A Novel Approach for Software Implementation of Graphical Authentication Methodology

Murtaza Alamshah
School Of Information Technology
Vellore Institute of Technology
Vellore, India
murtazaalamshah@gmail.com

Abhilasha Nanda
School Of Information Technology
Vellore Institute of Technology
Vellore, India
an7081@gmail.com

Pounambal M.
Asst. Professor (Sr.) (SITE)
Vellore Institute of Technology
Vellore, India
mpounambal@vit.ac.in

***Abstract*--The conventional method of authentication requires the user to remember a text based password which he enters in order to prove his legitimacy. Since security cannot be compromised, such passwords are usually lengthy and complicated else they would be cracked easily with various password hacking techniques. The user thus finds it difficult to remember such passwords and often tends to forget them. Therefore, a more secure and attractive method can be created using graphical authentication. In this paper we propose a system where the user can define one region per image over a sequence of images and the access is given if he clicks in the correct region for the given image. We have also introduced several user friendly functions which aim to provide additional security as well as ease of access to its users.**

1. INRODUCTION

People have the habit of keeping different passwords for different login areas and as a result they get confused between the passwords [1]. Moreover since most of the times people choose a password which is a simple dictionary word, they are prone to dictionary attack [2].

Therefore an alternate to text based password is required which overcomes the problem of remembering passwords and is also more secure. Graphical authentication serves well for this purpose as it also greatly increases the password space. Research shows that the human mind is far more efficient in remembering visual patterns than text based passwords. Use of images in books for primary classes is a well known example for the above mentioned statement. Images attract and also allow the reader to remember something associated with it more easily but such methodology of authentication is still very limited as much of the research has been made on its usability and less on its security [3]. Based on several analyses, graphical method of providing security has been proven very successful and promising [4]. There are several methods being proposed for this type of system such as drawing based technique and recall based technique [5]. Drawing based technique is limited to touch based screen as the user needs to draw a design which acts as the password. In the second technique, one can recall his password by pointing at the correct location in the images. Effects of several security attacks such as brute force attack can be minimized by applying this technique since the password space can be made too large depending upon the number of images used. Moreover the password is in non lingual form hence dictionary attack also becomes inefficient.

Therefore using the knowledge and proven success of graphical authentication, we propose and design a system which aims to provide more security and user operability. Along with the detailed explanation of the application, two algorithms have also been compared which can be used for graphical password authentication. Keeping in mind the concept of interoperability, the entire system has been created in java hence it is platform independent. The system is also designed to handle large amount of data, hence the system can take large number of images. Significant improvements have been made in the area of security such as email verification of the user and maintaining a log file. The system also includes various customization options such as defining actions the system must do when the retry attempts are exceeded. User friendly features like audio guidance is included which provides ease of access.

2. IMPLEMENTATION OF THE PROPOSED SYSEM

2.1 MONITORING

Monitoring involves checking the status of the applications whether they are running or not. This is done in two modes. The first mode is called the Active Mode. As soon as the user turns on his laptop, the java code automatically starts monitoring the applications just like an antivirus application which constantly checks for any harmful file and instantly blocks its execution. Whenever the user tries to open any application, the monitoring code restricts the user from opening it and the system makes two queries to the database in sequence. In the first query the system queries the database if regions are registered for the given number of images and in the second query it queries the database if the email is registered. The output of these two queries can lead to three conditions. First condition is defined when no registration has been made so far. It occurs when the first query and the second query both returns a null value. In such case the system will display the welcome screen as shown in figure 2 to the user and take him towards the registration page as shown in figure 3. The second condition occurs when partial registration is done. It can be further classified into two sub cases. In the first sub case email id not registered. Here, the first query returns a not null value and second query returns a null value. The system then displays the email registration page as shown in figure 4. In the second sub case the email is registered but password is not updated. It occurs when both the queries return a not null value.

