International Journal of Research in Advanced Engineering and Technology
ISSN: 2455-0876, Impact Factor: RJIF 5.44
www.engineeringresearchjournal.com
Volume 2; Issue 3; May 2016; Page No. 24-27

Review of graphical password: Pass image edge detection

Smita Patil

Computer Dept, PREC, Loni, Rahata Taluk, Ahmednagar, Maharashtra, India.

Abstract
Earlier for improving password usability and security multiple graphical password schemes are proposed and one of the important aspect of the graphical password schemes is security so this is useful for the introduction of attacks and also provides an in-depth analysis with specific schemes and they are categories in four way as according to authentication style and provides introduction and analysis for each schemes highlight security aspect. Edge pass uses to extract the edge of pass image for a graphical password. It is technique which based on calculating area in plane bounded by graph and this is the first step in graphical password system. It uses edge detection, image fusion and high frequency element extraction so the basic idea of algorithm is to be found process pixel I(x, y) is dark or light if it is light that is pixel I(x, y) then it can be called as edge else it should be background.

Keywords: improving password usability, Drawmetric schemes, Locimetric schemes, Cognometric schemes

1. Introduction

Generally a user authentication is a providing the user to key in their user name and password. This type of authentication of a user is used in many system. In survey's we found that many user choose easy password so they remember easily. Graphical password system or a technique is an alternative option to text based passwords. This paper focus on a graphical password system rather than text or alphanumeric passwords because user can easily understand image. on the other side edge detection is very important task for identify an object because humans can easily remember objects which is based on a edges from the above concept we are able to implement a graphical password authentication which is based on the edges and some other important concepts. Nowadays, password authentication is popular method which ensures guarantee information security as authentication is important aspect. We are familiar with traditional password schemes which uses string, alphanumeric characters, letters and digits, but due to limitation of memory of human users most users choose to set small or simple which can easily find out so this traditional schemes evolve security issue. Nowadays user have multiple account on social network, E-mails and on personal computer so they may choose to set same words for different account to reduce their brain work and memory burden but this methods also reduces security and alphanumeric password are also weak or insecure for the spyware attack, social engineering and shoulder surfing attack. More of the password attack also can be done by spyware and simple key-logging software and this attack can be avoided.

Methods for security

One of the method to improve the security is graphical password technique it is proposed in 1996 as alternative solution for the text based. the graphical password that are mainly depends on image rather than alphanumerical the main feature of this method is users are better at memorizing and recognizing image and it is also difficult for attackers to steal images and if the number of images in set is large then it becomes more difficult. These are the knowledge based mechanism the main goal of this scheme is to use images or shape to replace the text as the recognizing images are easy for users. This processes also known as dual coding theory. The image are represented in such way the perceptual feature is being observed and the text is represented using the symbols that convey some meaning so it is very easy for user re-merging images

The edge pass algorithm is most useful technique in graphical password scheme. The algorithm extract the edge of pass image and calculate area in plane bounded by graph. In this approach edge detection is very important task for identifying particular object because humans can easily recognize object based in the edges. The most important feature of the edge detection algorithm is a) it can be usable anywhere at any time and faster authentication. b) This is the easiest and simple was to train users. C) This is best method because it is easy to remember the images than password. d) It is the most secure method as system will provide strong defense against several type of attacks like shoulder surfing, brute force and guess attacks. These are methods for security.

2. Related Work

In general, graphical password schemes can be classified into two type that are recall based approach and recognition based [11]. In recall based approaches, the user is required to reproduce an event or to choose something he/she has select between the registration phases.

Numerous schemes have proposed by researchers for recall based technique such as jermnt.*et al*, developed technique where the appropriate user is to draw a shape as his/her secret information [7]. Another algorithm is proposed by Wiedenbeck *et al*, in their approach the appropriate user is supposed to select a preregistered point in the test image [10]. Also the recall based, recognition based is also widely developed. In this type user will have a challenges set which contains decoy and pass image. The decoy image are randomly generated by scheme between the verification process and other hand

password image will be users selected images. Basically authentication is very simple an appropriate user needs to correctly identify pass image from challenge set and then he/she will be authenticated.

