Integration of Sound Signature Authentication System

Bagrudeen Bazeer Ahamed[1] and Shanmugasundaram Hariharan[2]

*[1]Department of Information Technology,
Pavendar Bharathidasan College of Eng'g. & Tech.
[2]Department of Computer Science & Eng'g., T.R.P Engg.College*

*Tiruchirapalli, Tamil Nadu, S. India
bazeerahamed@gmail.com, mailtos.hariharan@gmail.com*

Abstract

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. Numbers of graphical password systems have been developed; Study shows that text-based passwords suffer with both security and usability problems. 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. It is well know that the human brain is better at recognizing and recalling images than text, graphical passwords exploit this human characteristic. We proposed a sound signature graphical password consists of user-chosen click points in a displayed image. In order to store passwords in cryptographically hashed form, we need to prevent small uncertainties in the click points from having any effect on the password. We achieve this by introducing a robust discrimination, based on multigrid discrimination.

Keywords: *Sound signature, Authentication, Human Factors*

1. Introduction

The image-handling component enables users to choose images or to introduce their own; the images are stored together with a collection of images provided by the system. For this password system to work well, it is important that the images be fairly intricate, with hundreds of interesting details that could be chosen as click regions (e.g., topographic maps, architectural images, cityscapes, certain landscapes, and renaissance paintings)[5]. The password selection component allows the user to select a new password. Assuming the user has already logged in (by using either a graphical or a conventional password), the user enters the "password" command. The system then prompts the user for a user name and current password. If the system accepts the current password, it lets the user specify a new image (or keep the current image), and set the safety parameter r for robust discrimination (or keep a default value).

The graphical password schemes we considered in this study have the property that the space of passwords can be exhaustively searched in short order if an offline search is possible [2]. So, any use of these schemes requires that guesses be mediated and confirmed by a trusted online system. In such scenarios, we believe that our study is the first to quantify factors relevant to the security of user-chosen graphical passwords. In particular, our study advises against the use of a Pass faces TM-like system that permits user choice of the password, without some means to mitigate the dramatic effects of attraction and race that our study quantifies [6]. As already demonstrated, for certain populations of users, no imposed limit on the number of incorrect password guesses would suffice to render the system adequately secure since, e.g., 10% of the passwords of males could have been guessed by merely two guesses [16].

A “zero-knowledge” approach of never showing a picture group twice gives immunity from eavesdropping, but separate tests showed that when groups were reused, the subjects’ accuracy improved [11]. They did not confuse the destructors with the images on which they had been trained, and thus could use our methods for longer times without the need for retraining.

A sound signature recognitions password system is introduced, as from the existing relationship system, we incorporated sound signature by clicking the image a beep sound is introduced, the same sound is produced in all the images, if we proceed the same click point in all the images with similar sound then the authentication proceeded to the login page, there we can read out the important messages [8].

The click-point fails in any relating images and sound or if we failed to click exactly, then it will not transmit to the login session. The mail advantage of this proposed system is to enhance authentication process in a high reliable one for the end users.

2. Related Work

2.1. Graphical Password Recognition System

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 [13]. 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 [14]. Each click results in showing a next-image, in Effect leading users down a “path” as they click on their sequence of points [1]. 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 [7]. Number of graphical password systems have been developed, Study shows that text-based passwords suffers with both security and usability problems.

2.2. Click-Based Graphical Passwords

The lab study confirmed earlier work that the usability of these passwords was good in terms of success rates and password-entry times and that participants’ opinions were favorable [12]. We additionally showed that participants were more accurate in targeting their click-points than previously suggested; indicating that smaller tolerance squares may be acceptable [8]. Finally, contrary to previous work, we found that the choice of image significantly influenced success rates. The field study represented the first large-scale, real-world study of click-based graphical passwords, showing that graphical passwords were adequate in terms of usability for real tasks. Password entry times were acceptable, accuracy was not quite as high as in-lab but still very good, and success rates improved with practice although they never reached those seen in lab.

3. Problem Definition

The problem with this existing 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 the existing system is the need for the predefined regions to be readily identifiable.

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.

4. Methodology

Practice, Password Generation, and Retention, as shown in Table 1. First, participants completed a Practice phase with two trials. For each trial, they created, confirmed, and logged in with one password [11].

This phase was used to explain the process and familiarize participants with the user interface. During Practice phase, participants were told that they did not need to remember their practice passwords and would not be asked about them again.

