Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 79 (2016) 561 – 568

Procedia Computer Science

Cued-Click Point Graphical Password Using Circular Tolerance to Increase Password Space and Persuasive Features

Karmajit Patra[a], Bhushan Nemade[b*], Debi Prasad Mishra[c], Prajnya Priyadarsini Satapathy[d]

[a] *Department of IT , College of Engineering and Technology,Bhubaneswar,*[b] *Thakur College of Engineering and Technology, Mumbai.*

Abstract

Graphical password can be used as an alternative to text based (alphanumeric) password in which users click on images to set their passwords. Text based password uses username and password. So recalling of password is necessary which may be a difficult one. Images are generally easier to be remembered than text and in Graphical password; user can set images as their password. Therefore graphical password has been proposed by many researchers as an alternative to text based password Graphical passwords can be applied to workstation, web log-in applications, ATM machines, mobile devices etc. This paper presents implementation of Cued click point (CCP) graphical password which uses circular tolerance. Then it is found that CCP with circular tolerance is better as compared to CCP with rectangular tolerance.

Keywords: Authentication; cued-click point (CCP); tolerance; password space

1. Introduction

Currently, four types of authentication techniques are used which are :

- Token based authentication
- Biometric based authentication
- Knowledge based(KB) authentication
- Mixed based authentication

However, KB authentication is used widely. KB authentication consists of text based (alpha-numeric password) and graphical password (Picture based password).

This research is based on Graphical Password which uses cued click point (CCP) technique for authentication. The CCP method uses a series of images for click point password creation [1]. Here, user clicks on one point per image for a sequence of images. The next image is based on the previous click-point. Here, a small error is found out in the existing CCP which can be modified by using circular tolerance. Also number of image for password creation in CCP can be minimized which helps less memory requirement for storing images.

The research is structured as follows: Section 2 covers related graphical password schemes, and relevant details. Section 3 describes about the current cued click point graphical password, its limitation. Section 4 describes proposed cued click point graphical password. Section 5 describes about system implementation. Section 6 describes about the implementation result and comparison of proposed CCP graphical password to existing cued click point graphical password. At last, future scope of research that fall beyond the scope of this research are described.

* Corresponding author.
E-mail address: dpmishra.07@gmail.com, patra.karmajit@gmail.com,bnemade@gmail.com

Peer-review under responsibility of the Organizing Committee of ICCCV 2016
doi:10.1016/j.procs.2016.03.071

2. Background to the research

Graphical password has been proposed as a possible alternative to text-based password. According to psychological study pictures (images) are generally easier to be remembered or recognized than text. The following related literatures are critically revised so as to provide contextual information which help in the proposed work.

S. Wiedenbeck et al. [5] proposed pass-point graphical password scheme in which password consists of a sequence of five different click points on a given image. During password creation user can select any pixel in the image as a click-points and during authentication the user has to repeat the same sequence of clicks in correct order within a system defined tolerance square of original click-points. Pass-point used the robust discretization technique.

S. Chaisson et al. [1][4] proposed cued click -point which was intended to reduce the HOTSPOT. CCP uses one click point on five different images instead of five click-points on one image. The next image to be displayed is based on previous click-point. While logging if user is unable to recognize the image then it automatically alters the user that their previous click point is incorrect and user can restart from beginning. S. Chaisson et al. [2] proposed Centred Discretization, a simpler discretization method for cued click point that eliminates false accepts and false rejects. It also allows for smaller tolerance regions without impacting the usability of the system.

Ali Mohamed et al [7] proposed Recognition Based Graphical Password interface. Here author have presented “Graphical Password Prototype Design”. Its features is about ease of use, memorize, creation, learning and satisfaction. To create the password the user should choose three images and sort them as he want in some order and save them. While login, user selects only these images for authentication.

Uma D. Yadav, Prakash S. Mohod [3] proposed click based graphical password system that guides, helps and encourages the user for password selection. The system combines the Persuasive features with the cued click point to make authentication system more secure. Basically during password creation the part of an image which is less guessable is highlighted and user has to select the click-point within the highlighted portion. During Login, images are displayed normally and user has to select the click point as chosen at the time of password creation but this time highlighted portion is not present.

3. Existing system

As shown in Fig1 [1], each click results a next-image. This is nothing but a path to traverse a sequence of images.

