IJCAT - International Journal of Computing and Technology, Volume 4, Issue 12, December 2017
ISSN (Online) : 2348-6090
www.IJCAT.org
Impact Factor: 0.835

Authentication by Image Segmentation and Shuffling

[1] Rupali Deshmukh; [2] Smita Rukhande

[1, 2] Department of Information Technology, Fr. C. Rodrigues Institute of Technology, Vashi
Navi Mumbai, Maharashtra, India,400703

Abstract

A Prevention of data theft such as bank account numbers, credit card information, passwords, work related documents, etc. is essential in today' communication systems, since many of our daily activities depend on the security of the data networks. Although Graphical Authentication Systems have been playing an important role in balking various kinds of bot attacks by acting as an additional mechanism over alphanumeric passwords, yet they have not been used for human authentication to its full potential. By exploiting its feature of easy memorability and the possibility of quadrillion permutation and combination of images that could form the graphical password, an independent human authentication system can be made. Thus, Graphical Password by Segmentation of Image is one such system that attempts to exploit the aforementioned criteria. This system segments the image like a grid, which has a maximum of 8 columns and 8 rows. Then, each segment of the image is dragged in a particular sequence onto an empty grid of size 8x8 and placed on a particular segment of the empty grid, to form the user' password. If the user chooses to shuffle the segments during registration, the image segments will be presented in a shuffled manner when the user logs into the system and the user needs to drag each segment of the image onto the same empty grid of size 8x8 in the correct sequence and position of the segments that user had specified during registration.

Keywords: *Data Theft, Communication Systems, Security, Bot Attacks, Alphanumeric Password, Graphical Password, Memorability*

1. Introduction

Graphical Authentication systems such as CAPTCHA and other Recognition Based Techniques have proved to be useful in many real time systems, but only to prevent bot attacks. Other recall based techniques such as draw a secret and pass points have been introduced as human authentication systems, but have not been implemented widely. [7]

Graphical passwords introduced so far have never been used as main authentication systems. The reasons are, that selecting the very same points on the image or using the mouse to draw on the image is a tedious job and to get the exact same design every time one draws with the mouse is nearly impossible. [7]

Graphical Password by Segmentation of Image (GPSI) is a human authentication system that can be used to provide security to all kinds of systems like web applications, digital lockers and even real lockers for that matter. Because Graphical Password by Segmentation of Image (GPSI) can be used independently to authenticate users, it has a potential to replace existing authentication systems such as alphanumeric passwords.

It also eliminates the need to select same intricate points on an image or draw the same design every time during login. [7]

2. Implementation

The flow of the system can be divided into two phases:

1. Registration Phase
2. Login Phase

2.1 Registration Phase

Apart from the general user credentials like username, email id, etc. the user is asked to provide an image and mention the number of rows (maximum of 8) and columns (maximum of 8) of the grid in which the user's image will be segmented as shown in Fig. 2.

User's image is then segmented into the grid of user specified rows and columns for the user to drag each segment onto the empty grid of size 8x8 as shown in Fig. 3 and Fig. 4 respectively. Fig. 4 shows that the image segments are put on numbers 1, 2, 3, 9, 10, 11, 17, 18, 19, but the user can put the image segments on any numbers, as shown in Fig 5. [1]