Earlier the Déjà vu was system which was depends on the has virtualization algorithm. Random art is one of the systems that generates image from an algorithm. For authentication purpose, an appropriate user is required to recognize the pass image from a challenge set.

Again, another scheme is introduced by Harada, *et al.,* they produce a monochrome from the user pass image look noisy. In that alpha bending was used for pass and decoy image. Unfortunately, this approach was difficult for user to identify or recognize the pass image because the generated image looks noisy and unclear to the users.

Medoka, *et al*, proposed a user authentication method which relies on combining an underlying frequency component of the decoy image with a high frequency component of the user pass images [12].

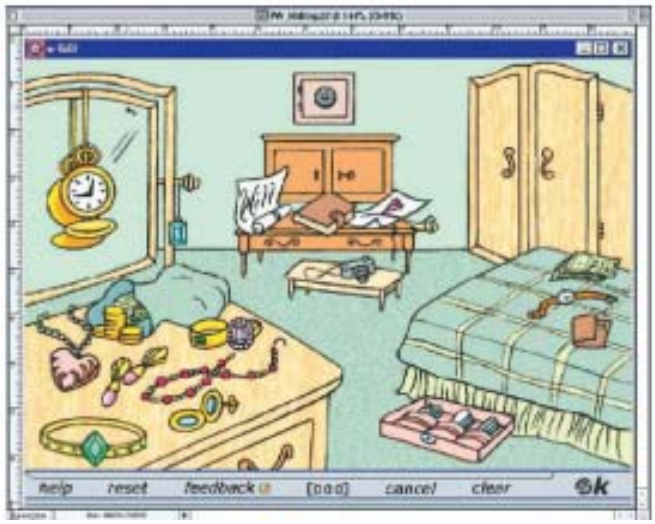

Fig 1: recall-based technique developed by Passlogix

3. Categorization of graphical password

Graphical password scheme have been proposed by blonder. Graphical password scheme classified into four categories that are drawmetric schemes, locimetric schemes, cognometric schemes and hybrid schemes. Hybrid schemes combine two or more of drawmetric, locimetric and also cognometric schemes

A. Drawmetric schemes

Draw metric schemes also called as recall based schemes. In this schemes a user reproduces an outline drawing on a grid that selected between the registration stages. DAS (draw a secret) was first scheme in draw metric schemes. DAS was proposed by Jermyn. In this schemes a user is asked to draw an intelligible picture using a mouse or stylus. In this scheme, a user is asked to draw an intelligible picture using a mouse or stylus. The drawing is consisting of one continuous stroke or several strokes separated by "pen-ups", on an N×Ngrid (usually a 5×5grid). The picture is mapped to a series of coordinate's pairs of the grid cells. This for a successful login, the user needs to re-draw the picture. The historical significant of DAS is language independent, making it abreast available to each user. Users are liberated from recurrence any alphanumeric string. However, there are some restrictions on drawing which impact on the usability performance of DAS, such as assuring every stroke is off the grid lines and redrawing in the exact position.

B. Locimetric schemes

Locimetric schemes also known as click based graphical password schemes are based on the loci method, san old and well known mnemonic. In Locimetric schemes, a user is feed with an image so that he or she can select any point in the specified region or any location in the image as a password click point. Blonder, the first graphical password scheme, was proposed in 1996, required the user to click on predetermined areas (or tag regions) of the predetermined graphical image in a predetermined sequence, as a resource of entering a password. This scheme possessed discrete advantages on to alphanumeric passwords. First, people generally find images easier to recall than alphanumeric sequences, particularly images with personal meaning. Second, such password scheme provides higher security than alphanumeric passwords, and even a very coarse matrix of predetermined areas yields increased security. However, Blonder's authentication system had some disadvantages. For example, predefined regions should be readily identifiable and the number of predefined regions is small, perhaps a few dozen in a picture. The password may require many clicks for adequate security increasing tedium for the users. In addition, it is more vulnerable to shoulder surfing compared to alphanumeric passwords.