Our specific hypotheses with respect to multiple password interference were:

1. Participants will have lower recall success rates with sound passwords than with Pass-Points passwords.
2. Participants in the sound condition are more likely than Pass-Points participants to use patterns across their own passwords.
3. Participants will recall sound passwords more slowly than Pass -Points passwords.
4. Participants in the sound condition are more likely than Pass-Points participants to create passwords that are directly related to their corresponding accounts.
5. Participants in the sound condition will make more recall errors than participants in the Pass-Points condition.

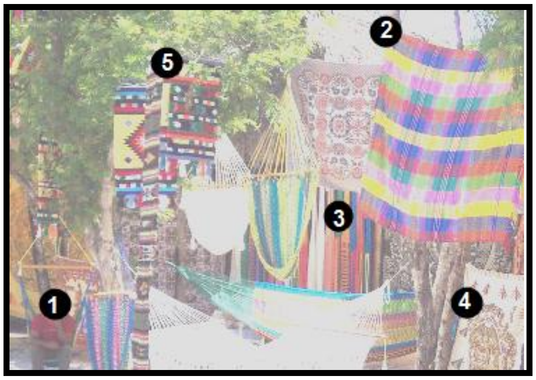
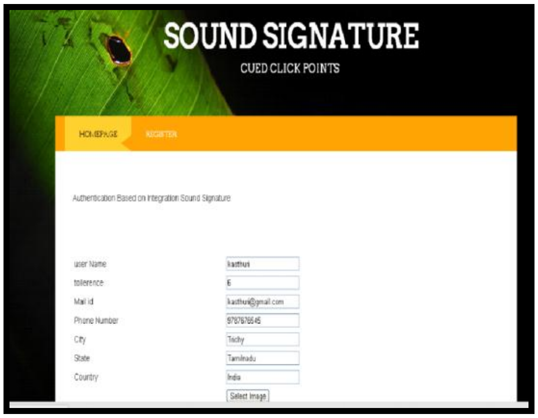


Figure 1. Pass-point Password Consists of 5 Ordered Click-points

5. Experimental Results & Analysis

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.



Authentication Based on Integration Sound Signature

user Name	kasthuri
tolerence	6
Mail id	kasthuri@gmail.com
Phone Number	9787676545
City	Trichy
State	Tamilnadu
Country	India

Figure 2. Registered Tolerance Sound Sign Login Process

Study says that sound signature or tone can be used to recall facts like images, text etc. [1]. 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 [14]. Profile vector is created.

Enters User ID and select one sound frequency which he wants 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.

The system creates user profile as follows-

Table 1. Attempts by Legitimate Users (5 attempts per LOGIN ID)

Sl.No.	Login ID	Login Trail	Accepted	Rejected
1	U1	5	4	1
2	U2	5	5	0
3	U3	5	3	2
4	U4	5	4	1
5	U5	5	5	0

6. 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-

$$d(p,q) = \sqrt{(p_1 - q_1)^2 + (p_2 - q_2)^2 + \cdots + (p_n - q_n)^2}$$

Above distance is calculated for each image if this distance comes out less than a tolerance value D[15]. The value of D is decided according to the application. In our system this value is selected by the user

$$\sqrt{\sum_{i=1}^{n}(p_i - q_i)^2}.$$

Master vector - (User ID, Sound Signature frequency, Tolerance)

Detailed Vector - (Image, Click Points)

As an example of vectors –

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

Sl.No	Login ID	Login Trail	Accepted	Rejected
1	U1	5	0	5
2	U2	5	0	5
3	U3	5	4	1
4	U4	5	0	5
5	U5	5	5	0

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)

```
</head>
<body>
<formname="pointform" method="post">
<divid="pointer_div"onclick="point_it(event)"style="background-
image:url('sun.jpg');width:500px;height:333px;">
<imgsrc="13.gif"id="cross" style="position:relative;z-index:2;"></div>
You pointed on x = <input type="text" name="form_x" size="4" /> - y = <input
type="text" name="form_y" size="4" />
```

