symmetry

MDPI

Article

LocPass: A Graphical Password Method to Prevent Shoulder-Surfing

Lip Yee Por [1,*], Lateef Adekunle Adebimpe [1,2], Mohd Yamani Idna Idris [1], Chee Siong Khaw [1] and Chin Soon Ku [3]

1 Department of Computer System and Technology, Faculty of Computer Science & Information Technology, University of Malaya, Kuala Lumpur 50603, Malaysia; dradebimpela@siswa.um.edu.my (L.A.A.); yamani@um.edu.my (M.Y.I.I.); wma180017@siswa.um.edu.my (C.S.K.)
2 Emmanuel Alayande College of Education, Oyo 211225, Nigeria
3 Department of Computer Science, Universiti Tunku Abdul Rahman, Kampar 31900, Malaysia; kucs@utar.edu.my
* Correspondence: porlip@um.edu.my

Received: 3 September 2019; Accepted: 29 September 2019; Published: 8 October 2019

Abstract: Graphical passwords are a method of authentication in computer security. Computer security is one of the disciplines of computer science. Shoulder-surfing attacks are a well-known threat to graphical passwords, although is getting commonly used especially in granting access for a secure system. Shoulder-surfing occurs when attackers skillfully capture important data/activities, such as login passwords, via direct observation or video recording methods. Many methods have been proposed to overcome the problem of shoulder-surfing attacks. After we reviewed some related works, we found out that most of the existing methods are still vulnerable to multiple observations and video-recorded shoulder-surfing attacks. Thus, we propose a new method to combat this problem. In our proposed method, we make used of two concepts to combat shoulder-surfing attacks. In the first concept, we used registered locations (something that only the users know) and 5 image directions (something that the users can see) to determine a pass-location (new knowledge). Secondly, the images used in our proposed method have higher chances to offset each other. The idea of offset could increase the password spaces of our proposed method if an attacker intended to guess the registered location used. By combining these two concepts, the pass-location produced by our proposed method in each challenge set could be varied. Therefore, it is impossible for the attackers to shoulder-surf any useful information such as the images/locations clicked by the user in each challenge set. A user study was conducted to evaluate the capabilities of the proposed method to prevent shoulder-surfing attacks. The shoulder-surfing testing results indicated that none of the participants were able to login, although they knew the underlying algorithm and they have been given sufficient time to perform a shoulder-surfing attack. Therefore, the proposed method has proven it can prevent shoulder-surfing attacks, provided the enrolment procedure is carried out in a secure manner.

Keywords: graphical password; shoulder-surfing; pass-location; authentication; cardinal directions

1. Introduction

In recent years, authentication has become very important. Authentication is used to secure systems so that only legitimate users can access them. Authentication can be categorised into three categories: token-based, biometric-based and knowledge-based [1]. Token-based authentication relies on what the users possess (e.g., ID card) to perform authentication, biometric-based authentication relies on users' attributes (e.g., thumbprint) to perform authentication, while knowledge-based authentication relies on what the users know (e.g., alphanumeric password) to perform authentication [1–12].

Alphanumeric passwords are the foremost and primary form of user authentication [13]. This form is easy to implement and has been used widely from the past up to today [14]. A secure password must be random and easy to remember [1]. However, a secure password that is made up of a random string (e.g., upper and lower cases, used special characters, must have at least eight characters long) is difficult for users to memorise. Therefore, the graphical password was introduced as an alternative to help users to memorise their password better [15].

Graphical passwords are a method of authentication in computer security. Computer security is one of the disciplines of computer science. Graphical passwords leverage human memory, since the human brain has significant memory capabilities to recognise and recall visual images [3,15]. The belief is that with a graphical password, a user can register random and secure password and still have no difficulty in remembering the registered password [3].

Fundamentally, graphical passwords can be divided into three forms, namely, recall, cued-recall and recognition-based systems [3]. Recall systems entail the users reproducing the previously drawn password object (e.g., a picture, icon, image, or shape). In cued-recall systems, users are presented with images and are required to click on previously registered points. In recognition-based systems, to login users need to recognise a set of registered objects and identify certain objects or pass-objects from among other decoy objects displayed [1–12].

In this study, we focus only on the recognition-based systems because these systems are less complex, and they have been implemented in many security systems, such as online banking systems [2]. The following is a review of selected related works on recognition-based systems.

2. Related Work

WYSWYE ("Where You See is What You Enter") was proposed by Khot et al. [5] (see Figure 1). There are two main procedures in this system—registration and authentication. During registration, a user is required to register four images from the 28 images shown. During authentication, a random image grid and an empty grid are generated and placed side by side on a login screen. The random image grid or the challenge grid consists of password images and decoy images. The empty grid or the response grid is used to acquire input from users. Users are required to use the challenge grid to find the required positions. After that, the users are required to apply the identified positions on the response grid.

According to [5], WYSWYE is able to prevent shoulder-surfing attack because attackers who are peeping over the shoulder or monitoring with hidden cameras/screen scrapper programs could only see the random positions clicked in the challenge set. However, this method has a weakness whereby each of the boxes in the respond grid is associated with 4 boxes at the challenge grid. For example in Figure 1d, box No. 1 in the respond grid is associated with A, B, F and G boxes in the challenge grid; box No. 2 is associated B, C, G and H boxes; box No. 3 is associated with C, D, H and I boxes; box No. 4 is associated with D, E, I and J boxes; box No. 5 is associated with F, G, K and L boxes; box No. 6 is associated with G, H, L and M boxes; box No. 7 is associated with H, I, M and N boxes; box No. 8 is associated with I, J, N and O boxes; box No. 9 is associated with K, L, P and Q boxes; box No. 10 is associated with L, M, Q and R boxes; box No. 11 is associated with M, N, R and S boxes; box No. 12 is associated with N, O, S and T boxes; box No. 13 is associated with P, Q, U and V boxes; box No. 14 is associated with Q, R, V and W boxes; box No. 15 is associated with R, S, W and X boxes; box No. 16 is associated with S, T, X and Y boxes. Therefore, attackers could observe the clicked images and filter out the decoy images in each challenge set. After multiple observations, the attackers might be able to work out the registered images. In other words, this scheme is still vulnerable to shoulder-surfing attack as the attackers can login as legitimate users by filtering out the decoy images after multiple observations [16].

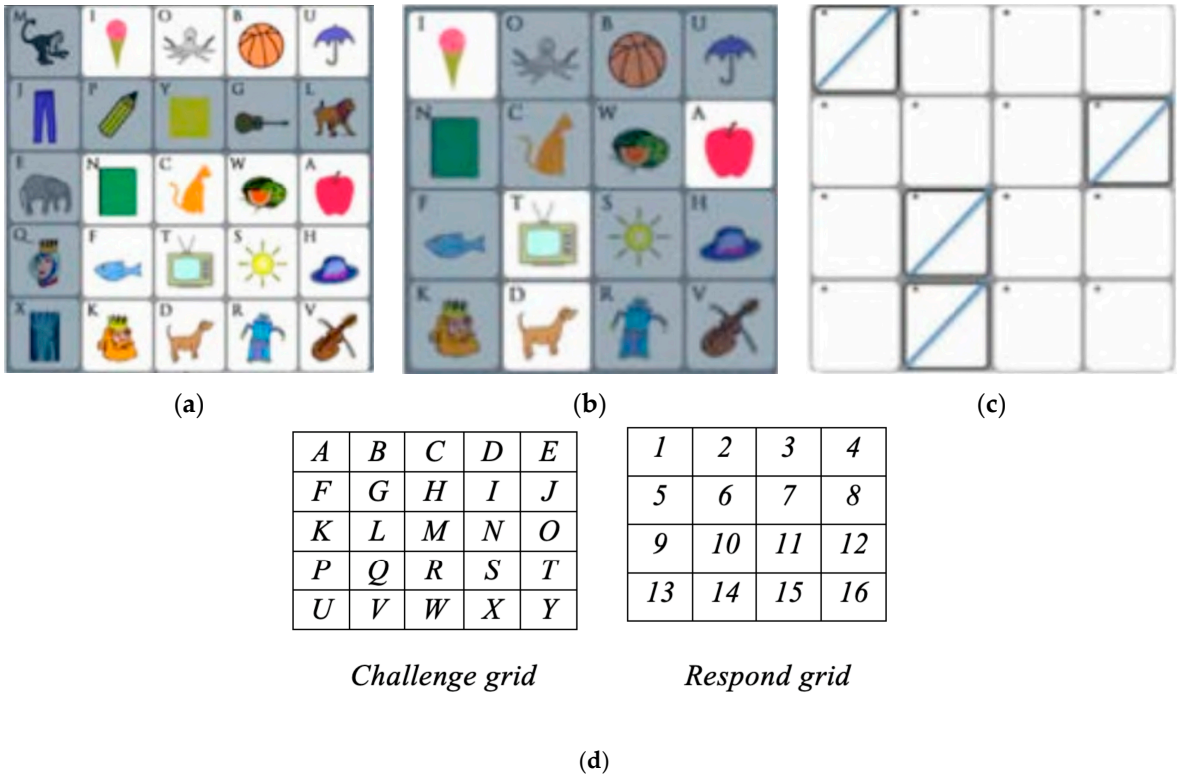


Figure 1. User interface of "Where You See is What You Enter" (WYSWYE; adopted from [5]). (**a**) Users need to mentally eliminate the row and column from the challenge grid that does not contain the password images (apple, dog, ice cream and television in this case); (**b**) Users need to identify the position of the password images in the reduced challenge grid; (**c**) Users need to click the position of the password images in the respond grid; (**d**) Example of notations used in the challenge grid and the respond grid to illustrate the weaknesses of WYSWYE.