C. Cognometric schemes

cognometric schemes are also called as recognition based schemes or search matrices schemes, involvement identifying whether one has seen an image before. In this schemes, the user creates a password by select several image from a large portfolio of image, by selecting image becoming the users password. Until authentication the user must successfully to endorse his/her password image from decoy image. Dhamija *et al*. Proposed Déjà vu in 2000, where users to choose a secure number of random art pictures from a set of pictures generated by a program in the registration stage. During authentication, the system shows a challenge to keep that contains both password pictures and decoy pictures. The user must to endorse which are the password pictures. It is convenient to store and transmit the art images generated by short primary seeds. Moreover, the art images make it hard to record or share with others. Déjà vu has discrete drawbacks, for instance, an obscure picture is difficult to remember and the password space is much smaller than that of alphanumeric passwords.

D. Hybrid schemes

Hybrid schemes are typically the combination of two or more of drawmetric schemes, locimetric schemes and also cognometric schemes. Hybrid schemes are used to overcome the limitations of a single scheme, such as shoulder surfing, hidden camera, or spyware, etc. We will provide a detailed depiction of these schemes, focusing on memory mode and initial function.

Jiminy uses image cue for helping user's selection easily to remember passwords. In this scheme, users are feed with

templates based on color that contain separate holes. The user first eclectic an image, chooses a colored template, picks a specific locality inside the image, then clicks on the position to location the template and lodgment the password. Between login, the users must analects the right template, place it on the correct location on the image then enter the characters visible through the holes from top to bottom. Compared to remembering alphanumeric passwords, this scheme only requires users to remember the precise location of template on the image. However, experiments show that users have difficulty in remembering precise locations and their selections tend to be predictable, suggesting doubt about the efficacy of hotspot resistance.

By using CAPTCHA i.e. (Completely Automated Public Turing tests to tell Computer and Humans Apart), proposed by GAO el at., retains benefit of graphical password schemes, while simultaneously to increase the expense for adversaries by orders of magnitude. In the register stage, user's eclectic and recall images as their password images (pass-images). To be authenticated, the user require to distinguish his pass-images as well as complete a test by recognizing and typing the adjunctive string beneath each pass-image. Although this scheme is nearly impossible for automated programs, it could be in dangerous if the adversary is a person and uses spyware as an assistant.

4. Edge detection

Calculating areas, identifying objects and others image segmentations are depends upon the edge detection. So, edges are an important part in digital image processing. Change from one pixel intensity to another is called an edge detection that creates a variation in the picture. Pixels with high intensity is known as edges and other parts is called as background. So, edges are very useful for visual processing.

Important features of an images such as the shape of the object in scene is shown by edge detection and this will reduce the quality of the data to be processed, so this technique is very important for computer vision. The important point is edge detection is to expand the lines in images which has an orientation and representation [6].

The algorithms of an edge detection in computer vision are depends on the detection of geometrical and physical properties of the objects

5. Proposed Graphical Password

The basic phases of our graphical password are shown in fig

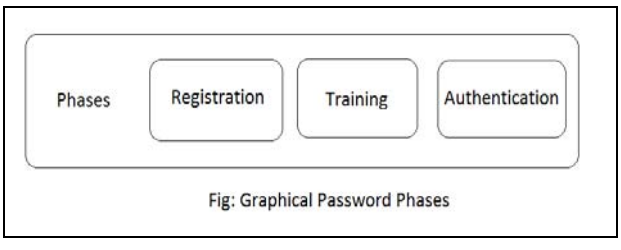

Fig: Graphical Password Phases

From above fig there are 3 phase's registration, training and authentication. Under the registration phase user are able to choose the pass images for the verification phases. In the training phase the proposed algorithm is used to train the user in how or she can recognize the pass-images from challenge set.

