# IMPLEMENTATION OF HYBRID AUTHENTICATION SYSTEM BASED ON SOUND SIGNATURE AND GRAPHICS FOR USER AUTHENTICATION

Thamraj N. Ghorsad[(1)], R. S. Pippal[(2)], Badri Prasad Patel[(3)]
M.Tech[(1)],Head, Department of C.S.E[(2)],Asst. Prof. Department of CSE[(3)]
RadharamanEngg.College. Bhopal, India (M.P.)[(1,2,3)]
raj.ghorsad@gmail.com[(1)],patel.rec@gmail.com[(3)]

***ABSTRACT****-Current authentication system commonly used Textual password. Users tend to choose their nick names, which make textual passwords easy to break. Many available graphical passwords have a password space that is less than or equal to the textual password space. In this Paper a graphical password system with a supportive sound signature to increase the remembrance of the password is discussed.*
*In this Paper a click-based graphical password scheme called Cued Click Points (CCP) is presented. This system password consist sequence of some images in which user can select one click-point of an 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, Tolerance, Graphical Images.

## 1. INTRODUCTION

The most common method used for authentication is textual password. But the main vulnerabilities is the difficulty of remembering those passwords. Studies have shown that users tend to pick short passwords or passwords that are easy to remember. Unfortunately, these passwords can be easily guessed or cracked. To eliminate these weaknesses, traditional alphanumeric passwords can be replaced by new graphical authentication systems, which can vary depending on the action the user is to perform. These systems can involve users:
a. identifying one or more images out of a group. b. Touching points of an image.
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). It is well know that the human brain is better at recognizing and recalling images than text, graphical passwords exploit this human characteristic we have use this following schemes for better Security purpose in Authentication.

### 1.1 Graphical Authentication

In this scheme, we use images for Authentication. When register the new user, first select the one image from given images and then click any four points that is pixel values in sequence which stored in System Database. When user log's in, first select the proper image and click points in same sequence then system

checks that image and click points are same or not. If incorrect then give the error and if it is correct then give permission for next authentication scheme.

### 1.2 Sound Signature

In this scheme, we use sound clips for Authentication. When register the new user, select one sound clip and play that clip then stored its pause time in System Database.

## 2. PROBLEM STATEMENT

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 system has been developed; Study shows that text-based passwords suffer with both security and usability problems. According toa 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.

It is well know that the human brain is better at recognizing and recalling images than text, graphical passwords exploit this human characteristic.

This dissertation uses images for Authentication. When register the new user, first select the one image from given images and then click any four points that is pixel values in sequence which stored in System Database, When user log's in, first select the proper image and click points in same sequence then system checks that image and click points are same or not. If incorrect then give the error and if it is correct then give permission for next authentication scheme.

## 3. SYSTEM DESIGN

### 3.1 Existing System:

In the existing system**,** Brostoff and sasse 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, 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 in effect, cued click points (ccp) is a proposed alternative to pass points.

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. 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.

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 has been developed; Study shows that text-based passwords suffer with both security and usability problems.

### 3.2 Disadvantages:

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.

### 3.3 Proposed System:

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. In daily life we see various examples of recalling an object by the sound related to that object 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.

**a. 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 (Raj, 5436, 25)

Detailed Vector

| Image | Click points |
|---|---|
| I 1 | (120,520) |
| I 2 | (121,521) |
| I 3 | (122,522) |
| I4 | (123,523) |
| I5 | (129,584) |

