ISSN: 2277-9655
(I2OR), Publication Impact Factor: 3.785

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

AUTHENTICATION OF GRAPHICAL PASSWORD SYSTEM BASED ON AUDIO SIGNATURE AND IMAGES

Latha.R*, M.Kavitha, B.Gayathri
Assistant Professor Department of MCA Vel Tech High Tech Dr.Rangarajan Dr.Sakunthala Engineering College, Avadi, Chennai-62.
PG Scholar Department of MCA Vel Tech High Tech Dr.Rangarajan Dr.Sakunthala Engineering College, Avadi, Chennai-62.
PG Scholar Department of MCA Vel Tech High Tech Dr.Rangarajan Dr.Sakunthala Engineering College, Avadi, Chennai-62.

DOI: 10.5281/zenodo.48317

ABSTRACT

Cyber-attacks as amplified at an incredible rate in the preceding decade. Due to this inclined data like Bank financial credit details, login details of the accounts are not protected. Thus to argue against this we need a forceful authentication technique.

In recent years different types of high-speed authentication systems are previously being urban such as token based, biometrics system, captcha etc. Each of the alive methods has their own intrinsic worth and demerits. So in this paper we proposed a new model for the authentication using integration of sound and image based password system. This system is difficult to satire and the safety measures principles cannot be breached easily.

KEYWORDS: Sound Signatures, Authentication, Images.

.

INTRODUCTION

Passwords are used for:-
(a) Validation (Establishes that the client is who they declare they are).
(b)Sanction (The process used to decide if the legitimate person is allowed to access specific in turn or functions) and,
(c) Access Control (Restraint of access-includes validation & sanction).

Mostly user select secret word that is humdrum. This happens with equally graphical and wording based passwords.

Users have a propensity to choose excellent password, regrettably it resources that the passwords have a propensity to follow mind-numbing patterns that are easier for attackers to presumption.

While the expectedness trouble can be solved by disallowing user pick and conveying passwords to users, this usually leads to usability matters while users cannot easily remember such unsystematic passwords.

Number of graphical password organism have been urban, learning shows that text-based passwords endures with both safekeeping and usability tribulations [3][6].

According to a recent news article, a security team at a company ran a set-up password cracker and within 30 seconds and they notorious about 80% of the passwords [1].

It is well know that the individual brain power is better at be acquainted with and recalling images than text [2][7],graphical passwords take advantage of this human point.

In this authentication is the development of seminal whether a user should be allow to access on meticulous system or resource .where us you cannot remember strong password easily .

The task of selecting weak password is more tedious so users should avoid from making such choice. Rather than increasing the burden on users it is easier to follow the classification submission for a secure password like images and sound.

In this paper we proposed a sound signature where as in the proposed work a click-based graphical password.

Schema called cued click point (CCP) is also presented .It means that our paper is presented with both sound signature and image.

PREVIOUS WORK

The Considerable work has been done in this area. The best known of these systems are Pass faces [4][7],Brostoff and Sasse. Blonder-style passwords are based on cued recall.

CUED CLICK POINT (CCP)

Fig1:-Graphical password Authentication

CCP is proposed substitute to passpoints.In CCP; Users snap one point on each image to a certain extent than on five points on one image.

It suggests cued-recalls and introduces visual cues that directly alert compelling users if they have made a slip when inward bound their most up-to-date click-point.

It also makes molest based on hotspot investigation more tough.

A user clicks on several previous chosen locations in a single image to login. As implemented by Passlogix Corporation, the user chooses quite a lot of predefined breadth in a picture as his or her password.

To login the user has to click on the same region. The problem with this scheme is that the numeral of predefined section is miniature perhaps. The password may have to be up to 12 clicks.

Another problem of this organization is the want for the predefined regions to be eagerly particular.

In upshot requires artificial, cartoon-like images slightly than multipart, real-world scenes. Cued Click Points (CCP) is a planned system.

Users can choose their imagery only to the amount that their click-point dictates the subsequently image..

If they dislike the resulting images, they could fashion a new password concerning poles apart click-points to get like chalk and cheese images.

