Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 11, November 2014, pg.377 – 384

RESEARCH ARTICLE

SIMPLE INTEGRATION OF SOUND SIGNATURE TO GRAPHICAL PASSWORD AUTHENTICATION SYSTEM

Suresh Vankayalapati[1], Jyothi Goddu[2], Kvn.Rajesh[3]

[1]M.Tech, Department of Information Technology, Vignan's Institute of Information Technology,
Visakhapatnam, Jawaharlal Nehru technological university,
Kakinada, Andhra Pradesh, India

[2]Assistant Professor, Department of Information Technology, Vignan's Institute of Information technology,
Visakhapatnam, Jawaharlal Nehru technological university,
Kakinada, Andhra Pradesh, India

[3]Assistant Professor, Department of Information Technology, Vignan's Institute of Information technology,
Visakhapatnam, Jawaharlal Nehru technological university,
Kakinada, Andhra Pradesh, India

[1] sureshvonkayala@gmail.com, [2] Jyothi506@gmail.com, [3] Kvn.rajesh@gmail.com

Abstract - In general we use alphanumeric characters, special characters, sound signature and images for passwords during registration process. Where the entered password should be matched with either sound signature or images that were stored in database. Whereas the images are checked with their exact pixel position (i.e. Hotspot).Hotspots are particular areas of image that have higher likelihood of being selected by users as password click-points. But in the existing system, it is easy to hack the system by identifying the single hot spot on the image. Hence, our proposed system is the used to improve the security by adding the multiple hot spots on the image.

Keywords - Sound Signature, Image Authentication, Audio Timing, CCP, Textual Passwords

1. INTRODUCTION

Passwords are used for Authorization and Access Control. Textual passwords are commonly used easy to break current authentication systems suffer from many weaknesses. Human Computer Interaction is important in 3 images areas authentication: security operations and developing secure systems. Mostly user select password 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. Based on the studies showing that human brain is best at recalling images than text, graphical positive identifications are to resolve memory burden and little password area problem of classical passwords. Another solution to generate strong passwords is password managers, which are immune to dictionary attacks. For maintaining the memorability, the password authentication system should encourage strong passwords. We propose that authentication schemes which allows the user choice to influencing users towards stronger passwords. The task of selecting weak passwords (which are easy for attackers to Predict) is more tedious, prostate users from making such choices. Textual passwords authentication system is commonly used easy to break. Current authentications systems suffer from many weaknesses. In this work duo to this traditionally

developed application is more security Cued Click Points of images some click different pixel position on the image. Various graphical password schemes have been features alternative to text-based passwords enter in the profile unfortunately any unauthorized person enter into our profile using textual user name and password but we have to restrict that person using sound signature and graphical password authentication image cued click point on like image.

Section 1: discussed about introduction of a system. Literature

2. LITERATURE REVIEW

S.Wiedenbeck, A. Brodskiy2011 [1], In which user is asked to select a sound signature, which helps the user in order to remember the click-points during login phase even if the user tries to login after a long time, and a tolerance dimension during password creation process.

DuhanPooja, Gupta Shilpi, 2012[2]. In which graphical passwords strength comes from those users can recall and recognize pictures more than words. Token based systems can also be used as way of authentication in banking systems. But cards are loss or theft. Biometric recognition scheme has its advantages and disadvantages based on several factors such as consistency, uniqueness.

Alankrita Ladage, Swap nil Gaikwad April 2013[3], discussed about sound signature used by the sound clips and the pause time. If the pause time and the sound clip entered previously are correct the user is authenticated otherwise the user is considered as outsider.

Sonia Chiasson, P. C. Van Oorschot, 2011[4], discussed about persuasion to influence user choice in click based graphical passwords encouraging users to select more random, and hence more difficult to guess, click points presentation process. We propose to extend our existing work for supporting sound signature processes for higher authentications in integrating security of data for accessing services.