Generally the framework consists of the changing of the raw image to a gray scale followed by the edge detection and also high spatial frequency component as shown in fig.

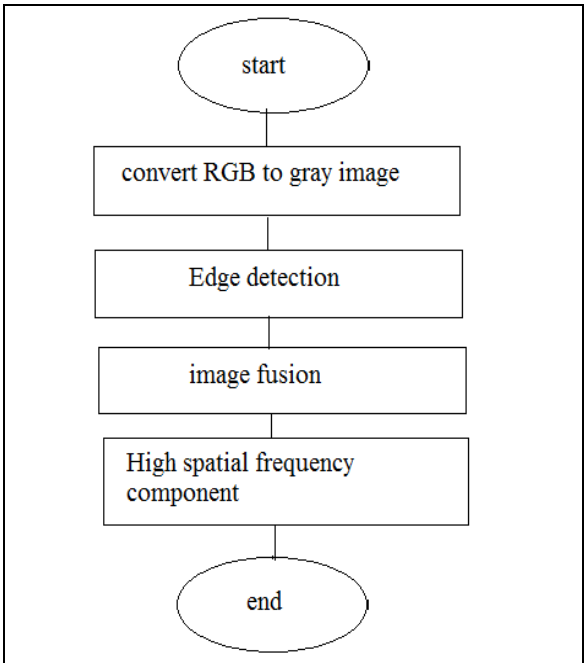

fig.proposed graphical password system

Edge pass algorithm

1. convert image to RGB
2. 2. insert 16 pixel from the input image into matrix H and pad the rest with 0
3. calculate standard deviation N, variance V and mean x for H
4. Calculate new matrix K
5. Perform cumulative trapezoid Z on H and K
6. decide whether the target pixel is in a light or a dark K region based on the Z/V:
7. Assign Y.

6. Edgepass Algorithm

The concept of edge pass is use to check weather cumulative trapezoid integration of a matrix (H, K) of given pixel I(x, y) is dark or light. If the value of target pixel y lights then the target pixel y is an edge. Else it is a background. Our proposed technique is depends upon the use of numerical integration which is a trapezoidal rule to approximate the definite integral where integral is defined as

$$\int_a^b f(x)\,dx = (b-a)\frac{f(a)+f(b)}{2} \qquad (1)$$

Where (b-a) is the height

A. Image Pre-Processing

From the following fig in first step converts the raw images to various appropriate formats such as RGB, or other suitable format for edge detection

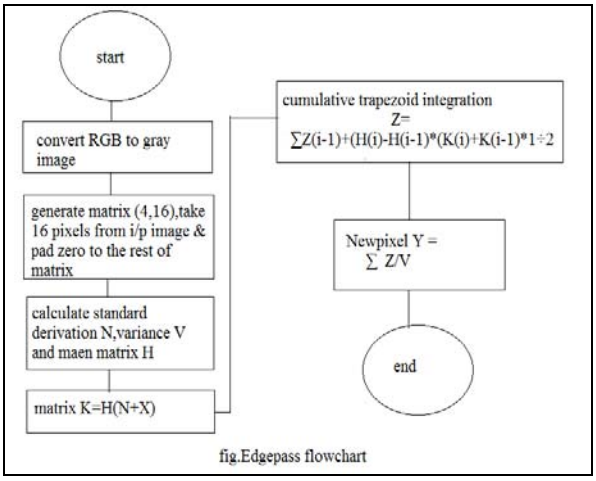

fig.Edgepass flowchart

B. Matrix H creation and Padding

In the 2nd step matrix H is generated with size of (4, 16). Then 16 pixels from the input image is inserted while the rest of indexes are padded with zero.

