International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 2 | ISSN : 2456-3307

Defensing Online Key detection using Tick Points

P. Prasanth[1], D. Stalin David[2]

[1]PG Scholar, Department of M.Sc(Software Engineering), PSN College of Engineering & Technology, Tirunelveli,Tamilnadu,India
[2]Research Supervisor, Department of M.Sc(Software Engineering), PSN College of Engineering & Technology, Tirunelveli,Tamilnadu,India

ABSTRACT

Usable security has unique usability challenges because the need for security often means that standard human – computer interaction approaches cannot be directly applied. An important usability goal for authentication systems is to support users in selecting better passwords. For this Defensing Online Key detection using Tick points gives four type of image password authentication to allow the register users. The major goal of this project work is to reduce the guessing attacks as well as encouraging users to select more random and difficult passwords to guess. To secure the file and mail server information using graphical images tick or click points passwords.

Keywords: Image encryption, Key Detection, Passwords, Tick points, Wide area network, Point of access, Security through obscurity

I. INTRODUCTION

The main issues of knowledge-based authentication, usually text-based passwords, are well known. Users tend to choose memorable passwords that are easy for attackers to guess, but strong system assigned passwords are difficult for users to remember. In this problem take this project focuses on the integrated evaluation of the Click points, Persuasive Cued Click Points, Crop image, Shuffle image graphical password authentication systems, including usability and security. An important usability goal for authentication systems is to support users in selecting better passwords, thus increasing security by expanding the effective password space. In click-based graphical passwords, poorly chosen passwords lead to the emergence of hotspots (portions of the image where users are more likely to select click-points, allowing attackers to mount more successful dictionary attacks). We use persuasion to influence user choice is used in click-based graphical passwords, encouraging users to select more random, and hence more difficult to guess, click-points. Image Encryption is a wide area of research. Encryption basically deals with converting data or information from its original form to some encrypted form that hides the information in it. The protection of image data from unauthorized access is important. Encryption is employed to increase the image security. The Encrypted Image is secure from any kind cryptanalysis.

The tent map and sine map are mainly used for its iterative process. The image data having special features like bulk capacity, high redundancy, and high correlation among pixels, not to mention that they usually are huge in size, which together make traditional encryption methods difficult to apply and slow to process. Sometimes image applications also have their own requirements like real-time processing, fidelity reservation, image format consistence, and data compression for transmission. By encrypting images, the content still has some degree of added security. The image encryption can be used to protect intellectual properties. Recently, new technologies have been developed which allows multimedia can be delivered to millions of household very quickly. In the future, entertainment industry will utilize Internet and satellites for multimedia distributions. The threat of unauthorized access during transmission over networks and the threat of illegal copy increase significantly. The image encryption will be using in many fields such as Medical Image Security, Surveillance, Software Renewable Security, Internet Multimedia Application.

In this concepts associated with web knowledge. This methodology will be developing the field of web technology. There will be an Admin user how is responsible for Portal settings and Portal Management. A user can able to register in the portal and able to upload Images. When Images are uploaded, object in the images are extracted and using visual feature extraction technique the object will be identified, based on the identification hidden tags are added with the image. When user is searching for the image, he has to provide query word which is compared with image hidden tags as well as post content given by the user and more relevant images are retrieved. To identify the object set of images or image features should be maintained in server database. To conquer the existing problem, we implemented an innovative system by using the object detection process in an image using openCV technique, which is called ACA Portal. When an user posting their images while they chance to forget the comments with the objects, while our proposed system will detect all the objects and provide appropriate image using object detection algorithm, then this objects will extracted from the image and recognized with large Dataset by using RANSAC Algorithm .Once object classification is recognized then classification will be converted to Hash Code (Hashing process) using SHA1 Algorithm for the purpose of more security. This Hash Code will be tagged with image as an automated hidden tag to the posted image. So when a search user trying search some image based query, this query will be converted to hash code and compared with the hidden tag hash code, if both are matching then it will sort with all images and send to the search user. Hence search user never misses any of images with respect to their query search. Consequently our proposed system will be very effective search with high secure. The proposed system innovated with the concept of Automated Concealed Annotation or Auto Hidden Tagging process, when a user upload an image without tag into the web, then the image objects are extracted and their visual features are compared with predefined object features and if there is a match then the auto tag process will add a corresponding hidden tag with that image. When user try to receive the image by query word then the query word will be compared with hidden tags and posted tags, based on the tag match either in post tag or in hidden tag the image will be retrieved and displayed to the search user.

