Graphical Password Authentication using image Segmentation for Web Based Applications

Maw Maw Naing, Ohnmar Win

Department of Electronic Engineering, Mandalay Technological University, Mandalay, Myanmar

How to cite this paper: Maw Maw Naing | Ohnmar Win "Graphical Password Authentication using image Segmentation for Web Based Applications" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-3 | Issue-4, June 2019, pp.1461-1464, URL: https://www.ijtsrd.com/papers/ijtsrd25184.pdf

IJTSRD25184

ABSTRACT

One of the most important topics in information security today is user authentication. User authentication is a fundamental component in most computer security contexts. It provides the basis for access control and user accountability. While there are various types of user authentication systems, alphanumeric passwords are the most common type of user authentication. They are versatile and easy to implement and use. However, it can either be long and secure or short and hard to remember. A graphical based password is one promising alternatives of textual passwords. According to human psychology, humans are able to remember pictures easily. In this paper, graphical passwords have been designed to try to make password more memorable and easier for people to use, and it is less vulnerable to brute force attacks than a text-based password. The aim of the system is to implement a strong security. The proposed system segments the image like a grid, which has a maximum four fragments. Then, each segment of the image is dragged in a particular sequence onto an empty grid of size 6x6 and placed on a particular segment of the empty grid, to form the user' password. When the user logs into the system, the user needs to drag each segment of the image onto the same empty grid of size 6x6 in the correct sequence and position of the segments that user had specified during registration.

Keywords: *Authentication, Graphical Passwords, Images Segmentation*

I. INTRODUCTION

Authentication based on passwords is used largely in applications for computer security and privacy. Currently the authentication methods can be broadly divided into three main areas. Token based, Biometric based, and Knowledge based authentication [1]. Text Based Password and Graphical Password are the type of Knowledge based Authentication. Graphical based passwords schemes can be broadly classified into four main categories: First is Recognition based Systems which are also known as Cognometric Systems or Searchmetric Systems. Recognition based techniques involve identifying whether one has seen an image before. The user must only be able to recognize previously seen images, not generate them unaided from memory. Second is Pure Recall based systems which are also known as Drwanmetric Systems. In pure recall-based methods the user has to reproduce something that he or she created or selected earlier during the registration stage. Third is Cued Recall based systems which are also called Iconmetric Systems. In cued recall-based methods, a user is provided with a hint so that he or she can recall his/her password. Fourth is Hybrid systems which are typically the combination of two or more schemes. Like recognition and recall based or textual with graphical password schemes [2]. The most common computer authentication method is for a user to submit a user name and a text password. The vulnerabilities of this method have been well known. One of the main problems is the difficulty of remembering passwords. Graphical passwords systems are the most promising alternative to conventional password based authentication systems.

Graphical passwords (GP) use pictures instead of textual passwords and are partially motivated by the fact that humans can remember pictures more easily than a string of characters [3]. The idea of graphical passwords was originally described by Greg Blonder in 1996 [4]. An important advantage of GP is that they are easier to remember than textual passwords. Human beings have the ability to remember faces of people, places they visit and things they have seen for a longer duration. Thus, graphical passwords provide a means for making more user-friendly passwords while increasing the level of security. The key feature of the system is that it uses image as a password which makes it more memorable. The proposed system requires a user to upload a memorable image and also remember the position of segmented images as registration.

II. Overview of proposed system

A. Appliances of Web Technology

Web is the most critical technology to carry data via internet. The primary function of a web server is to store, process and deliver web pages to clients. Generally, most of the web servers support server-side scripting using Active Server Pages (ASP), PHP or other scripting languages. Web servers are not only used for serving the World Wide Web but also found embedded in devices such as printers, routers, and webcam. No additional software has to be installed on the client computer because only a web browser is required.

There are three main parts in this technology. They are hypertext document, web server and web browser.

The communication between client and server takes place using the Hypertext Transfer Protocol (HTTP). Pages delivered are most frequently Hypertext Mark-up Language (HTML) documents, which may include images, style sheets and scripts in addition to text content. Hypertext document also called web document is a text document including HTML element.