Ho et al. proposed a method that allows both registered and decoy images to be used as the challenge set's input in 2014 [17] (see Figure 2). During the registration procedure, the user is required to register several images. The user is required to remember the sequence of the registered images. During the authentication procedure, a pass-image is obtained using the starting image, the cued image, and the proposed algorithm. Initially, the first registered image and second registered image are used as the starting image and the cued image respectively. After that, the pass-image is obtained using the proposed method. In the proposed method, the user is required to determine whether the cued image is on the imaginary half-line. If the cued image is not on the imaginary half-line, the amount of offset is fixed to one. Therefore, the immediate image after the starting image along the imaginary half-line is the pass-image. If the cued image is on the imaginary half-line, the user is required to check if the cued image is the last image on the imaginary half-line. If the cued image is not the last image on the imaginary half-line, the maximum offset is applied. Therefore, the last image along the imaginary half-line is the pass-image. If the cued image is the last image on the imaginary half-line, the amount of offset is reduced by one. Therefore, the image before the last image along the imaginary half-line is the pass-image. To determine the subsequent pass-image, the same method is used just that the current pass-image will be used as the starting image and the next registered image will be used as the cued image. This process is repeated until the final pass-image is obtained. To login, the user is required to click on the final pass-image.

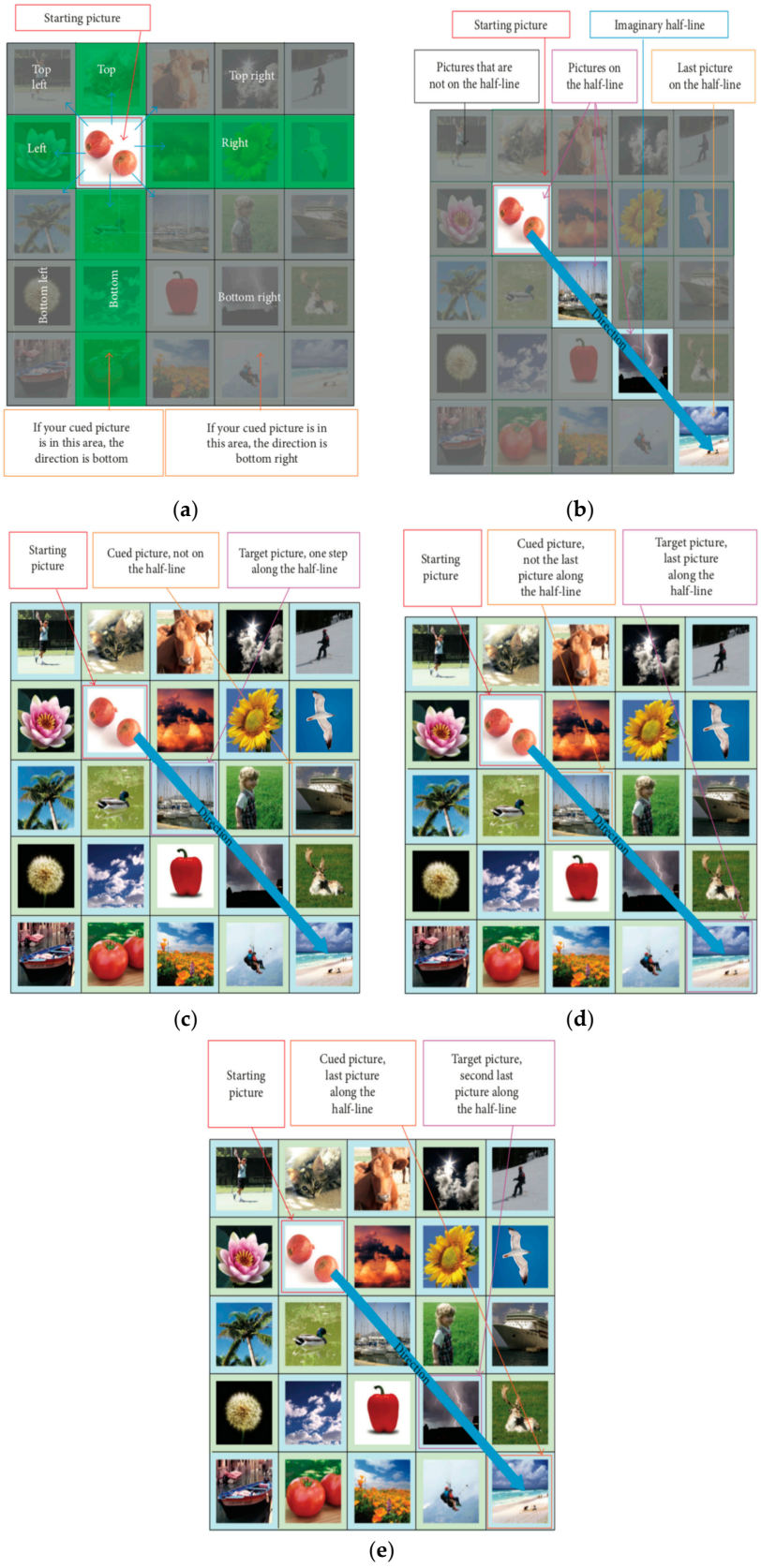


Figure 2. User interface of Ho et al.'s system (adopted from [17]). (**a**) Direction obtained from the cued picture; (**b**) Determine whether a cued picture is on the half-line; (**c**) Cued picture is not on the half-line; (**d**) Cued picture is on the half-line and not the last picture; (**e**) Cued picture is on the half-line and is the last picture.

According to [17], this method can prevent direct observation attacks. However, when multiple sessions are video-recorded the system is vulnerable to reverse engineering attacks [18]. Reverse engineering attacks exploit the fact that the registered images used in a challenge set are constant. Reverse engineering attack can be performed by ruling out some images that could not be the last cued image. After that, an attacker can obtain the remaining registered images by finding out the last starting image or ruling out more images. Therefore, attackers can find out the registered images and login as legitimate users.

Gokhale & Waghmare proposed a graphical password method in 2016 [19] (see Figure 3). During registration, a user is required to register several images from a list of 25 images. The user has to register at least six images, and the number of registered images must be even number. The user is required to remember the sequence of registered images. To make it easier for the user, a panel is used to display the selected registered images. However, these images will disappear after 5 seconds. After that, the user is required to choose the question from the question pool. Each question has a number associated with it. After selecting the question, the user is required to register a location as the answer to the question. The user can upload a background image from local storage or use one of the 25 images given by the system to make it easier for the user to memorise the selected location. The user is required to register three locations and each location must be associated with a question. During the authentication procedure, the user needs to obtain several pass-images using the registered images. To identify the location of the first pass-image, the first registered image is used to determine row information and the second registered image is used to determine column information. The intersection image is the first pass-image. This process is repeated for all of the pairs of registered images. After that, the user is presented with the three sets of registered questions randomly. The user is required to answer the questions by clicking on the locations associated with these questions during registration.

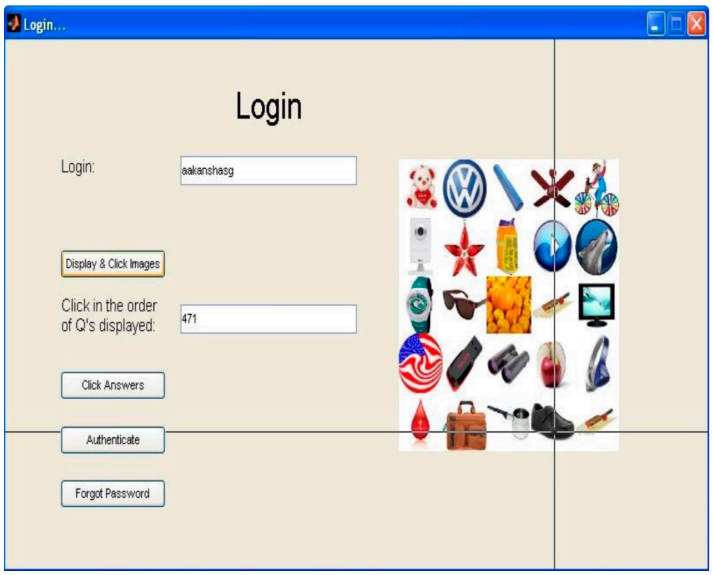


Figure 3. User interface of Gokhale & Waghmare's system (adopted from [19]).

