Preventing Shoulder-Surfing Attacks using Digraph Substitution Rules and Pass-Image Output Feedback

Lip Yee Por ^{1,*} , Chin Soon Ku ^{1,2} and Tan Fong Ang ¹

¹ Department of Computer System & Technology, University of Malaya, Kuala Lumpur 50603, Malaysia

² Department of Computer Science, Universiti Tunku Abdul Rahman, Kampar 31900, Malaysia

* Correspondence: porlip@um.edu.my

Received: 9 August 2019; Accepted: 26 August 2019; Published: 30 August 2019

Abstract: In this paper, we focus on methods to prevent shoulder-surfing attacks. We initially adopted digraph substitution rules from PlayFair cipher as our proposed method. PlayFair cipher is a modern cryptography method, which exists at the intersection of the disciplines of mathematics and computer science. However, according to our preliminary study it was insufficient to prevent shoulder-surfing attacks. Thus, a new method had to be proposed. In this new proposed method, we improvised the digraph substitution rules and used these rules together with an output feedback method to determine a pass-image. Our proposed method was evaluated with a user study. The results showed our proposed method was robust against both direct observation and video-recorded shoulder-surfing attacks.

Keywords: graphical authentication; user authentication; shoulder-surfing; digraph substitution rules; output feedback

1. Introduction

Password authentication is an essential security measure to protect resources from unwanted intruders, for example, online social media accounts, mobile phone authorizations, personal computers and so forth. There are many types of passwords. Text-based passwords are the most commonly used authentication methods [1]. Standard guidelines are available for strong text-based password selection. For example, a password must consist of at least eight characters including a combination of alphanumeric and special character as well as the mixture of upper and lower cases [2]. However, strong passwords are difficult to remember [3]. Therefore, most users prefer weak passwords as they are functionally easier to recall [4]. Graphical authentication, which uses images instead of texts for authentication, has been introduced to counter the issue with text recall [5,6].

There are three types of graphical password schemes – recognition-based, recall-based and cued recall-based [7]. In recognition-based graphical password, users authenticate by recognizing and identifying registered images. One of the very well-known recognition-based graphical passwords system is PassfacesTM. For recall-based graphical password, a user is required to reproduce the password created during the enrolment procedure without any hint/clue given. An example of such authentication method was designed by Jermyn and his associates [8] known as Draw-A-Secret (DAS). Chiasson et al. introduced Cued Click Point as a form of cued recall-based graphical password. Users are given clues to help them reproduce the registered password [9]. Even though the graphical password is able to improve users' memorability, password spaces are limited, hence its vulnerability is exposed to shoulder-surfing attacks [10–14].

A shoulder-surfing attack is a physical security threat initiated by a bystander who steals the password of a legitimate user via directly observing or video recording the password entry [15]. Currently, many methods have been proposed to address shoulder-surfing attacks [16–23]. However, most of

the methods are still vulnerable to shoulder-surfing attack. Hence, there is a need to carry out this research work to overcome shoulder-surfing attack.

In this paper, a method using digraph substitution rules and pass-image output feedback is proposed to address shoulder-surfing attacks. This paper is organized as follows: Section 2 discusses the related works. Section 3 presents the proposed user authentication method. Section 4 describes the methodology used for the evaluation. Section 5 presents the analyzed results that we have obtained from the evaluation. Finally, Section 6 discusses the future direction of this research work.

2. Related Works

Dhamija et al. developed a system using “random art” images. These images are generated using Andrej Bauer’s Random Art. During the enrolment procedure, a user needs to register five images. During authentication, twenty-five images are given for the user to select the registered images to login. According to the authors, using “random art” images can make it harder for users to describe, share and/or write down their passwords [16]. However, the images selected can be exposed using direct observation shoulder-surfing attacks.

PassfacesTM was proposed by Reference [17] utilizing human faces as images. A user is required to enroll four images during enrolment. Subsequently, the user needs to identify the images registered over four rounds before they can login. According to the authors, PassfacesTM can help users to remember their passwords better compared to text passwords. However, PassfacesTM remains susceptible to shoulder-surfing attacks.

As proposed by Reference [18], Convex Hull Click allows a user to register three icons during enrolment. During authentication, the user needs to visualize an area (also known as convex hull) that is formed by the three registered icons. The user has to select any one of the icons inside the convex hull area to login. The authors believed this method can prevent direct observation shoulder-surfing attack because the pass-icon used to login is a decoy icon. The same or different decoy icons can be used by the user to login as long as these decoy icons are within the convex hull. However, the registered images can never be clicked using this method. Therefore, it is exposed to video recorded shoulder-surfing attack whereby the registered icons will be revealed after attackers performing multiple videos recordings.