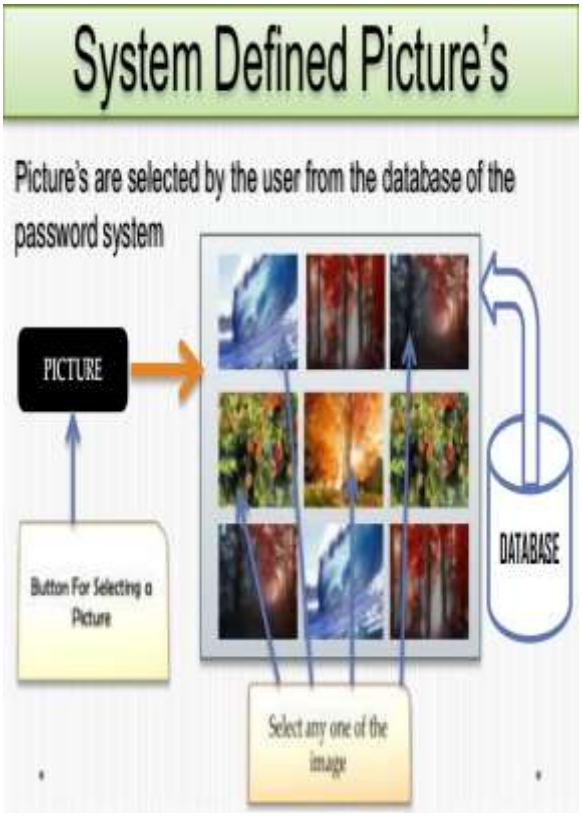


Figure: 2

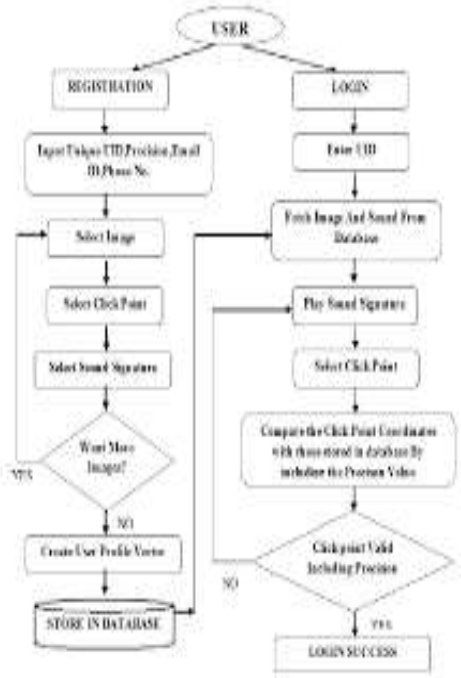
PROPOSED WORK

In the proposed vocation we have incorporated sound signature to aid in recalling the password. No classification has been developed so far-flung which uses sound signature in graphical password validation.

Study declare that sound signature or attitude can be used to recall particulars like descriptions, text etc [5]. In daily life we see various examples of recalling an purpose by the thud correlated to that item [5]. Our idea is to inspired human ability.

Profile Vectors: The proposed system fashion user profile as pursue:-
Master vector: (User ID, Sound Signature regularity, Forbearance).
Detailed Vector: (Image, Click Points).

System Flow Chart



Enters User ID and select one sound frequency which he fancy to be participate at login time, a forbearance value is also certain with will decide that the user is legitimate or a pretender. To create exhaustive vector user has to decide on progression of metaphors and clicks on each likeness at click aim of his preference. Profile vector is created.

Table: 1 Attempts by legitimate users (Five attempt by per login id)

NO	Login ID	Login Trail	Times Accepted	Time Rejected
1	U1	5	5	0
2	U2	5	4	1
3	U3	5	3	2
4	U4	5	5	0
5	U5	5	5	0
6	U6	5	5	0
7	U7	5	2	3
8	U8	5	1	4
9	U9	5	5	0
10	U10	5	4	1

Accuracy for Each Phase

Participants were awfully true in re-entering their passwords. As a launch of precision, all personage click-points in the back up and Login phases were evaluated.

This totaled 1569 click-points meant for the bear out segment and 1325 click-points for the Login segment. For each top, the accuracy was computed as the maximum of |xoriginal − xcurrent| and |yoriginal − ycurrent|.

All Click-points be well thought-out in the therapy, even those that were unproductive. A few times, applicant reaches an erroneous image and still proceeded to relate to on a peak. These were included in the 51+ grouping since the top was perceptibly over and done.

As indicated in Figure 3, 86% of points were within 4 pixels of the original click-point for the Confirm phase compared to 92% for the Login segment.

Declining in 4 pixels of the original top capital these click-points would have been conventional inside lenience square of 9x9 pixels.

