GRAPHICAL PASSWORD AUTHENTICATION USING PCCP WITH SOUND SIGNATURE

Nilesh Changune[1], Ganesh Shinde[2], Sagar Chaugule[3], Sandeep Helkar[4]

[1]*Student, Department of Computer Engineering, AISSMS COE, Pune, India*
[2]*Student, Department of Computer Engineering, AISSMS COE, Pune, India*
[3]*Student, Department of Computer Engineering, AISSMS COE, Pune, India*
[4]*Student, Department of Computer Engineering, AISSMS COE, Pune, India*

Abstract

Persuasive Cued-Click Point is an advanced method of cued click point of graphical password technique which includes usability and security evaluations. It also useful for reduces hotspot problem and hence it helps the user in selecting password of higher security. This paper includes the persuasion to influence user choice in click based graphical passwords, so that users select more desultory and more difficult to guess the passwords. In this paper includes sound signature for recover the password if user forgot password or click point ,then playing the sound signature which is selected at registration time then it set new password and access the account. This paper include dead zone new concept to avoiding Shoulder surfing attack in graphical password authentication.

Keywords: *Graphical Password, Authentication, Password Images, and PCCP etc…*

---***---

1. INTRODUCTION

Until recently computer and network security has been formulated as a technical problem. It is now widely acknowledged that most security mechanism cannot succeed without taking into account the user view. Human Being's are incapable of securely storing high-quality cryptographic keys and they have acceptable speed and accuracy when performing cryptographic operations [1]. With the in invention in technology new method develops to break security of system. Security engineers and researchers have making strides in protecting system to avoid damage. New passwords techniques are evolved in password security to protect system. With the drawbacks of token based and biometric based authentication system .New system of graphical password authentication developed.

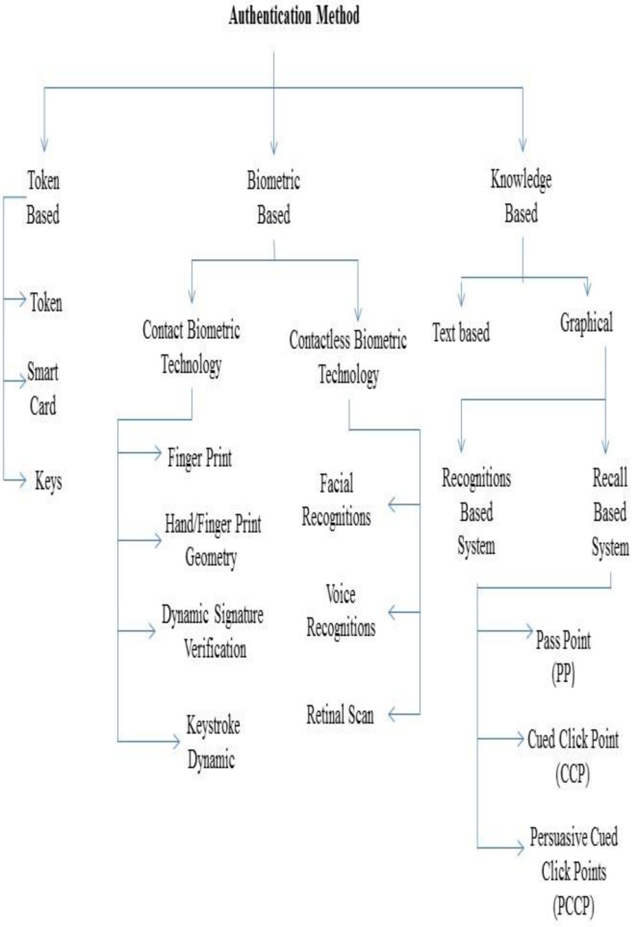

Chart-1: Classification of Graphical password

1.1 Recognition Based Techniques

At the time of registration user select set of images and during accessing system user must recognize that set of image while entering password.

1.2 Recall Based Techniques

Recall based is the technique in which system asked to the user to redraw or select something that is user is created or his selected at the registration time.
In this paper our technique is also recall based technique.

