Digital Innovations
& Contemporary Research in SCIENCE,
ENGINEERING & TECHNOLOGY

Vol. 7. No. 2, June, 2019

Article Progress Time Stamps

Article Type: Research Article
Manuscript Received: 8th April, 2019
Review Type: Blind
Final Acceptance:: 24th May, 2019
Article DOI: dx.doi.org/10.22624/AIMS/DIGITAL/V7N2P9

Article Citation Format
Adebimpe, L.A. (2019):
DPass: A Method for Preventing Shoulder-Surfing Attack
Journal of Digital Innovations & Contemp Res. In Sc., Eng &
Tech. Vol. 7, No. 2. Pp 105--114

DPass: A Method for Preventing Shoulder-Surfing Attack

Adebimpe, Lateef Adekunle
Department of Computer Science
Emmanuel Alayande College of Education
Oyo, Oyo State, Nigeria.
E-mail: dradebimpela@yahoo.com

ABSTRACT

Authentication is one of the methods used to grant access to legitimate users. Authentication is the most important component of a secure system. Today, graphical password is a common authentication method. However, graphical password is vulnerable to shoulder-surfing attack. Shoulder-surfing is a threat in which attackers obtain useful information to login as a legitimate user. Many shoulder-surfing resistance methods have been proposed. After analyzing some of the existing methods, the outcome indicated that they are susceptible to shoulder-surfing attacks. Though some of the systems can prevent direct observation, these systems become vulnerable when attackers observe multiple login sessions especially via video-recording. The aim of this research is to propose a new recognition-based graphical password method that can prevent shoulder-surfing attacks. In the proposed method a pass-image is determined by clicking a decoy image rather than registered image. This will deny shoulder-surfers opportunity of capturing registered image. Therefore, the proposed method can prevent shoulder-surfing attack provided the enrolment procedure is carried out in a secure manner.

Keywords Graphical Password, Shoulder-Surfing, Image, Authentication, Location

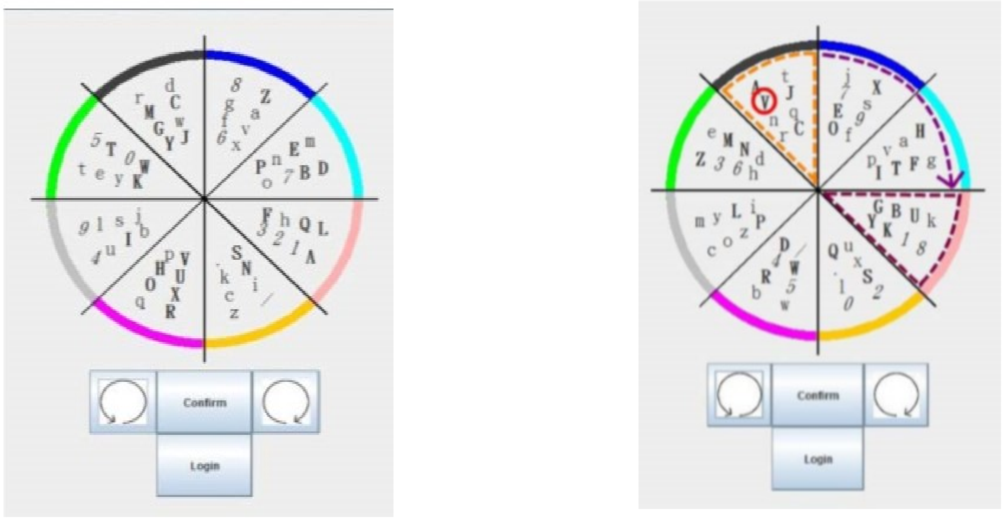
1. INTRODUCTION

Today, authentication is used for different purposes by many organizations [1]. Graphical password systems are commonly being used for user authentication. The convenience of graphical password has motivated plenty of studies. However, graphical password systems do encounter threats especially shoulder-surfing attack [2-7]. Many systems have been proposed to prevent shoulder-surfing attacks but the challenge of shoulder-surfing attacks still persist. The existing systems are susceptible to shoulder-surfing attacks [2-7]. Though some of the systems can prevent direct observation, these systems become vulnerable when attackers observe multiple login sessions especially via video-recording.

Hence, the need to carry out this research work. In this research, a new recognition-based graphical password method is proposed to prevent shoulder-surfing attacks.

