GPSI: Graphical Password by Segmentation of Image

Rashika Koul[1], Tanya Kumar[1], Ashwini Dhongade[1], Radhika Malpani[1], Rupali Deshmukh[2]

[1]Student, Department of Information Technology, Fr. Conceicao Rodrigues Institute of Technology, Vashi, Navi Mumbai
[2]Assistant Professor, Department of Information Technology,
Fr. Conceicao Rodrigues Institute of Technology, Vashi, Navi Mumbai

Abstract: **In today's technologically advanced era, it is imperative that there exists a convenient method for securing data. Computer security depends largely on passwords in order to authenticate human users. There are various software based authentication methods such as, alphanumeric passwords and hardware based methods such as, biometric authentication and token based authentication. But these methods are not able to comply with two conflicting requirements of a password, that is, security and memorability. Alphanumeric passwords can either be long and secure or short and hard to remember. On the other hand hardware based passwords like biometric have known to be insecure apart from being costly. Thus, Graphical Password by Segmentation of Image (GPSI) is the most efficient way to provide above features along with cheap development costs. 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 Graphical password by segmentation of image (GPSI) is to implement a strong security for a learning management system (LMS). The key feature of the system is that it uses image as a password which makes it more memorable. It allows user to input an image as its password and only user knows what the image looks like as a whole. On receiving the image, the system segments the image using a user specified mXn grid and stores them accordingly. The next time user logs into the system the segmented image is received by the user in a jumbled order, i.e. the segments of the image are shuffled. Now if user arranges the segments of the image in an order so as to make the original image he sent then user is considered authentic. Else the user is not granted access. The system does the image segmentation based on coordinates. The coordinates of the segmented image allow the system to fragment the image and store it as different parts.**

Keywords: **segmentation, grid, graphical password, shuffle, Fisher Yates algorithm, mapping sequence, mapping table**

I. INTRODUCTION

Computer security depends largely on passwords in order to authenticate human users. The main drawback of alphanumeric passwords is what we call the password problem, namely the fact that passwords are expected to comply with two conflicting requirements: a) Passwords should be easy to remember, and the user authentication protocol should be executable quickly and easily by humans. b) Passwords should be secure, i.e., they should look random and should be hard to guess; they should be changed frequently, and should be different on different accounts of the same user. They should not be written down or stored in plain text. Hence, graphical passwords act as alternative to alphanumeric passwords because they serve as a solution to the 'password problem'.

II. EXISTING SYSTEM

A study was done of different existing system and a comparison was made on the different existing system.

Table I. Comparison of Existing system

METHODS	ADVANTAGES	DISADVANTAGES
1. CAPTCHA	1. The usages of characters in the captcha images are recognizable by human readers and mostly easy to read. 2. The algorithm of this method makes it hard to read by OCR programs which mean that it is safer.	1. It can be understandable by computers with using powerful and intelligent software and hardware by removing the noise effects. 2. Some patterns could be hard to read by older and disabled human users.
2. PASS POINTS	1. The password generated is most difficult to break and not easily guessable. 2. Users in PassPoint system were able to easily and quickly create a valid password.	1. Users have more difficulty learning their passwords than alphanumeric users, taking more trials and more time to complete the practice. 2. The login time, in this method is longer than alphanumeric method.
3. DAS	1. The password generated is easily memorable. 2. This technique takes less time for login process than alphanumeric passwords.	1. User cannot remember the exact stroke order. 2. If user is not familiar with the input devices then the technique is difficult to use.
4. RECOGNITION BASED TECHNIQUE	1. Users will select images, icons or symbols from a collection of images. 2. The users can remember their passwords even after 45 days . 3. The password space of the recognition based techniques largely depends on the size of the content.	1. It is less secure than pure recall based technique. 2. Overly large storage requirement is a significant issue for recognition based techniques, since the size of a typical picture is much larger than the equivalent text.

5. PURE RECALL BASED TECHNIQUE	1. Users have to reproduce their passwords without being given any type of hints or reminder. 2. The users can hardly remember their passwords. 3. It is more secure than the recognition based technique.	1. It is difficult to calculate the password space of a recall based technique. 2. It is difficult to draw shapes with mouse. Most users are not familiar with using mouse.