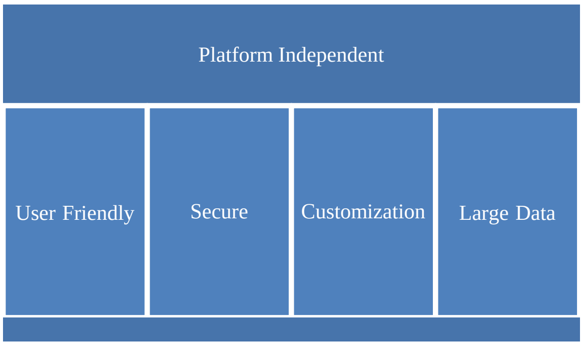
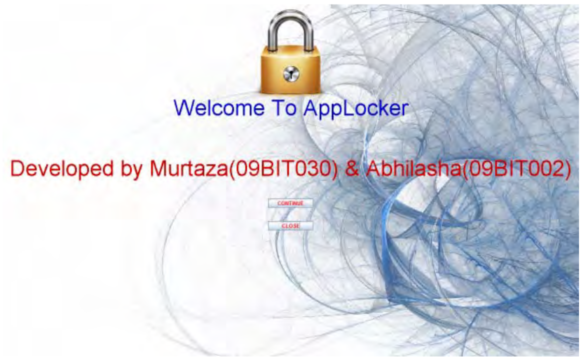


Fig 1


Welcome To AppLocker

Developed by Murtaza(09BIT030) & Abhilasha(09BIT002)

Fig 2

The system then checks for the password status[1] attribute value of the second query. 0 indicates that the password is not updated and 1 indicates that it is updated. If the attribute is set to 0 then system takes the user to the email registration page as shown in figure 4. In the third condition, complete registration is done. The system infers that the complete registration is done when both the queries return a not null value and the password status attribute[1] in the second query is set to 1. The system then takes the user to the login window as shown in figure 5. The second mode is called the Passive Mode**.** This mode is active when the user has logged in successfully. When the user logs in, the system stops monitoring the application for a certain period of time which is known as the sleep time. During the sleep period, the monitoring code does the reverse operation. If it finds the application to be open, instead of closing the application, it will allow it to remain open till the sleep time is not over.

[1] Password status attribute is a part of the registration process and will be explained in detail later in section 2.3

2.2 STORING REGIONS OF IMAGE

The following module deals with the registration process for the user. The user has namely two options for registration. Either he can choose option one to use the pre-defined images included in the software or he can switch to option two where he can select his own images. Option two can be more efficient in recalling passwords as the user himself chooses the images and thus has more probability to remember the regions registered. Whenever the user clicks on the image, its X and Y co-ordinates gets stored in an array. After the election of regions for all the images a database insertion query is made which inserts all the points into the database. The progress bar will keep the user updated about the number of images he has registered so far. If the user aborts the registration process in between, all of its registered points are deleted from the array and he has to start from the beginning. The predefined images are named from 101 to 101+ (n-1) where n is the number of images. In case of option 2, when the user selects his image, the image first gets copied into the installation directory. It is done to avoid any unwanted operations being made on that image like cut, renaming or deletion by the user. After getting copied into the installation folder, the user is free to make any changes to its original image in its original location. Each image is renamed in the installation directory in the sequence starting from 1001. So the Nth image selected by the user will be renamed as 100N in the installation directory. Also, at the time of registration of user defined images, the original path of the image is also copied into database temporarily. It is done in order to restrict the user from selecting the same image again. When the user selects the image, the system first queries the database to get all the original paths of the images selected so far. If the current image location matches with any one of the already stored addresses in the database, the system generates an error and asks the user to reselect a different image. After selecting all the regions in the images, the system inserts the pixel values into the database along with the option number. 1 indicates that the user has chosen the first option (pre-defined images) for authentication and 2 indicate that he has chosen second option (user-defined images) for authentication.