According to [19], this scheme is easy to use and can prevent shoulder-surfing attacks. However, since the locations are fixed, attackers can shoulder-surf the clicked locations easily [16]. Also, the attackers can filter out the registered images after multiple observations. This means that this scheme is still vulnerable to shoulder-surfing attacks.

Por et al. proposed a method that used digraph substitution rules in 2017 [1] (see Figure 4). During the registration procedure, the user is required to register two images. After that, the user is required to register either to use the first pass-image or the second pass-image to login. During authentication, the user is required to select a pass-image to login using digraph substitution rules.

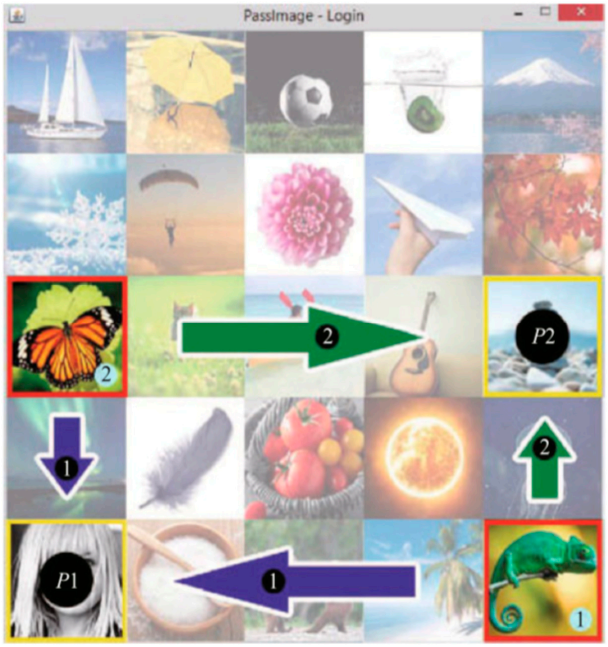


Figure 4. User interface of Por et al.'s system (adopted from [1]).

According to [1], this scheme can prevent shoulder-surfing attacks. However, if attackers know the underlying algorithm, they can easily trace the images clicked and obtain information about the registered images via multiple shoulder-surfer sessions [18].

3D graphical user authentication (GUA) was proposed by [20] (see Figure 5). During registration, the user is required to register five images from 150 images. These images are distributed on 6 polygons that consist of 5 × 5 grids at each polygon. During authentication, the user is required to identify and click the registered images by rotating the polygon.

Figure 5. User interface of 3D graphical user authentication (GUA) system (adopted from [20]).

According to [20], this system is easy to use and can prevent shoulder-surfing attacks. However, from our perspective, this system is vulnerable to shoulder-surfing attacks because the images clicked by the user are the registered images. Therefore, attackers can shoulder-surf the clicked images and use them to login.

Sun et al. proposed PassMatrix that used image discretisation algorithm in 2018 [21] (see Figure 6). During the registration procedure, a user is required to select several images. Each of the selected

images is converted into puzzles using an image discretisation algorithm. After that, the user is required to register one puzzle as the pass-image for each of the selected images. During authentication, a login indicator is generated. The login indicator is comprised of a letter and a number. After that, the random puzzles of the first selected image are shown. Each puzzle is associated with a letter at the horizontal bar and a number at the vertical bar. The user is required to shift the letter to the column on the horizontal bar and the number to the row on the vertical bar for each of the pre-selected puzzles. This process is repeated for all of the selected images.

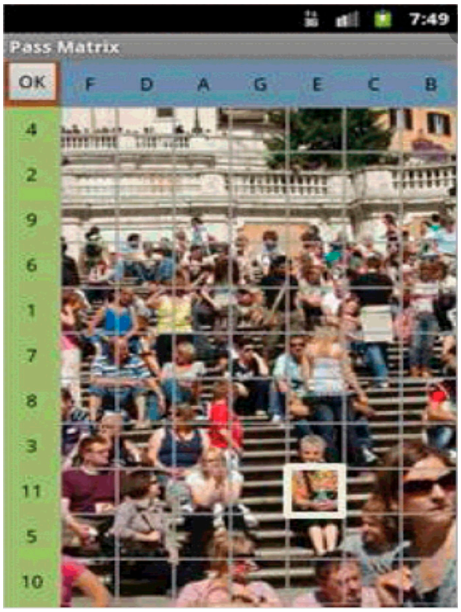


Figure 6. User interface of Sun et al.'s system (adopted from [21]).

According to [21], this system can prevent shoulder-surfing attacks. However, we still believe that this system is vulnerable to shoulder-surfing attacks due to the fact that the selected images and the puzzles are fixed, and attackers can shoulder-surf the pre-selected puzzle in each of the selected images to login after multiple observations.

Our review of the literature shows that there is still room for improvement in preventing shoulder-surfing attacks. Therefore, it is important to explore more methods to overcome this drawback. Hence, this research was carried out to overcome shoulder-surfing attacks, especially those using video-recording methods and multiple methods.

3. Proposed Method

The proposed method consists of two procedures—registration and authentication.

3.1. Registration Procedure

During the registration procedure, the user is required to register a User-ID and re-confirm the User-ID. After the User-ID registration process, the user is given a 5×5 grid (see Figure 7). The user is required to register at least one location from the given grid. The user can register the same location more than one time. The user is allowed to register up to N location, where N is the maximum number of locations that the user can remember. The user is also allowed to register the same location more than one time. After selection, the user is required to reconfirm the selected location. The password registration process is considered complete once the registered locations are saved in the database. Figure 8 shows a sample of registered locations and their order.

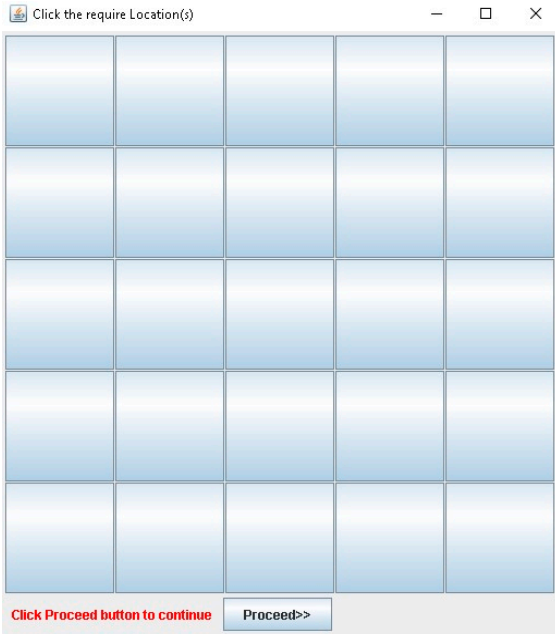


Figure 7. Password registration interface.

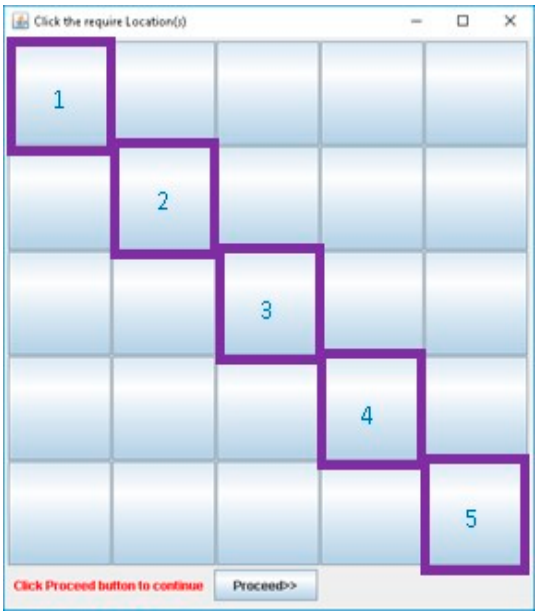


Figure 8. A sample of registered locations.

3.2. Authentication Procedure

During the authentication procedure, the user is required to enter the registered User-ID. After that, a challenge set that consists of a 5 × 5 grid is shown (see Figure 9). Five unique images (solid sphere, up arrow, down arrow, left arrow and right arrow) are used in every challenge set. There are 25 images used in total (1 Solid sphere image and 6 images for each of the different arrow). Uniform randomisation algorithm is used to select the images and the selected images are placed in the 5 × 5 grid cell. The user is required to use the proposed method to get the pass-location to login.

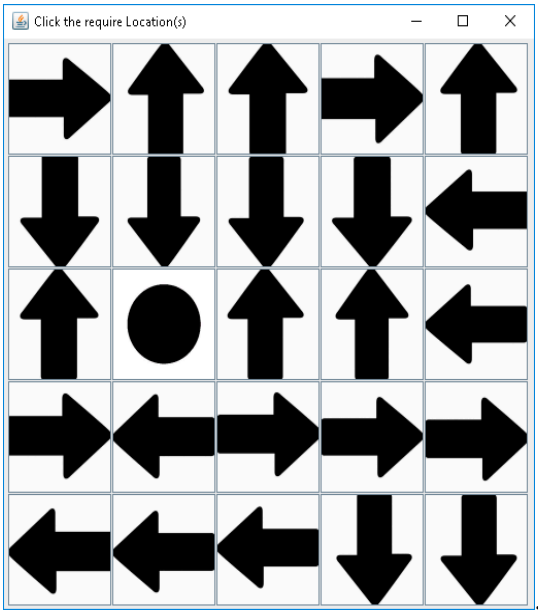


Figure 9. LocPass challenge set.