“Where You See is What You Enter” scheme proposed by Reference [19] required users to eliminate the row or column, which does not have the images enrolled. Similar elimination process is repeated for login until no more rows or columns can be eliminated. The authors claimed that this method can prevent direct observation shoulder-surfing attack because the user is not revealing any information about the registered images. However, we found that this method actually reveals the registered images in the final round of the elimination processes. The attackers can filter out the images by using multiple video recorded shoulder-surfing sessions. To obtain the information of the actual images enrolled, the attackers can compare the eliminated images within the final form of the remaining images with images in previously eliminated rows observed over multiple recordings.

Sonal et al. [20] proposed a graphical authentication system in 2015. This method requires a user to register several characters and a colour during enrolment. Subsequently, the user needs to rotate the colour sector to the places that have the selected characters. It is claimed that direct observation shoulder-surfing attack can be prevented as the characters and colour selected are not being exposed. Unfortunately, an attacker can filter out the colour sector and the characters that each of the colours contains when the user stop rotating. Therefore, by using multiple videos recorded shoulder-surfing sessions, there is a possibility for the attacker to know the selected colour and characters.

Kolay et al. [21] proposed a graphical authentication system using image segmentation method. An image is intentionally selected and then segmented into grids during enrolment. The segmented images are then given in a jumbled order. The user needs to click the correct segmented images and reproduce the registered image to login. While the system provides convenience for users, attackers are able to shoulder-surf the images chosen by the user.

Another graphical password system was proposed by Dhandha et al. [22] in 2017. For authentication process, the user is required to recognize the selected images and also the string associated with them. To login, the user must sequentially enter the strings according to the registered images. The authors believe this method can prevent direct observation shoulder-surfing attacks as only some of the registered images will be selected for authentication purposes. Moreover, the string associated with the registered images will be varied every time the login page is refreshed. Nevertheless, it is discovered that an attacker can filter out the decoy images, which are not selected by the user. After that, the attacker can map the string entered by the user with the images given. With multiple videos recorded shoulder-surfing sessions, the registered images can be revealed.

EvoPass was proposed by Reference [23]. During the enrolment procedure, a user needs to register four images. These registered images and the decoy images are transformed into sketches during authentication. All the sketched images will gradually be degraded until they contain minimum information of the registered images. The user needs to click the correct sketches that represent the registered images to login. The objective of the authors is to prevent direct observation attack even though part of the sketches is exposed. However, during the authentication procedure, the user can roll back if the user is unable to determine the sketches that represent the registered images. After rolling back, a new challenge set will contain the sketches that have more information of the registered images. At this moment, an attacker can have better opportunity to capture the clicked sketches using video recorded shoulder-surfing attack. Due to the fact that the images used in EvoPass are unique, the attacker can analyze the characteristic of the clicked sketches and used the most similar sketches to gain access to the system. Hence, this method is vulnerable to video recorded shoulder-surfing attacks.

After analyzing the weaknesses of the existing systems, it is evident that there are research gaps in addressing shoulder-surfing attacks. As such, this study was carried out with the aim to overcome both video-recorded and direct observation shoulder-surfing attacks.

3. The Proposed User Authentication Method

The proposed authentication system consists of two separate procedures, enrolment and authentication. To benchmark with existing methods, we used the same size of grid cell (5×5) as the standard.

3.1. Enrolment Procedure

The proposed system is inspired by a word game named Scrabble. The user is given 27 images (starting from the character A to the character Z, together with a “blank” block). For the proposed shoulder-surfing prevention method to work properly, the user needs to register at least two images. The user is allowed to register the same image more than once. However, the user can only register up to 25 unique images due to the maximum size of the grid cell (5×5), which has been fixed during the password verification process. The registration procedure is considered completed once the user has confirmed the registered images (see Figure 1). After confirmation, the system initials the user’s account status as “new”. Lastly, the information regarding the registered images and the account status of the user is stored in a file system.

Figure 1. Password Registration Process.

3.2. Authentication Procedure

For a first-time login, a user with “new” account status will be given a challenge set, consisting of a 5×5 grid cell, during the password verification process (see Figure 2). The proposed system will initially select the unique registered images and fill in the 5×5 grid cell using the uniform randomisation algorithm (let y be denoted as all the unique registered images). After that, the remaining grid will be filled by (25 minus y) decoy images using the uniform randomisation algorithm. As the user’s account is of “new” status, the two left-over decoy images will bind with the account and they will not be used thereafter to prevent FOA attacks [24]. The user’s account is then updated to “active” status. To login, the user is required to select the pass-images using our proposed method. Once the user has finished selecting the pass-images, the proposed system will check to see if the pass-images match the ones registered in the database. If the pass-images are matched, the user will be granted authorised access rights. An error message will be prompted to the user if the login process is not successful. A new challenge set will be given to the user. If the user fails to achieve authorisation after three continuous attempts; the user account will be blocked. This block feature is disabled when we conducted user study because we allowed the participants to have unlimited trials.