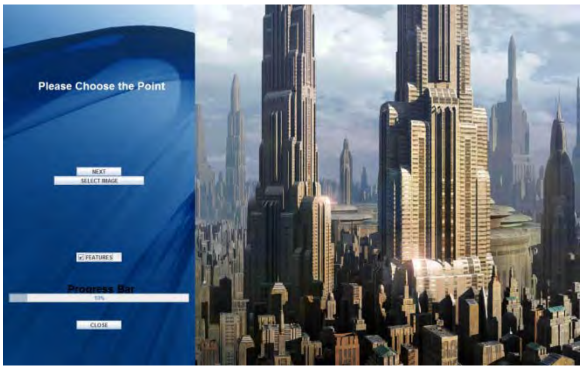


Fig 3

2.3 SECURITY VERIFICATION

Now the user needs to register a recovery email id and a password associated with it in order to complete the registration as shown in figure 4. The user provides a valid email id to the system and the system sends a random eight digit password to the specified email id. Internally the system now inserts the provided email id and the random generated password into the database with the password update status option set to 0. The user then checks his mailbox and copies the given random password and comes back to the same registration window. Now since he has received the password, he clicks on the

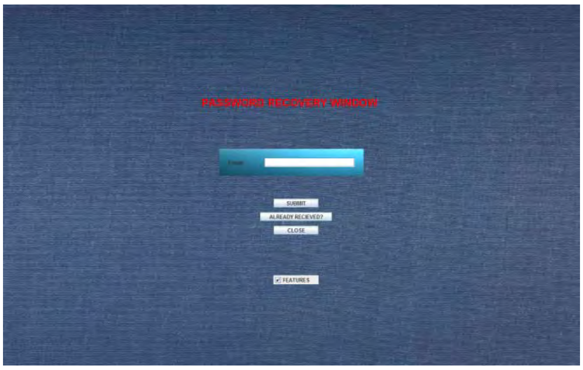


Fig 4

"Already Received" button and enters the received password and also enters the new 8 digit alphanumeric password of his choice. The system then checks for the password entered by the user and the password stored in the database by the system. If the passwords match, the user is asked to enter the new 8 digit alphanumeric password and the password update attribute is set to 1and it marks the end of the registration process otherwise if the passwords don't match he can either re-enter the email to receive a new password or he can check if he has made any error in copying. Till the user does not verify the received password and adds his new personal password, the registration process is not completed and the system will show the password recovery window asking the user to complete the registration.

2.4 LOGIN

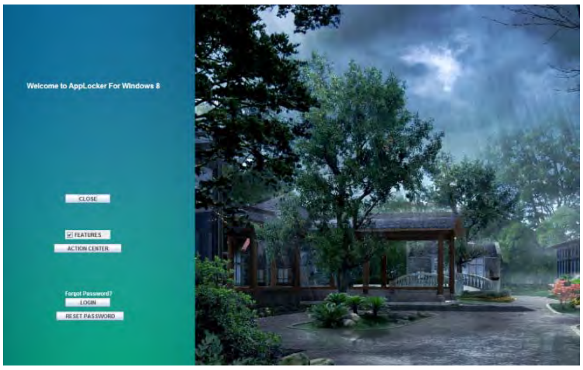
Once the registration is completed the system will start monitoring the applications and redirects the user to the login page as shown in figure 5 where he has been given maximum three attempts to enter the correct password.

2.4.1 IMAGE BASED

The system queries the database to find out the option number the user had selected during the time of registration. As stated earlier 1 stands for pre-defined images which are named from 101 to 101+ (n-1) and 2 stands for user defined images named from 1001 to 1001+(n-1).

Code for generating numbers within a to b int number=a + (int)(Math.random() * ((a - b) + a)); Where, a=lowerlimit=1
b=upper limit=n (Total number of images)

Randomly P number of images will be displayed one by one and the user has to click in the correct region for all the images correctly. The algorithm will check if the given input pixel is within the acceptable region of the registered pixel or not as shown in figure 6 and 7. To avoid repetition of the random number generated, each number is stored in a separate array. When a new random number is generated, it first checks the array to make sure that the currently generated number has not been generated previously.