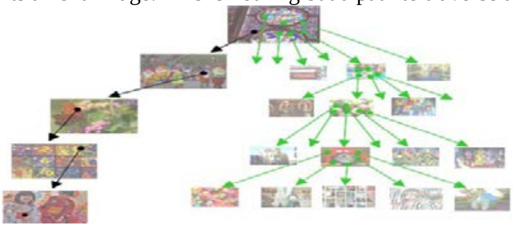


Fig 1- User navigates through images to form a CCP password. Each click determines the next image[1]

3.1 Limitations in the Existing system

- Large Memory Requirement to store images as compared to pass-point
- Small marginal error in the algorithm due to use of rectangular tolerance

3.1.1 Large memory requirement to store images

Here, one user clicks on one point per image. So, other points or pixels are not included for that user, simply wastage of all point. Wastage of all point in one image is nothing but wastage of this image. Suppose password length = 5 in cued click point method. So, first click on one point inside the first image, then next image come, then user repeats the same up to fifth click. So, alternatively user selects five images for password creation. As every user selects five images for their password, so number of images required to store in the server database increases. So, memory requirement increases. Whereas, in PassPoint; user uses five click points on one image. So, one image is sufficient for creating a password of length five rather five images.

Password space of both CCP and PassPoint are same but number of images used in CCP is very much more than that of PassPoint. Cued Click-Points (CCP) is the author’s proposed alternative to PassPoints as in PassPoint; HOTSPOTS arises which is then reduced by CCP.

3.1.2 Small error in the algorithm

S.Chiasson, et al. [2] suggested 2D discretization algorithm to match click point which are entered at the login stage to the original click point which are selected at the registration stage.

Let user clicks a point (x, y) pixel in an image in the registration stage. Let r is the tolerance in pixel, d^x and d^y are offset in X axis and Y axis respectively. i^x and i^y are segment identifier in X axis and Y axis respectively. Then the system calculates the following-

$$\mathbf{i^x = (int)\ (x\text{-}r)/(2*r) \qquad d^x = (int)\ (x\text{-}r)\%(2*r)}$$

$$\mathbf{i^{y} = (int)\ (y\text{-}r)/(2*r) \qquad d^{y} = (int)\ (y\text{-}r)\%(2*r)}$$

Let user clicks a point (x’, y’) pixel in an given image at the login stage. r is the tolerance in pixel which remains constant for both registration stage and login stage. Let $d^{x'}$ and $d^{y'}$ are offset in X axis and Y axis respectively. $i^{x'}$ and $i^{y'}$ are segment identifier in X axis and Y axis respectively. Then the system calculates the following-

$$\mathbf{i^{x'} = (int)\ (x'\text{-}\ d^{x})/(2*r)\ \text{and}\ \ i^{y'} = (int)\ (y'\text{-}\ d^{y})/(2*r)}$$

If $i^{x} = i^{x'}$ & $i^{y} = i^{y'}$, then the click-point (x’, y’) at login stage is accepted otherwise authentication failure occurs. But, it was seen mathematically that, at the login stage there are some point in the image which are larger than the actual tolerance distance, but still these points are accepted. These types of points may be called as false accept point in CCP.

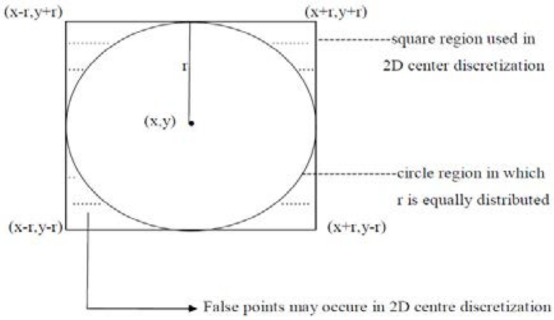

(x-r,y+r)
(x+r,y+r)
square region used in 2D center discretization
r
(x,y)
circle region in which r is equally distributed
(x-r,y-r)
(x+r,y-r)
False points may occure in 2D centre discretization

Fig 2-Occurrence of false accepts in 2D centre discretization

For example-

Registration Phase

Let user clicks a point (x, y)=(16,12) pixel in an given image. Then the system calculates the following in 2D centred discretization as follows –

(x, y)=(16 ,12) pixel r = 9 pixel

$$\begin{array}{ll} i^{x} = (16\text{-}9)/(2*9) & i^{y} = (12\text{-}9)/(2*9) \\ \quad = 7/18=0 & \quad = 3/18=0 \\ d^{x} = (16\text{-}9)\%18 & d^{y} = (12\text{-}9)\%18 \\ \quad =7\%18=7 & \quad =3\%18=3 \end{array}$$

Now (d^{x}, d^{y}) =(7,3) is stored in the database.