II. RELATED WORK

Our Research work majorly has two processes, one is Offline process and another is online process. The Offline process involved in activities when the user upload an image in the Portal and the Online process involved when a user is providing search keyword & getting the search image.New users are register to this project gives the basic information additionally register the secured graphical passwords. First give the usual information of name, address, date of birth, contact details, mail id, passwords, in the basic registration page. Next is click points is take five click points in single image, persuasive cued click points is take image is split small area tovisible one Alphanumeric character, crop image is take as crop image x,y,height,width values, shuffle image is take three image filename finaly check user registeration details it is ok finally registration finished. When the user upload an image he as to provide image but he may or may not provide comments about the image. In this process there is an object detection technique. This process will identify the objects in the image and extract it separately. The next step is visual feature extraction, for the entire object extracted in previous step, visual feature is generated & generated visual feature are compared with pre-stored object feature in the server. Based on comparison result the object identification is happen. Once object is identified auto tagging process will select corresponding tag names and link with images which are called hidden tags or auto tags.

Password selection module is display the four type of password if select one that is redirect to page selected module. Only allows register user and allow the password selection .In this process user has to provide query words for which he wants retrieve the image. The query words are usually search with the comments which are inputted by the user during upload process where as in this system query words are do search process with auto tags and user comments. Based on matched tags corresponding images are retrieved.

Unlike text messages, image data have special features such as bulk capacity, high redundancy, and high correlation among pixels, not to mention that they usually are huge in size, which together make traditional encryption methods difficult to apply and slow to process. Sometimes image applications also have their own requirements like real-time processing,

fidelity reservation, image format consistence, and data compression for transmission.

Simultaneous fulfilments of these requirements, along with high security and high quality demands, have presented great challenges to real-time imaging practice. One example is the case where one needs to manage both encryption and compression. In doing so, if an image is to be encrypted after its format is converted, say from a TIFF file to a GIF file, encryption has to be implemented be-fore compression.

However, a conventional encrypted image has very little compressibility. On the other hand, compression will make a correct and loss-less decipher impossible, particularly when a highly secure image encryption scheme is used. This conflict between the compressibility and the security is very difficult, if not impossible, to completely resolve.

III. IMPLEMENTATION OF PROPOSED SYSTEM

This paper consists of three units: permutation at pixel level unit, masking and permutation at bit level and performing affine transformation. In permutation at pixel level we are swapping the RGB components at pixel level. In masking and permutation at bit level we are implementing the tent and sine map to perform the key generation. From the result of hybrid tent and sine map we are choosing the three random numbers. In affine transformation we are multiplying the each RGB component with the randomly chosen numbers. Then the resultant matrix should be analyzed using three tests such as difference between the plain and the encrypted images, correlation coefficient analysis and information entropy analysis. In order to implement this idea we are using three modules such as Permutation at pixel level, Masking and permutation at bit level and Affine transformation. Initially all the components should be separated and then swapping operation should be performed using the rows and columns of the each components. At first swapping should be move towards right and the other two components should follow the same process. Then red components then move towards downward and these processes should be followed for the green and blue components. To address the issue of hotspots, Persuasive Cued Click Points (PCCP) was proposed. As with CCP, a password consists of five click points, one on each of five images. During password creation, most of the image is dimmed except for a small view port area that is randomly positioned on the image. Users must select a click-point within the view port. If they are unable or unwilling to select a point in the current view port. The view port guides users to select more random passwords that are less likely to include hotspots.