3.3. Proposed Method

The proposed method uses the cardinal direction concept to prevent shoulder-surfing attack [22]. There are four main cardinal directions in a compass—north, south, east and west. These four directions are also known as the cardinal points. Up arrow, down arrow, right arrow and left arrow are used in the proposed method to replace the north, south, east, and west directions respectively. To obtain the pass-location, firstly, the user is required to find the start image for navigation. The start image is represented by a solid sphere image, as highlighted in Figure 10. After that, the user is required to identify the image shown at each of the registered location. Then, the user is required to use the direction of the image to navigate from the Start image based on the five navigation movements—upward movement, downward movement, backward movement, forward movement and no movement.

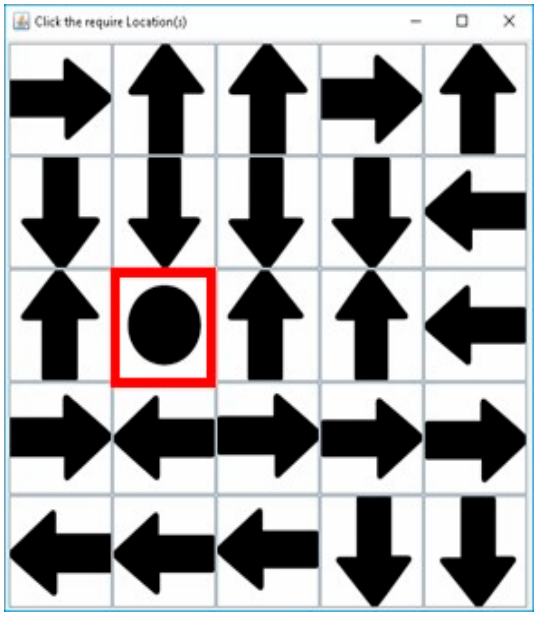
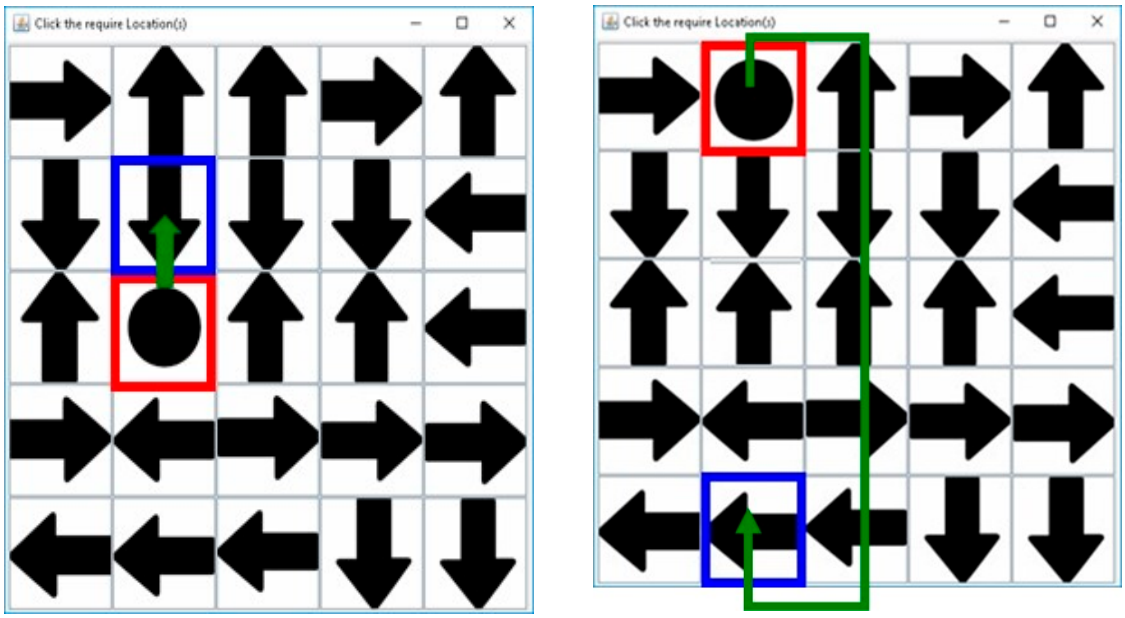


Figure 10. Start object (Solid sphere).

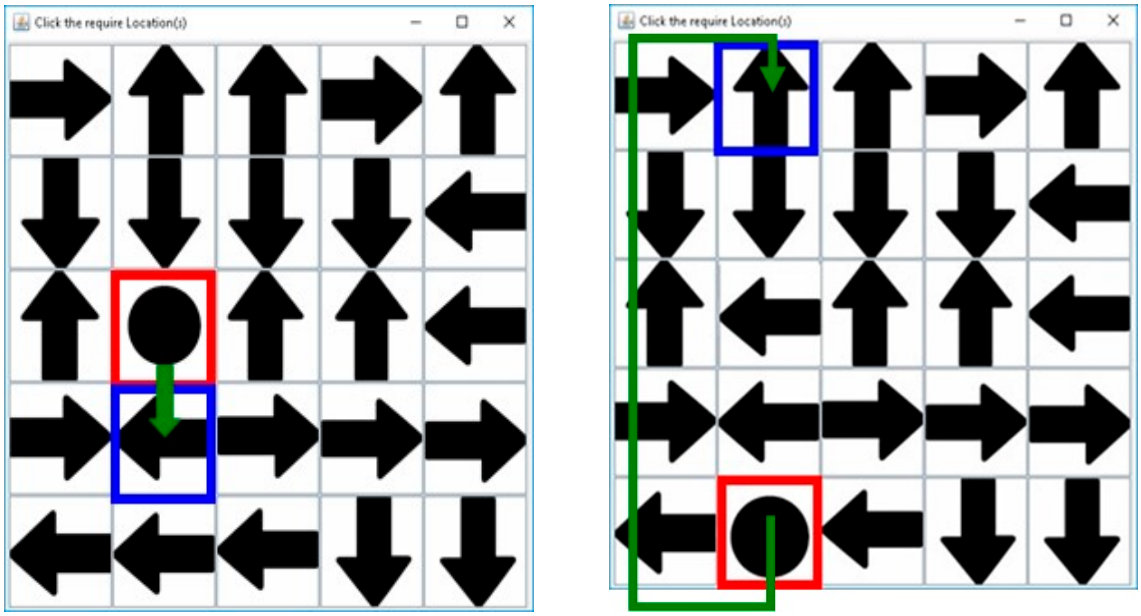
Upward movement: if an up arrow image is shown at the registered location, the pass-location is one location upward from the on-focus location (see Figure 11a). The on-focus location in this scenario is the start image. If the on-focus location is located at the top-edge of the grid cell, the pass-location is wrapped around to the bottom of the column (see Figure 11b). The direction of the movement is shown in green arrows, the on-focus location is highlighted in red boxes and the pass-location is highlighted in blue boxes.



(**a**) (**b**)

Figure 11. Upward Movement. (**a**) Regular case; (**b**) Special case.

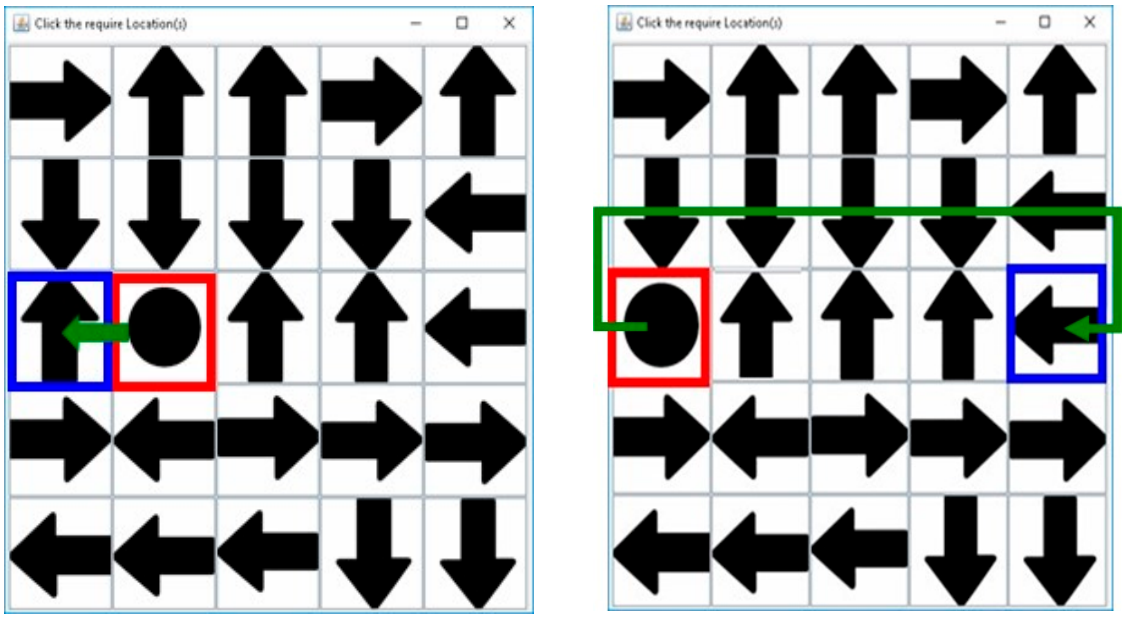
Downward movement: if a down arrow image is shown at the registered location, the pass-location is one location downward from the on-focus location (see Figure 12a). If the on-focus location is located at the bottom-edge of the grid cell, the pass-location is wrapped around to the top of the column (see Figure 12b).