**b. System Flow Chart**

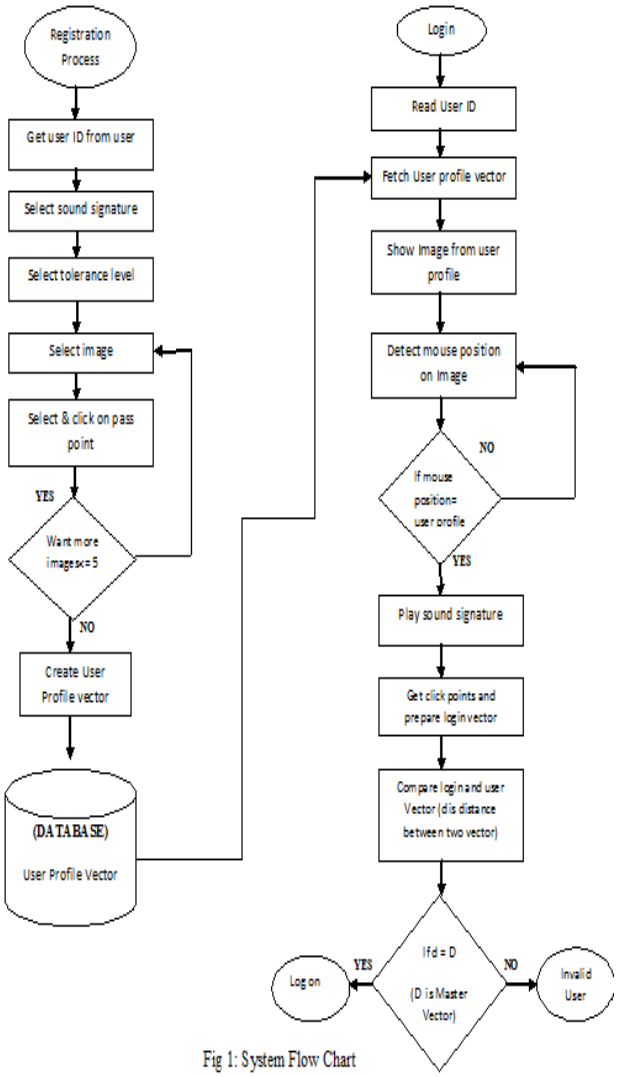



Fig 1: System Flow Chart

## c. Working

**Registration**

1. When new user register, first enter the all details which give in registration form.
2. Then select any one image from multiple images
   and also click the points.
3. Then select any one sound clip, play and pause that clip at particular time.
4. This all interactions stored in database.

## ➢ Authentication

1. Enter username and password.
2. Select proper image and their sequence of click


*ISSN: 2229-6913 (Print), ISSN: 2320-0332 (Online) -, Web Presence: http://www.ijoes.vidyapublications.com*

points.

3. Select proper sound clip and their pause time.
4. All interactions fetch from database then compared

one by one.
Then access granted to authorize user for access
applications.

## 4. EXPERIMENTAL RESULTS

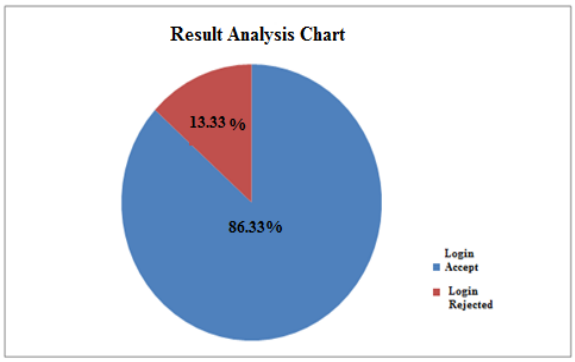
We conducted the result analysis of the proposed technique with 15 participants from engineering students for login trials. As the techniques are new, first the participants were briefed about the techniques. They were given demonstration for better understanding purpose. Then each user was requested to login. After that the usability study was conducted with the students and results the following.

Users reproduce their passwords, without having the chance to use thereminder marks of system. Although easy and convenient, it appears that users do notquite remember their passwords. Following are some of the algorithms which werecreated based on this technique.

| No. | Login ID | Login Trails | Times Accepted | Times Rejected |
|---|---|---|---|---|
| 1 | U1 | 5 | 5 | 0 |
| 2 | U2 | 5 | 5 | 0 |
| 3 | U3 | 5 | 5 | 0 |
| 4 | U4 | 5 | 4 | 1 |
| 5 | U5 | 5 | 5 | 0 |
| 6 | U6 | 5 | 5 | 0 |
| 7 | U7 | 5 | 5 | 0 |
| 8 | U8 | 5 | 5 | 0 |
| 9 | U9 | 5 | 5 | 0 |
| 10 | U10 | 5 | 5 | 0 |
| 11 | U11 | 5 | 4 | 1 |
| 12 | U12 | 5 | 5 | 0 |
| 13 | U14 | 5 | 5 | 0 |
| 14 | U16 | 5 | 5 | 0 |
| 15 | U17 | 5 | 5 | 0 |

Table 4.1: Frequency of Users opinions on system effectiveness.

It is observed that, as the user gets practiced over, he/she is able to login without any problem. Sound signature and session value will help the user to login for particular session.




Graph 4.1: Pie Chart Showingdesigns effectiveness

In the above Pie Chart We have seen that out of 100 percent 86.33% Logins are accepted and remaining 13.33% Logins are rejected So, blue portion will provide us the Login attempted region and red portion will provides us the login rejected portion.