III. PROPOSED SYSTEM

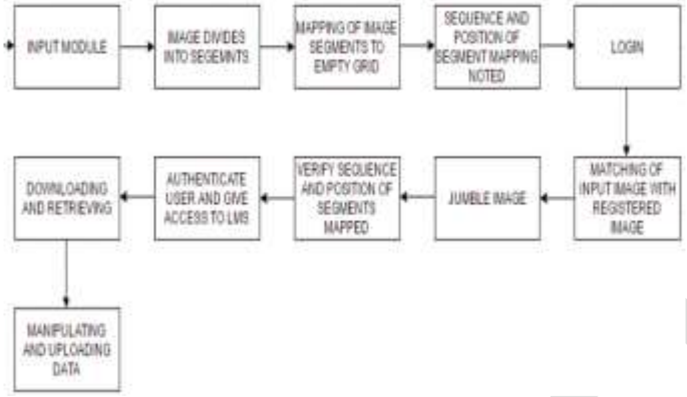
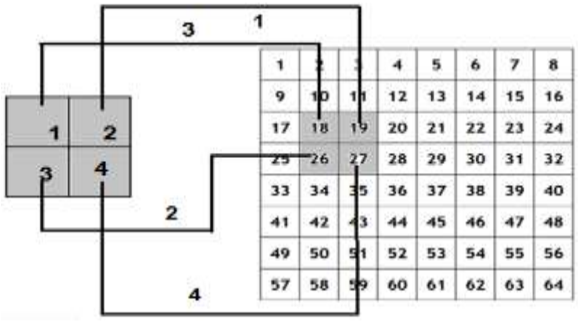

INPUT MODULE
IMAGE DIVIDES INTO SEGEMNTS
MAPPING OF IMAGE SEGMENTS TO EMPTY GRID
SEQUENCE AND POSITION OF SEGMENT MAPPING NOTED
LOGIN
MATCHING OF INPUT IMAGE WITH REGISTERED IMAGE
JUMBLE IMAGE
VERIFY SEQUENCE AND POSITION OF SEGMENTS MAPPED
AUTHENTICATE USER AND GIVE ACCESS TO LMS
DOWNLOADING AND RETREIVING
MANIPULATING AND UPLOADING DATA

Fig. 1 Block Diagram of GPSI

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

A. Registration Process:

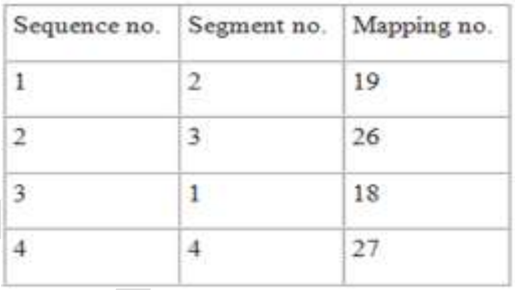
- *Input module:* The user will be asked to provide a unique image to the system and specify the number of grid segments the image will be divided into (Maximum of 8X8).
- *Image divides into segments:* Then the system will divide the user specified image into user specified grid segments. Each segment 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.
- *Sequence and position of segment mapping noted:* The position and order in which the user places the segments into the empty grid is noted in a mapping table and will act as authentication of the user.



1	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32
33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56
57	58	59	60	61	62	63	64

Fig. 2 Mapping process

Table II. Mapping table



Sequence no.	Segment no.	Mapping no.
1	2	19
2	3	26
3	1	18
4	4	27

Sequence of mapping: 19, 26, 18, 27

Fig. 2. depicts that the segments of an image (Which is segmented into 2X2 grid) are being mapped onto 4 corresponding segments of an empty grid of 8X8. This mapping of segments is done in a particular noted sequence. Considering that every segment of the empty grid and the image is associated with a unique number, each segment number of the image is written besides the segment number of the empty grid segment on which it is mapped, in the mapping table.

B. The Login Process:

- *Matching of input image with registered image:* The system will ask the user to provide the same image that he/she had provided at the time of registration. Only if the user provides the right image he/she can go on to the next step otherwise not.
- *Jumble image:* The system then segments and shuffles the image using Fisher Yates algorithm and presents it to the user along with an empty grid. The Fisher–Yates shuffle is an algorithm for generating a random permutation of a finite set. In plain terms, the algorithm shuffles the set. The algorithm produces an unbiased permutation: every permutation is equally likely. The basic method given for generating a random permutation of the numbers 1 through N goes as follows:

a) Store the segments from 1 through N (N=mXn) as numbers from 1 to N (N=mXn).
b) Pick a random number k between one and the number of unstruck numbers remaining (inclusive).
c) Counting from the low end, strike out the kth number not yet struck out, and write it down at the end of a separate list.
d) Repeat from step 2 until all the numbers have been struck out.
e) The sequence of numbers written down in step 3 is now a random permutation of the original numbers.
f) Since each of these numbers represent each image segment, the segments are also jumbled accordingly.

- *Verify sequence and position of segments mapped and authenticate user:* The user has to place the segments in the empty grid in the correct order and position (Same as saved in the mapping table during the registration process) to be considered as an authorised user.

C. The Learning Management System:

- *Uploading and manipulating data:* The users can upload, manipulate and delete data files like notices, notes, presentations, questions, quizzes etc.
- *Download and retrieve data:* The users can download the data according to their authorisation.

