

# A Graphical Authentication using Pixel Selection and Cued Click Points Selection

Mr. Devidas S. Thosar<sup>1</sup>, Vaishnavi P. Kolhe<sup>2</sup>, Vrushali A. Jadhav<sup>3</sup>,  
Priyanka A. Shinde<sup>4</sup>, Shraddha V. Bankar<sup>5</sup>

Assistant Professor, Department of Computer Engineering<sup>1</sup>

BE Students, Department of Computer Engineering<sup>2,3,4,5</sup>

Sir Visvesvaraya Institute of Technology, Nashik, Maharashtra, India

**Abstract:** *We have introduced a new way of Working with Pixel Image Verification and Cude Click Points. We have evaluated the usefulness and security of this project. The human mind remembers the image faster than the text. Users usually create passwords using a script, but by using these passwords there are many obstacles. Photo password that is easy to remember but hard to guess from hackers. Users can easily remember a strong password and passwords that can be remembered are easy to guess. This method is used to provide security. As technology grows security must be provided from now on we provide security using the alphanumeric method. There is another method called biometric but more expensive than Graphical password authentication. So we came up with this entry function using image pixel selection and point-click methods. The main purpose of the login operation is to use image pixels and point-click techniques to provide improved security for users The main goal of this project is to support users in choosing the best and safest passwords. The user will click on a specific part of the image to verify authenticity. Attractive click points will provide a series of images to increase security as it will give the attackers a greater burden. A series of images will be provided based on previous clicks of the image. Psychological research shows that one can remember a visual image beyond a series of alphanumeric characters. So remembering points in user pictures will be easier and it will be harder for the attacker to reach. Attractive clicks help users to select random areas to increase security. The advantages of a Graphical Password Scheme are ease of use and great security.*

**Keywords:** Graphical Password, Computer security, Cued Click Point (CCP), Computer Authentication

## I. INTRODUCTION

The problems of knowledge-based authentication, typically text-based passwords, are well known. Users often create memorable passwords that are easy for hackers to guess, but strong system assigned passwords are difficult for users to remember. A password authentication system should encourage strong passwords while maintaining memorability. We propose that graphical authentication and pixel selection schemes allow user choice while influencing users towards stronger passwords[1].

Based on the Psychological study user is able to remember images with long time span rather than textual words. To dispose of text based passwords, we proposed the technique of image based secured authentication. In proposed work a click-based graphical password scheme called Cued Click Points (CCP) is presented. In this system a password consists of sequence of some images in which user can select one click-point per image. Here we are giving a login functionality with using image pixels and there are set of images we are used for login process. This process is based on optical image processing techniques. Where system read the image pixels' location and stored into the database. While user access their devices that time all that pixels location should be identify and match[5].

There has been a great deal of type for graphical passwords since two decade due to the fact that primitive methods suffered from an innumerable number of attacks which could be imposed easily. Here we will progress down the taxonomy of authentication methods. To start with we focus on the most common computer authentication method that makes use of text passwords. Despite the vulnerabilities, it's the user natural tendency of the users that they will always prefer to go for short passwords for ease of remembrance and also lack of awareness about how attackers tend to attacks. Unfortunately, these

passwords are broken easily by intruders by several simple means such as masquerading, saves dropping and other rude means say dictionary attacks, shoulder surfing attacks, social engineering attacks[8].

## II. LIMITATION OF EXISTING SYSTEM

1. Large Memory Requirement to store images as compared to pass-point : Karmajit Patra,et al.[7]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 Pass Point; user uses five click points on one image. So, one image is sufficient for creating a password of length five rather five images.
2. Text Password Hack : Textual Passwords should be easy to remember at the same time easy to guess. But if a textual password is hard to guess then it is very difficult to remember also. Full password space for 8 characters consisting of both numbers and characters is 2.
3. Captcha : It takes more time to create any ID through this Sometimes difficulty in understanding and reading some Captcha.