## 5. COMPARISONS OF GRAPHICAL PASSWORD AUTHENTICATION SYSTEMS

### ❖ Comparisnos of alphanumeric password authentication systems and graphical password authentication systems

Alphanumerical username/passwords are the most common type of user authentication while graphical passwords are not much in use. But day by day the use of graphical password is increasing. Alphanumeric passwords are easy to implement and use and also graphical passwords are easy to implement and use. The requirement of the alphanumeric passwords is that they should be easily remembered by a user, while they should be hard to guess by fraudulent person [2]. These both requirements are for graphical passwords too and it gets satisfied as remembering images are much easier than remembering textual passwords. If short passwords are used then they are easily guessable and are target of dictionary and brute-forced attacks [3, 4, and 5]. Whereas if strong passwords are enforced a policy sometimes leads to an opposite effect, as a user may write his or her difficult-to-remember passwords on notes or on the notepad and if seen by some other user exposes it to direct theft that is misuse can be done. Whereas is graphical passwords are used these all problems do not arise.

### ❖ Comparison of OTP systems and graphical password authentication systems

The first and foremost advantage of OTP is that the user doesn't need to remember the password it is directly sent to the user to his / her mobile or email, while the graphical passwords are required to be remembered though remembering them is easy because human brains can easily remember images. But the OTP password is provided by token devices andthese token devices are very expensive. While providing graphical passwords is not expensive and doesn't need any device for generation.

### ❖ Comparison of Cued Click Points (CCP) and Cued Click Points with sound signature

In CCP password consists of one click-point per image. That is in the CCP technique the users are required to remember only one point in one image. The images are stored in the database as in the earlier methods too. This is done for a sequence of images. That is the user has to do the selection in sequential order only that is in the same order in which he or she did during registration. The next image is displayed only when the user clicks on the click point of previous image correctly. So the users receive immediate

implicit feedback whether they are on the correct track or not when logging in. So the Cued Click Points technique not only improves usability but also security.

Previously we have seen different graphical authentication techniques. In CCP we just used to click one point in one image and this is done for number of images as discussed previously. But in the CCP with sound signature we also have go select sound as a signature as this will provide the user with better authentication. The sounds of different birds or animal or the user's preferable sound will be stored in the database. Then when the user chooses the points in each image after this the user is asked to select the 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. That is here a graphical password system with a supportive sound signature helps to increase the remembrance of the password is designed. Very good performance has been shown by the system in terms of ease of use, speed and accuracy.

The observation for this method was that selecting and remembering only one point per image is much simpler or easier. Moreover seeing each image triggers the user's memory of where the corresponding point was located.higher security than PassPoints as the number of images increases the workload for attackers [14]. 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) [13].

Users preferred CCP as compared to Pass Points, as remembering only one point per image was easier and sound signature helped them considerably in recalling the click points [19]. And if the system has been integrated with sound signature it helps in recalling the password. It has been said that sound signature or tone can be used to recall facts like images, text etc [19, 20]. In daily life we see various examples of recalling an object by the sound related to that object [19, 20].

## 6. ACKNOWLEDGMENTS

We would like to express our appreciation to our parents and all the teachers and lecturers who helped us to understand the importance of knowledge and show us the best way to gain it.

## 7. CONCLUSION AND FUTURE WORK

Proposed scheme 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.

## 8. REFERENCES

[1] R. Dhamija, and A. Perrig. "Déjà Vu: A User Study Using Images for Authentication". In 9th USENIX Security Symposium, 2000.

[2]. X. Suo, Y. Zhu, and G. S. Owen, "Graphical passwords: A survey," in Proc. 21st Annu. Comput. Security Appl. Conf., pp. 463–472, Dec. 5–9, 2005.

[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.
[10] W. Jansen, "Authenticating Users on Handheld Devices "in *Proceedings of Canadian InformationTechnology Security Symposium*, 2003.
[11] J. Goldberg, J. Hagman, V. Sazawal, "Doodling Our Way To Better Authentication", CHI '02extended abstracts on Human Factors in Computer Systems, 2002.
[12] H. Zhao and X. Li, "S3PAS: A Scalable Shoulder-Surfing Resistant Textual-Graphical PasswordAuthentication Scheme," in *21st International Conference on Advanced Information Networking andApplications Workshops (AINAW 07)*, vol. 2. Canada, 2007, pp. 467-472.
[13] S. Man, D. Hong, and M. Mathews, "A shoulder surfing resistant graphical password scheme," in*Proceedings of International conference on security and management*. Las Vegas, NV, 2003.
[14] Z. Zheng, X. Liu, L. Yin, Z. Liu "A Hybrid password authentication scheme based on shape andtext" Journal of Computers, vol.5, no.5 May 2010.