Password consist on a one image, user must crop the particular view port. User first starting click point consider is x and y, then drag the remaining position consider height and width. This x, y, height and width points are stored in the data base. When the user login time crop the particular position in the image, that points are compared to the database value. First retrieved x, y points from the database, one or two pixel values are increase are decreased from that point, because user remember only the cropped image not only the x, y values. Because this project is user friendly.

Column Name	Data Type
intId	Int(11) AUTO_INCREMENT, Primary Key
varName	varchar(100)
varAddress	varchar(500)
varContact	varchar(15)
varGender	varchar(15)
varDob	varchar(15)
varEmail	varchar(200)
varPassword	varchar(100)
varCp	varchar(200)
varPccp	varchar(200)
varCrop	varchar(200)
varShuffle	varchar(200)
intSflcount	Int(11)

Column Name	Data Type
intId	Int(11) AUTO_INCREMENT, Primary Key
varTo	varchar(100)

varFrom	varchar(100)
varSubject	varchar(100)
varDate	varchar(100)
varFilename	varchar(100)
varUrl	varchar(500)

In masking we are using the tent and sine to generate the key for the encryption. The output from the tent formula should be given as an input to the sine formula. Then generating the sequence of matrix and reshape the matrix for the particular format then choose the random numbers is between 0 to 255.

In affine transformation multiply randomly chosen from the hybrid tent and sine map with the each matrix. Then add the matrix value with randomly chosen number. Generate the histogram for the obtained matrix and then results analysis should be performed for the obtained matrix and the actual matrix.

IV. RESULT ANAYSIS

The result analysis should be done to define the efficiency of the proposed system. In this system three security analysis should be done to define the difference between the encrypted image and the actual image. The first test is find the difference between the plain and the encrypted image (NPCR), then correlation coefficient analysis and then information entropy analysis.

The Number of Pixels Change Rate (NPCR) measure the percentage of different pixel values between two images. It is calculated for plain image and encrypted image.

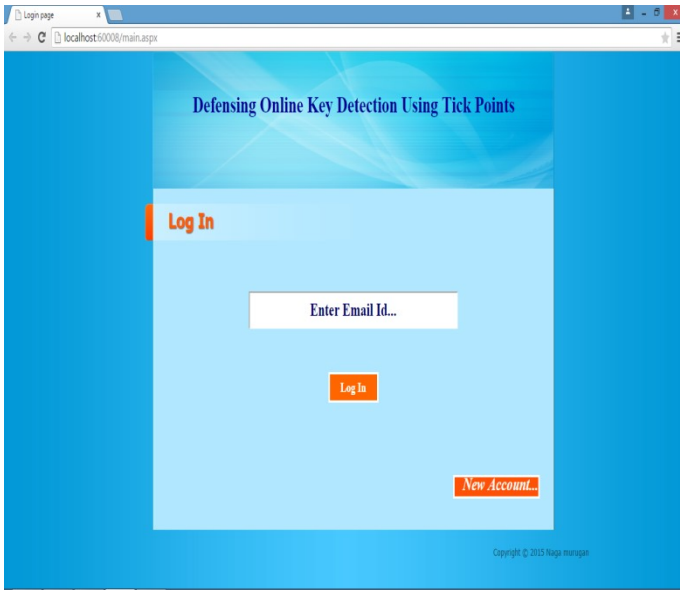
$$NPCR = \sum_{i,j} \frac{d(i,j)}{mn} \times 100\%$$