Figure 2. Password Authentication Process.

3.3. Proposed Method

The proposed method was inspired by Playfair cipher, a manual symmetric encryption technique invented in 1854 by Charles Wheatstone [25]. PlayFair cipher is a modern cryptography method, which exists at the intersection of the disciplines of mathematics and computer science. Playfair cipher

uses a 5 by 5 table containing a keyword. For our proposed method, we used a 5×5 grid cell and also alphabets with an extra “blank” block image. In Playfair cipher, the keyword is placed in the 5 by 5 table (dropping any duplicate letters) followed by the remaining alphabets in an ascending order. In this study, we proposed to use uniform randomization algorithm to ensure only 25 unique images are shuffled and placed into the 5×5 grid cell. The keyword in Playfair cipher is grouped in pairs before encryption process begins. In our proposed method, a pair of images (registered images or pass-images or the mixture of the both) is used to determine the pass-images before a user can login. Playfair cipher uses 3 digraph substitution rules to encrypt a plain text. The rules are as follows [25]:

- Rule 1: If the letters are not on the same row or column, replace them with the letters on the same row respectively but at the other pair of corners of the rectangle defined by the original pair.
- Rule 2: If the letters appear on the same column, replace them with the letters immediately below respectively (wrapping around to the top side of the column if the letter is located at the bottom of the column).
- Rule 3: If the letters appear on the same row of the table, replace them with the letters to their immediate right respectively (wrapping around to the left side of the row if the letter is located at the right most of the row).

Initially, we adopted these rules but it was insufficient to prevent shoulder-surfing attack after a preliminary study was conducted. Therefore, the rules were improvised to make it more robust against shoulder-surfing attack. The conditions of the modified rules are as follows:

- Scenario A: Both password images appear diagonal to each other
- Scenario B: Both password images appear on the same vertical vector
- Scenario C: Both password images appear on the same horizontal vector
- Scenario D: Both password images appear at the same location

Scenario A: Assuming that a user has registered 2 images (marked as p_1 and p_2) and both registered images appear diagonal to each other in Figure 3. To search for the pass-image for p_1 , the user is required to find the intersection image produced by the row and the column of the first and the second registered images respectively. The pass-image for p_1 is marked as i_1 . The step to finding the pass-image for p_2 is a reiteration of the previous step. To find the pass-image for p_2 (i_2), the user needs to find the intersection image produced by the row and column information of the second and first registered images respectively.

In general, the registered images and the pass-images can be denoted as $p_{1_{xy}}$, $p_{2_{xy}}$, $i_{1_{xy}}$ and $i_{2_{xy}}$ using the coordinates' presentation. The position of i_1 and i_2 in Scenario A can be determined using the following equations:

$$i_{1_{xy}} = (p_{2_x}, p_{1_y}) \quad (1)$$

$$i_{2_{xy}} = (p_{1_x}, p_{2_y}) \quad (2)$$

Scenario B: Assuming that a user has registered 2 images and both registered images appear on the same vertical vector in Figure 4. The pass-images for p_1 and p_2 in Figure 4a are immediately below their respective image. Special cases occur in Figure 4b when either the first or the second registered image is located at the bottom side of the column. For these cases, the pass-image is wrapped around to the topside of the column.

The location of the pass-images can be determined using Equations (3)–(6). Equation (3) is used when p_1 is located at the bottom of the column. In this special case, the pass-image for p_2 can be determined using Equation (6). If p_2 , the second registered image, is located at the bottom of the column, the pass-image for p_2 can be determined using Equation (4). In this special case, the pass-image for p_1 can be determined using Equation (5). For normal cases, Equations (5) and (6) are used to determine i_1 and i_2 respectively.

$$i_{1_{xy}} = (p_{1_x}, p_{1_{my}}) \quad (3)$$

$$i2_{xy} = (p2_x, p2_{my}) \quad (4)$$

$$i1_{xy} = (p1_x, p1_{(y-1)}) \quad (5)$$

$$i2_{xy} = (p2_x, p2_{(y-1)}) \quad (6)$$

where my is the maximum range of the y-axis of a $(m \times n)$ grid cell.

(a) Find the pass-image in Scenario A for p1

(b) Find the pass-image in Scenario A for p2

Figure 3. Our rules for Scenario A.

(a) Find the pass-images in Scenario B for p1 and p2

(b) Find the pass-images in Scenario B for Special Case

Figure 4. Our rules for Scenario B.

Scenario C: Assuming that a user has registered 2 images and both registered images appear on the same horizontal vector in Figure 5. The pass-images for p1 and p2 in Figure 5a are immediately right images. Special cases occur in Figure 5b when either the first or the second registered image is located at the right edge of the row. For these cases, the pass-image is wrapped around to the left side of the row.