## III. WORKING METHODOLOGY

### 3.1 Modules Information

#### 1. User Registration Process

- **Input:** User has to enter the user name, email id, contact number and text passwords. After filling all the required data in the registration form basic registration is successfully.
- **Output:** The user will receive a positive message from the system i.e. successfully registered.
- **System behavior:** The details entered by the user in registration phase will be saved into database. In case of any field Missing system will generate a negative message.

#### 2. Image Selection(Cued Click Points) Module:

- **Input:** The user gives browse button to select the images from the system then on that image click 5 click points. The User select at least 6-7 images. After that user successfully registered.
- **Output:** The user will receive a positive message from the system i.e. image Saved Successfully.
- **System behavior:** The details entered by the user in this phase that is the image and their click points will be saved into database.

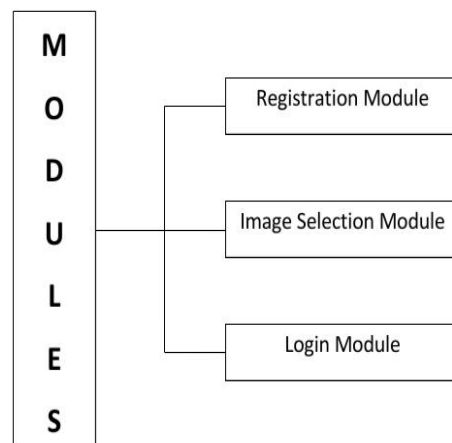


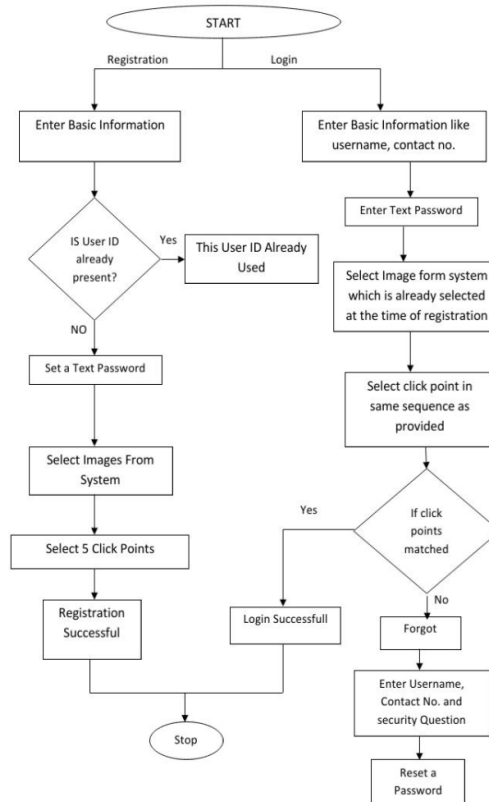
Figure 3.1: System Design Modules

### 3. User Login Process

- Input : The user provide the username and verify. The correct username, contact no. and text password gives the browse button to select the images from the system for password and select their click point in sequence.
- Output : The authentication confirmed message and open up the user account.
- System Behavior: The system verifies the username with the login name from the registration phase. If the username exists then the system will select the first image from the users system. The user clicks on the image sequence wise and the system verified the point with the help of database. If the point matches then user select next image from the system will be displayed for password so on up to no. of images user selected at the registration phase. Final click points verified and open the user system or user account.

### 3.2 Persuasive Cued Points

A click point is a location on an image that is selected by a user to set the password for authentication. The psychological study suggests that remembering a picture is easier than remembering a text. So a picture password is a good user friendly than a text-based password. For that reason, it is easy to remember the click points on pictures than to remember a string of characters.