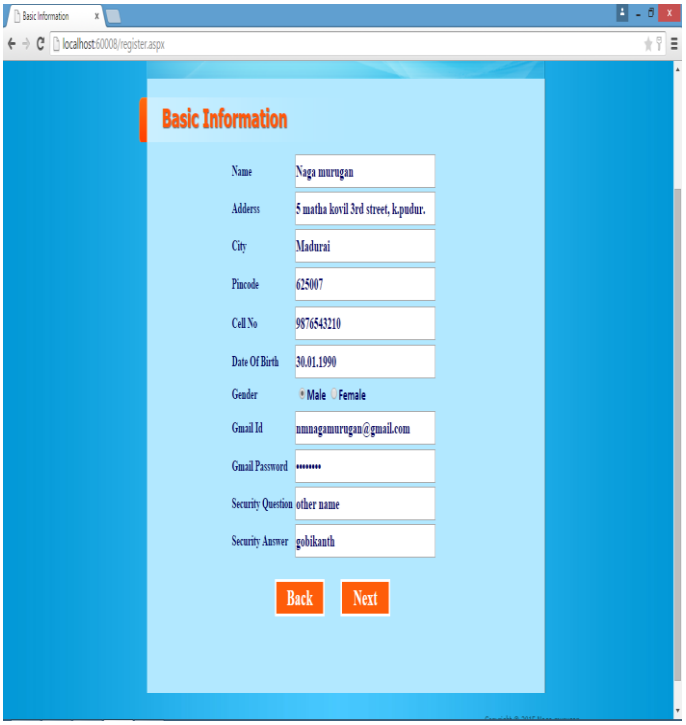
Where m and n are the width and height of the encrypted image. The NPCR value of the proposed systems achieved to 99.67%Histogram illustrates the distribution of pixels of an image. Histogram plays an important role in the security analysis. In our proposed system the encrypted image is taken for the histogram test. Then it is compared to the plain image histogram. Encrypted image should have histogram uniformity. The first module is to separating the RGB components using shifting and swapping operation using permutation process. At first swapping should be move towards right and the other two components should follow the same process. This paper consists of three units: permutation at pixel level unit, masking and permutation at bit level and performing affine transformation. In permutation at pixel level we are swapping the RGB components at pixel level. In masking and permutation at bit level we are implementing the tent and sine map to perform the key generation. From the result of hybrid tent and sine map we are choosing the three random numbers. In affine transformation we are multiplying the each RGB component with the randomly chosen numbers. Then the resultant matrix should be analyzed using three tests such as difference between the plain and the encrypted images, correlation coefficient analysis and information entropy analysis. In order to implement this idea we are using three modules such as Permutation at pixel level, Masking and permutation at bit level and Affine transformation. Initially all the components should be separated and then swapping operation should be performed using the rows and columns of the each components. At first swapping should be move towards right and the other two components should follow the same process. Then red components then move towards downward and these processes should be followed for the green and blue components. Encrypted image should have histogram uniformity. The first module is to separating the RGB components using shifting and swapping operation using permutation process. Then red components then move towards downward and these processes should be followed for the green and blue components. Encrypted image should have histogram uniformity. The first module is to separating the RGB components using shifting and swapping operation using permutation process. At first swapping should be move towards right and the other two components should follow the same process. This paper consists of three units: permutation at pixel level unit, masking and permutation at bit level and performing affine transformation. In permutation at pixel level we are swapping the RGB components at pixel level. In masking and permutation at bit level we are implementing the tent and sine map to perform the key generation. From the result of hybrid tent and sine map we are choosing the three random numbers. This paper consists of three units: permutation at pixel

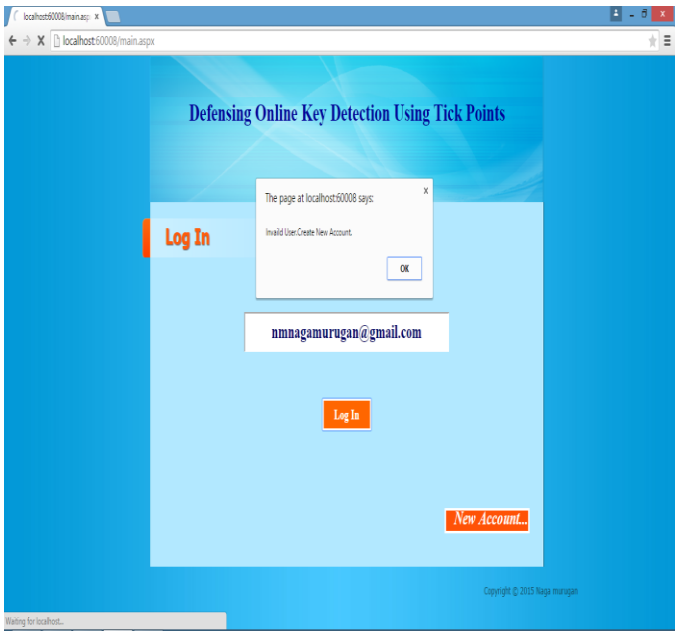
level unit, masking and permutation at bit level and performing affine transformation. In permutation at pixel level we are swapping the RGB components at pixel level. In masking and permutation at bit level we are implementing the tent and sine map to perform the key generation. From the result of hybrid tent and sine map we are choosing the three random numbers. In affine transformation