(a) Find the pass-images in Scenario C for p1 and p2 (b) Find the pass-images in Scenario C for Special Case

Figure 5. Our rules for Scenario C.

The location of the pass-images can be determined using Equations (7)–(10). Equation (7) is used when p1 is located at the right edge of the row. In this special case, the pass-image for p2 can be determined using Equation (10). If p2, the second registered image, is located at the right edge of the row, the pass-image for p2 can be determined using Equation (8). In this special case, the pass-image for p1 can be determined using Equation (9). For normal cases, Equations (9) and (10) are used to determine i1 and i2 respectively.

$$i1_{xy} = (p1_{((mx-x)+1)}, p1_y) \quad (7)$$

$$i2_{xy} = (p2_{((mx-x)+1)}, p2_y) \quad (8)$$

$$i1_{xy} = (p1_{(x+1)}, p1_y) \quad (9)$$

$$i2_{xy} = (p2_{(x+1)}, p2_y) \quad (10)$$

where mx is the maximum range of the x-axis of a $(m \times n)$ grid cell.

Scenario D: Assuming that a user has registered 2 images and both registered images appear on the same location in Figure 6. The pass-images for p1 and p2 are located at the same position as both registered images. The location of the pass-images can be determined using Equation (11).

$$i1_{xy} = i2_{xy} = p1_{xy} = p2_{xy} \quad (11)$$

Figure 6. Our rules for Scenario D.

As mentioned before, initially we adopted the digraph substitution rules. However, this proposal has a major drawback. If an attacker knows the 3 digraph substitution rules, naturally the attacker will be capable of deducing the registered images. In addition, the pass-images used to login can never be the same as the registered images. Thus, attackers can obtain the registered images by filtering out the clicked images using multiple observations attack. We used an example to illustrate the weaknesses of the digraph substitution rules. Assume that a user has registered the images as in Figure 7a. To become authorised, the user is required to click on the pass-images i1, i2, i3 and i4 in the correct order. However, a shoulder-surfer can easily identify the password images used when the user clicks on i1 and i2 using the original digraph substitution rules because p1 is associated with i1 and p2 is associated with i2 (see Figure 7b). This means that once the shoulder-surfer knows the underlying algorithm, the digraph substitution rules are vulnerable to shoulder-surfing attack.

In order to overcome these limitations, we have strengthened the 3 digraph substitution rules by incorporating an extra rule (Scenario D) as well as a new method to determine the pass-images in a challenge set. In our new method, a user is required to determine the first pass-image using the first and second registered images. To determine the next pass-image, the third registered image and the first pass-image are used. The process of determining the next pass-image is based on the next registered image and the current pass-image information (pass-image output feedback). The location of the pass-images can be determined using Equation (12).

$$i_n = \begin{cases} \text{dsr}(p_n, p_{(n+1)}) & \text{if } n = 1 \\ \text{dsr}(p_{(n+1)}, i_{(n-1)}) & \text{if } n \geq 2 \end{cases} \quad (12)$$

where i is denoted as the pass-image; p is denoted as the registered image; i_n and p_n are denoted as the sequence of a pass-image and the sequence of a registered image, respectively; n is a positive integer starting from 1; and dsr is denoted as the four proposed modified digraph substitution rules.

Assume that a user has registered the same images as in Figure 7a. To obtain i_1 using our new proposed method, p_1 and p_2 are used (see Equation (12), when $n = 1$). In Scenario A, i_1 can be determined using the digraph substitution rule.

(a) Example of the registered images

(b) Find the pass-images using the original digraph substitution rules

Figure 7. Digraph substitution rules weaknesses.

However, i_2 can no longer be determined using p_2 and p_1 in this proposed method. To determine the next pass-image (i_2), the next registered image (p_3) and the current pass-image information (i_1) are used (see Equation (12), when $n = 2$). By modifying the original method for determining i_2 , an attacker

is prevented from obtaining full knowledge of the registered images used. By using this proposed method, a shoulder-surfer is no longer able to identify the pass-images used based on the digraph substitution rules because p2 not associated with i2 (see Figure 8).

Figure 8. Our new proposed method for determining pass-images.

Figure 9 shows a sample challenge round to illustrate the proposed modified method for identifying pass-images. Assume that a user has registered the images as in Figure 9a. To obtain i1, p1 and p2 are used. As p1 and p2 appear to be diagonal to each other (Scenario A), the user needs to determine i1 by locating the intersection image of the first password image's row and the second password image's column (see Equation (1)). The user is then required to find i2 using p3 and i1. As both p3 and i1 appear on the same horizontal vector, to determine i2, the user can use the special case rule in Scenario C (see Equation (9)). After obtaining i2, the user is required to find i3 using p4 and i2. As p4 and i2 appear on the same vertical vector, to determine i3, the user can use the rule in Scenario B (see Equation (3)). To identify i4, the user is required to use p5 and i3. As p5 and i3 appear at the same location, to determine i4, the user can use the rule in Scenario D (see Equation (11)). The user is required to correctly click all the pass-images (i1, i2, i3 and i4). To find the pass-image for p2 according to their sequence to gain access to the proposed system. If the user clicks the pass-images incorrectly, a brand-new set for a challenge round will be given (see Figure 9c). The pseudocode of the proposed algorithm is shown in Figure 10.