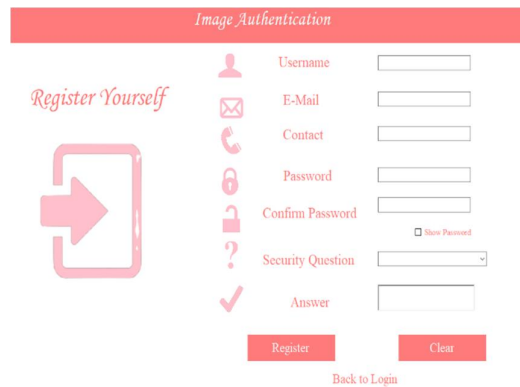
**Figure 3.2:** Flow chart of the design model

Persuasive cued click points are a well-known technique to execute a Graphical password scheme. The registration process is very simple and user-friendly. The user will select a series of images of his/her choice and interest. Later user has to choose a specific location on each image selected and the location will be saved by the system. As clicking on the same point is difficult, the user can click in a radius of that point selected. So this is the reason it is called persuasive cued click points. If the user selects the wrong location, then the access will be denied by saying

**IV. RESULT**

In the registration process user has to enter the details for user registration. The details entered by the user in registration phase will be saved into database. The system verify the username with the login name from the registration phase. If the username contact no. and text password is matched then window shows browse button then select the image from system. Image will be rotated at the time of login. The user click on the image for the click points as the sequence as provided at the time of registration. The system verified the point with the database. If the point matches then user select next image if user wants. Final click points verified and open up the user system or user account.

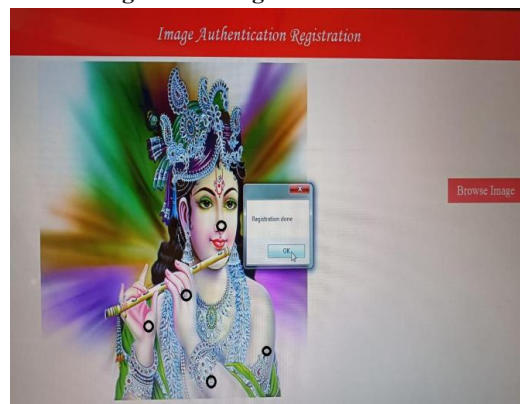
**V. SCREENSHOTS**



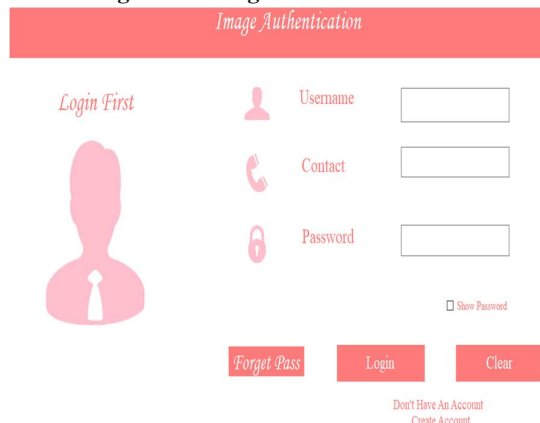
The screenshot shows a registration form with the following fields and elements:

- Register Yourself** (text)
- Image Authentication** (header)
- Username** (input field)
- E-Mail** (input field)
- Contact** (input field)
- Password** (input field)
- Confirm Password** (input field) with a **Show Password** checkbox
- Security Question** (dropdown menu)
- Answer** (input field)
- Register** (button)
- Clear** (button)
- Back to Login** (text link)

**Figure 5.1: Registration Process**



**Figure 5.2: Registration Successful**



The screenshot shows a login form with the following fields and elements:

- Login First** (text)
- Image Authentication** (header)
- Username** (input field)
- Contact** (input field)
- Password** (input field) with a **Show Password** checkbox
- Forget Pass** (button)
- Login** (button)
- Clear** (button)
- Don't Have An Account Create Account** (text link)

**Figure 5.3: Login Process**

## **VI. RESULT ANALYSIS**

Text Password is formal method is easy to hack, as if we open google chrome or mozilla firefox then in advance we have the security setting option in which by default the user name and password is saved, so it is not safe. In authentication process shoulder Surfing is possible as the cctv camera is at back then the fix image password can be captured. Therefore this process is also harmful to use. Image captcha by using optical character recognition the image pixel are captured which is not safe. Within 2 minute text captcha can be hacked. Now a days this all system can not be safe.