2. RELATED WORK

Manjunath et al proposed a graphical password method in 2014 [8]. During registration, a user is required to register a minimum of eight characters and maximum of fifteen characters from 64 characters comprises of 26 upper case letters, 26 lower case letters, 10 decimal digits, "." And "/" symbols. After that, the user is required to register one color from the eight color displayed. The user is also required to register a valid e-mail. During the authentication procedure, a circle comprises of eight equally sized sectors is generated. Each of the sector's arc is filled with unique color. The 64 characters are randomly distributed among these sectors. Thus, each sector contains 8 characters. The user is required to rotate the sector so that the sector that contains the first registered character aligned with the registered color. After that, the user is required to click "confirm" button. This process is repeated for all the registered characters. To login, the user is required to click the "login" button. If the login failed after three trials, the account is disabled and a link for reactivating the account is sent to the registered e-mail. According to the author, the method cannot prevent shoulder-surfing attack after multiple observations of more than two recorded video.



(a) (b)

Figure 1: User interface of Manjunath et al (adopted from [8]). (a) Before Rotation (b) After Rotation

Pooja et al. proposed a method that allows both registered and decoy images to be used as the challenge set images in 2015 [9]. During the registration procedure, a user is required to register user-id and password. After that, the user is required to register several images within the 4x4 grid cells consisting of 16 images. The user is required to remember the sequence of the registered images. During authentication, the user is required to login with the registered user-id and password. After that, the user obtains pass-image by identifying and clicking the registered images in the same sequence in which it was registered. According to the author, this method only minimized shoulder-surfing attack. However, the method is vulnerable to all forms of shoulder-surfing attacks - direct observation, multiple observations and video-recorded vulnerable to shoulder-surfing attack because the images clicked by the user are the registered images. Attackers can easily capture registered images and login as legitimate users.