Login Phase

Let user clicks a point (x’, y’)=(24,20) pixel in an given image. Then the system calculates the following in 2D centreed discretization -

(x’, y’)=(24 ,21) pixel

$$\begin{array}{ll} i^{x'} = (24\text{-}\ d^{x})/\ (2*9\ ) & i^{y'} = (21\text{-}\ d^{y})/(2*9) \\ \quad = (24\text{-}7)/\ (2*9\ ) & \quad =(20\text{-}3)/(2*9) \\ = 17/18=0 & \quad\quad = 17/18=0 \end{array}$$

As $i^{x} = i^{x'}$ & $i^{y} = i^{y'}$, so the click-point (x’, y’) = (24, 21) pixel is accepted in 2D centred discretization where Let apply distance equation to the above-

$$[(x\text{-}x')^{2} + (y\text{-}y')^{2}]^{1/2} = [(16\text{-}24)^{2} + (12\text{-}21)^{2}\ ]^{1/2} = 12 > r(=9)$$

So, 12 is is greater than the accepted tolerance r(=9), that means overall (24,21) click point is not the correct click point for authentication but it is accepted in 2D centred discretization algorithm. It occurs because false accepts is zero in 1-D space as that are within from the tolerance margin. However, since the same approach was suggested for the 2-D environment without further improvements, false acceptance occurs. When implementing centred discretization in a 2-D space, the tolerance shape is represented as a grid square. Hence, the tolerance distance (r) is not equal around the original click point. But if it is considered the shape as circle around the original click-point within tolerance margin or tolerance distance instead of grid square then this false accept can be avoided. Hence further formulas should extend centred discretization to avoid false accept.

3.2 Suggest a modification in the existing system

In CCP the image is divided into rectangular grids, that is why r is not equally distributed. But if the image is divided into circular grids, then r is equally distributed and this small error can be avoided.

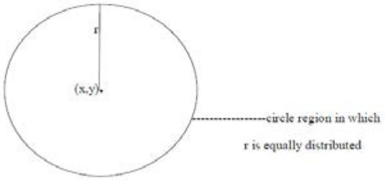


Fig 3 – Circular tolerance

If $[(x-x')^{2} + (y-y')^{2}]^{1/2} <= r$ then (x', y') is within tolerance r and system accepts the entry.
If $[(x-x')^{2} + (y-y')^{2}]^{1/2} > r$ then (x', y') is outside the tolerance r and system rejects the entry although it is located inside the grid square. In a more simplified manner the equation will be-
$(x-x')^{2} + (y-y')^{2} <= r^{2}$
Let we examine (24, 21) point which is used at login phase in the existing CCP.
$[(x-x')^{2} + (y-y')^{2}]^{1/2} = [(16-24)^{2} + (12-21)^{2}]^{1/2} = 12 > r(=9)$
So, 12 is greater than the accepted tolerance r(=9), so the click is rejected and authentication failure occurs.

4. Proposed system

4.1 Proposed System Flow Chart

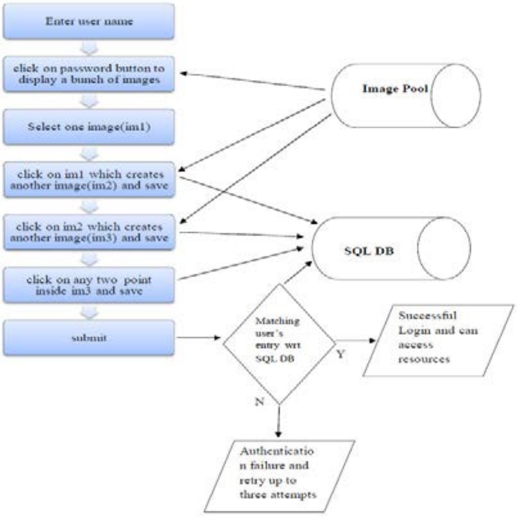

Enter user name
click on password button to display a bunch of images
Select one image(im1)
click on im1 which creates another image(im2) and save
click on im2 which creates another image(im3) and save
click on any two point inside im3 and save
submit
Image Pool
SQL DB
Matching user's entry wrt SQL DB
Y
N
Successful Login and can access resources
Authenticatio n failure and retry up to three attempts