Welcome to AppLocker For Windows 8

Fig 5

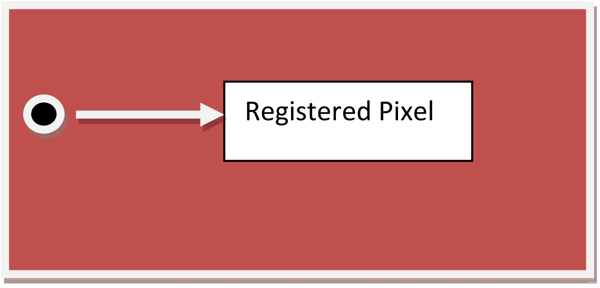


Fig 6

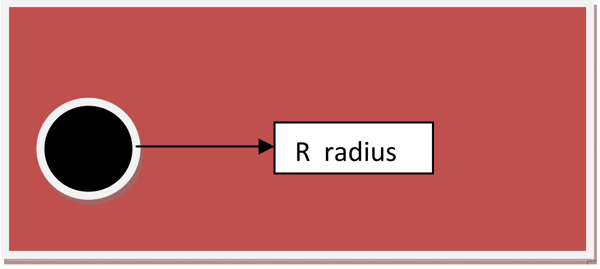


Fig 7

Pseudo Code: Set counter and **retry counter** to 0.
Measure the distance between the two points using the distance formula.
Distance=$\sqrt{(x-x1)^2 + (y-y1)^2}$ **Where,**
(x,y)= Initial Pixel Registered (x1,y1)= Pixel Registered at the time of authentication

If distance is less than or equal to the defined radius R, the pixel is accepted otherwise it is rejected. Each time a pixel entered is correct; the counter is incremented by 1. At the end if the counter value is equal to P then access is given else the system asks the user to retry. If password entered is wrong, retry counter is incremented by 1. If the retry counter is equal to 3 then appropriate action is taken. Action can either be Shutdown, logoff or lock the system. By default it is Shutdown though it can be customized by the user any time.

2.4.2 TEXT BASED

If the user forgets the region of an image he can alternatively login using the text password registered previously. The system queries the database for the associated email id given by the user. If the text password registered in the database matches the text password provided by the user, access is given else retry counter is incremented. When the retry counter is 3 any of the 3 previously mentioned actions is taken as defined by the user.

2.5 PASSWORD RESET AND RECOVERY

The user has the option to update or recover his lost password. If the user forgets pixel regions in one or more images but still remembers text based password, he has the option to update the pixel of any image. The user is first asked to enter the text based password and if it is correct he is redirected to the password update page as shown in figure 8. The user can select the image, set the new region and update query is executed in the database by the system. Alternatively, if the user forgets his text password then he can provide the same email id which he had given at the time of registration and can receive the password in his mailbox. The user also has the option to make a full hard reset of the password by entering the old password which authenticates his legitimacy.

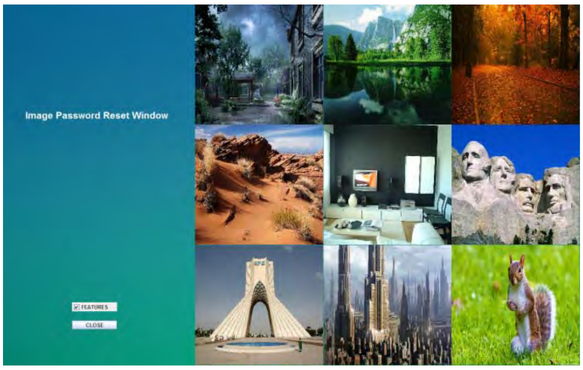
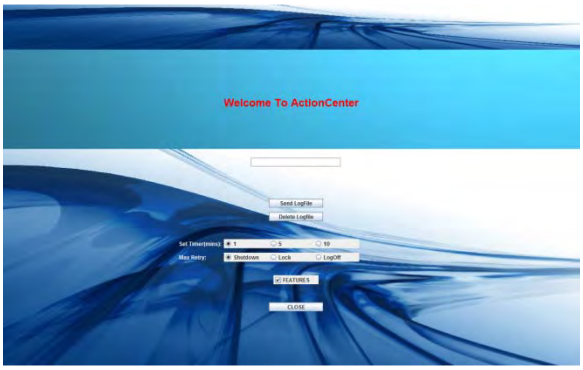


