Cued Click Points Graphical Images and Text Password along with Pixel based OTP Authentication

A.Abuthaheer
PG Scholar
Sri Ramakrishna Engg College
Tamilnadu, India

N.S.Jeya Karthikka
PG Scholar
Sri Ramakrishna Engg College
Tamilnadu, India

T.M.Thiyagu
Assistant Professor
Sri Ramakrishna Engg College
Tamilnadu, India

ABSTRACT

A graphical password uses images or representation of images as passwords. Human brain is easily remembering the Graphical image secret word compare to Text secret word. There are dissimilar graphical image secret word methods or graphical image secret word software's are available in the market. The proposed work merges Cued click points, text and token based verification. The main objective of this proposal is to reduce the guessing attacks as well as encouraging users to select more random, and difficult to guess password. Well known security threats like brute force attacks and dictionary attacks can be successfully abolished using this method.

Index Terms

Authentication, Graphical Passwords, Security, OTP;

1. INTRODUCTION

In early days, text based passwords are used for authentication. Text based passwords authentication is nothing but string of alphanumeric characters. Coming to text based passwords, users always creates password which is easy to remember but these passwords are easy for attackers to break. For more security, users use strong system assigned passwords which will be difficult for users to remember. Biometric and tokens [8][9] are used as an alternative to text based passwords but has its own drawbacks such as it requires extra hardware so these methods are costly. As an alternative to all these methods, graphical passwords are used because psychology studied that human brain can recognize images better than the text.

Graphical passwords are of three types: Click based graphical password scheme [10], choice based graphical password scheme and draw based graphical password scheme. In this proposed work, user clicks on sequence of five images. At the time of login phase images appear as per the random sequence. In the registration phase, user selects 5 images from the image pool or local drives. Based on the image selection server generate the signature during registration. While users coming to login phase, select images from the image pool based on image selected by registration phase and then the server generate the new signature based on image selection. If both the signatures are same, then only Pixel based One Time Password (OTP) is generated and sent to the user's mobile by server. Otherwise abort the user. Pixel values of all five clickable images will be used for calculating OTP. This proposed system provides three-way authentication and also provides higher security than other techniques.

2. BACKGROUND

Previously several Graphical image Password methods were introduced. Some of the techniques are given below,

2.1 Pass-points

S. Wiedenbeck et al. proposed pass-point graphical password scheme image password consists of a sequence of 5 different click points on single image. For password creation user selects any pixel in the image as a click-points and for login the user has to enter the same series of clicks in correct sequence within a system defined tolerance square of original click-points. The drawback with this method is the HOTSPOTS (the area of an image where user more likely to select the click-point) and it is easy for attackers to guess the password because user forms certain patterns in order to remember the secret code which results pattern formation attacks are easily possible. This method endures from these two major problems. To overcome these problems next method is to be implemented.

5
2
4
3
My India
My Pride
1

Figure: 1 Pass Points System

2.2 Cued Click Points

Cued Click Points was designed to reduce patterns [7] and to reduce the usefulness of hotspots for hackers. In preference to five click-points on one single image, CCP uses one clickable region on five distinct images. The next new image presented is based on the location of the previously entered click-point; it creates a path through an image set. One best feature of Cued Click Point[4] is that the explicit indication of authentication failure is only provided after the final click-point, to defend beside accumulative guessing attacks. But this method also has more drawbacks like false accept (the incorrect click point can be accept by the system) and false reject (the click-point which is to be correct can be reject by the system). In this existing method pattern realization attack is reduced but HOTSPOT remains since users are selecting their own click-point.

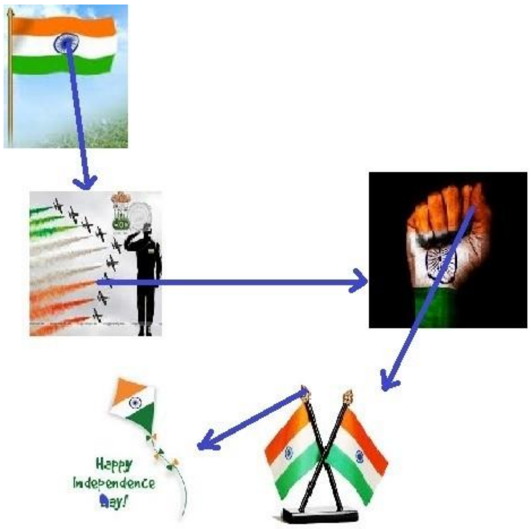
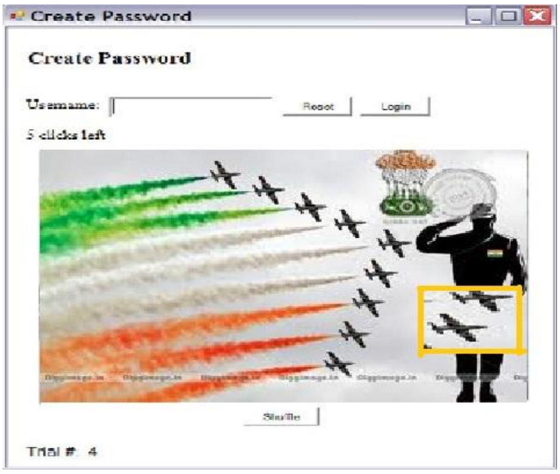