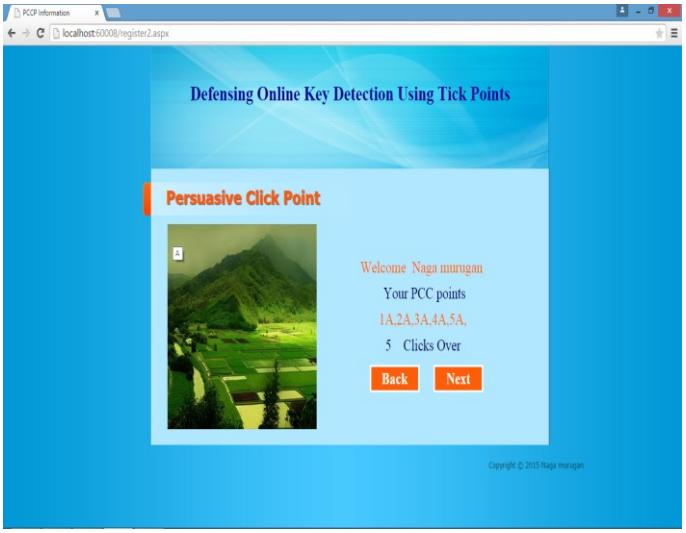
V. IMPLEMENTATION RESULTS

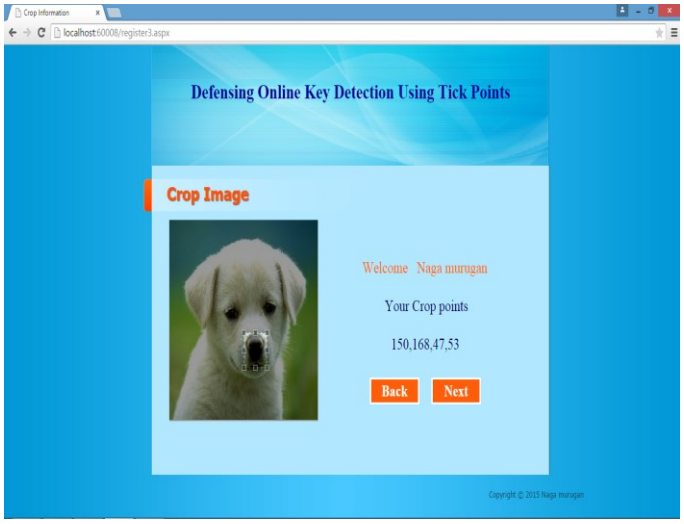
The implementation results can be shown as figure below