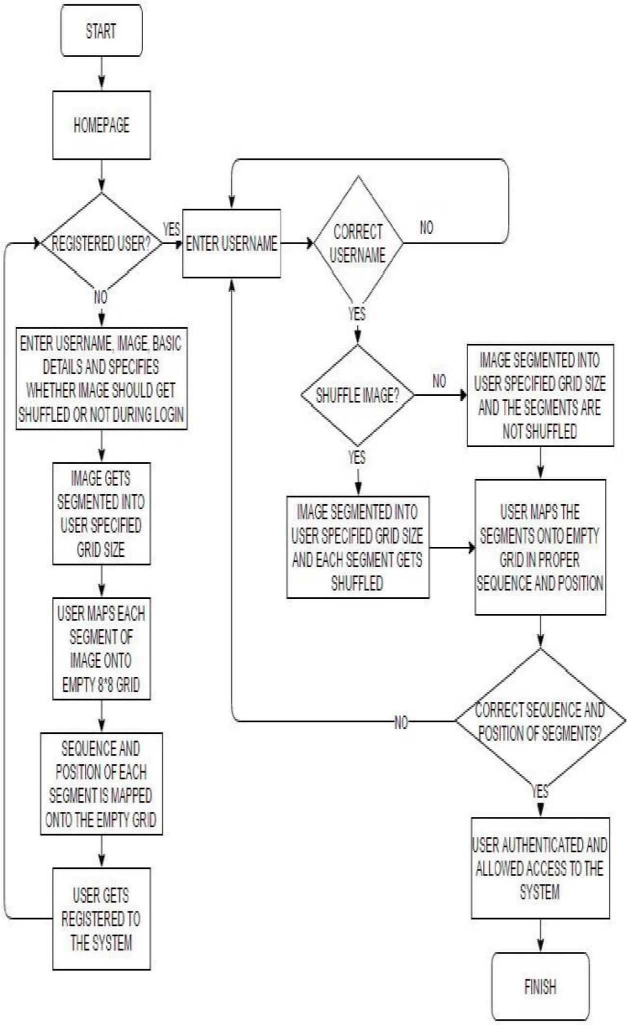
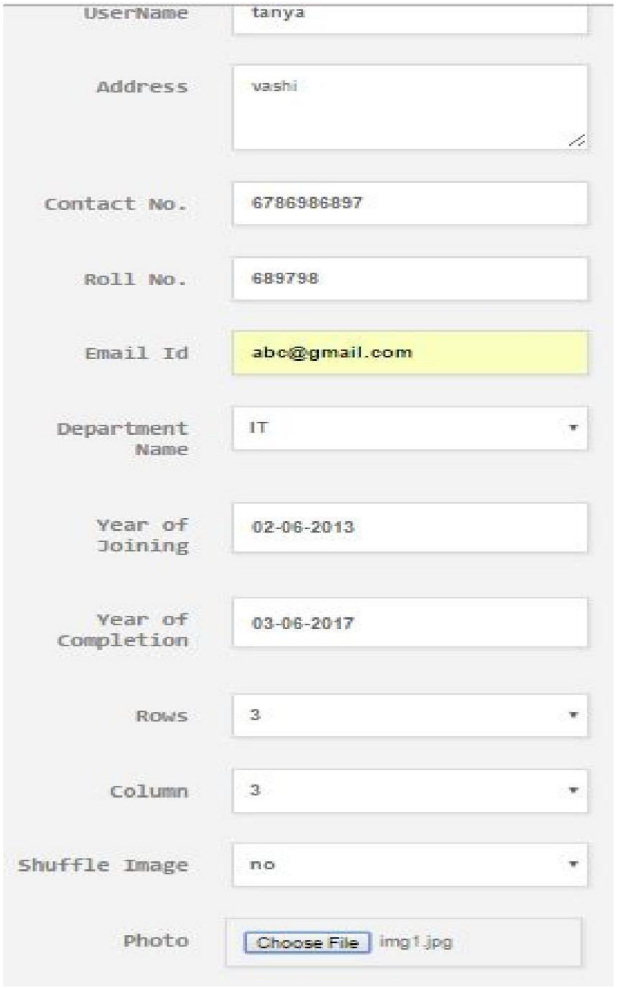