Web server is a system collecting the web document by using computer and can retrieve when it is required. The heart of the web is Uniform Resource Locater (URL). The address consisting of domain name and Uniform Resource Identifier (URI) is called URL. A URL will have the following format such as protocol name, domain name, path and parameter.

The basic function of web browser is to carry the data from user to web server and vice versa. The most popular web browsers are Microsoft Internet Explorer, Mozilla Firefox, Google Chrome, Apple Safari and Opera.

B. Database Management System

Database Management System is an application/ program-enabling user to store, organize, select and analyse data in a database. Hence it is needed for accessing information from a database. Some of Database Management Systems are MySQL, Microsoft SQL Server, Oracle, IBM DB2 etc. There are different types of DBMSs according to the management of database structures. Some of the types of DBMS are Hierarchical DBMS, Network DBMS, Relational DBMS, and Object-oriented DBMS. The most common used is the relational database. In relational database, data are store in data form. The table contains list of columns in which related data are entered, stored and also retrieve when required.
MySQL Database Server uses Relational database model for managing data. It is an open-source relational database application that uses structured query languages. MySQL Database Server is one of the widely used databases used in web applications. With MySQL, the user can add, access and manage content in database. SQL offers fast processing, ease, scalable and flexibility in use. Also MySQL is part of open-source PHP application. It is client-server system that consists of multi-threaded SQL server that supports different client programs, wide range of applications programming interface.

C. Image Segmentation

The system segments the uploaded image. The initiations steps are (1) upload a photo, (2) ask user about the segments they want and (3) take upload photo width and height. The basis methods for segmenting the image are as follows:

A. Assign the width and height of image. width=width of image and height=height of image.
B. Compute the horizontal and vertical segment of image. Horizontal segment= square root (fragment) and Vertical segment=square root (fragment).
C. Compute the width and height of segment. Width of segment= width/ Horizontal segment and High of segment= height/ Vertical segment.

D. Hash Function

The segmented image is encrypted by using Hash function in the system and it is stored into database. Firstly, the image is compared whether it is jpg or png format. If it is compact with the image format type, the format type is changed into the standard type again. The image is resized into (8*8) pixels which are converted into gray scale format. The system computes the mean value of the gray scale image and it also computes the bits which are based on whether the color value is above or below the mean value. The mean value will take out the bit value in 0, 1. If a gray value is higher than the mean value, it will be 1. Otherwise, it will be 0. In constructing Hash function, it sets the 64bits binary from left to right, top to bottom using big endian.

III. System FLOW

This figure below explains the flow of the system i.e. how data is being transferred from one module to another.