(**a**) (**b**)

Figure 12. Downward movement. (**a**) Regular case; (**b**) Special case.

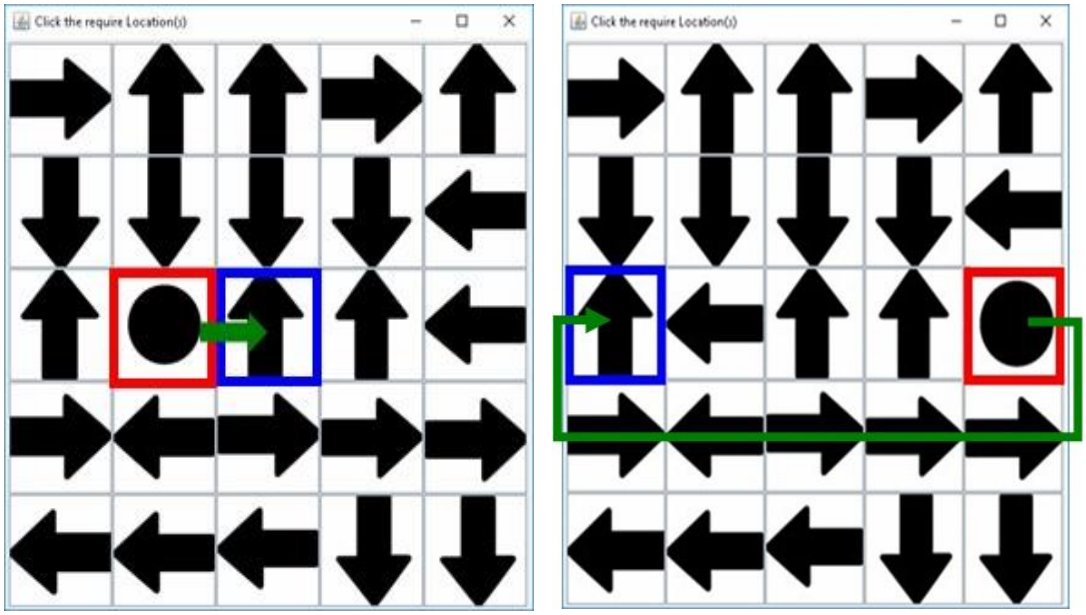
Backward movement: if a left arrow image is shown at the registered location, the pass-location is one location backward from the on-focus location (see Figure 13a). If the on-focus location is located at the left-edge of the grid cell, the pass-location is wrapped around to the rightmost column (see Figure 13b).



(**a**) (**b**)

Figure 13. Backward Movement. (**a**) Regular case; (**b**) Special case.

Forward movement: if a right arrow image is shown at the registered location, the pass-location is one location forward from the on-focus location (see Figure 14a). If the on-focus location is located at the right-edge of the grid cell, the pass-location is wrapped around to the leftmost column (see Figure 14b).



(**a**) (**b**)

Figure 14. Forward movement. (**a**) Regular case; (**b**) Special case.

No movement: if a solid sphere image is shown at the registered location, the pass-location is remained at the same location as the on-focus location (see Figure 15). Hence, there is no movement required.

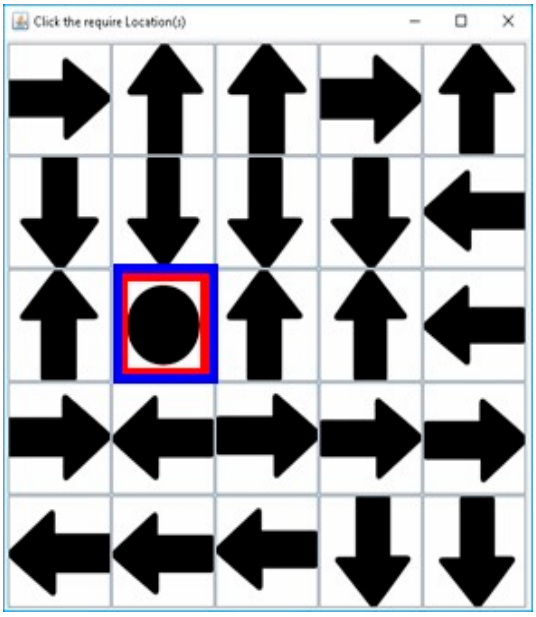


Figure 15. No Movement.

A sample challenge round is used to illustrate the proposed method (see Figure 16). Assuming that a user has registered five locations and their order are highlighted as in Figure 16, to obtain the pass-location, firstly, the user is required to find the start location. The start location is the location shown with a solid sphere image. After that, the user is required to identify the image shown at each of the registered locations.

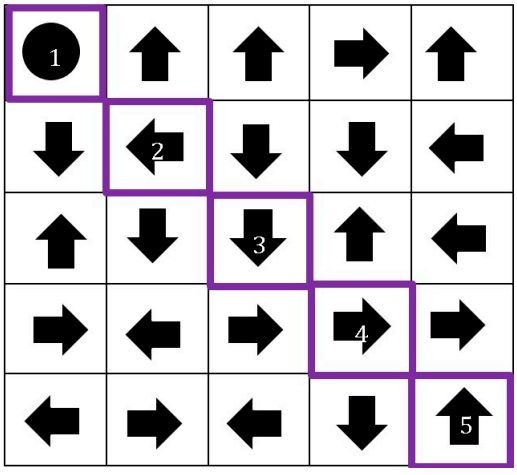


Figure 16. A sample challenge round.

The first registered location is a solid sphere image. Therefore, the pass-location remains at the same location as the on-focus location. Hence, there is no movement required (see Figure 17a). Next, the second registered location is detected. The proposed method will convert the pass-location to the on-focus location. The left arrow image shown at second registered location is used to determine the new pass-location. Since the on-focus location is located at the left-edge of the grid cell, the pass-location is wrapped around to the rightmost column after moving one location backward (see

Figure 17b). Since, the third registered location is detected, the pass-location is converted to the on-focus location. The image shown at the third registered location is used to determine the new pass-location. The third registered location is a down arrow image. Therefore, the pass-location is one location downward from the on-focus location (see Figure 17c). After that, the fourth registered location is detected. Similarly, the pass-location is converted to the on-focus location. The right arrow image shown at the fourth registered location is used to determine the new pass-location. Since the on-focus location is located at the right-edge of the grid cell, the pass-location is wrapped around to the leftmost column after moving one location forward (see Figure 17d). Again, another registered location is detected. The pass-location is converted to the on-focus location. The up arrow image shown at the fifth registered location is used to determine the new pass-location. Therefore, the pass-location is one location upward from the on-focus location (see Figure 17e). Since there are no more registered locations detected, the pass-location is the final location that the user needs to click to complete the challenge round (see Figure 17f). The final pass-location is shaded in grey.

