

“LOGIN FUNCTIONALITY USING IMAGE PIXEL AUTHENTICATION AND CUED CLICK POINTS”

Mr. Devidas S. Thosar
(Guide & Assistant Professor)

Ms. Vaishnavi P. Kolhe
Ms. Vrushali A. Jadhav

Ms. Priyanka A. Shinde
Ms. Sharddha V. Bankar

DEPARTMENT OF COMPUTER ENGINEERING
SIR VISVESVARAYA INSTITUTE OF TECHNOLOGY, NASHIK

ABSTRACT

We introduced a new technique Login Functionality using Image Pixels Authentication and Cued Click Points. We examined the usability and security of this project. A human mind remembers images more quickly than text. Usually the users create passwords by using text characters, but by using these text passwords there are many drawbacks. An image password easy to remember but hard to guess to the hackers. Users can't remember strong passwords easily and the passwords that can be remembered are easy to guess. so we came up with this login functionality using image pixels authentication and cued click points technique. The main purpose of the login functionality using image pixels authentication and cued click points techniques is to provide advanced security to the users

Keywords: Pixel authentications, Cued click points, CCTV, CCP

INTRODUCTION

Authentication is the process of determining whether a user should be allowed to access a particular system or resource. Users can't remember strong passwords easily and the passwords that can be remembered are easy to guess. A password authentication system should encourage strong and less predictable passwords while maintaining memorability and security. People are access their mobiles, TABs and laptops anywhere like coffee shops, mall, railway station, banks and those areas which are already in CCTV. They are totally aware about this environment where their devices are easily access and recorded in video footage. that time login information and other personal information recorded. For any hacker this kind of information is enough to hack their devices and miss use it easily without any extra efforts by using CCTV video footage. The purpose of this paper is to avoid this kind of unlike attacks. 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. So there will be no chance to hack the devices and personal information's.

In this paper, we propose a Cued Click Points (CCP) for image password authentication. A password consists of one click-point per image for a sequence of images. The next image displayed is based on the previous click-point so users receive immediate implicit feedback as to whether they are on the correct path when logging in. CCP offers both improved security and usability.

PROBLEM DEFINITION :

Password-based authentication is one of the simplest and most common authentication mechanisms used to provide computer security. However, people prefer to create short and simple passwords as it can recognize easily. This type of password is usually lead to password guessing easily and caused malicious activities. In addition, traditional authentications like passwords are the unwillingness of the users to remember long, challenging combination of numbers, letters and symbols that can be easily copy or guess. Therefore, users are

restricted to add numbers or special characters in their passwords but such policies make the passwords hard to remember.

Lastly, password thefts can and do happen on a daily basis because the password is not secure and allows attackers to steal or crack data easily. This may reduce the level security of the system. So, users need to choose a strong password like combine the alphabets, number and symbol together.

LITERATURE REVIEW

1. Sneha Mathew proposed Web based Graphical Password Authentication System in which password consists of a sequence of different click points on a given image. Graphical password has been proposed as a possible alternative to text-based password. Its features is about ease of use, memorize, creation, learning and satisfaction.

2. Dr Prakash Bethapudi proposed THREE LEVEL PASSWORD AUTHENTICATION SYSTEM in which he form a 3-level security system which increases the confidentiality to the password in a higher level. At each session user need to get authenticated so that it is able for them to proceed to the next level. LEVEL 1- authenticated by OTP generation via email, LEVEL 2- authenticated by explicit calculation-based method, LEVEL 3- authenticated by image ordering. After getting authenticated in all the levels the user can use the system. If fails to authenticate in any level then it is not possible to move to the next level.

3. Fatemeh Ghiyampour proposed Secure graphical password based on cued click points using fuzzy logic in which he present a graphical password based on cued recall in which is secured from shoulder surfing attack. Also, he propose an image encryption technique using a 2D cat map and edge detection technique in which it uses fuzzy logic inference to detect the edge of images. Then the user password is encrypted before storing it in the database using this method. Experiments illustrate that the proposed method has good performance in usability and security.