2. LITRATURE SURVEY

2.1 Pass Point

In the pass point technique user select the any one of the image .On that image user must select N click point at time of selecting a password. At the time of login user must select accordance with that sequence of click numbers. In the type user just recalling no. of clicks on that image. Within the specified system given tolerance square users pixel accept. The usability and security of this password scheme evaluated by original authors[2][3]. Though all precaution we took security concern is still an issue. The main problem in this type is creation of hotspot. User always tends to select similar click points which are already click by another user. Through harvesting sample or building attack dictionaries by image processing technique which leads to successful guessing of password.[4].

Fig-1: Passpoint

2.2 Cued Click Point

To reduce the hotspot creation problem in pass point method next cued click point method is useful. A password includes one click point per image for a sequence of images. The next image is displayed on previous click point. Different click point have different set of images path. It also makes attack based on analysis of hotspots more challenging. The wrong click goes to wrong path without an indication of failure login it only shows after final click on that image.

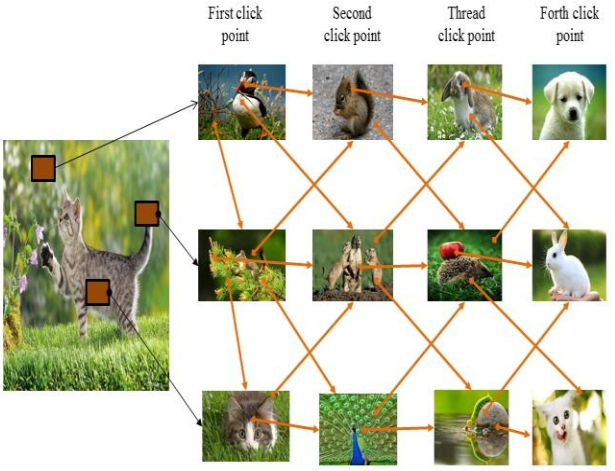

Fig-2: Cued Click Point

2.3 Persuasive Cued Click Points

Using cued click point as a base system new feature to encourage user to select more secure password and to make it more difficult to select passwords where all five click points fall within hotspots. When users creates password at the time of registration the image is slightly shaded only viewport part is visible to user which give user persuasiveness while creating password by which the hotspot problem is minimized. The Persuasive technology originally articulated by fogg[7] as using technology to motivate & influence people to behave in desired manner.

The theoretical password space for password system is the total number of unique passwords that could be generated according to system specification. Ideally, a larger theoretical password space lowers the like hood that any particular guess is correct for given password. For persuasive cued click points, the theoretical password space is $((w*h)/t^2)^c$ where the size of image pixels is (w*h) is divided by the size of tolerance square (t^2) to get number of tolerance square per image, raised to power of the number of click point in password.

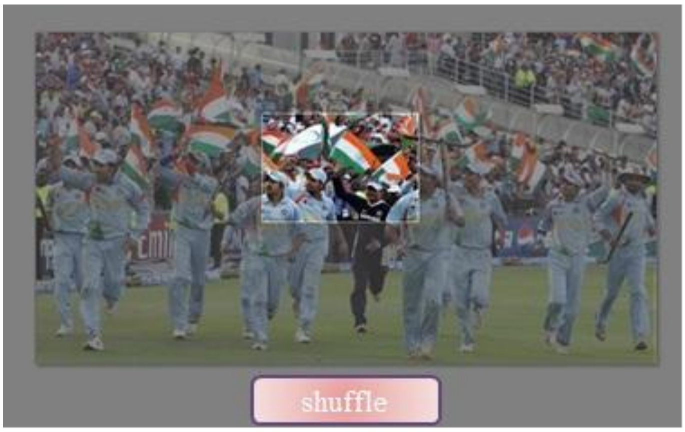

Fig-3: PCCP

3 PROPOSED SYSTEM

From literature survey it is conclude that in graphical password PCCP techniques is strong but not satisfied. In pccp technique the chances of shoulder surfing attack is more for avoiding shoulder surfing attack we are adding dead zone concept. Using the dead zone in pccp we create the password is more strong secure And also adding sound signature for forgot password. both are concept descripted below.

