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

Multilevel Graphical Authentication for Secure Banking

Hemavathy M, Nirenjena S
Department of Computer science and Engineering, IFET College of Engineering, Villupuram, Tamil Nadu, India

ABSTRACT

This evolution brings great expediency but also increases the possibility of divulging passwords to shoulder surfing attacks. Attackers can observe directly or use external recording devices to collect users' identifications. To overcome this problem, we proposed a novel authentication system PassMatrix, based on graphical passwords to resist shoulder surfing attacks. With a one-time valid login indicator and circulative horizontal and vertical bars wrapper the entire scope of pass-images, PassMatrix deals no hint for attackers to figure out or narrow down the password even they demeanor manifold camera-based attacks. We also implemented a PassMatrix prototype on Android and carried out real user experiments to evaluate its memorability and usability. From the experimental result, the future system achieves better resistance to shoulder surfing attacks while maintaining usability. We divide the image into several regions, and extract the distribution of the LDN features from them. LDN encodes the directional information of the image textures (i.e. the texture's structure) in a compact way. We avoided image comparison and brought in image feature comparison. (LDN comparison generates Six digit binary codes for each pixel) will be used for comparison.

Keywords: Pass Matrix, Graphical Passwords, Shoulder Surfing Attacks.

I. INTRODUCTION

TEXTUAL passwords have been the most widely used authentication method for decades. Comprised of numbers and upper and lowercase letters, textual passwords are considered strong enough to resist against brute force attacks [10]. However, a strong textual password is hard to memorize and recollect. Therefore, users tend to choose passwords that are either short or from the dictionary, rather than random alphanumeric strings. In this paper, we present a secure graphical authentication system to protect users from becoming victims of surfing attacks when inputting passwords in public through the usage of one-time login indicators.

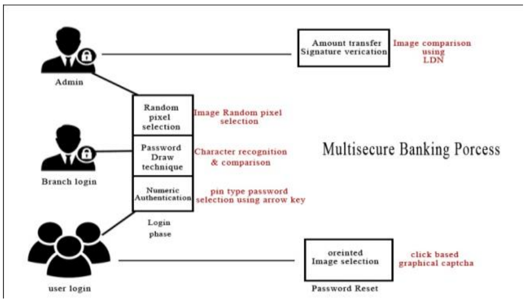


Figure 1. Multisecure Banking Process

Nowadays people are using the alphanumeric strings, patterns, swipe lock as their passwords for security to easy memorization. But sometimes it is very easy for the shoulder surfers to view the password which is used by the users. To confuse the shoulder surfers and hackers we can go for graphical a password which is a passmatrix. Here the passwords are used by images where the image which is stored in the database and the input what we put is not just compared, the intensity and features of the image are compared here. In this paper, we are using five Authentication Techniques namely 1. Random Pixel Selection 2. DAS technique 3. Arrow Key Authentication 4. LDN Generation 5. Image Rotation.

II. METHODS AND MATERIAL

A. Related Work

In April 2016, Sayli Chavan, Shardul Gaikwad, Prathama Parab and Govind Wakure proposed "Graphical Password Authentication System". Instead of using pin codes and alphanumeric strings they have used graphical passwords where the images are used as passwords. Here the passwords are being drawn with the help of the mouse pointer. The accurate password has to be drawn in the screen to login inside the account. Here two techniques have been introduced such as Recognition based system and Recall based system [1].

In September 2014, Delphin Raj K M and Nancy Victor proposed a paper on “A Novel Graphical Password Authentication Mechanism”. In this paper, the graphical passwords Captcha and a random number generator is used as a password. Here four phases are used (i.e.) choosing an image for setting the password, choosing a part of the image, choosing a number from a set of rolling numbers, choosing an alpha numeric password and finally, entering a CAPTCHA correctly[2].

In July 2013, V. Bhusari proposed a paper on “Graphical Authentication Based Techniques”. In this paper, the graphical authentication used is Cued Click Points (CCP), a cued recall graphical password technique and another technique which uses sound signature for password authentication [3].

In December 2014, Saranya Ramanan, Bindhu J S proposed a paper on “A Survey on Different Graphical Password Authentication Techniques”. Here they implemented four techniques named as recognition Based, pure recall Based, cued recall based and hybrid approaches [4].