SOFTWARE REQUIREMENT SPECIFICATION

INTRODUCTION :

The main objective of this project is to design a login functionality using image pixels authentication and cude click points scheme based on text-based password, image-based and cude click points for improving the security protection. This chapter will discuss about the basic concept of authentication using these authentication password to authenticate user and compare which approaches is the best. Besides, there will be some of related or existing approaches will be discussed as well.

PROJECT SCOPE :

Firstly, for user's scope, the user are able to register the application as a user. Besides, the users are also able to provide data regarding the registration form. The data is collected when the users done registered. This system is focusing on a firm or industry or institute where it will accessible only to some higher designation holding people, who need to store and maintain the crucial and confidential data secure. The system's scope is using two existing schemes which are text based password, image password and cude click points. The users need to input correct password in the previous level before continuing with the next level. So, this will help to improve the security level in authentication.

USER CLASSES AND CHARACTERISTICS :

Generally the users are classified into two:

- Administrator
- Users

Admin is responsible for the maintenance of the software and he will see for the security measures for the system. He should be given the authority to add and delete users.

Users can use the system to upload or download their files or documents.

ASSUMPTIONS AND DEPENDENCIES :

There are many dependencies and assumptions associated with the software. They are:

- Every user is expected to have a valid image password.
- The size of the files uploaded should not exceed the limit.

FUNCTIONAL REQUIREMENTS :

The various functional requirements of this project are the following :

- Selection of the first image during registration.
- Database module for maintaining the framework.

NON FUNCTIONAL REQUIREMENTS :

Non functional requirements are as follow :

- Security
- Reliability
- Maintainability
- Reusability
- Portability
- Extensibility

PERFORMANCE REQUIREMENTS :

The performance of the system lies in the way it is handled. Every user must be given proper guidance regarding how to use the system. The other factor which affects the performance is the absence of any of the suggested requirements.

SAFETY REQUIREMENTS:

To ensure the safety of the system, perform regular monitoring of the system so as to trace the proper working of the system. An administrator should be there to ensure the safety of the system. He has to be trained to handle extreme error cases.

SOFTWARE REQUIREMENTS :

Operating System : Windows 2000/XP

Language Used : C#

HARDWARE REQUIREMENTS :

1. Processor : Intel Pentium IV
2. Hard Disk : 80 GB
3. Display : 15" Monitor
4. CD Drive : 52X speed
5. Main Memory : 512 MB RAM

User Registration ;

In Registration phase, the system collects the basic details/information of the user like name, mobile and email, textual password, and image password. These all are encrypted and stored in the database. The registered users are the part of user module.

Login :

In login phase, the user will give the username, textual password, and image password for accessing the resource. It compares the given values with data already given by the user at the registration phase. If it matched, then he/she will be logged into the page.

ADVANTAGES :

- They are easy to remember and hard to guess.
- The security of the system or resource is very high.
- They happen to be human friendly passwords.

LIMITATIONS :

Using Mobile devices with small screens might be possible to increase safety by using smaller images while retaining the usability. On the other hand using larger images may appear to less clustering, symptomatic of a big issue in this method.

APPLICATIONS :

- Web Login-in Application.
- Mobile Device.

CONCLUSION

A new type authentication system, which is highly secure has been proposed in this project. This system, is also more user friendly. This system will definitely help Shoulder attack, Tempest attack and Brute-force attack at the client side. 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.

Image passwords are an alternative to textual alphanumeric password. It satisfies both conflicting requirements i.e. it is easy to remember & it is hard to guess. By the solution of the shoulder surfing problems, it becomes more secure & easier password scheme. By implementing encryption algorithm and hash algorithms for sorting and retrieving pictures and points, one can achieve more security image password is still immature more research is required in this field. While increasing the number of images and number of grides the security will be very high and the efficiency will be 100

Reference

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 (ICNSCS-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. [ICCPCT-2015]*, pp. 1-6, 2015.
3. G. Senthilkumar, K. Gopalakrishnan, V. S. Kumar., "Embedded image capturing system using 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. M. Sajjad *et al.*, "Raspberry pi assisted face recognition framework for enhanced law-enforcement services in smart cities," *Futur. Gener. Comput. Syst.*, 2017.
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. S. Ahmad Radzi., "A MATLAB-based convolutional neural network approach for face recognition system," *J. Bioinforma. Proteomics Rev*, vol. 2(1), pp. 1-5, 2016.