Figure 9. Example of a challenge round.

```

FUNCTION get authenticated (parameter: list of password image descriptions
x-coordinate, list of password image descriptions y-coordinate, list of user's
pass-images input x-coordinate, list of user's pass-images input y-
coordinate)
Initialize new empty list of pass-image's x-coordinate
Initialize new empty list of pass-image's y-coordinate
Initialize count as zero
Initialize hold x-coordinate as zero
Initialize hold y-coordinate as zero
Initialize maximum range of the x-axis grid cell
Initialize maximum range of the y-axis grid cell
FOR user's password image descriptions x-coordinate
IF count = 0 THEN
Initialize X1 as password image descriptions x-coordinate [count]
Initialize Y1 as password image descriptions y-coordinate [count]
INCREMENT count
Initialize X2 as password image descriptions x-coordinate [count]
Initialize Y2 as password image descriptions y-coordinate [count]
ELSE
SET X1 = password image descriptions x-coordinate [count]
SET Y1 = password image descriptions y-coordinate [count]
SET X2 = hold x-coordinate
SET Y2 = hold y-coordinate
END IF
/*digraph substitution rules and pass-image output feedback */
IF X1 = X2 && Y1 = Y2 THEN /*Scenario D*/
SET hold x-coordinate = X1
SET hold y-coordinate = Y1
ELSE IF X1 = X2 THEN /*Scenario C*/
SET hold x-coordinate = X1
SET hold y-coordinate = Y1 - 1
IF hold y-coordinate > maximum range of the y-axis THEN /*Special
case*/
SET hold y-coordinate = maximum range of the y-axis - hold y-
coordinate
END IF
ELSE IF Y1 = Y2 THEN /*Scenario B*/
SET hold x-coordinate = X1 + 1
SET hold y-coordinate = Y1
IF hold x-coordinate > maximum range of the x-axis THEN /*Special
case*/
SET hold x-coordinate = maximum range of the x-axis - hold x-
coordinate
END IF
ELSE /*Scenario A*/
SET hold x-coordinate = X2
SET hold y-coordinate = Y1
END IF
ADD hold x-coordinate into list of pass-image's x-coordinate
ADD hold y-coordinate into list of pass-image's y-coordinate
INCREMENT count
END FOR
RETURN (CALL match user's pass-images input (arguments: list of user's
pass-images input x-coordinate, list of user's pass-images input x-
coordinate, list of pass-image's x-coordinate, list of pass-image's y-
coordinate))
END FUNCTION
FUNCTION match user's pass-images input (parameter: list of user's pass-
images input x- coordinate, list of user's pass-images input x-
coordinate, list of pass-image's x-coordinate, list of pass-image's y-
coordinate)
IF number of user's pass-images input x-coordinate not equal to number of
pass-image's x-coordinate THEN
RETURN false
END IF
Initialize index to zero
FOR number of user's pass-images input x-coordinate
IF user's pass-images input x-coordinate is not equal to pass-image's x-
coordinate OR user's pass-images input y-coordinate is not equal to pass-
image's y-coordinate THEN
RETURN false
INCREMENT index
END FOR
RETURN true
END FUNCTION

```

Figure 10. Pseudocode of the proposed algorithm.

4. User Study Descriptions

A user study was conducted to assess the security and usability of the proposed method. For the security aspect, we explored whether our proposed method was feasible in preventing shoulder-surfing attack under natural and video recorded conditions. For usability aspect, we explored (i) the duration that the participants can remember their password, (ii) the duration that the participants can remember our proposed method and (iii) the time taken for the participants to login using their password and our proposed method.

As a preliminary study, we conducted the user study at the Faculty of Computer Science and Information Technology (FCSIT), University of Malaya (UM). This venue was chosen because we could have better access and follow up to the participants. The majority of the populations in this faculty are students. The user study was conducted based on a one participant per session basis. We used three phases to test our method proposed. The following are the description of the phases: For the first phase, a pre-survey was conducted to record the nickname, email address and contact number of each participant. We used this information to follow up with the participant weekly (from week 1 until week 4) on the usability aspect of our proposed method.

In the second phase, a demonstration of the proposed authentication system was presented to the participant. The participant was guided through the enrolment and authentication phases so that the participant can familiarize himself/herself with the proposed method. The participant was then requested to create his/her own password and used the registered password to login. The login time was recorded by the system using a scripting language. The purpose of recording the login time is to study the average time taken by the participant to login using his/her password and our proposed method.