C. Edge Detection

In this step ie in 3rd step matrix H padded with zeros; std deviation N, variance v and mean X of H are calculated based on below formulas 3, 4, 5

$$\sigma^2 = \sqrt{1/n \sum_{i=1}^{n} (X - \hat{X})} \qquad (3)$$

Where,

N= number of values
Xi= represents each values in the population
σ = is the std deviation
x = is the mean of population

$$\sigma^2 == \frac{\sum (x-\mu)^2}{n} \qquad (4)$$

μ = mean, numbers of values,
σ = is the variance and
x = represent each value in H.

$$\overline{x} = \frac{\sum_{i=1}^{n} Xi}{n} \qquad (5)$$

X= matrix H values
N= number of the values in H

In the next step matrix K is prepared to be used for cumulative trapezoid integration as shown in following equation

$$K=H-(N+X) \qquad (6)$$

In the fifth step, the cumulative trapezoid formula uses a step size of for our scheme and defined in equation 7:

$$Z=\sum Z\,(i-1) + (X\,(i)-X(i-1)x(Y(i)+Y(i-1)x\,\frac{1}{2} \qquad (7)$$

Where Z contains entire cumulative trapezoid values and I is the number of trapezoid. X represent matrix H and Y represents and Y represents the matrix K.

In the final step, to obtain the edge pass for a pixel Y defined as:-

$$Y=\sum \frac{Z}{V} \qquad (8)$$

Z= cumulative trapezoid values
V= variance of H
Y= target pixel values

Light means the result of the target pixel Y is within the range of white pixel in gray scale. Otherwise, it's dark.

7. Conclusion

This exploration paper introduced an algorithm for edge detection based on numerical integration. The implementation of this algorithm gives idea about to find whether the processes pixel I(x, y) is dark or light region. The use of trapezoidal integration in this scheme has decent results and is proper for detecting edges. In this study, distinct algorithm from recognition based, cued recall based, pure recall based and hybrid schemes of graphical password authentication are reviewed. During our research, we recognition several drawback which can cause attacks.

8. References

1. Housam Khalifa Bashier, Lau Siong Hoe, Pang Ying Han. Graphical Password: Pass-Images Edge Detection, 2013.
2. Atsushi Harada, Takao Isarida, Masakastu Nishigaki. A Proposal Of User Authentication Using Mosaic Images, Proc. Of Computer Security Symposium, 2004, 385-390.
3. Dhamijja R, Perrig A, Déjà Vu. A User Study, Using Images for Authentication, Proc. 9th Usenix Security Symposium, 2000.
4. Jianhoo Shi, Jitendra Malik. Normalized Cuts and Image Segmentation Ieee Trans. Pattern Analysis And Machine Intelligence. 2000; 22(8).
5. Leo Grady. Random Walks For Image Segmentation, Ieee Transaction On Pattern Analysis And Machine Intelligence 2006; 28(11):1768-1783,
6. Muthukrishnan R, Radha M. Edge Detection Techniques for Image Segmentation International Journal of Computer Science & Information Technology (Ijcsit). 2011; 3(6).
7. Jermyn I. Mayer A, Monrose F, Reiter MK, Rubin AD. The Design and Analysis of Graphical Password, In Proceeding of the 8th Usenix Security Symposium, 1996.
8. Xiaoyuan Suo, Ying Zhu G. Scott. Owen Department Of Computer Science Georgia State University Graphical Passwords: A Survey
9. Haichang GAO, Wei Jia, Fei Ye, Licheng Ma. Institute Of Software Engineering, Xidian University, Xi'an, P.R.China, a Survey on the Use of Graphical Passwords in Security International, 2013.
10. Wiednbeck S, Waters J, Birget JC, Brodskiy A, Memon N. Authentication Using Graphical Passwords: Basic Result," In Human–Computer Interaction International (Hcii 2005),Vegas, Nv, 2005.
11. Rachna Dhamij, Adrian Perrig, Déjà Vu. A User Study Using Images for Authentication.
12. Madoka Hasegawa, Yuichi Tanaka, Shigeo Kato. A Study on an Image Synthesis Method for Graphical Passwords" Ispacs 2009, 643-646.