IV. FLOW CHART

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

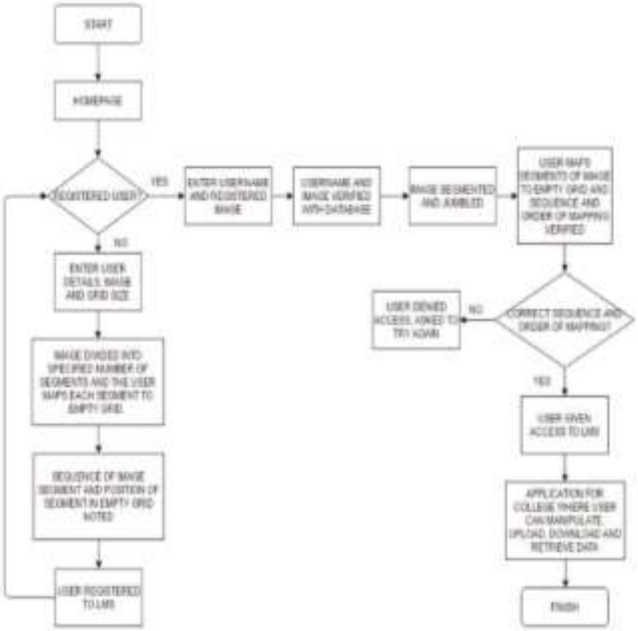

START
HOMEPAGE
REGISTERED USER?
YES
NO
ENTER USERNAME AND REGISTERED IMAGE
USERNAME AND IMAGE VERIFIED WITH DATABASE
IMAGE SEGMENTED AND JUMBLED
USER MAPS SEGMENTS OF IMAGE TO EMPTY GRID AND SEQUENCE AND ORDER OF MAPPING VERIFIED
ENTER USER DETAILS, IMAGE AND GRID SIZE
IMAGE DIVIDED INTO SPECIFIED NUMBER OF SEGMENTS AND THE USER MAPS EACH SEGMENT TO EMPTY GRID
SEQUENCE OF IMAGE SEGMENT AND POSITION OF SEGMENT IN EMPTY GRID NOTED
USER REGISTERED TO LMS
USER DENIED ACCESS, ASKED TO TRY AGAIN
NO
CORRECT SEQUENCE AND ORDER OF MAPPING?
YES
USER GIVEN ACCESS TO LMS
APPLICATION FOR COLLEGE WHERE USER CAN MANIPULATE, UPLOAD, DOWNLOAD AND RETRIEVE DATA
FINISH

Fig. 3 Flowchart for GPSI

V. CONCLUSION

The main argument for graphical passwords is that people are better at memorizing graphical passwords than text-based passwords. Our preliminary analysis suggests that it is more difficult to break graphical passwords using the traditional attack methods such as brute force search, dictionary attack, or spyware. Graphical password by segmentation of image (GPSI) which will use image as a password is designed to provide strong security to computer systems. It provides an exclusive method which segments an image. This paper explains the entire working of GPSI.

REFERENCES

[1]. J. C. Birget, D. Hong N. Memon, S. Man and S. Wiedenbeck., "The Graphical Passwords Project" Funded by the NSF Cyber Trust Program. <http://clam.rutgers.edu/~birget/grPssw/ >

[2]. Ragavendra .A, Jeysree .J, "GRAPHICAL PASSWORD AUTHENTICATION USING CaRP", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 4 Issue 2, February 2015

[3]. Ibrahim Furkan Ince, Ilker Yengin, Yucel Batu Salman, Hwan-Gue Cho, Tae-Cheon Yang, "DESIGNING CAPTCHA ALGORITHM: SPLITTING AND ROTATING THE IMAGES AGAINST OCRs", Third 2008 International Conference on Convergence and Hybrid Information Technology

[4]. Ahmet Emir Dirik, Nasir Memon, Jean-Camille Birget, "Modeling user choice in the PassPoints graphical password scheme"<https://cups.cs.cmu.edu/soups/2007/proceedings/p20_dirik.pdf>

[5]. Arti Bhanushali, Bhavika Mange, Harshika Vyas, Hetal Bhanushali and Poonam Bhogle, "Comparison of Graphical Password Authentication Techniques", International Journal of Computer Applications (0975 – 8887) Volume 116 – No. 1, April 2015

[6]. Saranya Ramanan, Bindhu J S, "A Survey on Different Graphical Password Authentication Techniques", International Journal of Innovative Research in Computer and Communication Engineering (An ISO 3297: 2007 Certified Organization) Vol. 2, Issue 12, December 2014

[7]. Xiaoyuan Suo, Ying Zhu, G. Scott Owen, "Graphical Passwords: A Survey.", DOI: 10.1109/CSAC.2005.27 · Source: DBLP Conference: 21st Annual Computer Security Applications Conference (ACSAC 2005), 5-9 December 2005, Tucson, AZ, USA

[8]. Arash Habibi Lashkari, Samaneh Farmand, Dr. Rosli Saleh, Dr. Omar Bin Zakaria, "A wide-range survey on Recall-Based Graphical User Authentications algorithms based on ISO and Attack Patterns ", (IJCSIS) International Journal of Computer Science and Information Security, Vol. 6, No. 3, 2009

[9]. Ronald Fisher, Frank Yates [1938]. Statistical tables for biological, agricultural and medical research (3rd ed.). <https://en.wikipedia.org/wiki/Fisher–Yates_shuffle>