In March 2015, Pawar Poonam A, Gayake Nalini B, Mane Kalpana T, Mudpe Ashwini M proposed a paper on “Graphical Password Authentication with Cloud Securing Method”. Here they are using cloud with graphical password with security purpose. The user need to handpicked two images from the set of images as their passwords, by using these four images is being created. Here they implemented three Authentication namely, Token base authentication, Biometric Base Authentication, Knowledge Base Authentication [5].

B. MODULES

1. Random pixel selection

To overcome the security fault of the traditional PIN method, the patience of obtaining passwords by observers in public, and the compatibility issues to devices, we introduced a graphical authentication system called Pass Matrix. In Pass Matrix, a password consists of only one pass-square per pass-image for a sequence of n images [8]. The number of images (i.e. n) is user-defined. Bellow figure demonstrates the proposed scheme, in which the first pass-square is located at in the first image, the second pass-square is on the top of the smoke in the second image at, and the last pass-square is at in the third image. In Pass Matrix, users choose one square per image for a sequence of n images rather than n squares in one image as that in the Pass Points scheme.

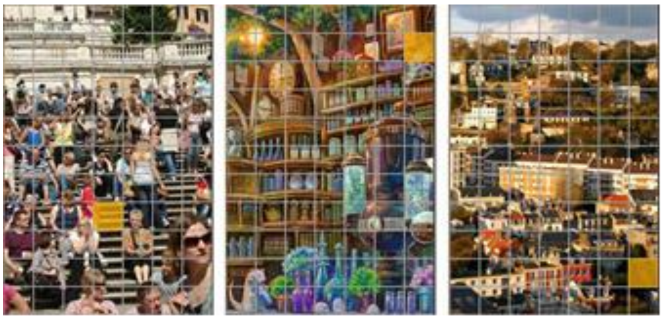
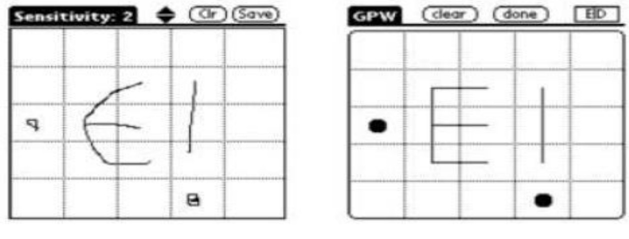


Figure 2. Random Pixel Selection

2. DAS technique

The graphical capability of handheld devices was pathetic the color and pixel it could show was partial. Under this constraint, the Draw-a-Secret (DAS) technique where the user is requisite to re-draw a pre-defined picture on a 2D grid. If the drawing traces the same grids in the same sequence, then the user is genuine. Meanwhile then the graphical ability of handheld devices has progressively and continuously improved with the latest advances in science and technology.



(a) User inputs desired secret (b) Internal representation

Figure 3. DAS Technique

3. Arrow keys Authentication

Instead of typing your password, we can use arrow keys to type your passwords. This is a secure way of entering your password.

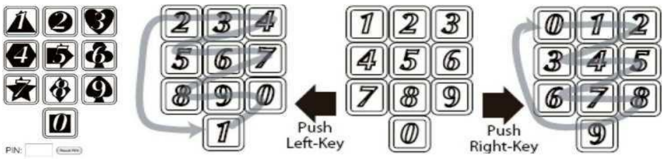


Figure 4. Arrow Keys Authentication

4. LDN Generation

LOCAL DIRECTIONAL NUMBER PATTERN (LDN) is a six bit binary code assigned to each pixel of an input image that represents the structure of the texture and its intensity transitions. The positive and negative responses provide valuable information of the structure of the neighborhood, as they reveal the gradient direction of bright and dark areas in the neighborhood. Thereby, this distinction, between dark and bright responses, allows LDN to differentiate between blocks with the positive and the negative direction swapped (which is equivalent to swap the bright and the dark areas of the neighborhood, by generating a different code for each instance, while other methods may mistake the swapped regions as one. Furthermore, these transitions occur often in the face, for example, the top and bottom edges of the eyebrows and mouth have different intensity transitions. Thus, it is important to differentiate among them; LDN can accomplish this task as it assigns a specific code to each of them.