Fig 4- Flow chart of proposed system

4.2 Calculating Password Space

Password space is the total number of unique passwords that could be generated according to the system specifications.
Let size of the image = w × h pixel, where w=width and h=height of the image
Size (Area) of the circular tolerance=$3.14(r+1)^{2}$, where r =tolerance in pixel
So password space= $[\text{size of the image} / \text{tolerance area}]^{n}$, where n=password length
$= [(w \times h)/ 3.14(r+1)^{2}]^{n}$ numbers
For example-
Image size= 451 × 331 pixel, Tolerance(r) =9 pixel
Password space= $(451 \times 331)/3.14 \times (9+1)^{2}$
$=2^{56}$ numbers

5. Implementation

5.1 System Parameter - The following system parameters are used in the coding. Fifty images are used for implementation and the images were collected from internet.

Table 1- List of parameters used with their values

Parameter	Values
Tolerance(r)	9 pixel
Circular tolerance size	3.14 × $(9+1)^2$ pixel
Image size	451×331 pixel
Frame size	600 × 600 pixel
Password length	5
Time duration to see circular tolerance	1000ms

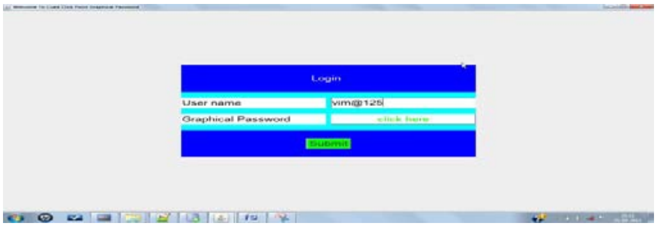
6 Results and Discussion

The proposed system is successfully implemented by using NETBIN IDE and ECLIPSE IDE. Then, snapshots are taken in step wise. The effect of different parameters; such as tolerance size, image size, password space, false accept point are numerically calculated under different boundary conditions. The numerical result for proposed system is compared with the existing system.

6.1 Stepwise implementation result

Login page

The login interface is designed to login to the system. After entering username, then user clicks “click here button” to create graphical password. 4.1show the login interface for the system.



Login

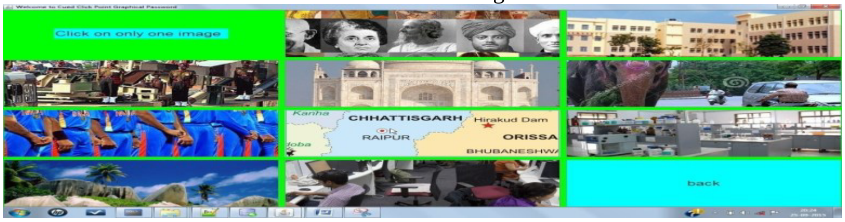
User name vim@125

Graphical Password

Fig 5.1- Login interface

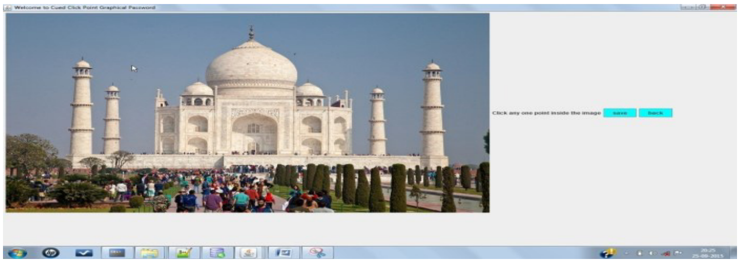
Image Selection

Then the system will direct the user to choose one image in the image selection interface as shown in Figure 4.2. In this interface there are ten images are shown on which user clicks on one selected image.



