SHOULDER SURFING RESISTANCE USING PENUP EVENT AND NEIGHBOURING CONNECTIVITY MANIPULATION

Por Lip Yee, Miss Laiha Mat Kiah
Department of Computer System and Technology
Faculty of Computer Science and Information Technology
University of Malaya, 50603 Kuala Lumpur, Malaysia.
porlip@um.edu.my, misslaiha@um.edu.my

ABSTRACT

Picture-based password has been proposed as an alternative authentication method to replace text-based password. Ensuring the security of picture-based password is not a simple task as picture-based objects are a lot easier to access and remember and can thus be easily guessed. In particular, shoulder surfing attack still remains as the main security threat encountered by many picture-based password authentication schemes, especially in drawmetric authentication scheme. In this paper, a novel shoulder surfing resistance mechanism has been proposed and evaluated. The proposed mechanism utilises penup event and neighbouring connectivity manipulation into a revised Background Pass-Go scheme. From the evaluation result, it has proven that the proposed mechanism achieves better results in resisting shoulder surfing attack while, at the same time, allowing a larger password space.

Keywords: Picture-Based Password, Graphical Authentication, Shoulder Surfing, Drawmetric, Background Pass-Go

1.0 INTRODUCTION

According to the authors in [10, 26], an authentication scheme can be classified into token-based, biometric-based and knowledge-based schemes. In the token-based authentication scheme, a token or an object, such as a key card, RFID card, bank card or a smart card, is used as an instrument for an authorised verification. It means that anyone who obtains a valid token can immediately gain access to resources regardless whether or not he is an authorised user. As a consequence, a biometric-based authentication scheme has been proposed to alleviate the legitimate identity issue.

The biometric-based authentication scheme uses personal and physiological characteristics of an authorised user, such as fingerprints, iris scan, speech and facial recognition to perform verification. It is undeniable that a biometric-based authentication scheme is more secure compared to the token-based authentication scheme in terms of identifying the lawful user's identity. However, the biometric-based authentication scheme is still not widely adopted due to some major drawbacks such as the exorbitant development cost required for setting up and maintaining such a system. Moreover, most biometric-based authentication schemes suffer from slow performance and often produce highly unreliable rate during an identification process [26]. For instance, most voice authentication schemes produce high error rates when tested in a noisy environment while the facial recognition schemes are still sensitive to variations in lighting conditions during verification, and fingerprint readers can be deceived by fake fingerprints [16]. As such a knowledge-based authentication scheme has been proposed.

In the knowledge-based authentication scheme, a user applies factoid recall element (something which a user knows) such as date of birth, mother's maiden name, car registration number, mobile phone number, as well as favourite items such as football player's or soccer club names, artist names, colour, and so forth, as passwords and PINs. One of the reasons that the knowledge-based authentication scheme turns out to be an accepted scheme is due to its ability to provide a fast and acceptable authentication process rate as compared to biometric-based schemes. In addition, most knowledge-based authentication systems do not require users to undergo a long or intensive training session compared with biometric-based authentication schemes during the first deployment [10].

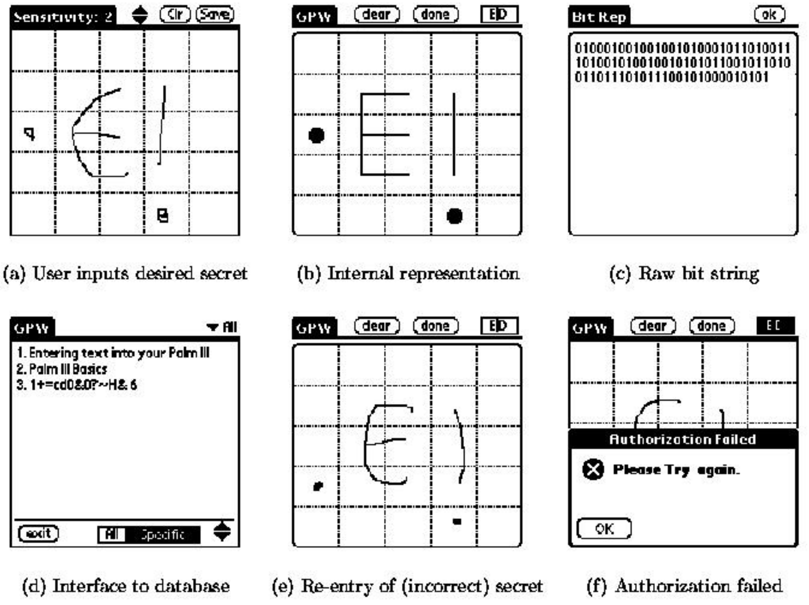
In the knowledge-based authentication scheme, there are two main categories: text-based passwords and picture-based passwords. Text-based passwords use alphanumeric characters as passwords or PINs. However, due to the challenge of achieving higher security level as mentioned in various reports [2, 5, 13, 14, 18], several policies and good password practices for text-based passwords have been suggested [3, 4, 12, 13, 17]. Since the main focus of this research is on the picture-based password authentication scheme, earlier schemes will not be discussed further.