Fig 8

2.6 ACTION CENTER

This is the customization feature of the software with several utility functions as shown in figure 9. It aims at providing extra features and security to the user. The first option provides information about the usage of the system via a log file. The user can receive and delete log details as and when he wants. This adds to the security of the application. Every fail or successful login gets recorded in the log file with date and time. Log file is created when a new user is registered. It is programmed to get updated under various situations like successful login, changes made in action center, exceeding retry attempts, updating of password, resetting of password, recovery of password. It also gets updated when the application gets closed unexpectedly. The second option allows the user to set the sleep time value. Sleep Time is the amount of time user can set for which the software won’t monitor the particular application after successful login. Default value is 1 minute. Finally, with the help of the third customization option the user can explicitly define what the system will do if login attempts have been exceeded.



Set Timer(mins): ● 1 ○ 5 ○ 10

Max Retry: ● Shutdown ○ Lock ○ LogOff

☑ FEATURES

Fig 9

2.7 EASE OF ACCESS

Audio help is provided for the users who are unfamiliar with such kind of technology. With every click on the button, an audio clip is played which tells the users what that button will do. This can be turned on/off by selecting/deselecting the checkbox provided at every page wherever the user goes. It sets the value to either 0 or 1. 0 indicates that feature is ON and 1 indicates that the feature is OFF.

3. ALGORITHM AND ITS EXECUTION TIME

We have compared our algorithm with Ray Casting algorithm and found our algorithm to be 12 times faster in terms of execution time. We are calculating the distance of the pixel registered by the user and the one he enters at the time of login. If the distance is acceptable or in other words lies inside the circle of given radius the point is accepted else rejected. Pseudo code for our algorithm has also been stated previously.

```
Using inbuilt java function:                    long start = System.nanoTime();
//calling function                              long executionTime = System.nanoTime() - start;
```

We found our average execution time to be **92928 nano seconds** compared to **1192705 nano seconds** with **RayCasting Algorithm** as inferred by figure 10.

4. SECURITY

Graphical password authentication has been proven far more secure than the traditional text based password. Since the password space is high as compared to text based, bruteforce attack is not efficient. Dictionary attacks also fail to provide access as the values are only in numerical form. Draw-A-Secret is the most efficient way to overcome bruteforce attack since it provides the largest password space [5]. Analysis shows that users don’t select regions of the image in any particular pattern, so Pattern-based attacks seem ineffective. Using cued click points the user is traversed along the correct path only when he clicks on the correct pixel for each of the given image else he is shown a different image. This technique is useful in minimizing the attacks based on hotspot analysis as once the attacker selects a wrong pixel in

