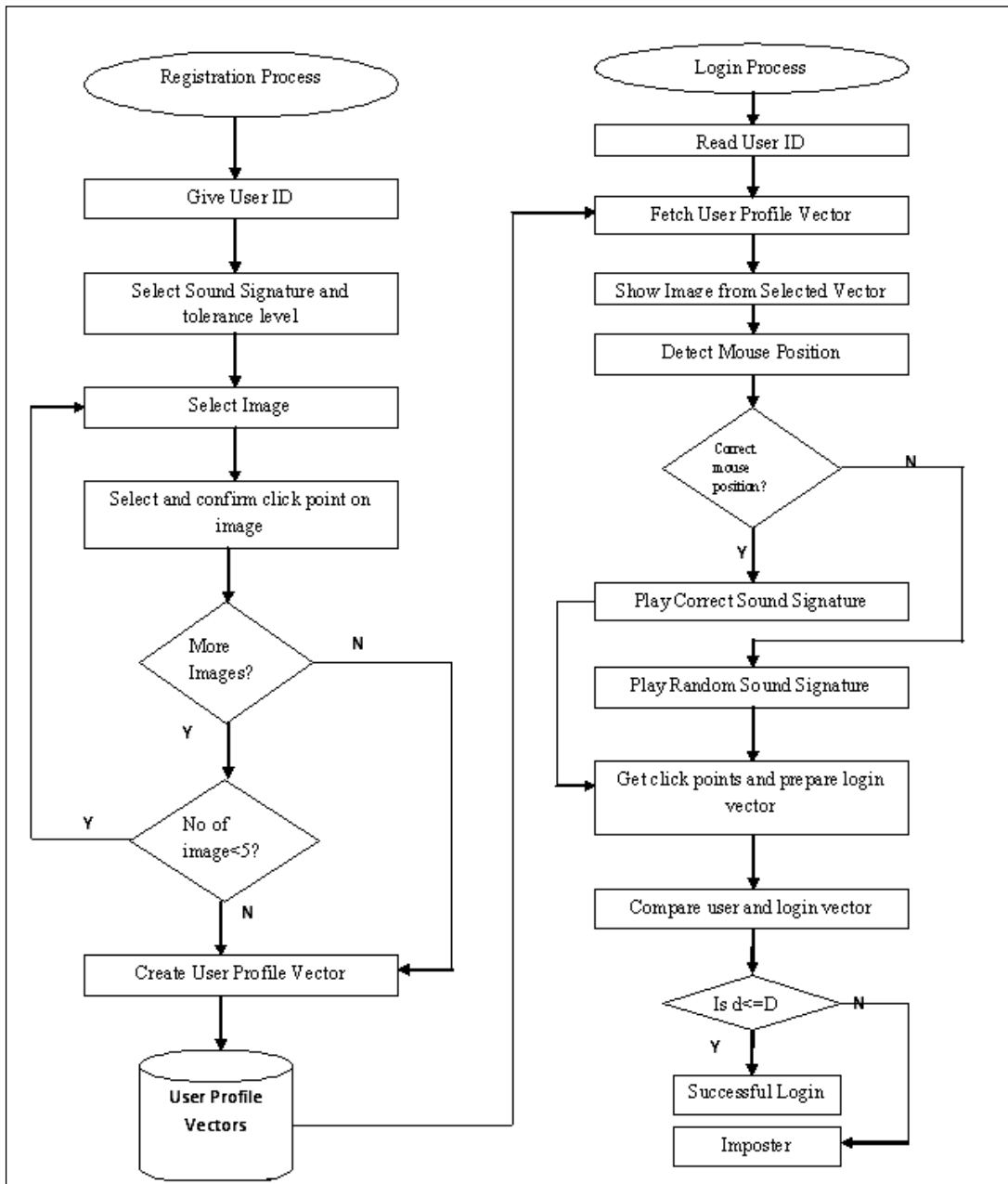


Fig. 2. System Flow Chart

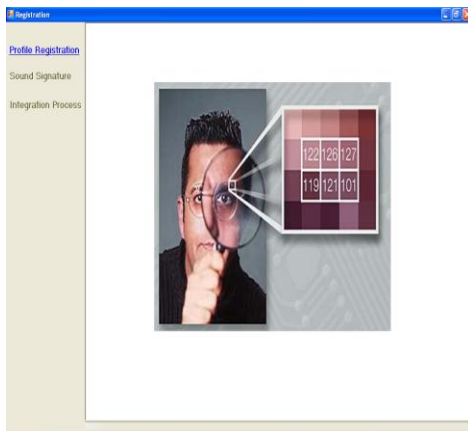
5. Experimental Results

The following are the user interfaces that are designed in .Net technology for implementing this proposed concept in this paper.