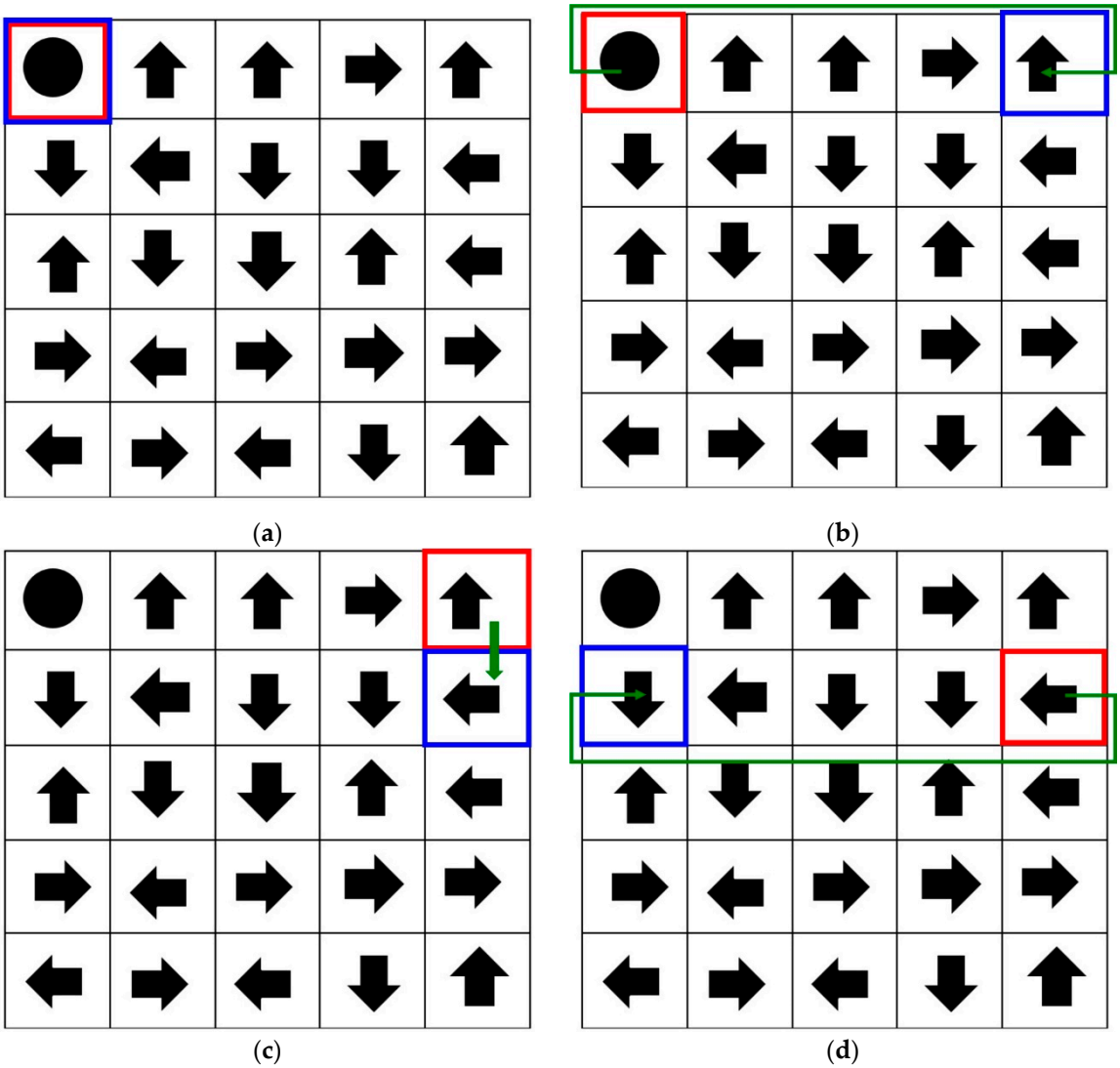
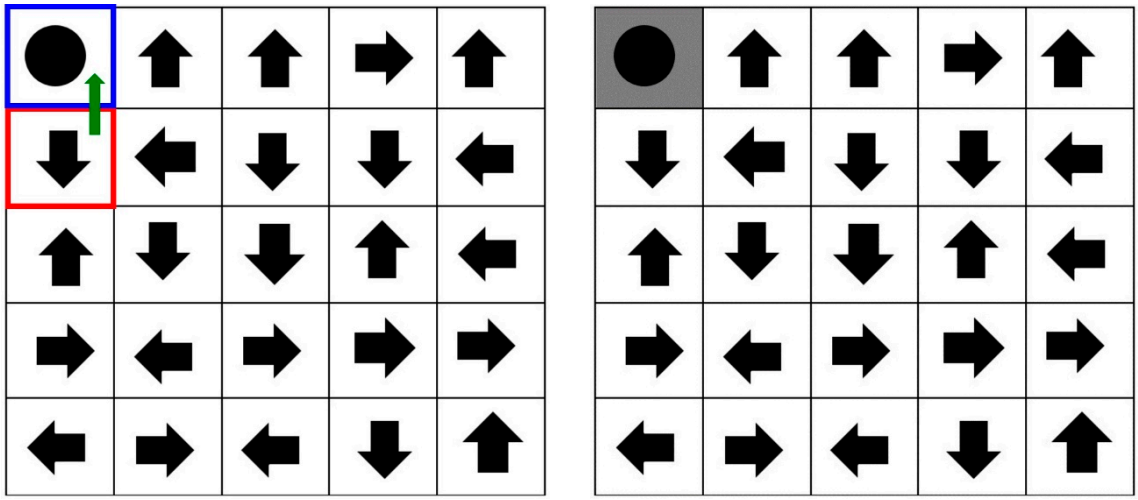


Figure 17. *Cont.*



(**e**) (**f**)

Figure 17. A process to obtain the pass-location. (**a**) First Movement; (**b**) Second Movement; (**c**) Third Movement; (**d**) Fourth Movement; (**e**) Fifth Movement; (**f**) Pass-location.

It was a known fact that recognition-based graphical password systems have limited password spaces compared to alphanumeric password systems [23,24]. Due to the limited password space issues, most graphical password systems are vulnerable to brute-force attack. To reduce brute-force attack while not affecting the user memorability, we have suggested that the user register at least three locations and our proposed system will enforce the user identifying the correct pass-location in three continuous attempts before the user can login. To increase the password spaces of our proposed method, we regenerate a new challenge set for the user regardless of whether the user clicks the pass-location correctly or wrongly in each challenge set. The images shown in the new challenge set are reshuffled using a randomisation algorithm. To restrict the number of trials by brute-force attackers, we have set a maximum trial of three for each user. If the user fails to login after three trials, his/her account will be blocked. This block feature can also reduce guessing attacks. However, during the user study, this feature was disabled so that the participants could have unlimited trials to perform the shoulder-surfing test.

4. User Study

We conducted a search using Thomson Reuters, Scopus and Google scholar databases. To our knowledge, user studies are the only method used to evaluate the feasibility of a method in reducing/preventing shoulder-surfing attacks [1,5,17,18,20,21,25,26]. Shoulder-surfing occurs when attackers skillfully capture important data/activities such as login password via direct observation or video recording methods. This behaviour cannot be formalised. Therefore, we tried to carefully design and imitate the actual scenarios of direct observation, multiple observations and video recorded shoulder-surfing attacks. To imitate direct observation scenarios, the participants could directly observe the login process. To imitate multiple observations scenarios, the participants were given unlimited chances to request for a live demonstration throughout the testing. To imitate video recorded shoulder-surfing scenarios, the participants were given unlimited chances to watch a pre-recorded video of a login session throughout the testing. They even could record and analyse the live demonstration using their mobile phones. Moreover, the related works (WYSWTE [5], Ho et al. [17], Por et al. [1], 3DGUA [20], Sun et al. [21]), which we are comparing, use user studies to evaluate their methods as well. Thus, we used a user study to evaluate the feasibility of our proposed method in preventing shoulder-surfing attacks.

4.1. Hypothesis

Null hypothesis (H_0). *Our proposed method, which uses the pass-location concept, can prevent shoulder-surfing attackers from obtaining the predefined registered locations regardless of gender.*

Alternative hypothesis (H_1). *Our proposed method, which uses the pass-location concept, cannot prevent shoulder-surfing attackers from obtaining the predefined registered locations regardless of gender.*

A hypothesis was made to evaluate whether our proposed method could prevent shoulder-surfing attackers from obtaining the predefined registered locations regardless of gender. To do so, the following methodology is used.

4.2. Participants

A user study was conducted to evaluate the feasibility of the proposed method in preventing shoulder-surfing attacks. 108 students from the Department of Computer Science (DCS), Ekiti State University (EKSU), Nigeria were invited to participate in this user study (Group 1). 49 participants were male and the rest were female. The total population at DCS, EKSU is 150. According to the required sample size table proposed by Krejcie and Morgan in 1970 [27], 108 is the sufficient sample size for the population of 150 with 95% confidence level with a Margin Error of 5%. This means that if the user study is repeated using the same method, the true population parameter will fall within 5% points of the real population value 95% of the time.

Based on the reviewer's comments, we conducted another user study with 30 participants who are technically competent from Oyo State, Nigeria (Group 2). This group of participants had backgrounds in computer security. They were either IT technical staffs or IT administrative who combat cyber crime or make/strengthen the company's security policy. A sample size of 30, it is often suggested, will produce an approximately normal sampling distribution [28,29]. Thus, a sample size of at least 30 was used in this case study to evaluate whether competency level is it a factor in influencing the result of our proposed method in preventing shoulder-surfing attacks. During the shoulder-surfing testing, this group was treated equally with the other participants, where they were required to go through the same procedures before attacking.

4.3. Procedure

Initially, the participants were required to go through a tutorial session to ensure they equipped themselves with the knowledge of how our proposed system works. After that, the participants were asked to login and familiarised themselves with the proposed method. The participants were instructed to watch a recorded video of a login session once they had confirmed they could perform the shoulder-surfing testing. Throughout the testing, the participants were allowed to replay the recorded video and they could request for a live demonstration as many times as they required. The participants could record and analyse the live demonstration using their mobile phones. The participants were then given unlimited trials to perform the attack. The results and feedback regarding the methods used by the participants were recorded.