Where as in our system we implement Cued Click Points based Image Authentication method. At the time of login process the image get rotated by some angle due to which the optical character recognition couldn't capture image. Our system is highly secure than other systems. In image captcha image pixels are recognized by hacker. In other hand our system login process image will be rotated therefore optical character recognition couldn't recognized pixels of image.

## **VII. CONCLUSION**

In this project "A GRAPHICAL AUTHENTICATION USING PIXEL SELECTION AND CUED CLICK POINTS SELECTION". A new type of authentication system, which is highly secure has been proposed in this project. This system is also more user-friendly. This system will help the Shoulder attack, Tempest attack, and Brute-force attack at the client-side. A security system is a time-consuming approach, it will provide strong security where we need to store and maintain crucial and confidential data secure. Such systems provide a secure channel of communication between the communicating entities. The ease of using remembering images as a password also support the scope of these systems.

## **VIII. FUTURE SCOPE**

In the future, it has great scope. It can be used everywhere instead of a text-based password. We can increase the security of this system by increasing the number of levels used, and the number of tolerance squares used. Presently there are many authentication systems but they have their advantages and disadvantages. Text passwords can be hacked easily with various methods whereas biometric authentication can cause more cost. This system is more secure and cheap than old methodologies. As well as this system allows for a more reliable and easily recognizable system to the users. As for how we have written over this system can be the best alternative to the text password.

## **REFERENCES**

- [1]. Y. Januzaj, A. Luma, Y. Januzaj, V. Ramaj., "Real-time access control based on face recognition," in International Conference on Network security Computer Science (ICNCS-15), pp. 7-12, 2015.
- [2]. M. Sahani, C. Nanda, A. K. Sahu, B. Pattnaik., "Home security system based on face recognition," 2015 Int. Conf. Circuits, Power Comput. Technol. [ICCPCT2015], pp. 1-6, 2015.
- [3]. G. Senthilkumar, K. Gopalakrishnan, V. S. Kumar., "Embedded image capturing system using the raspberry pi system," vol. 3, No. 2, pp. 213-215, 2014.
- [4]. M. R. Mulla., "Facial image based security system using PCA," pp. 548-553, 2015.
- [5]. M. H. Jusoh F. Bin Jamali, "Home security system using internet of things," 2017.
- [6]. S. S. Liew, M. Khalil-Hani, S. Ahmad Radzi, R. Bakhteri., "Gender classification: A convolutional neural network approach," Turkish J. Electr. Eng. Comput. Sci., vol. 24, No. 3, pp. 1248-1264, 2016.
- [7]. Karmajit Patraa, Bhushan Nemadab\*, Debi Prasad Mishrac, Prajnaya Priyadarsini Satapathyd "Cued-Click Point Graphical Password Using Circular Tolerance to Increase Password Space and Persuasive Features" 2016.
- [8]. A. R. Syafeeza, S. S. Liew, R. Bakhteri., "Convolutional neural networks with fused layers applied to face recognition," Int. J. Comput. Intell. Appl., vol. 14, No. 3, 2015.
- [9]. A. R. Syafeeza, M. Khalil-Hani, S. S. Liew, R. Bakhteri., "Convolutional neural network for face recognition with pose and illumination variation," Int. J. Eng. Technol., Vol. 6, No. 1, pp. 44-57, 2014.
- [10]. K. Syazana-Itqan, A. R. Syafeeza, N. M. Saad, N. A. Hamid, W. H. Bin Mohd Saad., "A review of finger-vein biometrics identification approaches," Indian J. Sci. Technol., vol. 9, No. 32, 2016.
- [11]. S. Ahmad Radzi, M. Khalil-Hani, R. Bakhteri., "Finger-vein biometric identification using convolutional neural network," Turkish J. Electr. Eng. Comput. Sci., vol. 24, No. 3, pp. 1863-1878, 2016.

- [12]. Devidas Thosar, Review on Advanced Graphical Authentication to resist shoulder surfing attack. DOI: 10.1109/ICACAT.2018.8933699, 19 December 2019, Published by IEEE.
- [13]. Devidas Thosar, Review on click points graphical passport, Volume 5 issue 2, August 2018, by Internation Journal of Research and Management(IJERN).