Click on only one image

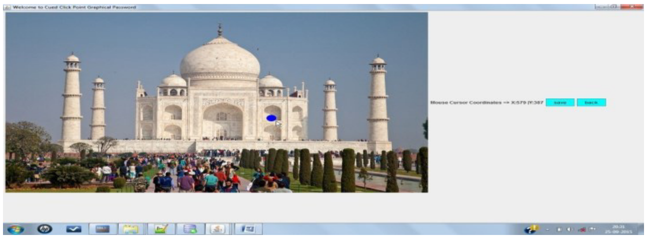
Fig 5.2- Image selection interface



Click any one point inside the image

Fig 5.3 -Selected image

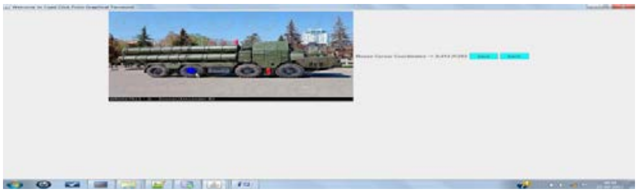
First Click on 1st Image to display 2nd image



Mouse Cursor Coordinates -> X:579 |Y:387

Fig 5.4- first click on 1st image to display 2nd image

Image Displayed after First Click and again click a position on the displayed image to generate third image

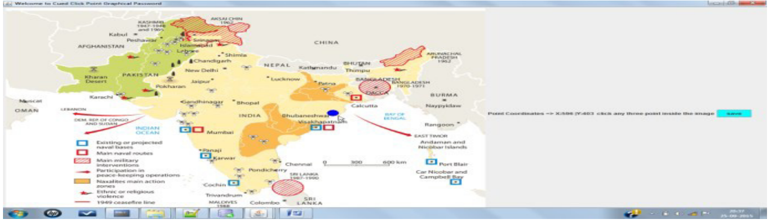


Mouse Cursor Coordinates -> X:[illegible]

Fig 5.5-Second click on 2nd image to display 3rd image

Image Displayed After Second Click and again click a position on the displayed image to generate fourth image

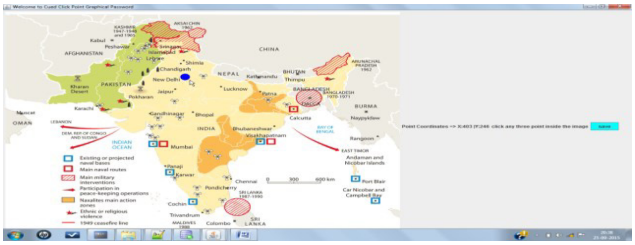
Fourth Click on the third Image



Point Coordinates -> X:506 |Y:403 click any three point inside the image

Fig 5.6- Third click on 3rd image

Fourth Click On 3rd Image

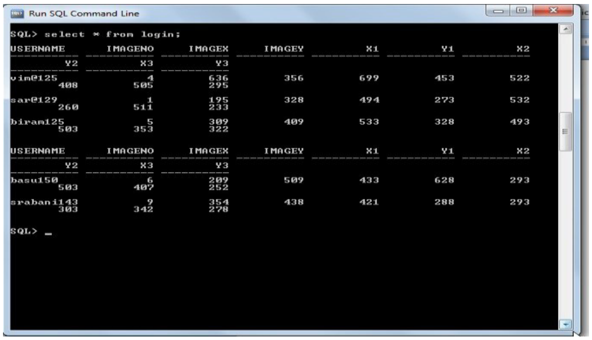


Point Coordinates -> X:403 |Y:246 click any three point inside the image

Fig 5.7- Fourth click on 3rd image

Then submit button is pressed in the login interface to submit the chosen password. Then message box indicate that the password has been saved.

From the above snapshot, total number of images selected for the password length four is three. But it is five for the existing system with same password length. The decrease in two image is due to, two click points on the last image that is third image and no more image displayed after fourth click point. So, memory requirement in the image pool decreases with some extent.



```
SQL> select * from login;

USERNAME      IMAGENO     IMAGEX     IMAGEY         X1         Y1         X2
---------- ---------- ---------- ---------- ---------- ---------- ----------
        Y2         X3         Y3
---------- ---------- ----------
vim@125             4        636        356        699        453        522
       408        505        295

sar@129             1        195        328        494        273        532
       260        511        233

biram125            5        309        409        533        328        493
       503        353        322

USERNAME      IMAGENO     IMAGEX     IMAGEY         X1         Y1         X2
---------- ---------- ---------- ---------- ---------- ---------- ----------
        Y2         X3         Y3
---------- ---------- ----------
basu150             6        209        509        433        628        293
       503        407        252

srabani143          9        354        438        421        288        293
       303        342        278

SQL> _
```