5. Results

5.1. Shoulder-Surfing Testing Result

The shoulder-surfing testing results indicated that none of the participants was able to login although they knew the underlying algorithm and they have been given sufficient time to perform shoulder-surfing attacking (see Table 1). The shoulder-surfing testing results also indicated that none of the participants from Group 2 was able to login, although they were technically competent. This means that the hypothesis testing does not reject H_0. In another word, the user study results have shown

that the proposed method that uses pass-location concept could resist direct observation, multiple observations and video-recorded shoulder-surfing attacks regardless of gender. This claim was made because the participants have gone through a tutorial session and they have familiarised themselves with the proposed method before they could perform the shoulder-surfing test. Moreover, the user study was carefully designed to imitate the actual scenarios of direct observation, multiple observations and video recorded shoulder-surfing attacks. This means that the user study results have shown that our proposed method that uses the pass-location concept could resist direct observation, multiple observations and video-recorded shoulder-surfing attacks regardless of gender and competency level.

Table 1. Results of shoulder-surfing prevention according to gender.

Group	Gender	Count of Participants that Can Login via SSA [1]	Count of Participants that Can Prevent		
			DO [2]	MO [3]	VR [4]
1	Female	0%	54.63%	54.63%	54.63%
	Male	0%	45.37%	45.37%	45.37%
2	Female	0%	23.33%	23.33%	23.33%
	Male	0%	76.67%	76.67%	76.67%
Total		**0%**	**100.00%**	**100.00%**	**100.00%**

[1] Shoulder-surfing attack; [2] Direct observation shoulder-surfing attack; [3] Multiple observations shoulder-surfing attack; [4] Video-recorded shoulder-surfing attack.

5.2. Usability Testing Result

Figure 18 shows mean time for ten successful logins. As shown in the chart, as participants became more familiar with the system, the time taken to login decreased.

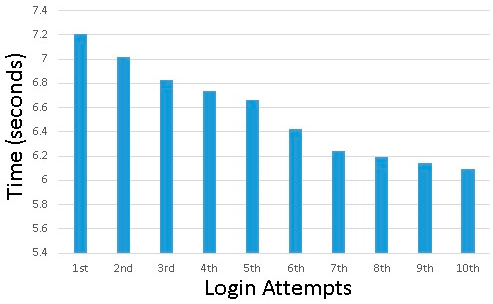


Figure 18. Mean times for ten successful logins.

Table 2 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 was 4.0 seconds. The maximum time taken by the participants for a successful login was 20.0 seconds. The mean time indicated an average login time of 6.55 seconds. 6.55 seconds is the average time taken to login successfully by all the participants after completing ten successful logins. The median login time for all the successful login attempts was 6.0 seconds. This indicates that on the average, 50% of the login attempts required 6.0 seconds to login. The Standard Deviation of 1.63 seconds indicates that the login times were relatively close and not too far apart. This was further buttressed with mode of 6.0 seconds which indicates that majority of the successful login times were 6.0 seconds.

5.3. Comparison with Other Selected Related Works

Table 3 shows the login time comparison between the proposed method and other related works. Method [1] reported that it has the minimum login time followed by our proposed method then method [17]. In terms of maximum login time, our proposed method had the shortest login time, followed by the method in [1], then the method in [17]. On average, our proposed method still had a

shorter login time than method [1] and method [17]. The reason our proposed method was able to produce the shortest login time on average might due to several factors: (i) we only required the users to memorise the registered locations (something that only the users know) and the method we used to login, and based on that we could say that our proposed method did not add to the memory burden of the users as much as other methods; (ii) we used 5 image directions (something that the users can see) to determine a pass-location (new knowledge), and the users do not need to remember these images, they only need to use the direction shows on top of the registered locations (something that only the users know) and the users would eventually know how our proposed method works when they saw the direction of the images.

Table 2. Results of shoulder-surfing prevention according to gender.

Item	Time (Seconds)
Minimum	4.0
Maximum	20.0
Mean	6.55
Median	6.0
Standard Deviation	1.63
Mode	6.0

Table 3. Login time comparison.

Method	Min Login Time (Seconds)	Max Login Time (Seconds)	Mean Login Time (Seconds)
WYSWTE [5]	No Specify	No Specify	No Specify
Ho et al. [17]	16.1	184.2	53.5
Por et al. [1]	3.0	28.0	9.67
3DGUA [20]	No Specify	No Specify	No Specify
Sun et al. [21]	No Specify	No Specify	No Specify
Proposed Method	4.0	20.0	6.55

Table 4 shows the shoulder-surfing resistant comparison between our proposed method and other selected related works. In the table it can be seen that, all the reviewed methods were able to resist direct observation shoulder-surfing attack. However, when it comes to video-recorded shoulder-surfing attack testing, our proposed method and method [17] are the only two that can resist it. The reason that both of our methods could do so is that the pass-image/location produced by our methods in each challenge set could be the registered images/locations, the decoy images/locations, or both. Therefore, when attackers video recorded the clicked images/locations, they might not be able to figure out whether these images/locations are the decoy or registered images/locations.

Table 4. Shoulder-surfing resistant comparison.

Method	DO [1]	MO [2]	VR [3]
WYSWTE [5]	Resist	Could not Resist	Could not Resist
Ho et al. [17]	Resist	Could not Resist	Resist
Por et al. [1]	Resist	Could not Resist	Could not Resist
3DGUA [20]	Resist	Could not Resist	Could not Resist
Sun et al. [21]	Resist	Could not Resist	Could not Resist
Proposed Method	Resist	Resist	Resist

[1] Direct observation shoulder-surfing attack; [2] Multiple observations shoulder-surfing attack; [3] Video recorded shoulder-surfing attack.

When it comes to multiple observation shoulder-surfing attacks, our proposed method is the only one that can resist them. The main reason that our proposed method could resist multiple observation shoulder-surfing attacks is because our method does not produce any useful information

for the attackers when they shoulder-surf the images/locations clicked by a user. Unlike in the method in [17], where the images/locations clicked by the user could indirectly allow the attackers to obtain useful information for determining the pass-images/locations used when they reversed engineered the authentication processes based on the images/locations clicked.

Lastly, the password space estimation of the related works and our proposed method is presented at Table 5.

Table 5. Password space estimation.

Method	Password Length (n)	Password Space in (r) Rounds
WYSWTE [5]	4	$28!/(28-n)!$
Ho et al. [17]	n	$25!/(25-n)!$
Por et al. [1]	2	$(25!/(25-n)!) \times r$
3DGUA [20]—cannot register same image during registration phase	n	$150!/(150-n)! \times r$
3DGUA [20]—can register same image during registration phase	n	$150^n \times r$
Sun et al. [21]	n	$77^n \times r$
Proposed Method	n	25^r

6. Discussion

In this study, we have proposed a method that makes use of the registered locations (something that only the users know) and 5 image directions inspired by Cardinal directions (something that the users can see) to determine a pass-location (new knowledge).

We conducted a search using Thomson Reuters, Scopus and Google scholar databases. To our knowledge, user studies are the only method used to evaluate the feasibility of a method in reducing/preventing shoulder-surfing attacks [1,5,17,18,20,21,25,26]. Shoulder-surfing occurs when attackers skillfully capture the important data/activities such as login password via direct observation or video recording methods. This behaviour cannot be formalised. Moreover, the related works (WYSWTE [5], Ho et al. [17], Por et al. [1], 3DGUA [20], Sun et al. [21]), which we are comparing use user studies to evaluate their methods. Thus, we use a user study to evaluate the feasibility of our proposed method in preventing shoulder-surfing attacks.

The user study was carefully designed to imitate the actual scenarios of direct observation, multiple observations and video recorded shoulder-surfing attacks. The participants were given unlimited trials to perform shoulder-surfing attacks. They could even request the demonstrator demonstrates the authentication process and record the authentication process using their mobile phones for further analysis. The shoulder-surfing testing results indicated that none of the participants was able to login, although they knew the underlying algorithm and they were given sufficient time to perform a shoulder-surfing attack. Hence, we conclude that our proposed method can resist shoulder-surfing attacks in regards to direct observation, multiple observations and video-recorded shoulder-surfing attacks, regardless of gender and competency level.

There are two factors that enable our proposed method to withstand shoulder-surfing attack. Firstly, the registered locations and the images used in our proposed method are meaningful. By combining both types of meaningful information, our proposed method produces useful knowledge. This knowledge is then be used to determine the pass-location in each challenge set. Nevertheless, this new knowledge will not make any sense to the attackers if they obtained it using shoulder-surfing attacks.

Secondly, the images used in our proposed method have higher chances to offset with each other. Offset in this context is referring to "No movement". No movement could only happen if the registered location shown a solid sphere image or the registered locations are made up of left arrow and right arrow images, or up arrow and down arrow images. The idea of offset could increase the password spaces of our proposed method if an attacker intended to guess the registered location used. For example, in Figure 10 the pass-location is located at the solid sphere image. To get such location, a

user must either register a location at the solid sphere image (case i), or the registered locations must either shown both left and right arrows (case ii), or both up and down arrows (case iii), or the registered locations are make up of the two or more repetitive case i, ii, or iii individually (case iv) each, or the registered locations are make up of the any combination among case i, ii, iii and iv (case v). This means that, the number of registered locations used to produce a "no movement" result between 1 and N. N is denoted as a positive integer. Therefore, it is clear that our proposed method could improve the password spaces and this would eventually make it more difficult for the attackers to guess how many registered locations a user is using.