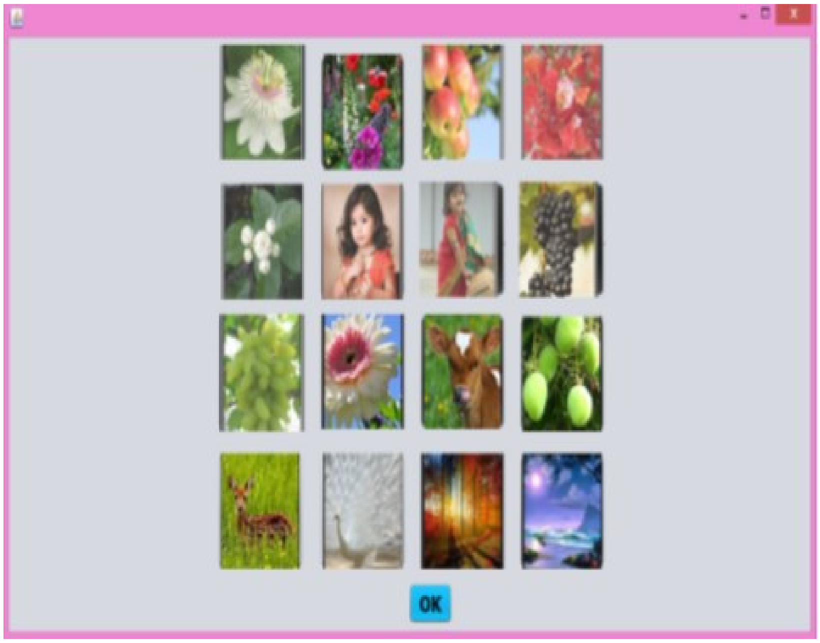


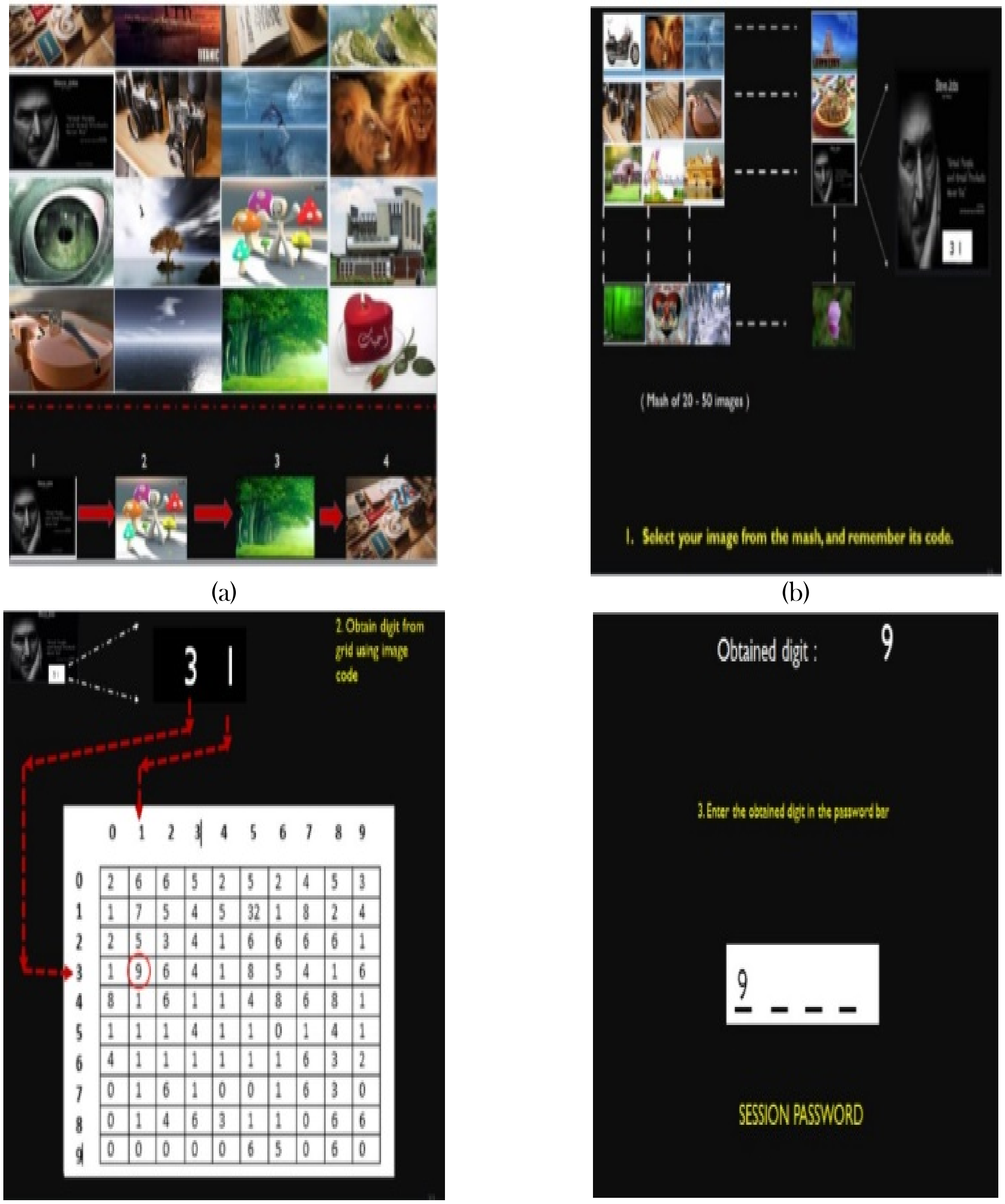
Figure 2: User interface of Pooja et al's system (adopted from [9])

Agrawal et al proposed a graphical authentication method in 2016 [10]. During registration, a user is required to register username and password. After that, the user is required to register four images from sixteen images shown on a 4x4 grid. The user is required to remember the sequence of the registered images. The four registered images would be used to obtain four-character session password. One character each for each of the registered images.

To ease the user memorability, a panel is used to display the registered images as they are being selected. During the authentication procedure, two grids of 10x10 are generated – alphanumeric grid and pictorial grid. The alphanumeric grid or the response grid is used to acquire session password. The pictorial grid or the challenge grid is consisted of registered images and decoy images. Each image has a number associated with it.

The user is required to use the challenge grid to obtain number associated with the first registered image. The number is made up of two characters. The first character is used to determine row information and the second character is used to determine column information. After that, the user is required to apply the row and column information to find the session password on the response grid. The intersection character is the first character of the session password.

This process is repeated for all the registered images. After that, the user is required to login with the session password obtained. According to the authors, this system can prevent shoulder-surfing attack. However, the system is vulnerable to shoulder surfing attack because if attackers know the underlying algorithm, they can easily trace the session password entered and obtain the information about the registered images via multiple shoulder-surfer sessions.