5. Histogram Generation

In this module, the histogram is generated based on the query image selected from the image dataset. The horizontal axis of the graph represents the tonal dissimilarities, while the vertical axis represents the number of pixels in that specific tone. The left side of the horizontal axis signifies the black and dark areas, the intermediate represents medium grey and the right hand side represents light and pure white areas. The vertical axis represents the size of the area that is seized in each one of these zones. Hence, the histogram for a very dark image will have the mainstream of its data points on the left side and center of the graph. Contrariwise, the histogram for a meticulous bright image with rare dark areas and/or shadows will have most of its data points on the right side and center of the graph.

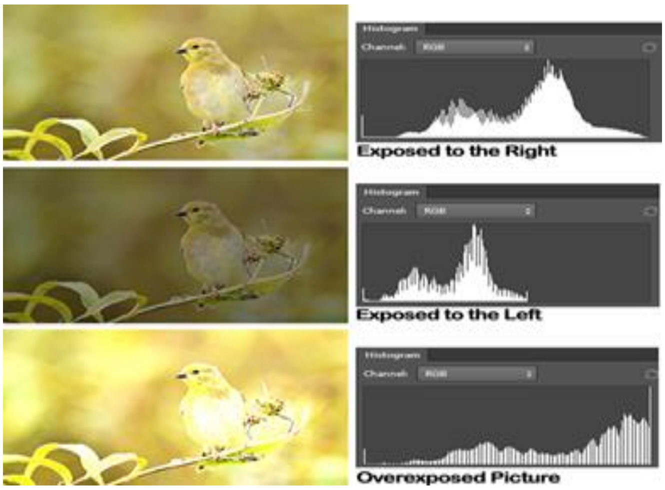


Figure 5. Histogram generation

In the first user can register can upload the photo and provide the necessary details once photo are uploaded in the image dataset folder and indexed. Image stored in the data set folder are preprocessed, divided into blocks and saved. We extract the entire feature automatically and the features are stored separately according to which LDN code is generated. LDN Code is in binary format which is saved in separate folder during the comparison it will be used to verify the image.

6. Edge Detection

Edge detection embraces a variety of mathematical methods that targets at identifying points in a digital image at which the image brightness changes harshly or, more authoritatively, has discontinuities. The points at which image brightness changes sharply are normally planned into a set of curved line segments termed edges. The same problem of finding discontinuities in 1D signal is known as step detection and the delinquent of finding signal discontinuities over time is known as change detection. Edge detection is an essential instrument in image processing, machine vision and computer vision, particularly in the areas of feature detection and feature extraction.

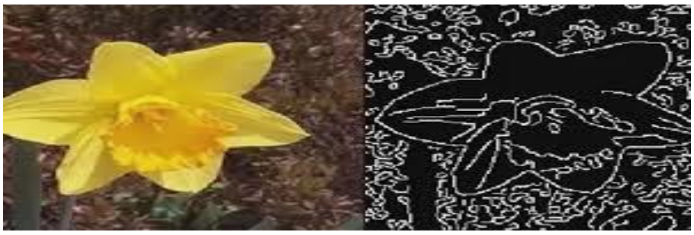


Figure 6. Edge Detection

7. Image Rotation

In this module, there are two steps
1. Registration phase
2. Login phase

User Registration Phase:

When the user wants to get any service from the system, first he/she needs to register with the system. Registered users will be saved in the server. This phase is executed only once at the time of registration. The registration form is depicted in

Step1: User chooses a user id.
Step2: User needs to choose a password. Once the user chooses a password and enters remaining data required for registration and confirms, he/she is successfully registered.

Login:
Registering with the server is the first step. After registration with the system to acquire the services he/she rearrange the login by using following steps.
Step 1: User enters the user id.
Step 2: Then he/she needs to click on the grid of images that are displayed in the 3X5 grid in the same sequence corresponding to the distorted images presented as CAPTCHA in a 1X5 grid.
Step 3: If the user is authorized and has entered correct CAPTCHA the system provides access to the web page.