Fig 5.8- Taking five user names and passwords and store it in the SQL D

6.2 Numerical results

Case 1

Tolerance(r)=9 pixel, image size= 451 × 331 pixel ,password length=5

Table 6.1- CCP with rectangular tolerance and circular tolerance for r = 9

CCP Tolerance area type	**Size (In pixel)**	**Password space wrt the above image size**	**% of false accept point wrt tolerance area**
rectangular (▭)	19 × 19	2^{43}	13
circular (◯)	3.14 ×(9+1)^2	2^{56}	0

Case 2

Tolerance(r) = 6 pixel, image size= 451 × 331 pixel, password length=5

Table 6.2- CCP with rectangular tolerance and circular tolerance for r=6

CCP Tolerance area type	**Size (In pixel)**	**Password space wrt the above image size**	**% of false accept point wrt tolerance area**
rectangular (▭)	13 × 13	2^{48}	8.87
Circular (◯)	3.14 ×(6+1)^2	2^{49}	0

From the above two table, it is found that, password space of CCP with circular tolerance is higher than that of rectangular tolerance. The percentage of false accept point is calculated as: [(area of rectangular tolerance- area of circular tolerance) / area of rectangular tolerance]×100 The decrease of password space of rectangular tolerance is due to some error caused by false accepting point. The false accept point of rectangular tolerance can be avoided by circular tolerance.

7 Conclusion and future work

The proposed Cued Click Points is basically based on the nature of click point on the image and circular tolerance. The image and click point are one to one relation in nature till (n-2)th click point where n is the password length. Here, a password length of four uses three images where it is five image for the existing system. Numerical result shows that password space can be increased if circular tolerance is used in place of rectangular tolerance. Also, false accept point can be avoided if circular tolerance is used in the existing system.

Pictures are easier to remember than text based password .So, now a days, it has seen that there is a growing interest in using graphical passwords as an alternative to the traditional text-based passwords. The proposed CCP can be used as an alternative to text based password in the application area like web login, ATM card application, mobile app etc.

Future scope of research that are not yet to be done in this research are-

- Hash function can be used to display random image rather than predefined image for better security.
- The system can be integrated to web application for authentication to access resources.
- The system can be integrated to Mobile App with touch screen facility.

References

[1] Chiasson, Sonia, et al. "Persuasive cued click-points: Design, implementation, and evaluation of a knowledge-based authentication mechanism." *Dependable and Secure Computing, IEEE Transactions on* 9.2 (2012): 222-235.

[2] Chiasson, Sonia, et al. "Centered Discretization with Application to Graphical Passwords." *UPSEC*. 2008.

[3] Yadav, Uma D., and Prakash S. Mohod. "Adding Persuasive features in Graphical Password to increase the capacity of KBAM." *Emerging Trends in Computing, Communication and Nanotechnology (ICE-CCN), 2013 International Conference on*. IEEE, 2013.

[4] Chiasson, Sonia, Paul C. van Oorschot, and Robert Biddle. "Graphical password authentication using cued click points." *Computer Security–ESORICS 2007*. Springer Berlin Heidelberg, 2007. 359-374.

[5] Wiedenbeck, Susan, et al. "PassPoints: Design and longitudinal evaluation of a graphical password system." *International Journal of Human-Computer Studies*63.1 (2005): 102-127. Eljetlawi, Ali Mohamed. "Graphical Password: Usable Graphical Password Prototype." *J. Int'l Com. L. & Tech.* 4 (2009): 298.

[6] Wiedenbeck, Susan, et al. "Authentication using graphical passwords: Effects of tolerance and image choice." *Proceedings of the 2005 symposium on Usable privacy and security*. ACM, 2005. Jermyn, Ian, et al. "The design and analysis of graphical passwords." *Proceedings of the 8th USENIX Security Symposium*.

[7] Eljetlawi, Ali Mohamed. "Graphical Password: Usable Graphical Password Prototype." *J. Int'l Com. L. & Tech.* 4 (2009): 298.

[8] Rajashri, Mr Aniket G. Jadhav Ms, D. Dipak Ms Lavina P. Dadlani, and Mr Mangesh K. Manke. "Graphical Password For Email Application By Persuasive Click Points Using Centered Discretization" (2014).

[9] Gani, Abdullah. "A new algorithm on Graphical User Authentication (GUA) based on multi-line grids." *Scientific Research and Essays* 5.4 (2010): 3865-3875.