(a)

1. Select your image from the mash, and remember its code.

(b)

2 Obtain digit from grid using image code

	0	1	2	3	4	5	6	7	8	9
0	2	6	6	5	2	5	2	4	5	3
1	1	7	5	4	5	32	1	8	2	4
2	2	5	3	4	1	6	6	6	6	1
3	1	9	6	4	1	8	5	4	1	6
4	8	1	6	1	1	4	8	6	8	1
5	1	1	1	4	1	1	0	1	4	1
6	4	1	1	1	1	1	1	6	3	2
7	0	1	6	1	0	0	1	6	3	0
8	0	1	4	6	3	1	1	0	6	6
9	0	0	0	0	0	6	5	0	6	0

(c)

Obtained digit : 9

3.Enter the obtained digit in the password bar

9 _ _ _ _

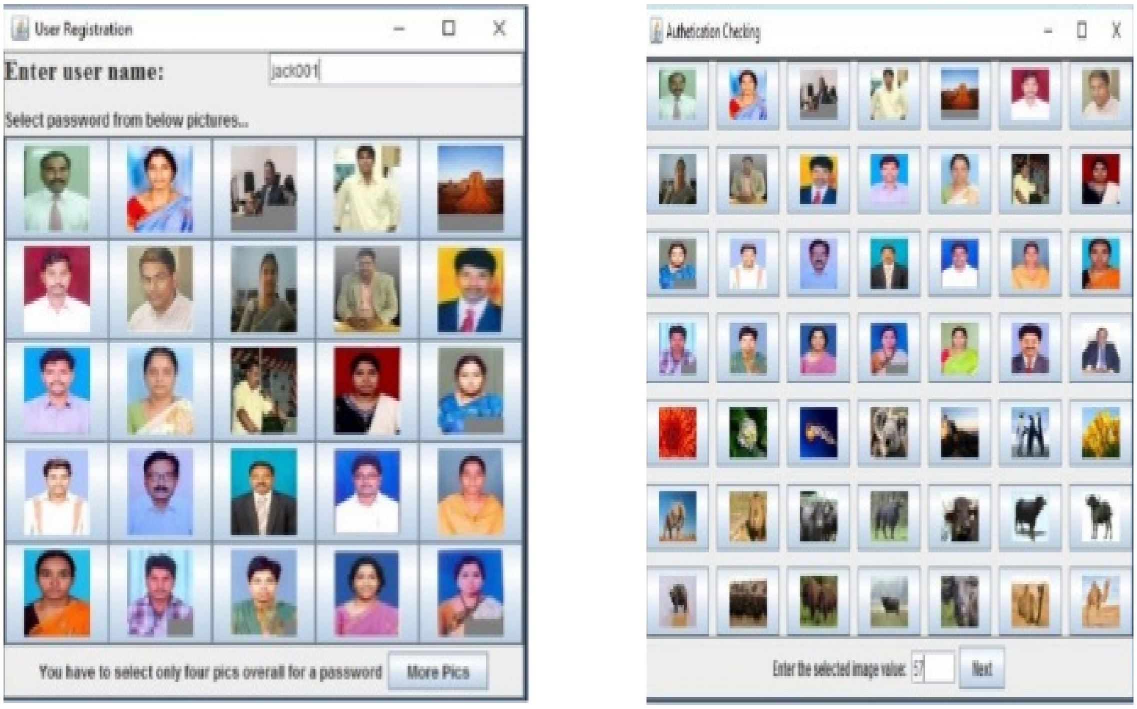
SESSION PASSWORD

(d)

Figure 3: User interface of Agrawal et al's system (adopted from [10]).
(a) Image Registration (b) Pictorial Grid (c) Alphanumeric Grid (d) Session Password

Vijayakumari et al. proposed a graphical authentication method based on Passface Scheme in 2017 [11]. During the registration procedure, a user is required to register username. After that, the user is required to register four images from the images shown on a 5x5 grid. The user can request new images from the server. During authentication, the user is required to enter username and indicate the size of the challenge grid to be displayed. After that, a challenge grid consisted of registered images and decoy images is generated.

The user is required to obtain pass-image by clicking directly on the first registered image or by entering the row and column information of the first registered image. This is repeated for all the registered images. According to the authors, this scheme can prevent shoulder-surfing. However, since the registered images and pass-images are fixed, an attacker can shoulder-surf information to login after multiple observations.



Enter user name: jack001

Select password from below pictures...