Figure 3. Click-point Source Code

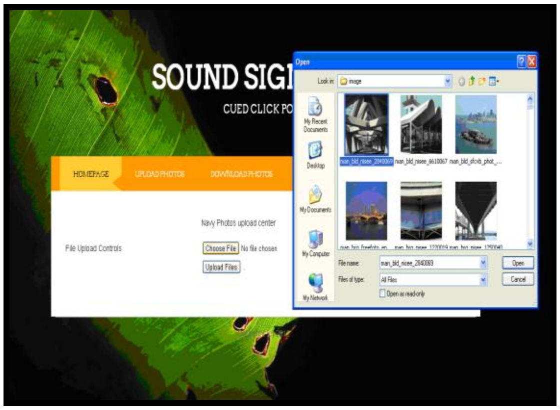


Figure 4. User Uploading the Images for Sound Verification

The benefit for the above system study is

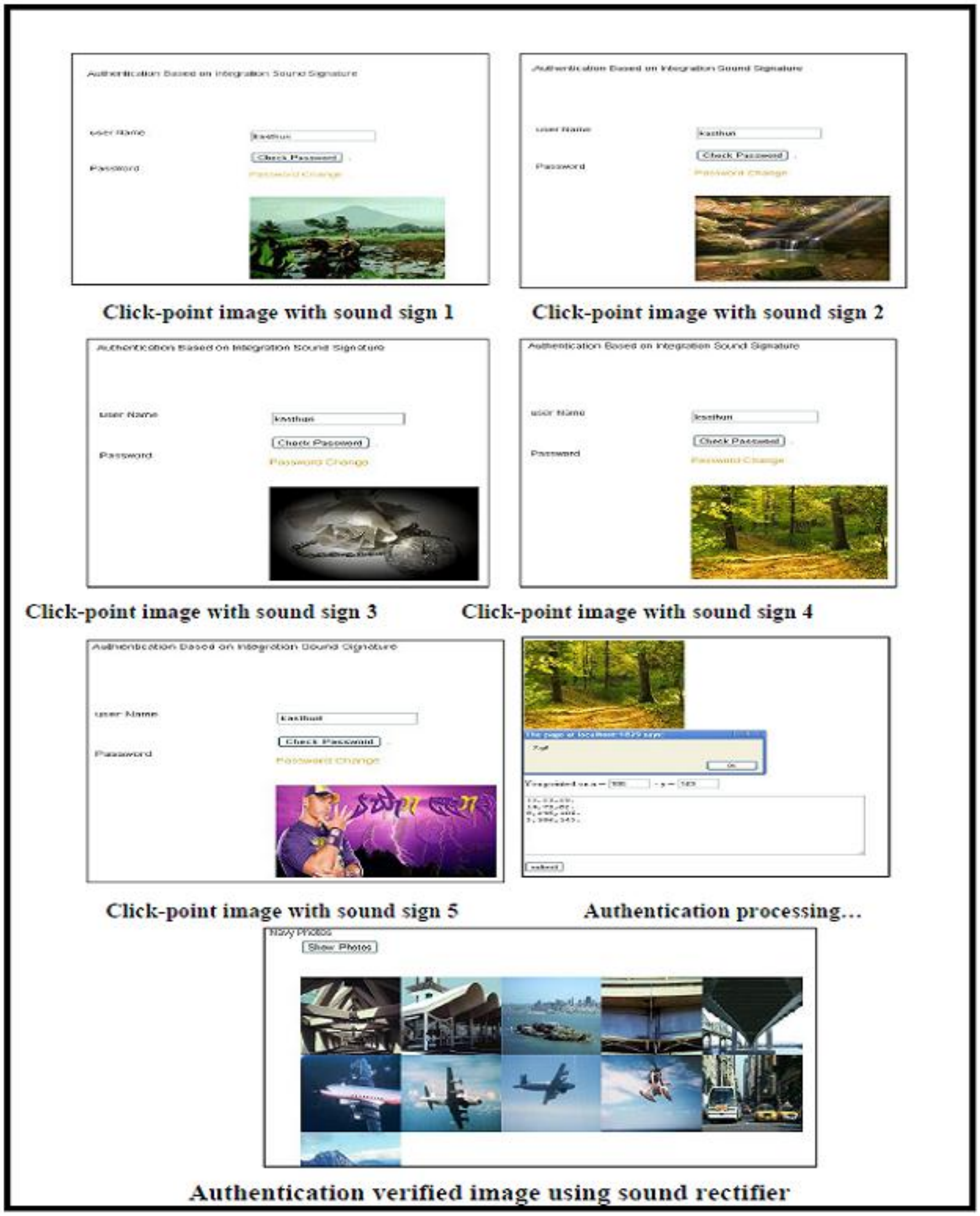
- The sound signature will be used to help the user to login.
- The System also has a very good Performance in terms of speed, accuracy, and ease of use.

Recognition: (also known as cognometric [10] or searchmetric [9]) Users recognize and identify images from a previously memorized portfolio from a larger set of decoy images. Example systems include PassFaces [9] and D ́ej`a Vu [12].

Cued-recall: (also known as locimetric [10]) Users identify and target previously selected locations within one or more images. The images act as memory cues to help recall these locations. Example systems include PassPoints [30] and Persuasive Cued Click-Points [5].