START
HOMEPAGE
REGISTERED USER?
YES
NO
ENTER USERNAME
CORRECT USERNAME
NO
YES
ENTER USERNAME, IMAGE, BASIC DETAILS AND SPECIFIES WHETHER IMAGE SHOULD GET SHUFFLED OR NOT DURING LOGIN
SHUFFLE IMAGE?
NO
YES
IMAGE SEGMENTED INTO USER SPECIFIED GRID SIZE AND THE SEGMENTS ARE NOT SHUFFLED
IMAGE GETS SEGMENTED INTO USER SPECIFIED GRID SIZE
IMAGE SEGMENTED INTO USER SPECIFIED GRID SIZE AND EACH SEGMENT GETS SHUFFLED
USER MAPS THE SEGMENTS ONTO EMPTY GRID IN PROPER SEQUENCE AND POSITION
USER MAPS EACH SEGMENT OF IMAGE ONTO EMPTY 8*8 GRID
CORRECT SEQUENCE AND POSITION OF SEGMENTS?
NO
YES
SEQUENCE AND POSITION OF EACH SEGMENT IS MAPPED ONTO THE EMPTY GRID
USER AUTHENTICATED AND ALLOWED ACCESS TO THE SYSTEM
USER GETS REGISTERED TO THE SYSTEM
FINISH

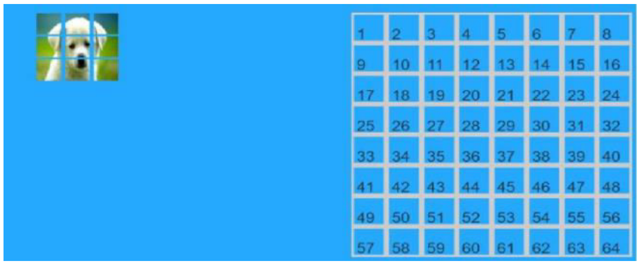
Fig. 1. Flowchart of Graphical Password by Segmentation of Image

The image is segmented using Block-Based Normalised-Cut Algorithm, whose basic unit of clustering is image block instead of individual pixel. Block-based algorithm not only decreases the time and storage complexity, but also improves the discrimination power of visual feature vector.[5]



UserName	tanya
Address	vashi
Contact No.	6786986897
Roll No.	689798
Email Id	abc@gmail.com
Department Name	IT
Year of Joining	02-06-2013
Year of Completion	03-06-2017
Rows	3
Column	3
Shuffle Image	no
Photo	Choose File img1.jpg

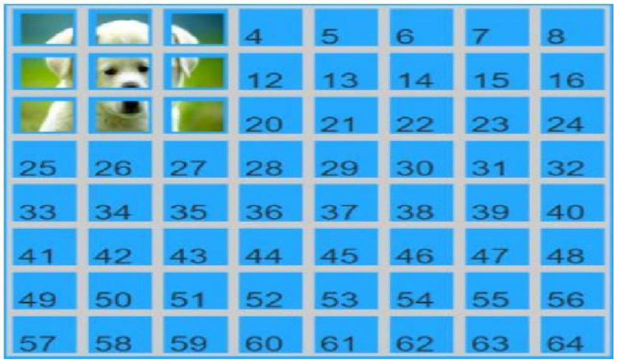
Fig. 2. Registration form



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. 3. Segmented image

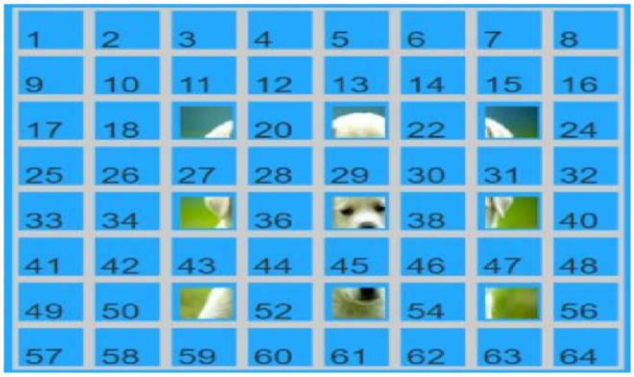
Image chosen by the user during registration is presented to user in segmented form as shown in fig 3.