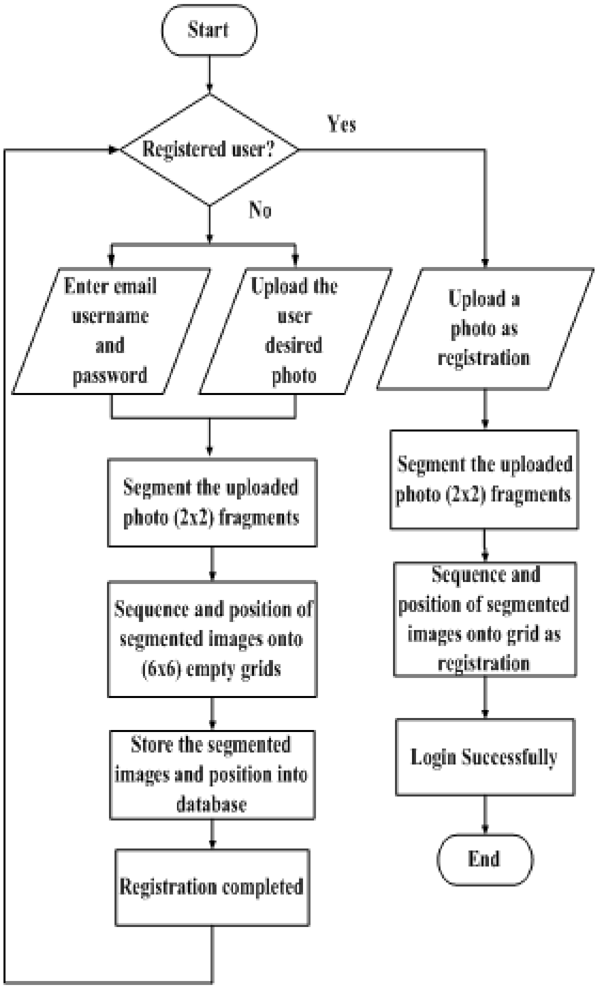

Start
Registered user?
Yes
No
Enter email username and password
Upload the user desired photo
Upload a photo as registration
Segment the uploaded photo (2x2) fragments
Sequence and position of segmented images onto (6x6) empty grids
Store the segmented images and position into database
Registration completed
Segment the uploaded photo (2x2) fragments
Sequence and position of segmented images onto grid as registration
Login Successfully
End

Figure 1: Flowchart of Graphical Password Authentication Using Image Segmentation for Web Based Applications

IV. System Implementation

The proposed system is aimed to provide a system which gives strong authentication to the user and protects user data from unauthorized access. The proposed system consists of four parts:

A. Registration Process:

- **Input module:** The user will be asked to upload a unique image to the system and enter username password and email address as shown in fig.2.
- **Image divides into segments:** Then the system will divide the uploaded image into 2x2 grid segments as shown in fig.3. Each segment will be associated with a unique number.
- **Mapping of image segments to empty grid:** The system will then present the segmented image alongside an empty grid and ask the user to place the grid segments from segmented image into the empty grid. The segments of the empty grid will also be associated with a unique number.
- **of segment:** The position in which the user places the segments into the empty grid is stored in database and will act as authentication of the user.

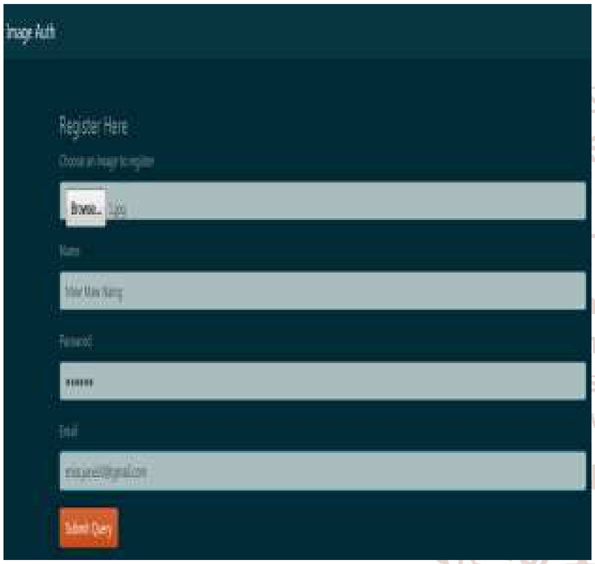


Figure 2. Registration Form

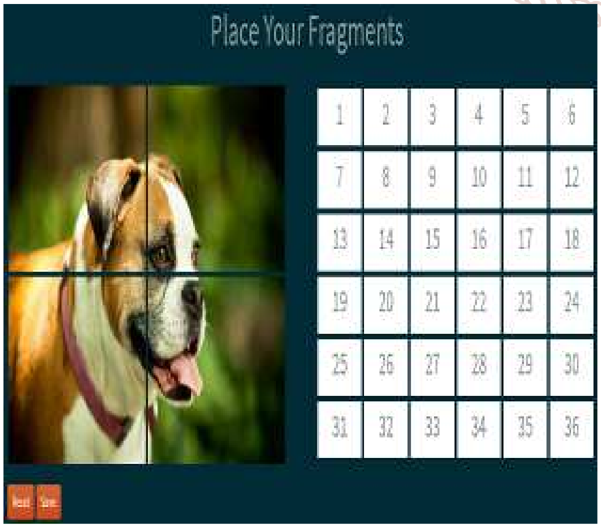


Figure 3. Segmented Image

User has to drag and drop each segment of image anywhere on a 6x6 empty grid as shown in fig.4. User is supposed to remember the sequence and position of where the segment is mapped in an empty grid.

Fig.5 shows how each segment and their position number are saved represented by imghash and position. System is implemented by encryption and decryption of data for the authentic user's data. Further the data cannot be retrieved by any hacker as it will be in encrypted form.