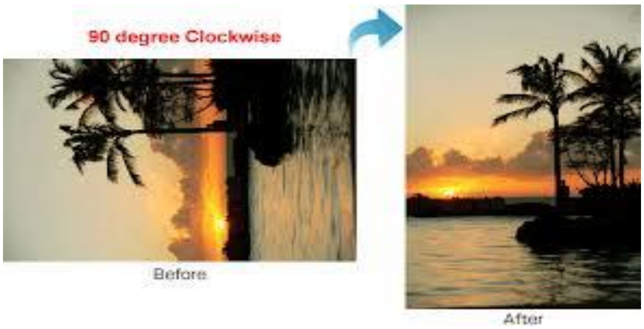


Figure 7. Image Rotation

C. Existing system

In order to be more secure than the surviving Android pattern password with entropy 18:57 bits against brute force attacks, users have to set two pass-images and use the graphical technique to obtain the one-time login indicators [9]. Like most of other graphical password authentication schemes, Pass Matrix is liable to random predict events constructed on hot-spot analyzing. TEXTUAL passwords have been the utmost widely used authentication method for spans. Entail of numbers and upper- and lower-case letters, textual passwords are reflected strong enough to resist against brute force attacks [7]. According to an artifact in Computer world, a security crew at a large company resisted a network password cracker and unpredictably splintered approximately 80% of the employees' passwords within 30 seconds [3]. Textual secret codes are often uncertain due to the trouble of holding solid ones.

Drawback:
Textual passwords are susceptible to eves dropping, dictionary attacks, social engineering and shoulder surfing. Graphical passwords are introduced as alternative techniques to textual passwords. Most of the graphical schemes are vulnerable to shoulder surfing. To report this problematical, text can be combined with images or colors to produce session passwords for authentication.

III. RESULTS AND DISCUSSION

Proposed Systems

This enlargement carries ceaseless accessibility but also raises the opportunity of divulging secret word to shoulder surfing spasms. Muggers can distinguish directly or practice peripheral recording devices to accumulate users' credentials. To incredulous this delinquent, we suggested an innovative authentication system Pass Matrix, based on graphical secret word to counterattack shoulder surfing attacks. With a one-time in force login gage and circulative horizontal and vertical bars wrapper the complete scope of pass-images, Pass Matrix offers no intimation for muggers to figure out or slight down the secret word even they conduct multiple camera-based attacks. A proportion of investigation on secret word authentication has been completed in the literature. Among all of these planned provisions, this tabloid emphasis essentially on the graphical-based authentication systems. To grasp onto this tabloid summarizing, we will subsidize an ephemeral review of the most related structures that were mentioned in the preceding section. The truthfulness standpoint motivations on the prosperous login rates in both sessions, together with the practice logins. The usability perspective is measured by the amount of time users spent in each Pass Matrix phase.

LDN technique is based on image feature taking out and appraisal to bring more safekeeping and precision.

Advantage:

These skills are predictable to spawn session secret word using text and colors which are sturdy to shoulder surfing. The specific activities and the preference of workers that the attacker may take value of to figure out the potential secret word.

1. Any message between the client device and the server is sheltered by SSL so that sachets or evidence will not be snooped or interrupted by muggers during broadcast.
2. The user and the waiter tactics in our endorsement scheme are in control.
3. The control panel and the integral canopy of mobile devices are problematic to protect, but a trivial area (around 1.5 cm^2) is easy to be sheltered from spiteful people who influence shoulder surf secret word.
4. Workers are capable to register an account in a place that is safe from observers with ruthless intention otherwise surveillance cameras that are not under proper administration.

Banking Process:

In the admin section, the admin will add bank details and add details provided in a unique login with security for each branch so that each branch will maintain their customer details with credit details and reports. User will have secure login for creating transaction like fund transfer and sighted reports.