i) Login Form



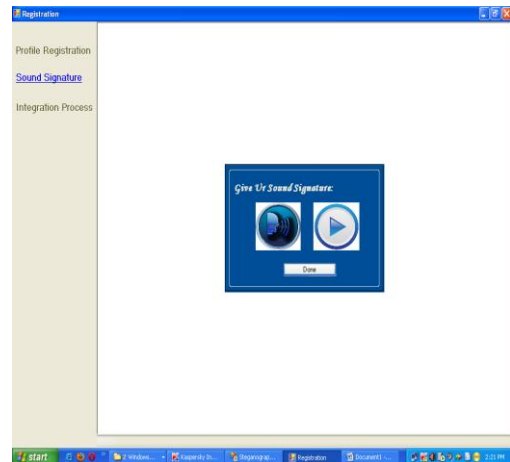
ii) Registration Form



iii) Profile Registration Form



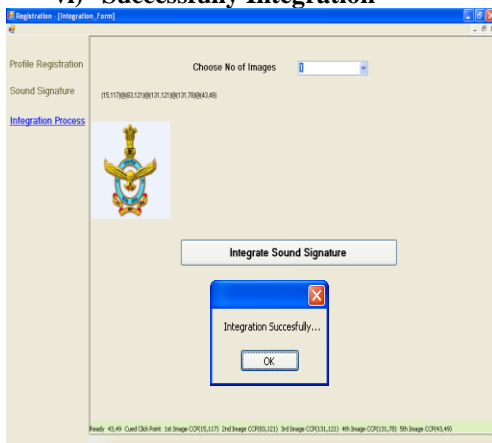
iv) Sound Signature



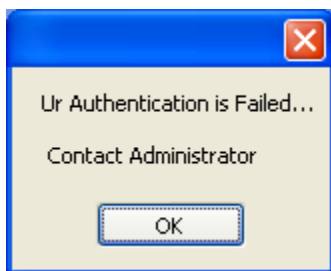
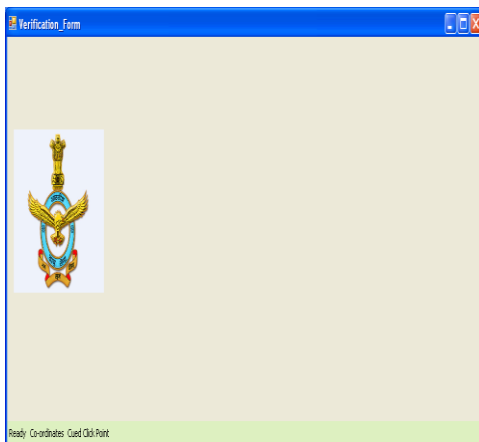
v) Integrating Sound Signature



vi) Successfully Integration



vii) Verification Authentication



6. Conclusion

In this paper, we have proposed a novel authentication approach for password authentication which uses sound signature to recall graphical password click points. Till today, there was no implementation of such a kind of system which is helpful for any user who is logging after a long time.

7. References

- [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] 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.
- [3] Blonder, G.E. Graphical Passwords. United States Patent 5,559,961, 1996.
- [4] Chiasson, S., R. Biddle, R., and P.C. van Oorschot. A Second Look at the Usability of Click-based Graphical Passwords. *ACM SOUPS*, 2007.
- [5] 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.
- [6] Davis, D., F. Monrose, and M.K. Reiter. On User Choice in Graphical Password Schemes. *13th USENIX Security Symposium*, 2004.
- [7] R. N. Shepard, "Recognition memory for words, sentences, and pictures," *Journal of Verbal Learning and Verbal Behavior*, vol. 6, pp. 156-163, 1967.
- [8] Cranor, L.F., S. Garfinkel. *Security and Usability*. O'Reilly Media, 2005.

8. About the Authors



Anita Rout is currently pursuing her M.Tech in Computer Science and Engineering at Gokul Institute of Technology and Science Engineering College Bobbili. Her area of interests includes Image Processing, Networks.



Mogali Madhu Babu is currently working as an Assistant Professor in Computer Science and Engineering department, Gokul Institute of Technology and Science Engineering College Bobbili. His area of interests include Networks, Data Mining, Image Processing