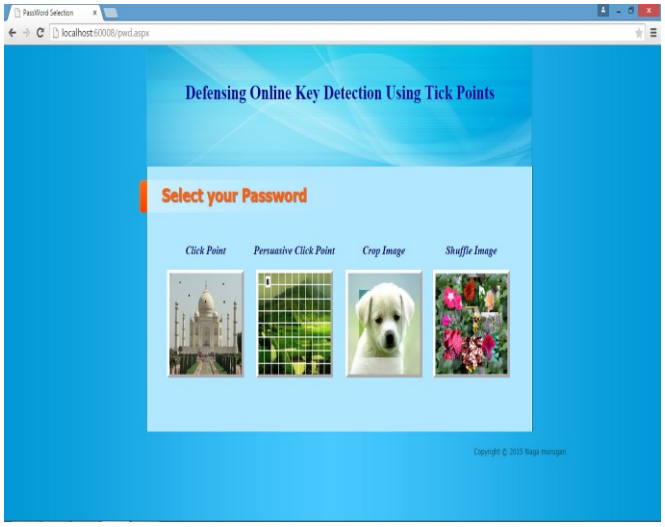




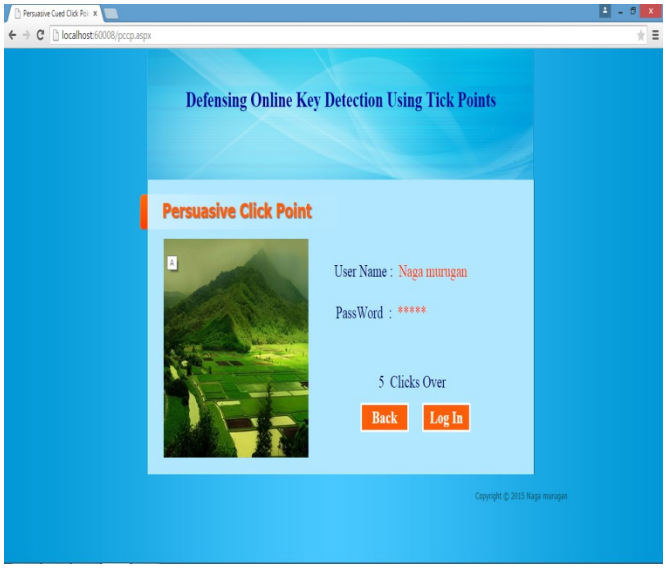


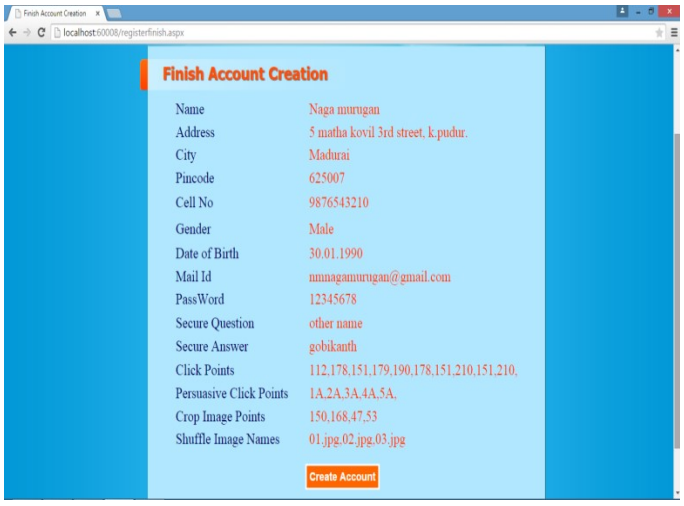


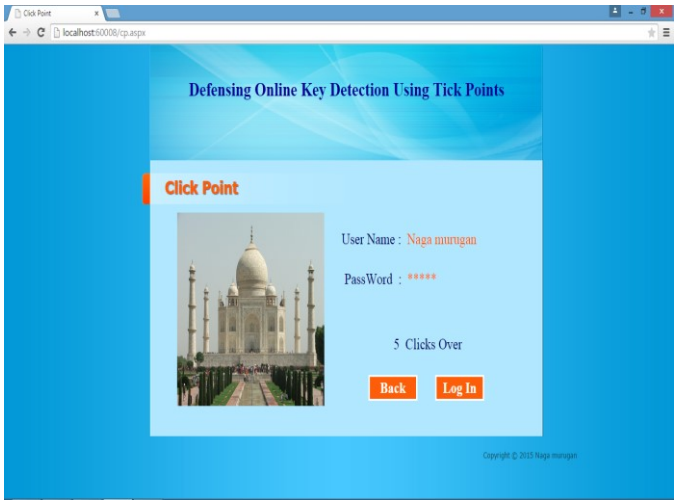

Defensing Online Key Detection Using Tick Points
Crop Image
Welcome Naga murugan
Your Crop points
150,168,47,53
Back
Next