For final phase of testing, a successful login video was prepared and presented to each participant. We secured the registered images information before presenting the video. After that, another new challenge round was demonstrated in front of the participant. In this challenge round, the participant was advised to use his/her cell phone to record the entire authentication process. The participant was then given unlimited trials to login based on the video given. The participant can watch the pre-prepared video, use his/her record video and even request that the demonstrator show them the login process using an entirely new challenge set as many times as the participant required. At the end of the shoulder-surfing testing, the result was recorded.

For usability testing, we followed up with the participant a week after the participant has conducted the shoulder-surfing testing. Without any hints or information about the proposed method, the participant was requested to login using his/her registered images. The result of whether the participant can remember his/her registered images and our proposed method was recorded. We only followed up with those participants who can remember his/her registered images and our proposed method the subsequent week until the fourth week.

5. Results and Discussions

A total of 187 students from FCSIT, UM participated in this user study. The shoulder-surfing test showed that none of the participants were able to find the pass-images used to login. The results have proven that our proposed method is resistant to shoulder-surfing.

Our proposed method is a method that can resist both direct observation and video recorded shoulder-surfing methods compared to the reviewed methods (see Table 1). The authors used the concept of indirect input to prevent direct observation attack in CAS [26] and TI-IBA [27]. In related works by Por [24] and Haque & Imam [28], the researchers used the concept of partial registered images selection to prevent direct observation attack. However, the images can still be discovered when multiple login sessions are recorded and observed. After a period of time, attackers are able to filter out the decoy images used in every challenge set. In our work, we used digraph substitution rules and pass-image output feedback to prevent adversaries from finding the correct pass-images used in each challenge set. By using this proposed method, a shoulder-surfer is no longer able to identify the

pass-images used based on the digraph substitution rules. Therefore, it makes our proposed method robust against shoulder-surfing attackers. Nevertheless, we still need to ensure we had secured the registered images information during the enrolment procedure.

Table 1. Comparison Of The Related Work-Shoulder-Surfing Attack.

Graphical Authentication System	Resist Direct Observation	Resist Video Recorded Attack
Cognitive Authentication System (CAS) [26]	YES	NO
Temporal Indirect Image-Based Authentication (TI-IBA) [27]	YES	NO
Por [24]	YES	NO
Haque and Imam [28]	YES	NO
Proposed Method	YES	YES

Figure 11 shows the user memorability test result of our proposed method. About 49% of the participants can still remember their registered images and use our proposed method to login a week after they have completed the shoulder-surfing test. In week 2, the percentage drops to 36% followed by 23% and 11% in week 3 and week 4 respectively. The main reason behind the login failure is inability to remember the registered images and/or the proposed method. 87% of the participants reported that they could not remember our proposed method. 43% of the participants reported that they could not remember their registered images. Majority of the participants did feedback to us that the Scrabble images used in our password registration process are quite similar to alphanumeric password. The reason that they cannot recall their registered images during the user memorability test was because they used random images, which made them have difficulty to remember.

Figure 11. User memorability test result.

Passwords always comply two fundamental contradicted requirements where they must be secure and easy to remember [29]. From this study, we have found that there is a trade-off in our proposed method between the resistance of shoulder-surfing attack and user memorability. To improve the utility of passwords, we have introduced another function where the users are allowed to opt for using only the registered images to login or using our proposed method to login. We also included a user's manual to help the users to understand our proposed method better if they want to use the more secure method to login.

Table 2 shows the login time analysis for our proposed method. On average the login time taken for the participants to login using our proposed method are varied. The login time increased from 58.3 to 134.7 then 144.1 seconds for the first three weeks. There are few reasons that caused the login time to be varied. Due to the fact that the participants were guided at Week 0 to familiarize themselves with our proposed method, therefore, the login time at Week 0 is lesser compared to Week 1 and Week 2. After a week, most of the participants have forgotten their registered images and/or our

proposed method. As a result, the login time increased about 2 times. The same reason goes to Week 2. During Week 3 and Week 4, the login times decreased. According to the feedback of the participants, most of them already could recall and memorize their registered images and our proposed method respectively. This is the reason that allowed the participants to login faster at Week 3 and even 2.5 times faster at Week 4 compared to Week 3.

Table 2. Login Time Analysis.

Week	No. of Participant	Average Login Time (Second)
0	187	58.3
1	92	134.7
2	68	144.1
3	44	115.0
4	21	43.8

Table 3 summarizes the comparison of the mean time to login between the related works and the proposed method. The minimum mean time to login for the proposed method is shorter compared to system [26]. The main reason that the proposed system takes longer time for the users to login is due to the trade-off of the shoulder-surfing prevention method that has been proposed. Finding a balance to fulfil the two contradictory requirements of a password (password must be secure and easy to remember) is very challenging [5,17–19]. Since our main focus in this research work is to prevent shoulder-surfing attack, the issues of users spending longer time to login will not impact the significance of this paper. For future work, more usability studies will be conducted to improve the login time of the proposed method and user memorability.