Figure: 2 Cued Click Points System

2.3 Persuasive Cued Click Points

For creating Persuasive Cued Click Points persuasive feature is added to CCP. PCCP encourages users to select less probable passwords. For password generation PCCP uses requisites like viewport & shuffle. When users making a secrete word, the images are a little monochromic except for a viewport for to avoid known hotspots the viewport is positioned casually. The most useful benefit of PCCP is hackers have to improve their presumptions. Users have to choose a clickable area within the highlighted viewport and cannot click outside of the viewport unless they press the shuffle button to randomly reposition the viewport. At the time of password creation users may shuffle as often as desired but it slows the process of password generation. Only during the password generation, the viewport & shuffle buttons are displayed. After the secrete word generation process, graphical images are presented to users casually without the viewport & shuffle button. Then user has to choose exact clickable area on particular image. Now a day's PCCP is a best technology but has security problems [3][5]. Fig No.3. shows the password creation process including viewport & shuffle button. Using this method HOTSPOT problem is reduced, but this method is difficult to remember the exact clickable area.


Create Password

Create Password

Username:

5 clicks left

Trial #: 4

Figure: 3 Persuasive Cued Click Points System

3. PROPOSED SYSTEM

3.1 Introduction

In this system, user clicks on sequence of five images. At the time of login phase images appear as per the random sequence. In the registration phase, user selects 5 images from the image pool or local drives. Based on the image selection server generate the signature during registration. While users coming to login phase, select images from the image pool based on image selected by registration phase and then the server generate the new signature based on image selection. If both the signatures are same, then only Pixel based One Time Password (OTP) is generated and sent to the user's mobile by server. Otherwise abort the user. This proposed system provides three-way authentication and also provides higher security than other techniques.

In this proposed system first generate the application for graphical password authentication system. In this creation of the application the runtime image are added and existing database images also considered for registration process. It handles the user requests, response to user and connects with database. After the creation of the application in the database then enrol the images in the image pool with user information .Then user click the images in the database based on this process the signature are generated to each user. Then authentication process is started to login users with images selected by user in image pool. In the second step newly generated signature are verified with registered signature .If it satisfies then create the one time password (OTP) and send to mobile. Otherwise eliminate the user.

3.2 Architecture Diagram

The overview of main components of the cued click points and pixel based one time password authentication system and their properties are shown in Fig No.4,

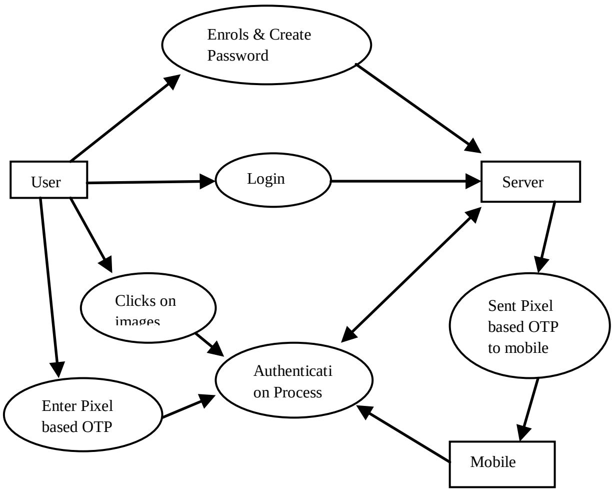


Figure: 4 Pixel based OTP Authentication along with CCP Method

In that CCP along with OTP authentication, first user can enrol the personal details and also create the text and graphical password [6]. While creating the graphical password, one signature was generated based on algorithm. There after going to login process, based on image clicking one more signature was generated by Server. If the both Signature are same, then only pixel based OTP was created based on algorithm. There after the server can sent the OTP to user's mobile. In

Authentication phase server can verify the image pixel, sequence and one time password.

3.3 Implementation

3.3.1 Modules Description

- ✓ Enrolls Images with User Information and Generate Graphical Password.
- ✓ Authentication Process While Logging Users.
- ✓ Implementing the Process of Single Sign on Mechanism.

3.3.1.1 Enrols Images with User Information & Generate Graphical Password

In Registration Process first user Provide necessary Information of user & create Text Password. After that User Pick five Images from Local drive or Image pool. User Click on Picked Images and Generate Graphical Password. Pixel value of five Images are Stored in Server side. Based on the image selection server can generate the signature for authentication.