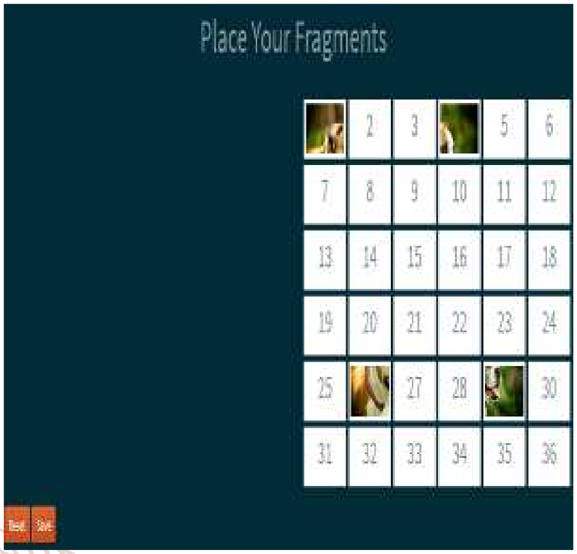
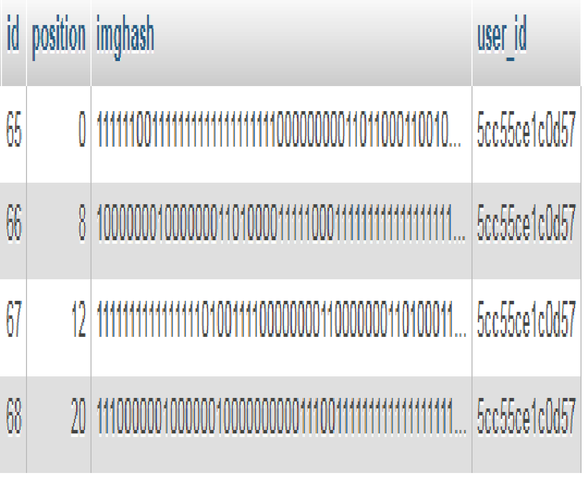


Figure 4. Setting of User



id	position	imghash	user_id
65	0	111111001111111111111111111100000000011011000110010...	5cc55ce1c0d57
66	8	1000000010000000110100001111100011111111111111111...	5cc55ce1c0d57
67	12	1111111111111111010011110000000001000000011010001 1...	5cc55ce1c0d57
68	20	111000000100000010000000000111001111111111111111...	5cc55ce1c0d57

Figure 5. Snapshot of Database for 2x2 Fragments

B. The Login Process:

- **Matching of input image with registered image:** The system will ask the user to upload the same image that he/she had provided at the time of registration.
- **Image divides into segments***:* The system then segments the image using algorithm and presents it to the user along with an empty grid.
- Verify sequence and position of segments mapped and authenticate user: The user has to place the segments in the empty grid in the correct position (Same as saved in the database during the registration process) to be considered as an authorized user.

C. The Learning Management System:

After the user is authenticated he will be directed to the web page. This is an application which is developed for the department of a university, wherein data can be shared between the students and the faculty, faculty and the HOD, and HOD and students.

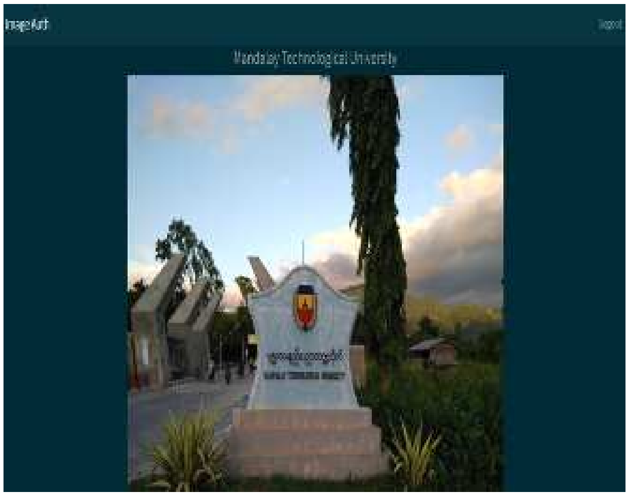


Figure6. Learning Management System User Homepage

D. Forget Password

If the uploaded photo is damaged or lost then the user can click forget password as shown in fig.5. After clicking forget password user will be redirected to a page wherein the recovery email and password will be entered. If the recovery email and password is correct then the uploaded photo will be given to him.