You have to select only four pics overall for a password

Enter the selected image value: 57

(a)

(b)

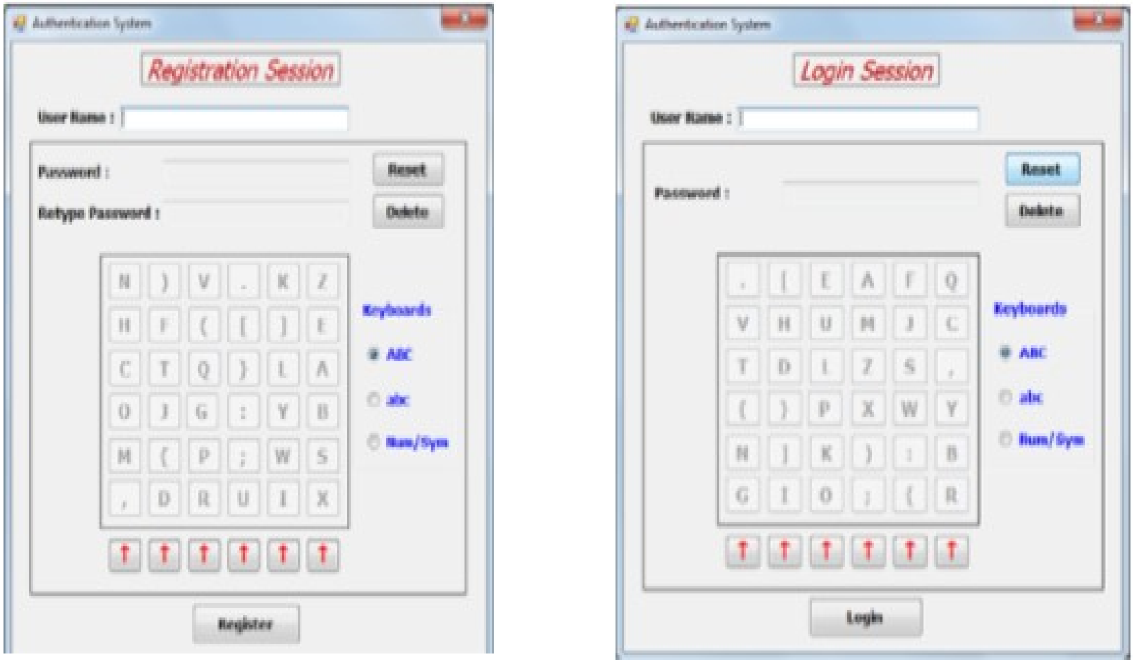
Figure 4: User interface of Vijayakumari et al (adopted from [11]). (a) Registration (b) Authentication

Al-Husainy & Uliyan proposed an authentication method that used transpose operation in 2018 [12]. During registration, a user is required to register username and password. After that, the user is required to register a secret password using the proposed method. During authentication, the user is required to enter the secret password using the proposed method.

In the proposed method, alphanumeric characters are distributed on 3 keyboards that consist of 6x6 grids at each keyboards. The user is required to switch among these keyboards to select desire character. Below the keyboard are six arrows that can be used to select a particular character. To enter a particular character, the user is required to click the arrow button that points to column containing that character.

The first click indicates the column information of the character. The system automatically performs a matrix transpose operation by flipping the keyboard over its diagonal (each row becomes column and each column becomes row). The user is required to click the arrow button that points to the desire character. The second click indicates the row information of the character. This process is repeated to enter all the characters in the secret password. According to the author, this system is easy to use.

However, the system is vulnerable to shoulder surfing attack when multiple sessions are video-recorded. Attackers can easily shoulder-surf the row and column information with the clicked arrows and obtain the characters that form the secret password.



N	)	V	.	K	Z
H	F	(	[	]	E
C	T	Q	}	L	A
O	J	G	:	Y	B
M	{	P	;	W	S
,	D	R	U	I	X

(a)

.	[	E	A	F	Q
V	H	U	M	J	C
T	D	L	Z	S	,
(	)	P	X	W	Y
N	]	K	}	:	B
G	I	O	;	{	R

(b)

Figure 5: User interface of Al-Husainy & Uliyan (adopted from [12]). (a) Registration (b) Authentication

3. PROPOSED SYSTEM

The proposed system is divided into registration process and authentication process

3.1 Registration Process

During the registration process, a 4x4 grid is displayed. The user is required to register one image from the given grid. After that the user is required to select a four-digit figure. The user is required to reconfirm the selected figure. Each of the digit in the registered figure determines the number of mental movement(s) the user intend to make to the right, left, up and down from the registered image to login.