			4	5	6	7	8
			12	13	14	15	16
			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. 4. Setting of user

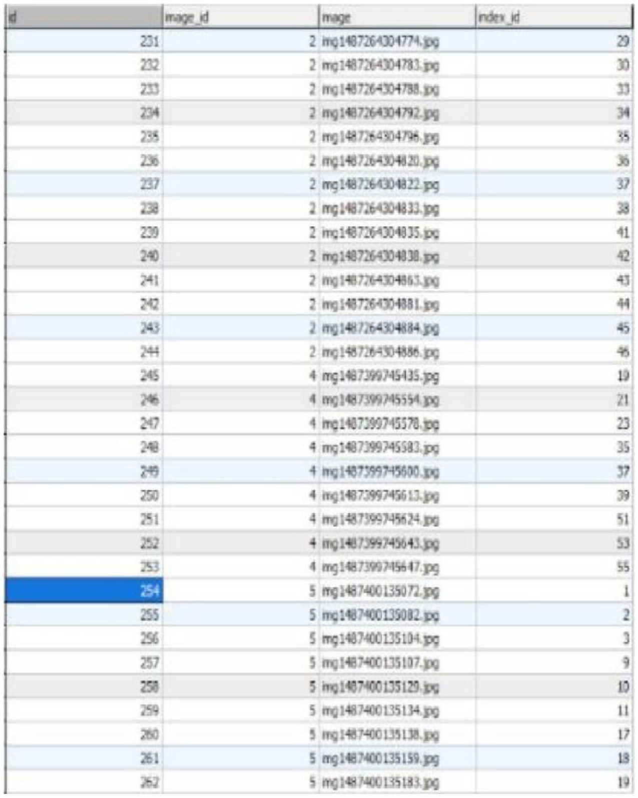
User is asked to drag and drop each segment of image anywhere on a 8x8 empty grid as shown in fig 4.User is supposed to remember the sequence and position of where the segment is mapped in a empty grid.



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

Fig. 5. A different complex example of user

Last 9 tuples of the database table in fig. 6 shows how each segment is saved in the same sequence in which the user had picked them up along with their position number represented by index_id.



id	image_id	image	index_id
231	2	img1487264304774.jpg	29
232	2	img1487264304783.jpg	30
233	2	img1487264304788.jpg	33
234	2	img1487264304792.jpg	34
235	2	img1487264304796.jpg	35
236	2	img1487264304820.jpg	36
237	2	img1487264304822.jpg	37
238	2	img1487264304833.jpg	38
239	2	img1487264304835.jpg	41
240	2	img1487264304838.jpg	42
241	2	img1487264304863.jpg	43
242	2	img1487264304881.jpg	44
243	2	img1487264304884.jpg	45
244	2	img1487264304886.jpg	46
245	4	img1487399745435.jpg	19
246	4	img1487399745554.jpg	21
247	4	img1487399745578.jpg	23
248	4	img1487399745583.jpg	35
249	4	img1487399745600.jpg	37
250	4	img1487399745613.jpg	39
251	4	img1487399745624.jpg	51
252	4	img1487399745643.jpg	53
253	4	img1487399745647.jpg	55
254	5	img1487400135072.jpg	1
255	5	img1487400135082.jpg	2
256	5	img1487400135104.jpg	3
257	5	img1487400135107.jpg	9
258	5	img1487400135129.jpg	10
259	5	img1487400135134.jpg	11
260	5	img1487400135138.jpg	17
261	5	img1487400135159.jpg	18
262	5	img1487400135183.jpg	19

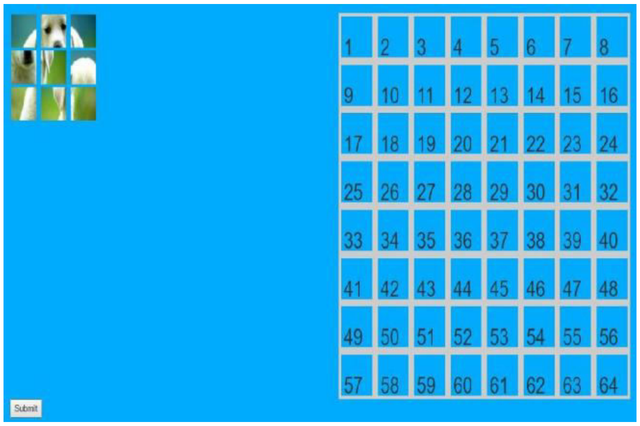
Fig. 6. Snapshot of database for 3x3 image segmentation