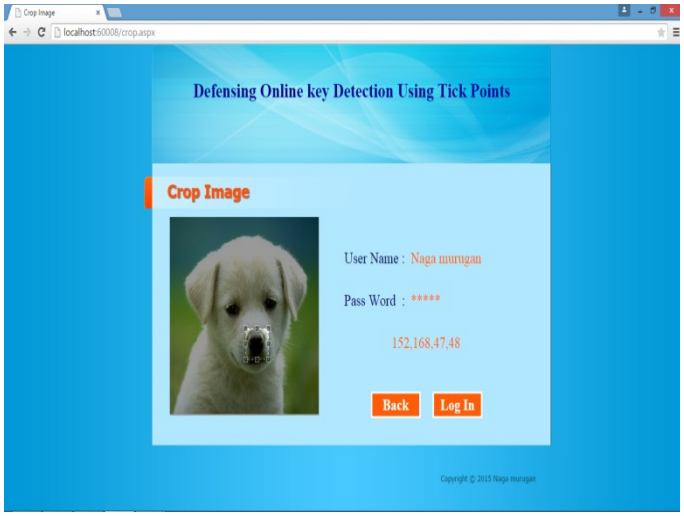

Defensing Online Key Detection Using Tick Points
Select your Password
Click Point
Persuasive Click Point
Crop Image
Shuffle Image

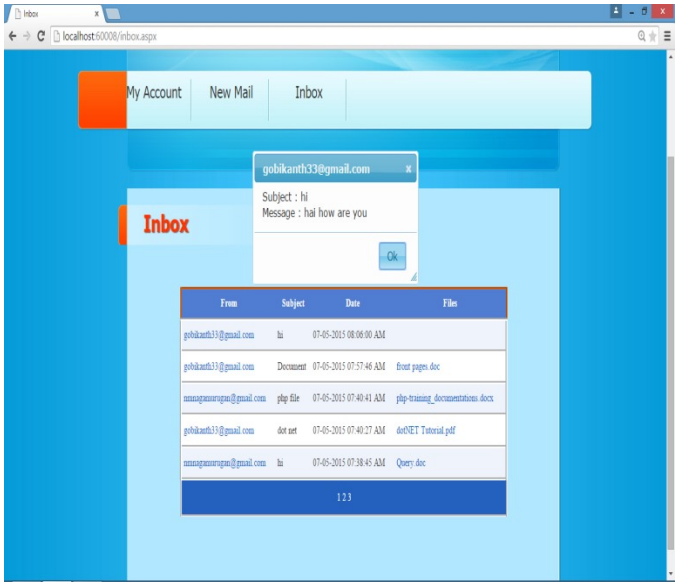

Defensing Online Key Detection Using Tick Points
Shuffle Image
Welcome Naga murugan
Your Selected Images
01.jpg 02.jpg 03.jpg
3 Click Over
Back
Next


Defensing Online Key Detection Using Tick Points
Persuasive Click Point
User Name : Naga murugan
PassWord : *****
5 Clicks Over
Back
Log In


Finish Account Creation
Name Naga murugan
Address 5 matha kovil 3rd street, k.pudur.
City Madurai
Pincode 625007
Cell No 9876543210
Gender Male
Date of Birth 30.01.1990
Mail Id nmnagamurugan@gmail.com
PassWord 12345678
Secure Question other name
Secure Answer gobikanth
Click Points 112,178,151,179,190,178,151,210,151,210,
Persuasive Click Points 1A,2A,3A,4A,5A,
Crop Image Points 150,168,47,53
Shuffle Image Names 01.jpg,02.jpg,03.jpg
Create Account


Defensing Online Key Detection Using Tick Points
Click Point
User Name : Naga murugan
PassWord : *****
5 Clicks Over
Back
Log In