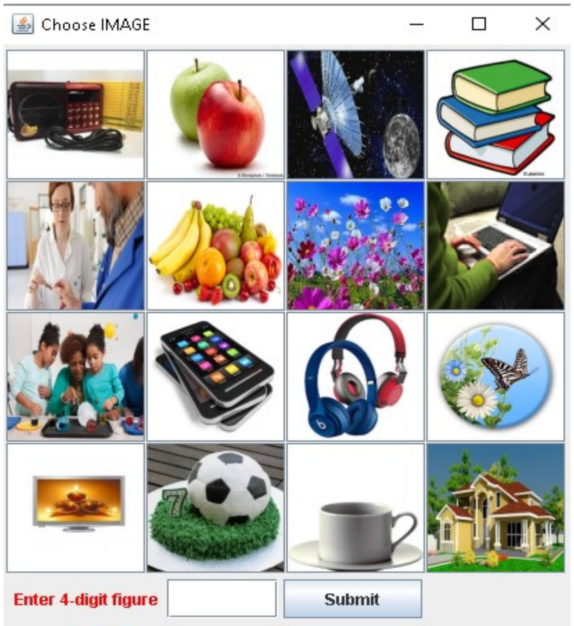


Figure 6: Registration interface

3.2 Authentication Process

During the authentication process, a challenge set that consists of 4x4 grid is shown. Uniform randomization algorithm is used to select and place the images in the 4x4 grid cell. To obtain the pass-image, the user is required to mentally move from the current position of the registered image based on the value of digits in the registered figure. The first digit determines the number of movement to the right from the registered image. The second digit determines the number of movement to the left from the registered image. The third digit determines the number of movement upward from the registered image. The fourth digit determines the number of movement downward from the registered image. The user is required to identify pass-image by clicking on the last image on which the mental movements terminates. The believe is that clicking on a decoy image rather than the registered image will hinder shoulder-surfing attackers from identifying registered image. To login, the user is required to click the correct pass-image in three consecutive rounds. After each attempt, the images shown in the challenge set are reshuffled using randomization algorithm. A new challenge set will be displayed automatically regardless of whether the user clicks the pass-image correctly or wrongly.

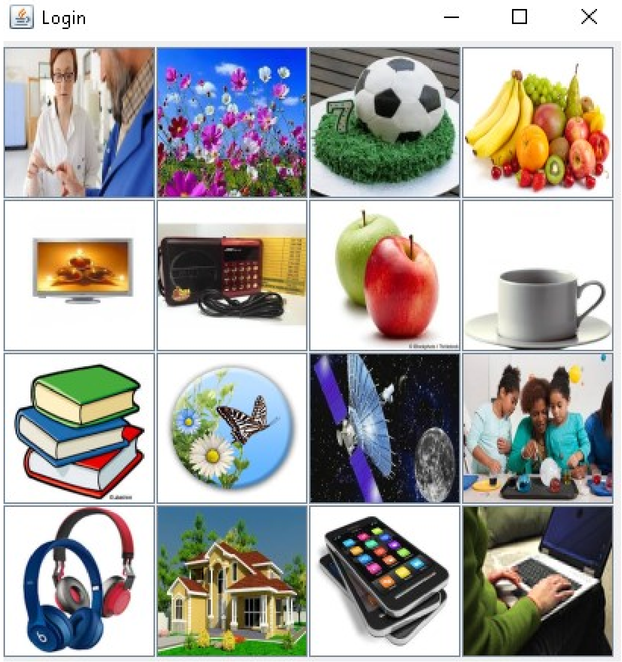


Figure 7: DPass challenge set

4. EVALUATION

4.1 Participants

To evaluate the feasibility of the proposed method in terms of preventing shoulder-surfing attacks, 123 participants were invited to participate in the user study. 76 participants were male and 47 were female.

4.2 Procedure

The participants were given tutorial to gain knowledge of the workability of proposed system. The participants were allowed to record the authentication process using their mobile phones. After that, the participants were given unlimited trials to perform the attack.

4.3 Results

Shoulder-Surfing Attack:

The results indicated that none of the participants was able to login. Hence, they were not successful in performing shoulder-surfing attack.