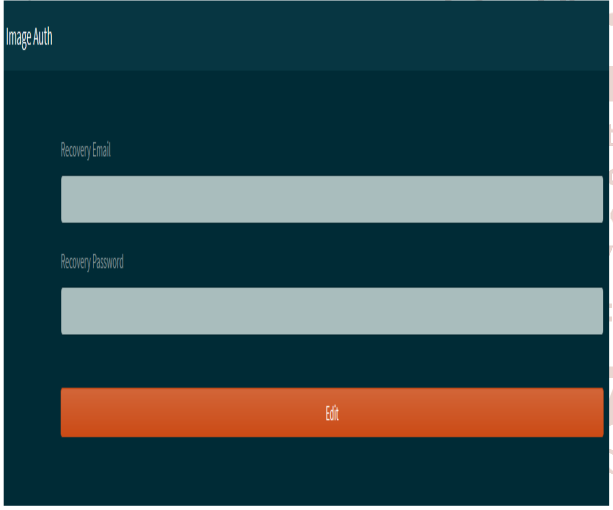


Figure 7. Forget password Form

V. Conclusion

The proposed graphical password authentication system is based on exclusive segmentation methods and Hash Visualization technique. The graphical password is the alternative approach of the current text passwords. Text passwords are the most common computer authentication methods using alphanumerical usernames and passwords but the methods have some significant drawbacks such as it is hard to remember the type passwords for users. The main advantage of graphical password authenticated systems is that users are better at memorizing graphical passwords than text-based passwords and it is more difficult to break graphical passwords using the traditional attack methods such as brute force search, dictionary attack, or spyware. The proposed graphical password authentication use the image as a password and the system is designed to provide strong security to computer systems. Although the images are easier to remember or to recognize than texts, it is necessary more storage space to store the image. In the system, MYSQL database management system is used to store the image data and also use the data encryption methods that make the user data more secure and the data cannot be easily attacked by the hackers. The graphical passwords are used in web log-in application, ATM machines and also mobile devices and the proposed system is aimed to the authentication process of web based application.

Acknowledgement

The authors would like to thank Dr.Ohnmar Win, Professor, Department of Electronic and Communication Engineering for kindly permitting to prepare for this paper, for her fruitful advice, close supervision, encouragement and numerous invaluable guidance. The author would also thank to all teachers and friends who willingly helped the author throughout the preparation of the paper.

References

[1] Mayur H Patel, Nimit S Modind "Authentication Using Text and Graphical Password" International Journal of Science and Research (IJSR) Volume 4, Issue 5, May 2015

[2] Wazir Zada Khan, Mohammed Y Aalsalemand Yang Xiang "A Graphical Password Based System for Small Mobile Devices " IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 5, No 2, September 2011

[3] Patric Elftmann, Diploma Thesis, "Secure Alternatives to Password- Based Authentication Mechanisms" Aachen, Germany October 2006

[4] G. E. Blonder. Graphical password, U.S. Patent 5559961, Lucent Technologies, Inc. (Murray Hill, NJ), August 1995.

[5] Krishan Chand, Ashish Anand "Graphical Password System Using Image Segmentation" Volume 2, Issue 5, May 2016

[6] Rohitkumar Kolay, Animesh Vora, Vinaykumar Yadav "Graphical Password System Using Image Segmentation" International Research Journal of Engineering and Technology (IRJET) Volume 04, Issue 03, Mar -2017

[7] Rupali Deshmukh; Smita Rukhande "Authentication by Image Segmentation and Shuffling"IJCAT-International Journal of Computing and Technology, Volume 4, Issue 12, December 2017

[8] Rashika Koul, Tanya Kumar, Ashwini Dhongade, Radhika Malpani, Rupali Deshmukh "Graphical Password by Segmentation of Image" *International Journal of Research and Scientific Innovation (IJRSI)/ Volume* III, Issue XI, November 2016

[9] Sana Ansari, Prof. Avinash Shrivas "Implementation of Authentication Mechanism Using Image Segmentation for Web Based Applications"