3.1 Sound Signature

User must select sound at the time of registration. When user not memorize the password that time the user click on forgot password button then system gives sound clip if user play the correct sound then system gives the permission to create new password and gives the image sequence for creating password otherwise system goes through exit mode.

3.2 Dead Zone

Dead zone is concept take for avoiding shoulder surfing attack. Shoulder surfing concept is if user enter the password and select the images sequence of his password and any person standing backside of user and looking the password sequence then there is many chances of hack your account by using guessing attack. This concept is shoulder surfing.

But using the dead zone concept we can avoid that attack. The dead zone is some particular area that is allocated user on registration time which is store in all image sequence. If click on that area the system shows image sequence from starting image. If user enter the password and some person looking that then user can select the wrong click point then system gives wrong image sequence to user which is dead zone is present then user click on dead zone then again system gives correct image sequence. This process we can repeated many time then this person is confused and the very hard to crack password by using shoulder surfing attack.

3.3 Modules Description

3.3.1 Registration

1. Sign up initiate
2. Select password images sequence
3. Select manual image
4. Select graphical password for each image
5. Calculate hash (digital signature algorithm) for each point using discretized centralization
6. Accept string for sound signature
7. Register

3.3.2 User Sign In

1. Start sign in
2. Display image #1
3. Accept password
4. If required generated sound signature
5. Calculate hash using digital signature algorithm and discretized centralization
6. Authenticate each image
7. If invalid signature found show random invalid image for re-verification
8. If re-verification is ok continue accepting graphical password for next image
9. If all image authenticate login

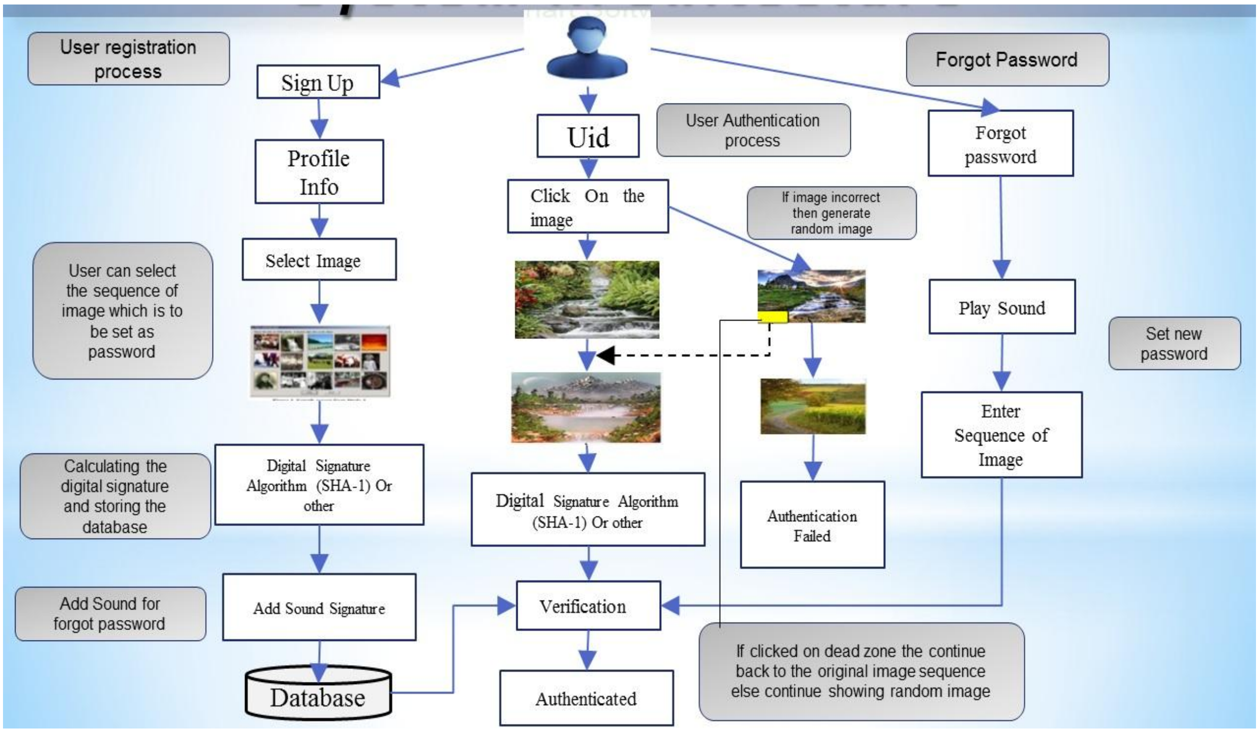
User registration process
Sign Up
Profile Info
Select Image
User can select the sequence of image which is to be set as password
Calculating the digital signature and storing the database
Digital Signature Algorithm (SHA-1) Or other
Add Sound for forgot password
Add Sound Signature
Database
Uid
User Authentication process
Click On the image
If image incorrect then generate random image
Digital Signature Algorithm (SHA-1) Or other
Authentication Failed
Verification
Authenticated
If clicked on dead zone the continue back to the original image sequence else continue showing random image
Forgot Password
Forgot password
Play Sound
Set new password
Enter Sequence of Image