7. Conclusions

This research has expanded the mechanisms available for preventing shoulder-surfing attacks and broadened knowledge on preventing shoulder-surfing attacks. We have proposed and demonstrated a new method in which pass-location is determined by navigating the direction based on the images displayed in the registered positions. This would no doubt contribute greatly to knowledge in graphical passwords, and ultimately information security research.

In future we will still work on exploring more meaningful images and hoping these images can be deployed to determine a pass-image/location in a challenge set. Moreover, we will also look into other suitable ways to deploy the images that have the offset attribute to increase the password space.

Author Contributions: Conceptualisation, L.Y.P., C.S.K. (Chee Siong Khaw) and L.A.A.; methodology, L.Y.P., M.Y.I.I., C.S.K. (Chee Siong Khaw) and L.A.A.; software, C.S.K. (Chee Siong Khaw), L.A.A. and C.S.K. (Chin Soon Ku); validation, L.Y.P., C.S.K. (Chin Soon Ku) and M.Y.I.I.; formal analysis, L.Y.P., C.S.K. (Chee Siong Khaw) and L.A.A.; investigation, L.Y.P. and C.S.K. (Chin Soon Ku); resources, L.Y.P., C.S.K.(Chin Soon Ku); data curation, C.S.K. (Chee Siong Khaw) and L.A.A.; writing–original draft preparation, L.A.A. and C.S.K. (Chee Siong Khaw); writing–review and editing, L.Y.P., M.Y.I.I. and C.S.K. (Chin Soon Ku); visualisation, C.S.K. (Chee Siong Khaw) and L.A.A.; supervision, L.Y.P. and M.Y.I.I.; project administration, C.S.K. (Chin Soon Ku); funding acquisition, L.Y.P.

Funding: This research was funded by Bantuan Khas Penyelidikan (BKS) from the University of Malaya, Malaysia, grant number BKS022-2018 and Fundamental Research Grant Scheme from the Ministry of Higher Education, Malaysia, grant number FP114-2018A.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Por, L.Y.; Ku, C.S.; Islam, A.; Ang, T.F. Graphical password: Prevent shoulder-surfing attack using digraph substitution rules. *Front. Comput. Sci.* **2017**, *11*, 1098–1108. [CrossRef]
2. Dhamija, R.; Perrig, A. Deja Vu-A User Study: Using Images for Authentication. In Proceedings of the USENIX Security Symposium, Denver, CO, USA, 14–17 August 2000.
3. Biddle, R.; Chiasson, S.; Van Oorschot, P. Graphical passwords: Learning from the first twelve years. *J. ACM Comput. Surv.* **2012**, *44*, 19–41. [CrossRef]
4. Gupta, S.; Sahni, S.; Sabbu, P.; Varma, S.; Gangashetty, S.V. Passblot: A highly scalable graphical one time password system. *Int. J. Netw. Secur. Appl.* **2012**, *4*, 201–216. [CrossRef]
5. Khot, R.A.; Kumaraguru, P.; Srinathan, K. WYSWYE: Shoulder surfing defense for recognition based graphical passwords. In Proceedings of the 24th Australian Computer-Human Interaction Conference on—OzCHI '12, Melbourne, Australia, 26–30 November 2012.
6. Al-Ameen, M.N.; Wright, M.; Scielzo, S. Towards Making Random Passwords Memorable: Leveraging Users' Cognitive Ability Through Multiple Cues. In Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing System, Seoul, Korea, 18–23 April 2015.
7. Anwar, M.; Imran, A. A Comparative Study of Graphical and Alphanumeric Passwords for Mobile Device Authentication. In Proceedings of the 26th Modern AI and Cognitive Science Conference 2015, Greensboro, NC, USA, 25–26 April 2015.
8. Ku, W.C.; Yeh, Y.C.; Cheng, B.R.; Chang, C.J. A sector-based graphical password scheme with resistance to login-recording attacks. *IEICE Trans. Inf. Syst.* **2015**, *98*, 894–901. [CrossRef]
9. Kulkarni, P.J.; Malwatkar, G.M. The graphical security system by using CaRP. In Proceedings of the International Conference on Energy Systems and Applications, Pune, India, 30 October–1 November 2015.

10. Zhao, Z.; Ahn, G.J.; Hu, H. Picture gesture authentication: Empirical analysis, automated attacks, and scheme evaluation. *ACM Trans. Inf. Syst. Secur.* **2015**, *17*, 14. [CrossRef]
11. Bianchi, A.; Oakley, I.; Kim, H. PassBYOP: Bring your own picture for securing graphical passwords. *IEEE T. Hum.-Mach. Syst.* **2016**, *46*, 380–389. [CrossRef]
12. Assal, H.; Imran, A.; Chiasson, S. An exploration of graphical password authentication for children. *Int. J. Child-Comp. Int.* **2018**, *18*, 37–46. [CrossRef]
13. Alsaiari, H.; Papadaki, M.; Dowland, P.S.; Furnell, S.M. A Review of Graphical Authentication Utilising a Keypad Input Method. In Proceedings of the Eighth Saudi Students Conference, London, UK, 31 January–1 February 2016.
14. Maity, M.; Dhane, D.M.; Mungle, T.; Chakraborty, R.; Deokamble, V.; Chakraborty, C. A Secure One-Time Password Authentication Scheme Using Image Texture Features. In Proceedings of the International Symposium on Security in Computing and Communication, Jaipur, India, 21–24 September 2016.
15. Por, L.Y.; Lim, X.T.; Su, M.T.; Kianoush, F. The design and implementation of background Pass-Go scheme towards security threats. *WSEAS Trans. Inf. Sci. Appl.* **2008**, *5*, 943–952.
16. Islam, A.; Por, L.Y.; Othman, F.; Ku, C.S. A Review on Recognition-Based Graphical Password Techniques. In *Computational Science and Technology, Lecture Notes in Electrical Engineering*; Alfred, R., Lim, Y., Ibrahim, A., Anthony, P., Eds.; Springer: Singapore, 2019.
17. Ho, P.F.; Kam, Y.H.S.; Wee, M.C.; Chong, Y.N.; Por, L.Y. Preventing Shoulder-Surfing Attack with the Concept of Concealing the Password Objects' Information. *Sci. World. J.* **2014**, *2014*, 1–12. [CrossRef] [PubMed]
18. Por, L.Y.; Ku, C.S.; Ang, T.F. Preventing Shoulder-Surfing Attacks using Digraph Substitution Rules and Pass-Image Output Feedback. *Symmetry* **2019**, *11*, 1087. [CrossRef]
19. Gokhale, M.A.S.; Waghmare, V.S. The shoulder surfing resistant graphical password authentication technique. *Procedia Comput. Sci.* **2016**, *79*, 875–884. [CrossRef]
20. Katsini, C.; Raptis, G.E.; Fidas, C.; Avouris, N. Does image grid visualisation affect password strength and creation time in graphical authentication? In Proceedings of the 2018 International Conference on Advanced Visual Interfaces, Castiglione della Pescaia, Grosseto, Italy, 29 May–1 June 2018.
21. Sun, H.M.; Chen, S.T.; Yeh, J.H.; Cheng, C.Y. A shoulder surfing resistant graphical authentication system. *IEEE Trans. Depend. Secur.* **2018**, *15*, 180–193. [CrossRef]
22. Cardinal Directions and Ordinal Directions: GEOLOUNGE. Available online: https://www.geolounge.com/cardinal-directions-ordinal-directions/ (accessed on 8 October 2017).
23. Renaud, K.; De Angeli, A. Visual passwords: Cure-all or snake-oil? *Commun. ACM* **2009**, *52*, 135–140. [CrossRef]
24. Renaud, K.; Mayer, P.; Volkamer, M.; Maguie, J. Are Graphical Authentication Mechanisms as strong as Passwords. In Proceedings of the Federated Conference on Computer Science and Information Systems, Krakow, Poland, 8–11 September 2013.
25. Por, L.Y. Frequency of occurrence analysis attack and its countermeasure. *Int. Arab J. Inf. Technol.* **2014**, *10*, 189–197.
26. Por, L.Y.; Kiah, M.L.M. Shoulder surfing resistance using penup event and neighbouring connectivity manipulation. *Malays. J. Comput. Sci.* **2010**, *23*, 121–140.
27. Krejcie, R.V.; Morgan, D.W. Determining sample size for research activities. *Educ. Psychol. Meas.* **1970**, *30*, 607–610. [CrossRef]
28. The National Institute for Health Research (NIHR) Research Design Service (RDS) for the East Midlands/Yorkshire & the Humber 2007: Sampling and Sample Size Calculation. Available online: https://pdfs.semanticscholar.org/ae57/ab527da5287ed215a9a3bf5f542ae19734ea.pdf (accessed on 20 September 2019).
29. Smith, Z.R.; Wells, C.S. Central Limit Theorem and Sample Size. In Proceedings of the Annual Meeting of the Northeastern Educational Research Association, Kerhonkson, New York, NY, USA, 18–20 October 2006.