S. Chiasson, A. Forget, R. Biddle, and P.C. van Oorschot, 2009[5],described in their work that according to human psychology; one can memorize the click points easily when compared to the textual passwords. The number of click points and the number of images included in the password creation depend upon the user's choice.
A.Perrig and D. Song 1999[6], discussed that 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.

Birget, J.C. D. Hong.Memon September 2006[7], discussed that the user can click only one point or the number of points he can remember based on his memorizing capability on each of the images rather than on clicking on several points on one single image.

S.Wiedenbeck, J.C.Birget, A.Brodskiy, N. Memon, ACM SOUPS", 2005[8], discussed about recall-based techniques; a user selects images during the registration and is asked to reproduce something that he or she created during the registration phase.

Section 2: discussed about Literature Review of system. Architecture of Authentication System.

3. SYSTEM MODULES

Fig.3.1 Shows the Modules for integration of text, sound and image for the generation of password authentication system.

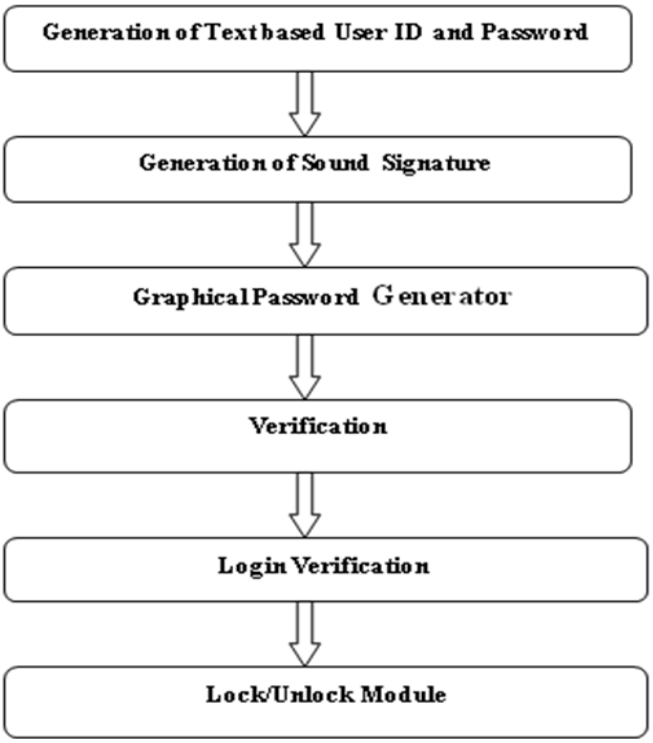

Fig.3.1. Architecture of System Modules Proposed Authentication System

User Registration Maintenance Module:
This module allows the registration of the users. The users are created with security accounts in the SQL Server database. Each user is associated with password. Only users having these accounts can access the application to perform any specific task.

Associate Sound Signature Module:
The module allows the user to choose an audio file at runtime or use his voice for creating sound file. This audio is converted to binary format and this binary file is then encrypted and associated with the graphical password and dumped into the SQL database. It strengthens the security of the protected data.

Graphical Password Generator Module:
The module allows the user to generate password from images. The user has to specify the required image and click on the image to generate strokes. Each stroke provides a pair of co-ordinates x, y location from the image. The co-ordinates in the pattern are clicked and the number of strokes along with the image is redirected to the database after performing encryption. The source image can be deleted as the application does not have a direct dependency on the physical file as the image and click information has been directed to SQL database.

Verification Module:
During verification phase, the details that the user enters during registration phase and login phase are verified.

Login Verification Module:

In this user details compared with database information, if both are equal user can login for accessing data and modification also possible. While registration image clicks done and corresponding pixel positions are return in the form of the tolerance and compare that with registration information. Same process done in sound-module which is part of the registration form as well.