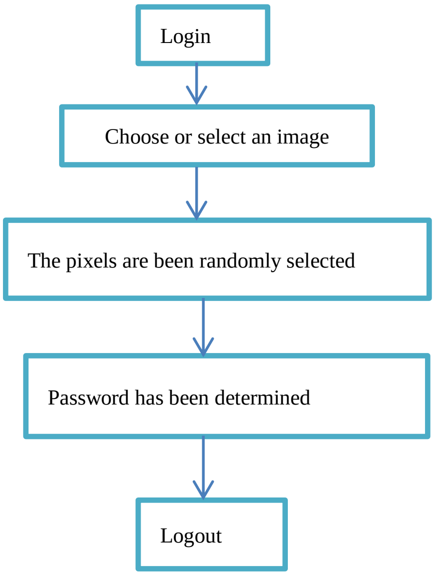

Login
Choose or select an image
The pixels are been randomly selected
Password has been determined
Logout

Figure 8. Flowchart for Random pixel selection

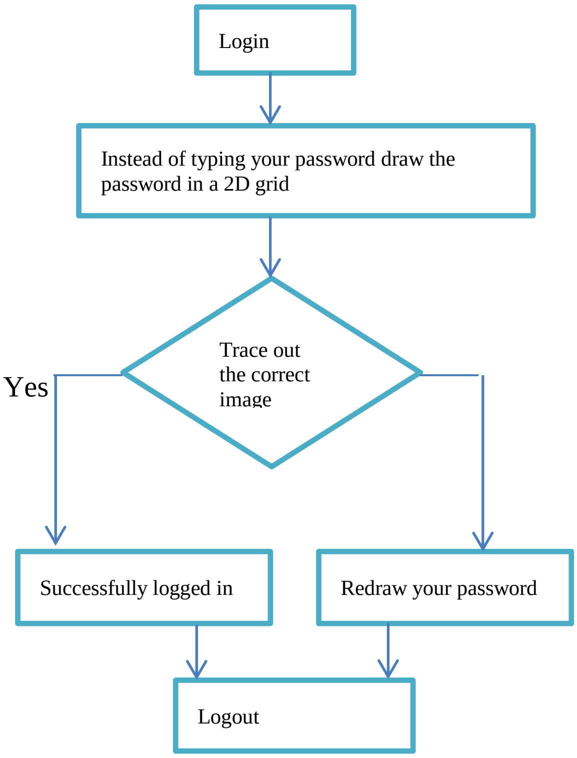

Login
Instead of typing your password draw the password in a 2D grid
Trace out the correct image
Yes
Successfully logged in
Redraw your password
Logout

Figure 8. Flowchart for DAS Technique

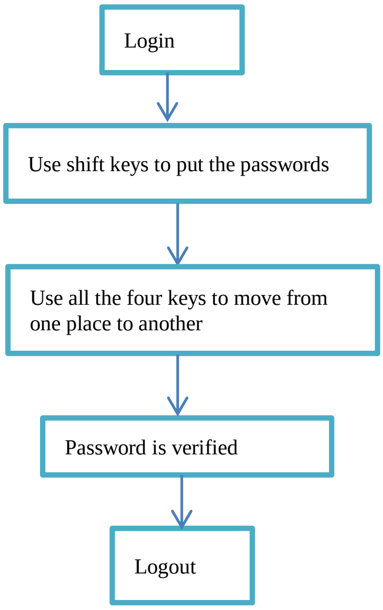

Login
Use shift keys to put the passwords
Use all the four keys to move from one place to another
Password is verified
Logout

Figure 9. Flowchart for Arrow Key Authentication

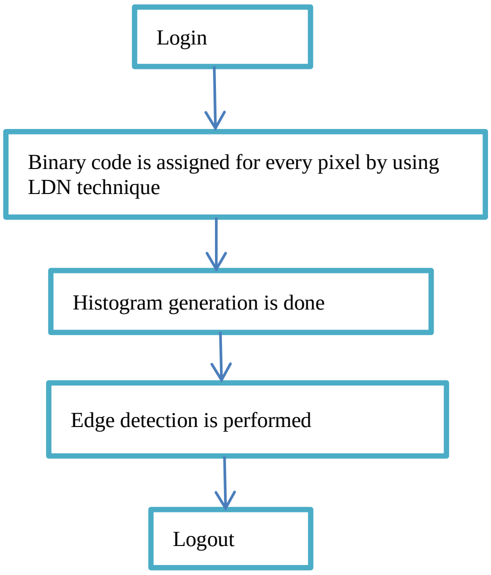

Login
Binary code is assigned for every pixel by using LDN technique
Histogram generation is done
Edge detection is performed
Logout