ALGORITHMS USED IN REGISTRATION

1. E= $\{X\}_K$ denotes the symmetric encryption of message X under the key K.

2. X stands for the concatenation of the messages $X_j \quad j = 1,2,3\ldots.N$

3. X_j $=\mathrm{Hash}(Xj - 1)$ is the one way hash of X.

4. K_j $=\mathrm{Hash}(Wj\,,Xj)$ W-masking bit

5. S_j $=\mathrm{Hash}(Sj - 1,\{Ej\}Kj\,,Wj)$ is the j^{th} value of the hash-chain

6. $\mathrm{MACK}(S)$ denotes the message authentication code of X under K.

7. $\mathrm{Sign}(S)_{Kd}$ stands for the signature of S with K.

// K_p stands for the public-key of the service s and K_d is the corresponding private-key of s.

3.3.1.2 Authentication Process While Logging Users

While User coming to Authentication phase, first step select images from the image pool *and* then based on image selection server generate the signature. Second step verify the registration signature with newly generated signature. If both the signature are same the password is generate and send to the mobile. Otherwise abort the user.

ALGORITHMS USED IN LOGIN STATE

1. A_j $=\mathrm{Hash}(Aj - 1)$ denotes the authentication key of the j^{th} click

2. K_j $= \mathrm{Hash}(Wj\,,Aj)$

3. E_j $=\{A\}_{K}$

4. Y_j $=\mathrm{Hash}(Yj - 1,\{Ej\}Kj\,,Wj)$ is the j^{th} value of the hash-chain.

5. MACK(Y) denotes the message authentication code of X under K.

6. Generate $\mathrm{sign}((Y)_{kp}$

7. if $(\mathrm{Sign}((X)Kd \quad == \quad \mathrm{sign}((Y)kp)$

Generate password and send to mobile

8. Else drop the user

3.3.1.3 Implementing the Process of Single Sign on Mechanism

Based on the image pixel value server can generate the password. Pixels values are taken for calculates the Mean values and then calculate variance. The Server can generate the Random Sequence of digits for calculating One Time Password. The randomly generated sequence is individually added with each element of variance. There after take the mean value of newly calculated arrays. This is the Final OTP. These values will be sent to mobile from the Server.

4. EVALUATION OF PERFORMANCE AND RESULTS

4.1 Evaluation of Performance

In this evaluation of performance chapter we evaluated the usability of PCCP; Pixel based OTP with CCP through performance measures. To show the performance in context, we compared Pixel based OTP with CCP to the other authentication schemes tested under similar conditions. The distributions contain all user-chosen click-points for the given scheme for graphical passwords that were, at smallest amount, effectively re-entered at least once during login. In the Fig.No.5, this random distribution would appear as a curved diagonal line. In comparison, the PCCP graph shows that in the worst case, half of all click-points are confined within the most popular 0.00075 percent of hotspots within the distribution, while in the best case 0.00200. This indicates that CCP click-points have a flatter distribution and thus an attack dictionary based on hotspots should be less effective for CCP than for the other schemes. This analysis focused on individual click- points, not complete passwords. However with the endorsed implementation, hackers get no partial opinion on correctness partway through an offline guess on CCP. Better user interface design can influence users to select stronger passwords. A key feature in PCCP [5] and CCP is that creating a harder to guess password is the path of smallest resistance, likely making it more useful than schemes where secure behaviour adds an extra problems on users. The approach has proven successful at reducing the formation of hotspots and patterns, thus growing the good password space.

4.2 Results

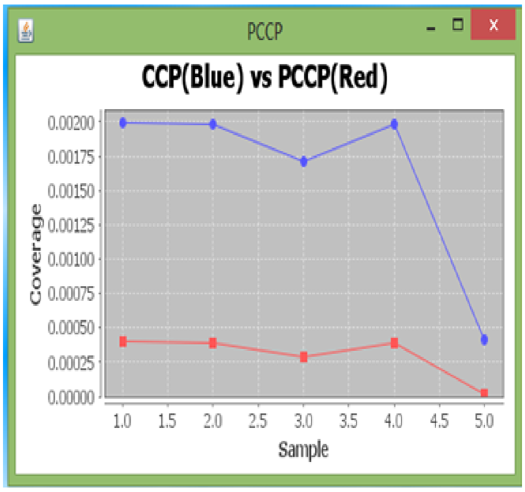


Figure: 5 Cumulative frequency distribution of hotspot coverage for CCP&PCCP

Table: 1 Input Parameters of CCP and PCCP for calculating Coverage Ratio

Images	Height	Width	Click Area	View Port Height	View Port Width	PCCP Coverage Ratio	CCP Coverage Ratio
Image 1	177.0	284.0	10*10	100	100	0.00039575	0.00198934
Image 2	168.0	300.0	10*10	100	100	0.00039368	0.00198413
Image 3	210.0	278.0	10*10	100	100	0.00028341	0.00171292
Image 4	168.0	300.0	10*10	100	100	0.00039368	0.00198413
Image 5	387.0	620.0	10*10	100	100	0.00001737	0.00041677