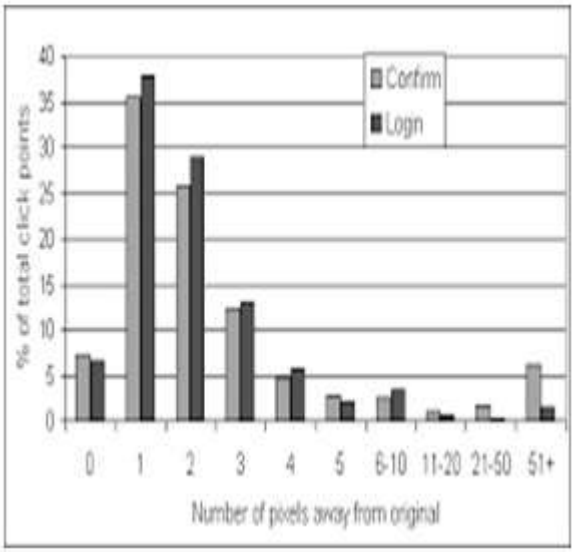


Figure 3: Accuracy for each phase

System Tolerance

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

$$D(p,q)=\sqrt{(p_1-q_1)^2+(p_2-q_2)^2+....(p_nq_n)^2} = \sqrt{\sum_{i=1}^{n}(p_i-q_i)^2}$$

Above distance is calculated for each image if this distance comes out less than a tolerance value D.

The worth of D is resolute according to the claim. In our system this value is selected by the user.

Table: 2 Attempts by imposter users (Five attempt by per login id by randomly selected imposters)

NO	Login ID	Login Trail	Times Accepted	Time 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

SYSTEM DESIGN

[1] User defined Picture:-

Pictures are selected by the User from the Database or any other image support device.

[2] User defined Sound:-

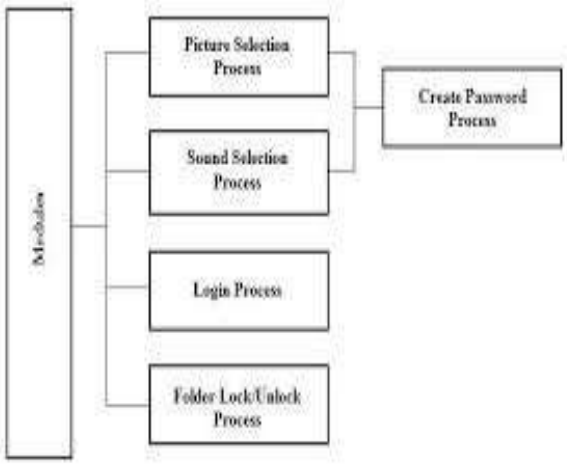
.Sounds are produce by the User and the sounds are stored in the Database.

[3] Login Process:-

We have to select the pictures to continue the login process.

[4] Folder Lock/Unlock Process:-

The picture that we select for login process can be in the Lock/Unlock folder.



By producing the sound and by selecting the pictures we can create a password

EXPERIMENTAL RESULTS

Data collected from 10 contributors. Each contestant was asked to catalogue themselves and then each was invited to for login trail 5 times as legitimate user (Table 1) and 5 times as impostor randomly the as shown in the Table 2.

According to the data generated FAR is 2.0 which are very good for Graphical password verification organization.

CONCLUSION AND FUTURE WORK

We have proposed a work of fiction approach which uses sound signature to call to mind graphical password click points.

In which it provides more security using hotspot technique .Where the proposed system is much more secure compared to the existing system as this system uses three stage of confirmation.

REFERANCES

1. Blonder, G.E. Graphical Passwords. United States Patent 5, 559, 961, 1996. Mechanism", IEEE Trans, Vol 9, Issue 2.
2. S.Chiasson, P. van Oorschot, and R. Biddle, “Graphical password authentication using Cued Click Points” in European Symposium on Research in Computer Security (ESORICS), LNCS 4734, September 2007.
3. Birget, J.C., D. Hong, and N. Memon. “Graphical Passwords Based on Robust Discretization.” IEEE Trans. Info. Forensics and Security, 1(3), September 2006
4. Cranor, L.F., S. Garfinkel. Security and Usability.O’Reilly Media, 2005.
5. R. N. Shepard, "Recognition memory for words, sentences, and pictures," Journal of Verbal Learning and Verbal Behavior, vol.6, pp.156-163, 1967.
6. 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,
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.