2.2 Login Phase

During login, when the user wishes to access the system the image segments will be presented in a shuffled manner as shown in fig. 7, if the user has enabled shuffling during registration. Otherwise, segments are displayed without shuffling as shown in fig. 8. The shuffling is done using Collections.shuffle function in java.util package, which basically uses the Fisher-Yates Shuffle [2] algorithm explained as follows:

1. Store the segments from 1 through N as numbers from 1 to N where N=mxn and m and n are number of rows and columns respectively.
2. Pick any random number k between one and the number of unstruck numbers remaining (inclusive).
3. 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.
4. Repeat from step 2 until all the numbers have been struck out.
5. The sequence of numbers written down in step 3 is now a random permutation of the original numbers.

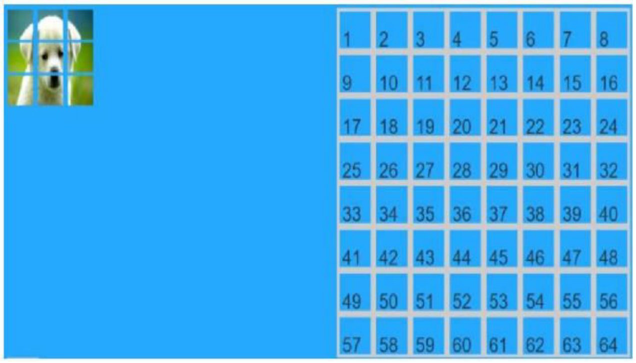
6. Since each of these numbers represent each image segment, the segments are also jumbled accordingly. [2]



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. 7. Shuffled Image

Image chosen by the user during registration phase is segmented,shuffled and presented to user during login phase as the user choses to shuffle image during registration phase.



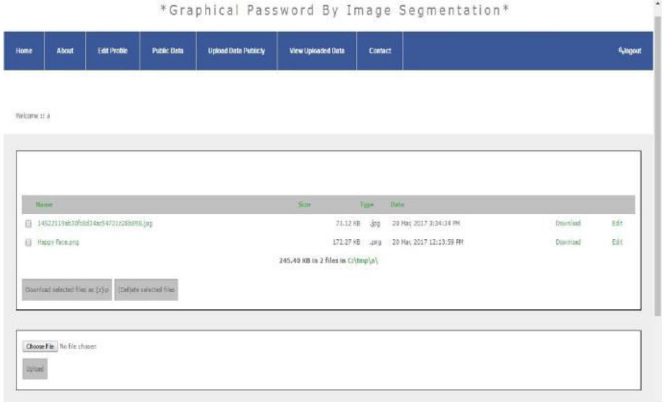
1	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32
33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56
57	58	59	60	61	62	63	64

Fig. 8. Unshuffled Image

Image chosen by the user during registration phase is segmented,unshuffled and presented to user during login phase as the user choses to unshuffle image during registration phase.

To be considered as authentic, the user has to drag the segments onto the empty grid of size 8x8 in the correct sequence and at the correct position. [1]