Fig-4: Architecture of Proposed System

4. CONCLUSION

In graphical password authentication pccp technique is strong but it is not avoided the shoulder surfing attack. That's why we are adding dead zone concept in pccp technique by using this concept we are avoiding the shoulder surfing attack, and try to create strong password for security. Also adding the sound signature for forgot the password.

ACKNOWLEDGEMENTS

The authors would like to thanks to all which are working related to graphical password authentication field. All this helps me to improve my presentation work.

REFERENCES

[1] C.Kaufman, R.Perlman and M.speciner. "Network Security:PRIVATE Communication in a PUBLIC World.Prentice Hall,2nd edition" 2002.

[2] Wiedenbeck, S., Birget, J. C., Brodskiy, A., and Memon, N. "Authentication Using Graphical Passwords: Effects of Tolerance and Image Choice. Symp. On Usable Privacy and Security (SOUPS)" 2005

[3] Wiedenbeck, S., Waters, J., Birget, J.C., Brodskiy, A., and Memon, N. PassPoints: "Design and longitudinal evaluation of a graphical password system." Int. Journal of Human- Computer Studies 63, 102-127, 2005.

[4] Thorpe, J. and van Oorschot, P.C. "Human-Seeded Attacks and Exploiting Hot-Spots in Graphical Passwords. USENIX Security" Symp. 2007.

[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] S. Chiasson, A. Forget, R. Biddle, and P. van Oorschot, "Influencing Users towards Better Passwords: Persuasive Cued Click- Points," Proc. British HCI Group Ann. Conf. People and Computers: Culture, Creativity, Interaction, Sept. 2008.

[7] B. Fogg, Persuasive Technologies: Using Computers to Change What We Think and Do. Morgan Kaufmann Publishers, 2003

[8] Jermyn, A. Mayer, F. Monrose, M. Reiter, and A. Rubin. The design and analysis of graphical passwords. In 8th USENIX Security Symposium, August 1999.

[9] Security Analysis of Graphical Passwords over the Alphanumeric Passwords by G. Agarwal,1Deptt.of Computer Science, IIET, Bareilly, India 2,3 Deptt. of Information Technology, IIET, Bareilly, India 27-11-2010.

BIOGRAPHIES

Nilesh Changune is a student at AISSMS COE, Pune. He is pursuing Bachelor's Degree in Computer Engineering in Savitribai Phule Pune University, Pune, Maharashtra, India.

Ganesh Shinde is a student at AISSMS COE, Pune. He is pursuing Bachelor's Degree in Computer Engineering in Savitribai Phule Pune University, Pune, Maharashtra, India

Sagar Chaugule is a student at AISSMS COE, Pune. He is pursuing Bachelor's Degree in Computer Engineering in Savitribai Phule Pune University, Pune, Maharashtra, India.

Sandeep Helkar is a student at AISSMS COE, Pune. He is pursuing Bachelor's Degree in Computer Engineering in Savitribai Phule Pune University, Pune, Maharashtra, India