Other approaches to authentication are token-based systems and biometrics. While applicable in some cases, these have potential drawbacks, such as risks of loss, and privacy implications [11]. Password managers have also been proposed, but usability issues and the dangers of centralization remain unsolved problems [7].

In cued-recall click-based graphical passwords [4, 30], passwords consist of clicking on specific locations on one or more images. To log in, the user must click on these previously selected locations. The user is not expected to repeat exact pixel selections. In most systems, an invisible tolerance square is defined around each click-point so that any of the enclosed pixels are considered acceptable. Alternatively, a grid may be visible to users [3] recalling the click points.



Click-point image with sound sign 1

Click-point image with sound sign 2

Click-point image with sound sign 3

Click-point image with sound sign 4

Click-point image with sound sign 5

Authentication processing…

Authentication verified image using sound rectifier

Figure 5. Recognition of Sound by Clicking the Image

7. Conclusion & Future Enhancement

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, . 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] S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy and N. Memon, “PassPoints: Design and longitudinal valuation of a graphical password system”, International Journal of Human-Computer Studies, vol. 63, **(2005)**, pp. 102-127.

[2] D. Weinshall, “Cognitive Authentication Schemes Safe against Spyware”, (Short Paper), IEEE Symposium on Security and Privacy, **(2006)**.

[3] G. E. Blonder, “Graphical Passwords”, United States Patent 5,559,961, **(1996)**.

[4] D. Davis, F. Monrose and M. K. Reiter, “On User Choice in Graphical Password Schemes”, 13th USENIX Security Symposium, **(2004)**.

[4] J. C. Birget, D. Hong and N. Memon, “Graphical Passwords Based on Robust Discretization”, IEEE Trans. Info., Forensics and Security, vol. 1, no. 3, **(2006)** September.

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

[6] L. F. Cranor and S. Garfinkel, “Security and Usability”, O’Reilly Media, **(2005)**.

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

[8] 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] X. Suo, Y. Zhu and G. S. Owen, “Graphical Passwords: A Survey”, Annual Computer Security Applications Conference, **(2005)**.

[11] F. Tari, A. A. Ozok and S. H. Holden, “A Comparison of Perceived and Real Shoulder-surfing Risks between Alphanumeric and Graphical Passwords”, ACM SOUPS, **(2006)**.

[12] J. Thorpe and P. C. van Oorschot, “Human-Seeded Attacks and Exploiting Hotspots in Graphical Passwords”, 16th USENIX Security Symposium, Cued Click Points 17, **(2007)**.

[13] P. C. van Oorschot and S. Stubblebine, “On Countering Online Dictionary Attacks with Lgin Histories and Humans-in-the-Loop”, ACM Trans. Information and System Security, vol. 9, no. 3, **(2006)**, pp. 235-258.

[14] D. Weinshall, “Cognitive Authentication Schemes Safe Against Spyware”, (Short Paper), IEEE Symposium on Security and Privacy, **(2006)**.

[15] S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy and N. Memon, “Pass Points: Design and longitudinal evaluation of a graphical password system”, International Journal of Human-Computer Studies, vol. 63, **(2005)**, pp. 102-127.

[16] J. Yan, A. Blackwell, R. Anderson and A. Grant, “Password Memorability and Security: Empirical Results”, IEEE Security & Privacy Magazine, vol. 2, no. 5.

Authors

B. Bazeer Ahamed received a Bachelor of Technology in Anna University, Chennai and Master in Computer Science in Anna University of Technology, Tiruchirapalli. He has six years of teaching experiences. At present he is working as Assistant Professor in IT department, Pavendar Bharathidasan College of Engineering and Technology, Trichirappalli-9. He has published more than Five research papers in the international journals and international conferences. His research interests include Data Mining,Web Mining, Software Engineering and distributed computing. His career plan is to continue the research in the Web Mining and Data Warehousing.

Dr. S. Hariharan received his B.E degree specialized in Computer Science and Engineering from Madurai Kammaraj University, Madurai, India in 2002, M.E degree specialized in the field of Computer Science and Engineering from Anna University, Chennai, India in 2004. He holds his Ph.D degree in the area of Information Retrieval from Anna University, Chennai, India. He is a member of IAENG, IACSIT, ISTE, CSTA and has 8 years of experience in teaching. Currently he is working as Associate Professor in Department of Computer Science and Engineering, TRP Engineering College, India. His research interests include Information Retrieval, Data mining, Opinion Mining, Web mining. He has to his credit several papers in referred journals and conferences. He also serves as editorial board member and as program committee member for several international journals and conferences.