2.3 Learning Management System



Graphical Password By Image Segmentation

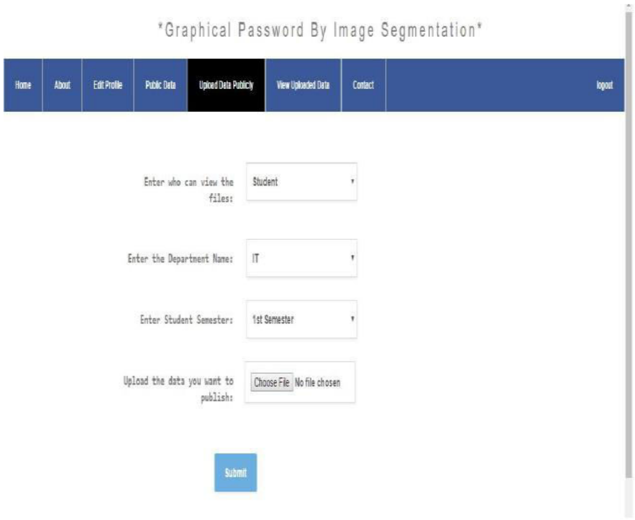
Welcome :: a

	Name	Size	Type	Date		
□	14522119ab39fe8d34ac54731c28b898.jpg	73.12 KB	.jpg	20 Mar, 2017 3:34:34 PM	Download	Edit
□	Happy face.png	172.27 KB	.png	20 Mar, 2017 12:13:59 PM	Download	Edit

245.40 KB in 2 files in C:\tmp\a\

Fig. 9. Learning Management System User Homepage

After the user is authenticated he will be directed to the Learning Management System. This is an application is developed for the department of a college, wherein data can be shared between the students and the faculty, faculty and the hod and hod and students. It allows the user to grant access to the other users to view and download the data/file.



Graphical Password By Image Segmentation

Enter who can view the files: Student

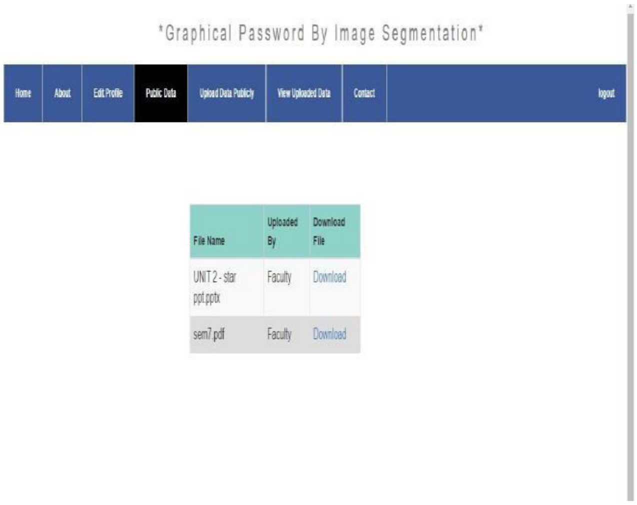
Enter the Department Name: IT

Enter Student Semester: 1st Semester

Upload the data you want to publish: Choose File No file chosen

Fig. 10. User giving access to other users to view and download data.

User can choose between student/faculty/hod of particular department i.e, IT/COMPS/EXTC/MECH/ELEC and also the semester to which he wants to grant access to download and view data as shown in fig 10.



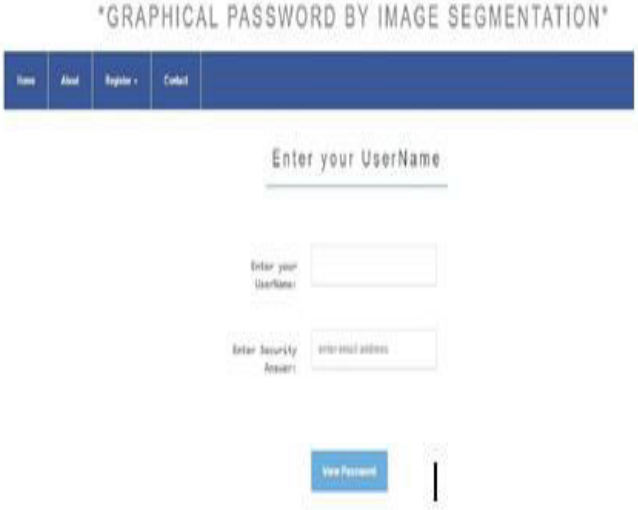
File Name	Uploaded By	Download File
UNIT 2 - star ppt.pptx	Faculty	Download
sem7.pdf	Faculty	Download

Fig. 11. Public data that this user is given access to.