Table 3. Comparison of Related Work-Mean Time To Login.

Graphical Authentication System	Mean Time to Login (Seconds)
CAS [26]	135.0 [10,26]
TI-IBA [27]	25.8 [27]
Por [24]	Not Available
Haque and Imam [28]	Not Available
Proposed Method	144.1 (max), 43.8 (min)

6. Conclusions

Figure 12 shows an example of an online banking application, which uses graphic to assist users to key in their password. Most of these online banking applications have one major weakness whereby if an attacker input a non-existent username in the system, these systems will not show any graphic/passphrase or they will show different graphic/passphrase although same username is used. Such online banking applications are defenseless to frequency of occurrence analysis and shoulder-surfing attacks because attackers can try out as many usernames as they want to determine whether the username exist in the system before they break the password. To break the password, the attacker can shoulder-surf the conventional password input by the users easily. Thus, it is crucial to have awareness on such security threat and propose a countermeasure towards these attacks.

Figure 12. An example of weak online banking system [30] that uses graphic to assist users to key in their passwords.

In this paper, we have presented, a new approach of shoulder-surfing resistance using digraph substitution rules and pass-image output feedback was proposed. Originally, we adopted digraph substitution rules from PlayFair cipher in our proposed method. However, it was insufficient to prevent shoulder-surfing attack after a preliminary study was conducted. As a result, we have improvised the rules so that it can meet the objectives of this research work.

After implementing our proposed method, we conducted a user study to evaluate our proposed method in terms of security and usability. The evaluation results proved that our proposed method is robust to both direct observation and video-recorded shoulder-surfing attacks. In terms of usability, the evaluation results were not sufficiently convincing. The reason most of the participants were not being able to recall their registered images was because they used random images, which made them have difficulty to remember their registered images. Moreover, many participants could not remember how our proposed method works. We also found out that the Scrabble images used did not incur burden for the participants to recall their registered images.

Passwords always comply two fundamental contradicted requirements where they must be secure and easy to remember [29]. From this study, we have found that there is a trade-off in our proposed method between the resistance of shoulder-surfing attack and user memorability. To improve the utility of passwords, we have introduced another function where the users are allowed to opt for using only the registered images to login or using our proposed method to login. We also included a user's manual to help the users to understand our proposed method better if they want to use the more secure method to login. With this feature, we do believe our proposed method can provide better protection against shoulder-surfing attack.

In the future, we will research on methods, which can use the dataset images to induce recall on the method and vice versa. We believe that the findings and effort in this study will contribute in the realm of graphical authentication.

Author Contributions: Conceptualization, L.Y.P. and C.S.K.; methodology, L.Y.P., T.F.A. and C.S.K.; software, C.S.K.; validation, L.Y.P., C.S.K. and T.F.A.; formal analysis, L.Y.P., C.S.K.; investigation, L.Y.P., T.F.A. and C.S.K.; resources, L.Y.P., C.S.K.; data curation, C.S.K.; Writing—Original draft preparation, C.S.K.; Writing—Review and editing, L.Y.P., T.F.A. and C.S.K.; visualization, C.S.K.; supervision, L.Y.P. and T.F.A.; project administration, C.S.K.; funding acquisition, L.Y.P.

Funding: This research was funded by BKP Special grant number BKS022-2018 from the University of Malaya, Malaysia and also Fundamental Re-search Grant Scheme (FRGS) grant number Fp114-2018A from the Ministry of Higher Education, Malaysia.

Conflicts of Interest: The authors declare no conflict of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript, or in the decision to publish the results.