[10] Jali, Mohd, Steven Furnell, and Paul Dowland. "Quantifying the effect of graphical password guidelines for better security." *Future Challenges in Security and Privacy for Academia and Industry*. Springer Berlin Heidelberg, 2011. 80-91.

[11] Chiasson, Sonia. *Usable authentication and click-based graphical passwords*. Diss. CARLETON UNIVERSITY Ottawa, 2008.

[12] al-Khateeb, Haider, Carsten Maple, and Marc Conrad. "Enhancing usability and security in click-based visual password systems." (2010).

[13] Lavanya Reddy, L., and K. AIluraiah. "ECCP: Enhanced Cued Click Point Method for Graphical Password Authentication." *International Journal of Advanced Research in Computer Science and Software Engineering, Volume3, Issue8, August2013ISSN X* 2277128 (2013).

[14] Iranna, A. M., and Pankaja Patil. "Graphical password authentication using persuasive cued click point." *International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering* 2.7 (2013).

[15] Dirik, Ahmet Emir, Nasir Memon, and Jean-Camille Birget. "Modeling user choice in the PassPoints graphical password scheme." *Proceedings of the 3rd symposium on Usable privacy and security*. ACM, 2007.

[16] D.Anu Radha "A Persuasive Cued Click-point based Authentication Mechanism with Dynamic User Blocks." IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 1, Issue 1, March, 2013

[17] Suo, Xiaoyuan, Ying Zhu, and G. Scott Owen. "Graphical passwords: A survey." *Computer security applications conference, 21st annual*. IEEE, 2005.

[18] Lashkari, Arash Habibi, et al. "Shoulder surfing attack in graphical password authentication." *arXiv preprint arXiv:0912.0951* (2009).

[19] Lashkari, Arash Habibi, et al. "A Wide range Survey on Recall Based Graphical User Authentications Algorithms Based on ISO and Attack Patterns." *arXiv preprint arXiv:1001.1962* (2010).

[20] Van Oorschot, Paul C., Amirali Salehi-Abari, and Julie Thorpe. "Purely automated attacks on passpoints-style graphical passwords." *Information Forensics and Security, IEEE Transactions on* 5.3 (2010): 393-405.

[21] Hafiz, Muhammad Daniel, et al. "Towards identifying usability and security features of graphical password in knowledge based authentication technique."*Modeling & Simulation, 2008. AICMS 08. Second Asia International Conference on*. IEEE, 2008.

[22] Fulkar, Ashwini, et al. "A study of graphical passwords and various graphical password authentication schemes." *World* 1.1 (2012): 04-08.

[23] Lashkari, Arash Habibi, et al. "A complete comparison on pure and cued recall-based graphical user authentication algorithms." *Computer and Electrical Engineering, 2009. ICCEE'09. Second International Conference on*. Vol. 1. IEEE, 2009.

[24] Suo, Xiaoyuan. "A design and analysis of graphical password." (2006).

[25] Chiasson, Sonia, et al. "Influencing users towards better passwords: persuasive cued click-points." *Proceedings of the 22nd British HCI Group Annual Conference on People and Computers: Culture, Creativity, Interaction-Volume 1*. British Computer Society, 2008.

[26] Chiasson, Sonia, et al. "User interface design affects security: Patterns in click-based graphical passwords." *International Journal of Information Security*8.6 (2009): 387-398.

[27] Chiasson, Sonia. *Usable authentication and click-based graphical passwords*. Diss. CARLETON UNIVERSITY Ottawa, 2008.

[28] Elftmann, Patrick. "Secure alternatives to password-based authentication mechanisms." *Lab. for Dependable Distributed Systems, RWTH Aachen Univ*(2006).

[29] Davis, Darren, Fabian Monrose, and Michael K. Reiter. "On User Choice in Graphical Password Schemes." *USENIX Security Symposium*. Vol. 13. 2004.

[30] Jermyn, Ian, et al. "The Design and Analysis of Graphical Passwords." *Usenix Security*. 1999.

[31] Vachaspati, P. S. V., A. S. N. Chakravarthy, and P. S. Avadhani. "A Novel Soft Computing Authentication Scheme for Textual and Graphical Passwords."*International Journal of Computer Applications* 71.10 (2013).

[32] Birget, J., et al. "Authentication using graphical passwords: basic results”."*ACM International Conference Proceeding Series*. Vol. 93. 2005.