Lock/Unlock Module:
Protecting of our data and information from certain unwanted and prying eyes may become a dilemma if you end up with enough personal and private data on your computer or on your external storage devices. With information changing hands and data transfer figures at record numbers, critical files and folders like these need robust protection so that intruders or unauthorized users are stopped right in their tracks – whether to read, view, copy, move or delete them. If it is personal or confidential, it needs protection! Folder lock uses GPAS for protecting your files.

Section 3: discussed about Architecture of Authentication System. Methodology

4. METHODOLOGY

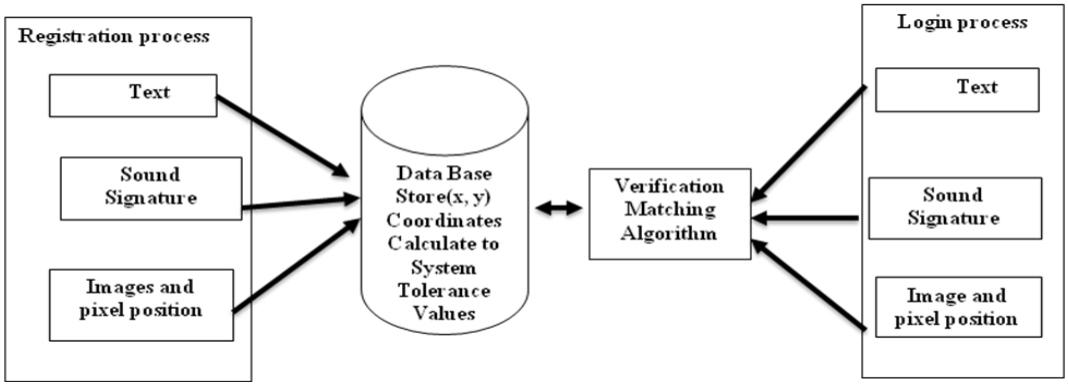

Fig4.1. Architecture of Integration of sound signature to graphical password authentication system

Registration process is used to provide security to document using text password (ie user name and password) ,to overcome hacking of text password more security is provided by using sound signature . Sound Signature using .wave form of timer tone is used as password. If someone is trying to hack the second process then we provide more security using images and pixel positions using x and y coordinates. In login, if verification matches from database then only login to the system is done. If verification does not matches can't access the secure document that will be checked from database retrieval system.

Section 4 : discussed about Methodology. Algorithm

Algorithm:

As Flows shows integration of sound signature in graphical password authentication system.
Begin:
Step.1:-Read Text (T),Sound signature(S), and two pixel position cooridinates (p ,q) of five Images(I) in Registeration Process.

Step.2:- if (Text==T) then
Success
else
Failure
//Text Password Failures enter into next level
end
Step.3:- if (Sound Signature==S) then
Success

else
Failure
end

"S" is Sound Signature provide secure freqence of sound and time.

//if this provide fails enter into next level.

Step.4:-Repeat for Count<- 1,2,3,4,5
if (Image(x,y)==I)(x,y))then
Success
else
Failure
end

"I"Image provides security to our document using pixel position authentication system.

Step.5:- Distance between two vectors logging in with pixel position(p,q) x andy is acalculated as

$$d(x,y)=\sqrt{(x_1-y_1)^2+(x_2-y_2)^2+\ldots\ldots+(x_n-y_n)^2}$$

pixcel position on image p(x corridinates) =x1,x2,x3,x4,x5,.....xn.
pixcel position on image q(y corridinates) =y1,y2,y3,y4,y5,.....yn.

Step.6:- Above value is caluculated for each images if the distance comes out than a tolerance values.the value of decided to the applications.in oursystem value is select by the user.

$$\sqrt{\sum_{i=1}^{n}(x_i-y_i)^2}$$

Step.7:- end

Section 4: discussed about Algorithm. Implementation

5. IMPLEMENTATION

Fig.5.1 shows the overal implementation of home page, consisting of two modules

Registation:The first process of this system is to register, which the user generates his pasword based on the alphanumeric characters, special characters, sound signature and images as an inputs for the protection of files/data. This will provide security in personal data files in registration process.