Equations used in coverage ratio calculation:

Image click ratio= $(10\times10)\div(\text{height}\times\text{width})$

View Port ratio= $(100\times100)\div(\text{height}\times\text{width})$

PCCP Coverage Ratio $=$ Image Click ratio$\times$ View Port ratio

CCP Coverage ratio $=$ Image Click ratio

In this Fig.No.5, the performance of the CCP (Cued Click Point with Pixel based OTP) and the performance of PCCP (Persuasive Cued Click Point) measures the coverage results in the number of input samples. The number of input samples are shown in the X axis and the Coverage of the result are measured in Y axis. The CCP (Cued Click Point with Pixel based OTP) and PCCP(Persuasive Cued Click Point) measure the coverage result in the number of input samples, it shows that the proposed CCP coverage is most important result in the samples. CCP's segments were the longest and within range of the random distributions. Given that no other spatial patterns are apparent for PCCP. This Proposed work suspects that these shorter segments are an artefact of the viewport positioning algorithm, which vaguely favoured more focal areas of the image.

Image click ratio is measured based on the width and height in the original image. The height and width was changed according to the image was used in the application. In this proposed work we, measured the image click ratio for each and every image used in the project work. If we taken 5 images the image ratio is measured to five images. The viewport is situated randomly, rather than explicitly to avoid known hotspots, since such statistics might allow hackers to improve guesses and could lead to the formation of new hotspots. The viewport's size is anticipated to proposal a variety of distinct points but still cover only an acceptably small fraction of all possible points. View port ratio is calculated based on the rectangle boundary was selected in the image; their corresponding height and width are selected measure the view port.

PCCP coverage ratio is measured by multiplying the image ratio and view port ratio. Compare to PCCP, CCP with pixel based OTP authentication method becomes more efficient for authentication system.

5. CONCLUSION AND FUTURE WORK

5.1 Conclusion

In this system, users first choose an ordered sequence of 5 images and then select single image to click-draw their secrets. At the time of login phase images appear as per the certain series. For registration, user selects 5 images from the image group. User select the image one by one and one image is selected after user click shuffle button then select the next images. Based on the image selection server can generate the signature during registration. While user coming to authentication phase, first step select images from the image pool based on image selected by registration phase and server can generate the signature based on image selection. Second step verify the registration signature with newly generated signature. If both the signature are same the OTP is generate and send to the mobile. Otherwise abort the user. This proposed work provides higher security than other techniques.

5.2 Future Work

Some future works will be carried out and illustrated as follows. To improve the security of the system our future work will consider the multi-factor authentication techniques. Multi-factor technique may combine the graphical password and visual cryptography.

6. REFERENCE

[1] Sonia Chiasson, Elizabeth Stobert, Alain Forget, Robert Biddle, and Paul C. van Oorschot, 2012," Persuasive Cued Click-Points: Design, Implementation, and Evaluation of a Knowledge-Based Authentication Mechanism," to be published in IEEE Transactions, vol. 9, no. 2.

[2] Biddle R, Chiasson S, and van Oorschot P,2012, "Graphical Passwords: Learning from the First Twelve Years," to be published in ACM Computing Surveys, vol. 44, no. 4.

[3] Chiasson S, Biddle R, and van Oorschot P,2007, "A Second Look at the Usability of Click-Based Graphical Passwords," Proc. ACM Symp. Usable Privacy and Security (SOUPS).

[4] Chiasson S, van Oorschot P, and Biddle R,2007, "Graphical Password Authentication Using Cued Click

Points," Proc. European Symp. Research in Computer Security (ESORICS), pp. 359-374.

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

[6] Chiasson S, Forget A, Stobert E, van Oorschot P, and Biddle R, 2009,"Multiple Password Interference in Text and Click-Based Graphical Passwords," Proc. ACM Conf. Computer and Comm. Security (CCS).

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

[8] Jain A, Ross A, and Pankanti S,2006, "Biometrics: A Tool for Information Security," IEEE Trans. Information Forensics and Security (TIFS), vol. 1, no. 2, pp. 125-143.

[9] O'Gorman L, 2003,"Comparing Passwords, Tokens, and Biometrics for User Authentication," Proc. IEEE, vol. 91, no. 12, pp. 2019-2020.

[10] Stobert E, Forget A, Chiasson S, van Oorschot P, and Biddle R,2010, "Exploring Usability Effects of Increasing Security in Click-Based Graphical Passwords," Proc. Ann. Computer Security Applications Conf. (ACSAC).