Other users can provide access to this user to view and download data and the files which the user is given access can be viewed and downloaded under ‘public data’ as shown in fig 11.

2.4 Forgot Password

If the user forgets his password then can click forget password. After clicking forget password user will be redirected to a page wherein the username and a security question will be asked. If the username and security question is correct the the password will be given to him.



Enter your UserName:

Enter Security Answer: enter email address

Fig. 12. Forget password

user is asked to provide correct username and email id as shown in fig 12.. If username and email id matches with that of mentioned by the user during registration phase then user will be directed to the link that will provide user with the correct password.

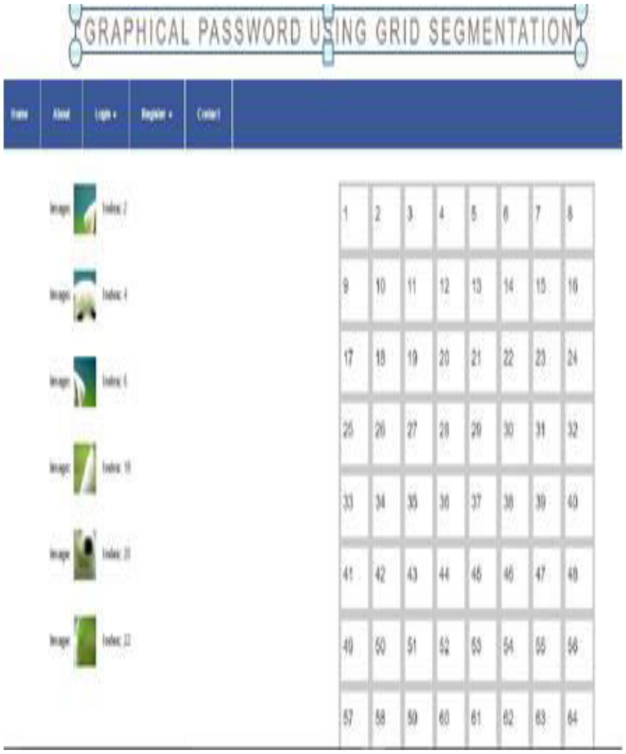


Image: Index: 2

Image: Index: 4

Image: Index: 6

Image: Index: 18

Image: Index: 31

Image: Index: 22

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. 13. Password with proper index and sequence retrieved

After the user provides correct username and email id then the password with correct sequence and index as set by the user during registration phase is provided to user as shown in fig 13.

3. Conclusion

Graphical passwords offers better security than text-based passwords because many people, in an attempt to memorize text-based passwords, use plain words rather than the recommended jumble of characters. A dictionary search can often hit on a password and allow a hacker to gain entry into a system in seconds. But in a series of selectable images, possible combinations that could form the graphical password are so many that it would take millions of years to break into the system. [3]

This study concludes that more the number of rows and columns, more will be the number of segments of the image and thus more will be the length and security of the password. Shuffling the segments of the image can prevent shoulder surfing attack, as each time the shuffled output will be different, thus the user will pick the same segment from different positions each time while logging into the system.

References

[1] Rashika Koul, Tanya Kumar, Radhika Malpani, Ashwini Dhongade, Rupali Deshmukh, “GPSI: Graphical Password by Segmentation of Image” International Journal of Research and Scientific Innovation (IJRSI) | Volume III, Issue XI, November 2016 | ISSN 2321-2705

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

[3] Margaret Rouse, “ graphical password or graphical user authentication (GUA)”. <http://searchsecurity.techtarget.com/definition/graphical-password>

[4] 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

[5] Haiyu Song, Xiongfei Li , Pengjie Wang, Jingrun Chen, “ Block-Based Normalized-Cut Algorithm for Image Segmentation”, Online ISBN 978-3-642-05173-9

[6] 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/ >

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

[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] 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

[10] 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

[11] 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.