Login: This Module process in security mostly in used in re user name and password system check with our personal data files.

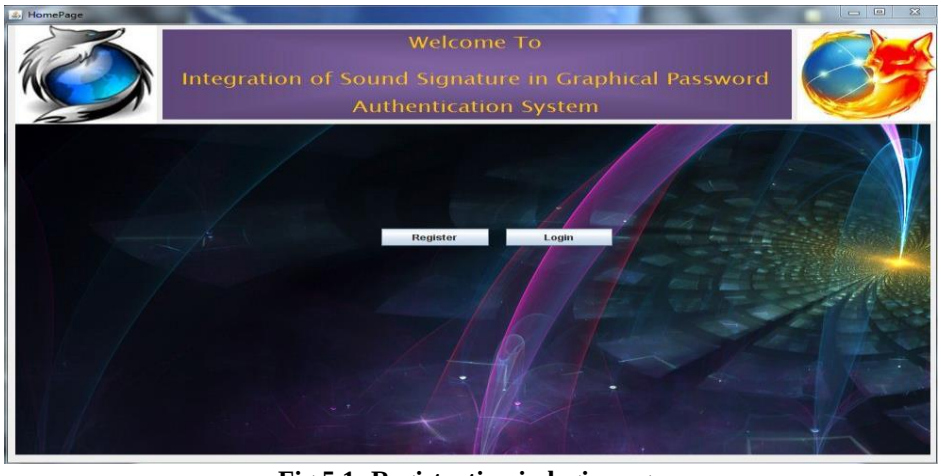

Fig.5.1: Registration in login page

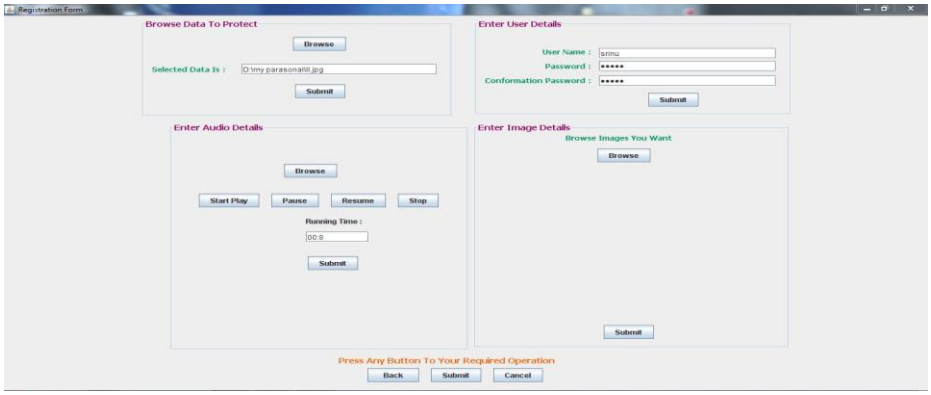

Fig.5.2: Interface of audio details

Inter face of audio sound signature in graphical password authentication system browsing data to protected in theselect data is security in some file.Next process in sound signature enter in to audio frequency browsing file .wave from ring tone setting sound start play of sound running time of setting particular time compress in the sound signature of browsing file. Next enter into an interface audio frequency of sound signature in particular .wav format tone play of sound signature and time. Browsing into a audio file upload .wave Frome of frequency particular time compression in audio sound signature.

Fig.5.3: Interface of submission images and Ccp details

Next enter in to browsing selecting of 5images and then some pixel position in different areas on the image cued click point on the image it is stored in data base .Select in 5 images of conformatio correct image and reset of image in the culd-click point of some pixel of position in the image in culd-click point then submet in click.press any buttion to your registration operation back,submet,cancel select submet buttion.browsing file secqure to storaged in database then recive in data file of sql connected file name.