4.4 Usability

The feedback from the questionnaire given to the participants indicated that 97.6% of the respondents strongly agreed that the proposed method is easy to use. The remaining 2.4% agreed that the proposed system is easy to use. Table 1 shows the statistics of the successful login time. As shown in the table, the user study result indicated that the minimum time taken by the participants for a successful login is 5.0 seconds. The maximum time taken by the participants for a successful login is 18.0 seconds. The mean time indicated an average login time of 8.2 seconds.

Table 1: Statistics of successful login time

item	time (seconds)
Minimum	5.0
Maximum	18.0
Mean	8.2

Memorability:
To assess the memorability of the proposed system, experiment was performed on how well the users can remember their password after a period of time. In the experiment, the participants were instructed to register an account and then come back after three weeks to login into the registered accounts. The result after three weeks indicated that all the participants were able to login successfully into their account.

5. DISCUSSION

Many shoulder-surfing resistance methods have been proposed. This research began with the reviewing of some of these methods. The outcome of the review indicated that it is important to explore more methods to overcome the challenge of shoulder-surfing attack. It is against this backdrop that a new method was proposed in this research to prevent shoulder-surfing attack. The result of the user study conducted to evaluate the proposed method in terms of preventing shoulder-surfing attack indicated that none of the participants was able to login successfully. Therefore, the proposed method is able to prevent shoulder-surfing attack.

7. Future Work

This research only focus on preventing shoulder-surfing attacks, other security threats are not covered in this research work. Therefore, the future work should consider other types of graphical password threats.

REFERENCES

[1] Sun, H.M., Chen, S.T., Yeh, J.H., & Cheng, C.Y. (2018). A shoulder surfing resistant graphical authentication system. IEEE Transactions on Dependable and Secure Computing. 15(2), 180-193.

[2] Katsini, C., Raptis, G.E., Fidas, C., & Avouris, N. (2018, May). Does image grid visualization affect password strength and creation time in graphical authentication?. In Proceedings of the 2018 International Conference on Advanced Visual Interfaces 33-37.

[3] Por, L.Y., Ku, C.S., Islam, A., & Ang, T.F. (2017). Graphical password: prevent shoulder-surfing attack using digraph substitution rules. Frontiers of Computer Science. 11(6), 1098-1108.

[4] Mackie, I., & Yıldırım, M. (2018, July). A novel hybrid password authentication scheme based on text and image. In *IFIP Annual Conference on Data and Applications Security and Privacy* (pp. 182-197). Springer, Cham.

[5] Siddiqui, M. U., Umar, M. S., & Siddiqui, M. (2018, December). A Novel Shoulder-Surfing Resistant Graphical Authentication Scheme. In *2018 4th International Conference on Computing Communication and Automation (ICCCA)* (pp. 1-5). IEEE.

[6] Assal, H., Imran, A., & Chiasson, S. (2018). An exploration of graphical password authentication for children. International Journal of Child-Computer Interaction.18, 37-46.

[7] Othman, N. A. A., Rahman, M. A. A., Sani, A. S. A., & Ali, F. H. M. (2018, December). Directional Based Graphical Authentication Method with Shoulder Surfing Resistant. In *2018 IEEE Conference on Systems, Process and Control (ICSPC)* (pp. 198-202). IEEE.

[8] Manjunath, G., Satheesh, K., Saranyadevi, C., & Nithya, M. (2014). Text-based shoulder surfing resistant graphical password scheme. *International Journal of Computer Science and Information Technologies*, *5*(2), 2277-2280.

[9] Pooja, K. S., Prajna, V. D., Prathvi, Ashwini, N. (2015). Shoulder-surfing resistance using graphical password authentication in ATM systems. International Journal of Information Technology & Management Information System (IJITMIS), 6(1), pp. 1-10.

[10] Agrawal, S., Ansari, A. Z., Umar, M. S. (2016). Multimedia graphical grid based text password authentication: For advanced users. Thirteenth International Conference on Wireless and Optical Communications Networks (WOCN), pp. 1-5.

[11] Vijayakumari, R., Kancherla, G. R., & Bobba, B. R. (2017). Shoulder-Surfing Resistant Graphical Password System for Cloud. *International Journal of Applied Engineering Research*, 12(16), 6091-6096.

[12] Al-Husainy, M.A.F., & Uliyan, D.M. (2018). A Smooth Textual Password Authentication Scheme Against Shoulder Surfing Attack. *Journal of Theoretical & Applied Information Technology*, 96(9)