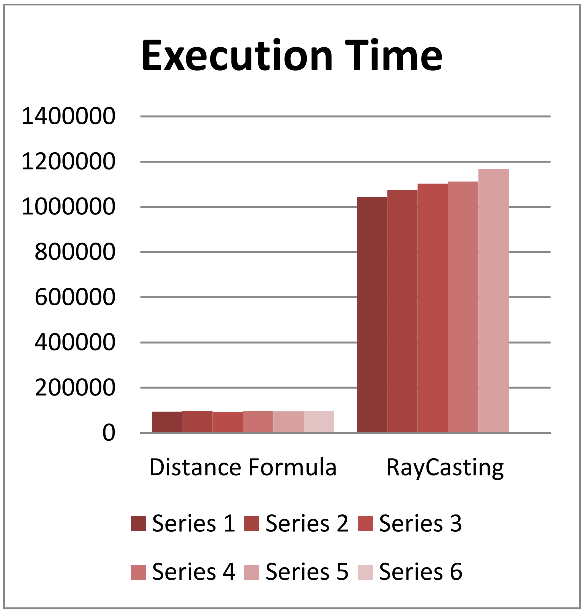


Fig 10

the image the system will confuse him by displaying random number of images which are not the part of the authentication. [6]. Entering passwords in public places is highly vulnerable for **Shoulder Surfing Attack** [7]. Capturing screenshots of login screen with camera in public places is very easy and thus posses a very high risk of intrusion [8]. Several techniques have been introduced to minimize the effectiveness of this attack. One such method could be enhancement of the algorithm proposed by Shuhaib K P and Sobin C C [6] by providing multiple paths for authentication as it increases the work of the attacker to observe the body movements for all the correct paths. Increasing the number of click points per image can also provide additional layer of security [8]. This methodology does not successfully overcome the shoulder surfing attack but delays the password cracking time. Introduction of neural networks and back propagation schemes have been proven very promising in the enhancement of graphical authentication [9].

5. CONCLUSION AND FUTURE WORK

Users have tendency to forget text based password more easily and quickly as compared to image based passwords. Research shows that text based passwords are far more vulnerable to attacks hence graphical password authentication is the most suited alternative available. We have successfully designed and implemented a system which uses the principle of graphical cued click points (CCP) as stated by Sonia Chiasson and her teammates [8]. We have given special focus to both security and usability by providing log file information and ease of access to the user. Although this technique provides more security than its predecessors, it still requires improvement in its password authentication scheme.

6. REFERENCES

[1] K. V. Renaud "Guidelines for designing graphical authentication mechanism interfaces" International Journal of Information and Computer Security, Volume 3 Issue 1, June 2009 Page 60-85

[2] Mudassar Raza, Muhammad Iqbal, Muhammad Sharif and Waqas Haider "A Survey of Password Attacks and Comparative Analysis on Methods for Secure Authentication" World Applied Sciences Journal 19 (4): 439-444, 2012

[3] J. Yan. A. Blackwell, R. Anderson and A. Grant, "Password Memorability and Security: Empirical Result", IEEE Privacy and Security, Vol. 2, 2004, pp. 25-31.

[4] Susan Wiedenbeck, Jim Waters, Jean-Camille Birget, Alex Brodskiy, Nasir Memon," Authentication using graphical passwords: effects of tolerance and image choice" SOUPS '05 Proceedings of the 2005 symposium on Usable privacy and security. Pages 1-12

[5] Muhammad Daniel Hafiz1, Abdul Hanan Abdullah2, Norafida Ithnin3, Hazinah K. Mammi4 "Towards Identifying Usability and Security Features of Graphical Password in Knowledge Based Authentication Technique" Second Asia International Conference on Modeling & Simulation Pages 306-403

[6] Shuhaib K P, Sobin C C "An Efficient Method for Graphic Password Authentication" MES Journal of Technology and Management, Page 123-125

[7] Arash Habibi Lashkari, Dr. Omar Bin Zakaria, Samaneh Farmand, Dr. Rosli Saleh "Shoulder Surfing attack in graphical password Authentication", (IJCSIS) International Journal of Computer Science and Information Security,Vol. 6, No. 2, 2009

[8] Sonia Chiasson, Paul C. van Oorschot, Robert Biddle "Graphical Password Authentication Using Cued Click Points." ESORICS 2007: 359-374

[9] ASN Chakravarthy, Prof.P S Avadhani "A Probabilistic Approach for Authenticating Text or Graphical Passwords Using Back Propagation", IJCSNS International Journal of Computer Science and Network Security, VOL.11 No.5, May 2011