Section 5: discussed about Implementation. Results

6. Results

Output module in the browsing output file location to store in data base open in data base file enter re username and password enter in to the data base list enter in to data base file name login id enter in to the mouse position user Play sound signature to Play random sound Get click points and prepare login vector in to Compare login and user login on next Fetch User profile in Show Image from user Detect mouse position on cued click point correct on mouse position pixels position clicking on image positions. Next browsing output location to storage browsing output file location database connected in database file name open in secure file show me in file in this project is privacy integration sound signature in graphical password authentication system more security in personal files.

Fig 6.1: Output Module

Data collected from 4 participants. Each participant was asked to register himself/herself and then each was invited to for login trail times as legitimate user and 5 times as impostor randomly. By using the system the observation of resultes giving 99% accureance of security rather than other traditional systems.

Table.6.1.Results with tolerance values

Users	User name,passwd	User leveles	X Corridition	Y Corridination	Tolarence value
1	User-4, password-4	3	75,73,73,73,74	85,85,86,87,85	27.018513
2	User-5, pass-5	3	73,74,74,71,73	88,89,87,88,88	33.660065
3	User-ravi, pass-ravi	3	3,84,82,122,81	3,41,73,67,39	81.969505
4	User-valli, pass-valli	3	1,86,122,82,60	0,39,64,72,67	74.397585

Section 6: discussed about Results. Conclusion

7. CONCLUSION

The use of graphical images and sound signatures strengthens the security system by almost removing the chances of getting breached. This application can be used for providing security to any application by placing this application over any application which is needed to be secured and whose security system is to be enhanced. 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. We can provide more security through combination of graphical passwords and sound signature. It provides more security to the data.

Section 7: discussed about Conclusion. Acknowledgment

8. ACKNOWLEDGMENT

I would like to thank Principal of Vignan's Institute of Information Technology Dr. K. Alice Mary, for her encouragement to me during the work. I would like to thank our ever-inspiring Head of the Department of Information Technology, Mr. B. Prasad, for his spontaneous response to every request though he was busy with his hectic schedule of administration and teaching. I would like to express my deep sense of thanks to my project guideMs.G.Jyothi Assistant Professor for enlightening me with constructive suggestions for solving my problems patiently and helping me to improve the quality of work.

REFERENCES

[1] **S**.Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy, and N. Memon. "Pass Points: Design and evaluation of a graphical password system", *International Journal of Human Computer Studies*, 2011.

[2] DuhanPooja, Gupta Shilpi, SangwanSujata, &Gulati Vinita "Secured authentication: 3D password, "International Journal Of Engineering and Management Sciences, I.J.E.M.S.(242 – 245), VOL.3(2),2012..

[3] Alankrita Ladage, Swapnil Gaikwad, Chougule A B,"Graphical Based Password Authentication", International Journal of Engineering Research and Technology, volume 2, no.4, April 2013.

[4] Sonia Chiasson, Member, IEEE journal, Alain Forget, Elizabeth Stobert, Robert Biddle, Member, IEEE, And P. C. Van Oorschot, Member in IEEE journal, "Persuasive Cued Click-Points: Design, Implementation, And Evaluation Of A Knowledge- Based Authentication Mechanism", Edition: Oct, 2011.

[5] S. Chiasson, A. Forget, R. Biddle, and P.C. van Oorschot, "User Interface Design Affects Security: Patterns in Click-Based Graphical Passwords," Int'l J. Information Security, vol. 8, no. 6, pp. 387- 398, 2009

[6] 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.

[7] Integration of Sound Signature in Graphical Password Authentication System International Journal of Computer Applications (0975 – 8887) Volume 12– No.9, January 2011

[8] Wiedenbeck, S., J.C. Birget, A. Brodskiy, and N. Memon. Authentication Using Graphical Passwords: Effects of Tolerance and Image Choice. ACM SOUPS, 2005.

[9] S. Wiedenbeck, J.C. Birget, A. Brodskiy, N. Memon,"Authentication Using Graphical Passwords: Effects of Tolerance and Image Choice. ACM SOUPS", 2005.