VI. CONCLUSION

A major advantage of Tick point, Persuasive cued click point, crop, shuffle passwords easy to understand and user's brain easy to store image and it gives strong password to easy access help to interface for images this scheme is its large password space over alphanumeric passwords. There is a growing interest for Graphical passwords since they are better than Text based passwords, although the main argument for graphical passwords is that people are better at memorizing graphical passwords than text-based passwords. Online password guessing attacks on password-only systems have been observed for decade's .Present-day attackers targeting such systems are empowered by having control of thousand to million node botnets. In previous Text-based login protocols, there exists a security-usability trade-off with respect to the number of free failed login attempts. In contrast, Graphical is more restrictive against brute force and dictionary attacks while safely allowing a large number of free failed attempts for legitimate users. Graphical is apparently more effective in preventing password guessing attacks, it also offers more convenient login experience, Graphical appears suitable for organizations of both small and large number of user accounts.

VII. REFERENCES

[1]. H. Lidong, Z. Wei, W. Jun and S. Zebin, "Combination of contrast limited adaptive histogram equalisation and discrete wavelet transform for image enhancement," in IET Image Processing, vol. 9, no. 10, pp. 908-915, 10 2015.

[2]. H. Xu, G. Zhai, X. Wu and X. Yang, "Generalized Equalization Model for Image Enhancement," in IEEE Transactions on Multimedia, vol. 16, no. 1, pp. 68-82, Jan. 2014.

[3]. W. Fan, K. Wang, F. Cayre and Z. Xiong, "Median Filtered Image Quality Enhancement and Anti-Forensics via Variational Deconvolution," in IEEE Transactions on Information Forensics and Security, vol. 10, no. 5, pp. 1076-1091, May 2015.

[4]. T. Celik, "Spatial Entropy-Based Global and Local Image Contrast Enhancement," in IEEE Transactions on Image Processing, vol. 23, no. 12, pp. 5298-5308, Dec. 2014.

[5]. M. Nikolova and G. Steidl, "Fast Hue and Range Preserving Histogram Specification: Theory and New Algorithms for Color Image Enhancement," in IEEE Transactions on Image Processing, vol. 23, no. 9, pp. 4087-4100, Sept. 2014.

[6]. L. Wang, L. Xiao, H. Liu and Z. Wei, "Local brightness adaptive image colour enhancement with Wasserstein distance," in IET Image Processing, vol. 9, no. 1, pp. 43-53, 1 2015.

[7]. X. Fu, J. Wang, D. Zeng, Y. Huang and X. Ding, "Remote Sensing Image Enhancement Using Regularized-Histogram Equalization and DCT," in IEEE Geoscience and Remote Sensing Letters, vol. 12, no. 11,

[8]. F. Kou, W. Chen, Z. Li and C. Wen, "Content Adaptive ImageDetail Enhancement," in IEEE Signal Processing Letters, vol.22, no. 2, pp. 211-215, Feb. 2015.

[9]. S. Kwon, H. Lee and S. Lee, "Image enhancement with Gaussian filtering in time-domain microwave imaging system for breast

cancer detection," in Electronics Letters, vol. 52, no. 5, pp. 342-344, 3 3 2016.
[10]. Y. V. Shkvarko, J. I. Yañez, J. A. Amao and G. D. Martín del Campo, "Radar/SAR Image Resolution Enhancement via Unifying Descriptive Experiment Design Regularization and Wavelet-Domain Processing," in IEEE Geoscience and Remote Sensing Letters, vol. 13, no. 2, pp. 152-156, Feb. 2016.
[11]. Sanjay Kumar Maurya et al, "Image enhancement by intensity based interpolation and selective threshold", in IEEE International Conference on Communication Systems and Network Technologies,pp.174-178,2012.
[12]. A.Temizel et al ,"Wavelet domain image resolutionenhancement using cycle-spinning", Electron.Lett.,vol 41,no.3,pp.119-121,Feb.3,2005
[13]. Hasan et al,"Image Resolution Enhancement by using discrete and stationary Wavelet decomposition", in IEEE Transactions on Image Processing, vol. 20, no. 5, pp. 1458-1460, May. 2011.
[14]. Jianwei et al, "The Curvelet Transform: A review of recentapplications.", in IEEE Signal Processing Magazine,2010.