References

1. Gokhale, A.; Waghmare, V. A Study of Various Passwords Authentication Techniques. *Int. J. Comput. Appl.* **2014**, (3), 1–5.
2. Text Password Survey: Transition from First Generation to Second Generation. Available online: <http://blogs.ubc.ca/computersecurity/les/2012/04/Text-Password-SurveyGAYA.pdf> (accessed on 20 April 2017).
3. Tank, H.; Harsora, V. A Survey on Secure Virtual Password and Phishing Attack. In Proceedings of the 4th International Conference on Computer Science and Information Technology (ICCIT 2015), Gujarat, India, 1–15 March 2015.
4. 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*, 838623. [CrossRef] [PubMed]
5. Elftmann, P. Secure Alternatives to Password-Based Authentication Mechanisms. Diploma Thesis, Laboratory for Dependable Distributed Systems RWTH Aachen University, Aachen, Germany, 2006.
6. Golar, P.C.; Adane, D.S. Critical analysis of 2-dimensional graphical authentication systems. In Proceedings of the 2016 International Conference on Computing, Analytics and Security Trends (CAST), Pune, India, 19–21 December 2016.
7. Bhanushali, A.; Mange, B.; Vyas, H.; Bhanushali, H.; Bhogle, P. Comparison of Graphical Password Authentication Techniques. *Int. J. Comput. Appl.* **2015**, *116*, 11–14. [CrossRef]
8. Jermyn, I.H.; Mayer, A.; Monroe, F.; Reiter, M.K.; Rubin, A.D. *The Design and Analysis of Graphical Passwords*; USENIX Association: Berkeley, CA, USA, 1999.
9. Chiasson, S.; Paul C.; Van Oorschot, P.C.; Biddle, R. Graphical password authentication using cued click points. In *European Symposium on Research in Computer Security*; Springer: Berlin/Heidelberg, Germany, 2007; pp. 359–374.
10. Biddle, R.; Chiasson, S.; Van Oorschot, P. Graphical passwords: Learning from the first twelve years. *J. ACM Comput. Surv.* **2012**, *44*, 19–41. [CrossRef]
11. Gao, H.C.; Wei, J.; Ye, F.; Ma, L.C. A survey on the use of graphical passwords in security. *J. Softw.* **2013**, *8*, 1678–1698. [CrossRef]
12. Por, L.Y.; Ku, C.S.; Amaul, I.; Ang, T.F. Graphical password: Prevent shoulder-surfing attack using digraph substitution rules. *Front. Comput. Sci.* **2017**, *11*, 1098–1108. [CrossRef]
13. 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.
14. Simha, T.S.; Srinivasulu, D. Pass Matrix checks for Login Authentication. *Int. J. Comput. Sci. Trends Technol.* **2017**, *5*, 5–13.
15. Khedr, W.I. Improved keylogging and shoulder-surfing resistant visual two-factor authentication protocol. *J. Inf. Secur. Appl.* **2018**, *39*, 41–57. [CrossRef]
16. Dhamija, R.; Perrig, A. Deja Vu: A User Study Using Images for Authentication. In Proceedings of the 9th USENIX Security Symposium, Denver, CO, USA, 14–17 August 2000.
17. The Science Behind Passfaces. Available online: <http://www.realuser.com/published/ScienceBehindPassfaces.pdf> (accessed on 20 April 2017).
18. Wiedenbeck, S.; Waters, J.; Sobrado, L.; Birget, J.C. Design and evaluation of a shoulder-surfing resistant graphical password scheme. In Proceedings of the Working Conference on Advanced Visual Interfaces, Venezia, Italy, 23–26 May 2006.
19. 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, Melbourne, Australia, 26–30 November 2012.
20. Sonal, G.; Poonam, K.; Ketaki, M.; Bhagyashri, S. Shoulder Surfing Resistant Graphical Password Scheme. *Int. J. Sci. Res. Dev.* **2015**, *3*, 105–111.
21. Kolay, R.; Vora, A.; Yadav, V. Graphical Password Authentication Using Image Segmentation. *Int. Res. J. Eng. Technol.* **2017**, *4*, 1694–1698.

22. Dhandha, C. Parekh: Enhancement of Password Authentication System Using Recognition based Graphical password for web Application. *Int. J. Adv. Res. Comput. Sci.* **2017**, *8*, 1135–1138.
23. Yu, X.; Wang, Z.; Li, Y.; Li, L.; Zhu, W.T.; Song, L. EvoPass: Evolvable graphical password against shoulder-surfing attacks. *Comput. Secur.* **2017**, *70*, 179–198. [CrossRef]
24. Por, L.Y. Frequency of occurrence analysis attack and its countermeasure. *Int. Arab J. Inf. Technol.* **2014**, *10*, 189–197.
25. William, S. *Cryptography and Network Security: Principles and Practice*, 4th ed.; Prentice Hall: Upper Saddle River, NJ, USA, 2006.
26. Weinshall. Cognitive authentication schemes safe against spyware. In Proceedings of the IEEE2006 Symposium on Security and Privacy, Berkeley/Oakland, CA, USA, 21–24 May 2006.
27. Yamamoto, T.; Kojima, Y.; Nishigaki, M. A shoulder-surfing resistant image-based authentication system with temporal indirect image selection. In Proceedings of the International Conference on Security and Management, Las Vegas, NV, USA, 13–16 July 2009; pp. 188–194.
28. Haque, M.A.; Imam, B. A New Graphical Password: Combination of Recall & Recognition Based Approach. World Academy of Science, Engineering and Technology. *Int. J. Comput. Electr. Autom. Control Inf. Eng.* **2014**, *8*, 320–324.
29. 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.
30. Maybank2u: An Online Banking System. Available online: <https://www.maybank2u.com.my/home/m2u/common/login.do> (accessed on 24 August 2019).

© 2019 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0/>).