Figure 10. Flowchart for LDN technique

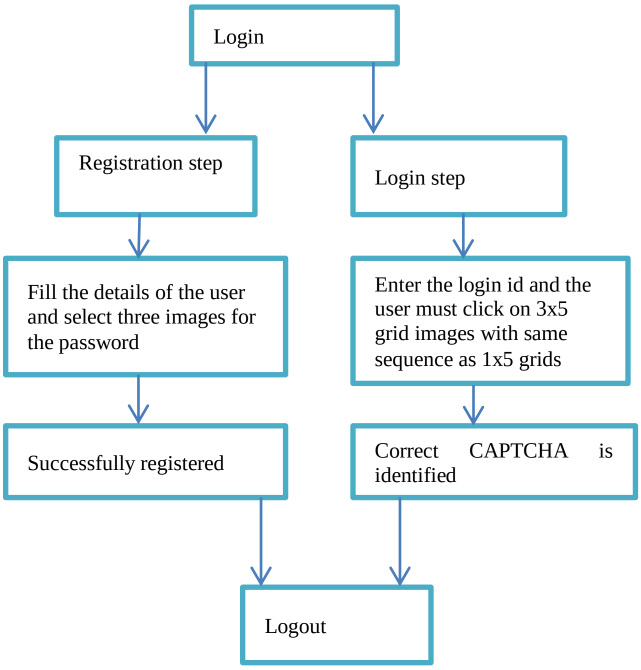

Login
Registration step
Login step
Fill the details of the user and select three images for the password
Enter the login id and the user must click on 3x5 grid images with same sequence as 1x5 grids
Successfully registered
Correct CAPTCHA is identified
Logout

Figure 11. Flowchart for image rotation

IV.CONCLUSION

Thus the graphical passwords is more secure than using the normal pin code and alphanumeric strings to avoid the shoulder surfing attacks, the brute force attacks and the dictionary attacks. The using of the graphical passwords is exceedingly secure because the hackers will find it difficult to analyse the accurate passwords. Here the time complication is being condensed because the time required for relating the secret word takes some time to complete this method. Hence the time complexity is being decreased. The number of trials for accessing the passwords has being increased.

V. REFERENCES

[1]. Sayli Chavan, Shardul Gaikwad, Prathama Parab and Govind Wakure, "Graphical Password Authentication System" , International Journal of Computer Science and Mobile Computing, Vol.4 Issue.4, April 2015.

[2]. Delphin Raj K M and Nancy Victor, "A Novel Graphical Password Authentication Mechanism", International Journal of Advanced Research in Computer Science and Software Engineering,Vol.4, Issue.9,September 2014.

[3]. V. Bhusari, "Graphical Authentication Based Techniques", International Journal of Scientific and Research Publications, Vol.3, Issue.7, July 2013.

[4]. Saranya Ramanan, Bindhu J S, "A Survey on Different Graphical Password Authentication Techniques", International Journal of Innovative Research in Computer and Communication Engineering, Vol.2, Issue.12, December 2014.

[5]. Pawar Poonam A, Gayake Nalini B, Mane Kalpana T, Mudpe Ashwini M, "Graphical Password Authentication with Cloud Securing Method" , International Journal of Multidisciplinary Research and Development, 2015; 2(3): 763-768.

[6]. K. Gilhooly, "Biometrics: Getting back to business," Computer-world, May, vol. 9, 2005.

[7]. "Realuser," http://www.realuser.com/.

[8]. S. Wiedenbeck, J. Waters, J. Birget, A. Brodskiy, and N. Memon, "Passpoints: Design and longitudinal evaluation of a graphical password system," International Journal of Human-Computer Studies, vol. 63, 2005.

[9]. S. Wiedenbeck, J. Waters, L. Sobrado, and J.-C. Birget, "Design and evaluation of a shoulder-surfing resistant graphical password scheme," in Proceedings of the working conference on Advanced visual interfaces, ser. AVI ’06. New York, NY, USA: ACM, 2006.

[10]. H. Zhao and X. Li, "S3pas: A scalable shoulder-surfing Resistant textual-graphical password authentication scheme," in Advanced Information Networking and Applications Workshops, AINAW’07. 21st International Conference on, vol.2. 2007