The idea of a picture-based password authentication scheme was pioneered by Greg Blonder who also holds the US patent 5559961 in 1996. Throughout the years, various picture-based password schemes have been proposed to exploit the utility of pictures or images for user authentication. In 2005, De Angeli and her research partners proposed a cluster of three categories (locimetrics, drawmetrics and cognometrics) for classifying picture-based password authentication [1]. The terminology and description for cognometrics, locimetrics, and drawmetrics have been expanded by Moncur and Lepalâtre in 2007 [18] and the cognometrics terminology has been revised to searchmetrics by Karen and De Angeli in 2009 [27]. According to the authors in [1, 18], a locimetric system is a mnemonic system which enables a user to identify any relevant points or objects with or without the aid of various recalling methods when performing an authentication. In the drawmetric authentication scheme, users are required to draw a preset outline figure on a grid. The position, sequence, as well as the visual appearance of a redrawing, are then used as the analysis metrics for users' verification. In searchmetric authentication scheme, users are required to identify 'target' images/icons/symbols (which have been identified by the users during their password creation stage) along with a set of distracter images/icons/symbols for an authorised authentication [8, 18, 27].

Currently, existing picture-based password authentication schemes especially those from drawmetric authentication schemes fail to address the issue of shoulder surfing security threat [20, 21, 22]. As a result, a drawmetric authentication scheme that utilises pen up event and neighbouring connectivity manipulation has been proposed to address the aforementioned issue.

The remainder of this paper is organised as follows. Section 2 presents an analysis of numerous drawmetric authentication schemes and Section 3 presents the design of the proposed scheme as well as its encoding mechanism. In Section 4 and 5, the experimental results and analysis are discussed. Finally, a discussion section and conclusion are presented to summarise the deliverables of the proposed scheme.

2.0 RELATED WORK



```
010001001001001010001011010011
101001010010010101011001011010
01101110101110010100001010 1
```

1. Entering text into your Palm III
2. Palm III Basics
3. 1+=cd0&0?~H& 6

Please Try again.

(a) User inputs desired secret (b) Internal representation (c) Raw bit string

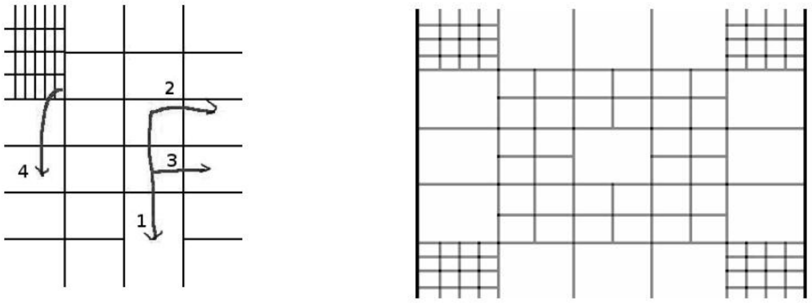
(d) Interface to database (e) Re-entry of (incorrect) secret (f) Authorization failed

Fig. 1: Draw A Secret Scheme (adapted from [11])

In 1999, Ian Jermyn and friends proposed a well-known drawmetrics scheme named Draw A Secret (DAS) [1, 11]. DAS is a pure recall picture-based password scheme. According to the authors in [8], in pure recall based picture-based password schemes, a user is required to reproduce his/her password without being given any hints or cues. During the password creation phase, users are allowed to create their password by drawing a free-form image or other figures on a grid. According to [20, 21, 22], the underlying algorithm for DAS scheme involves storing the coordinates of grid cells where the user puts his pen down, draws a line and then lifts his pen up. A bit-string will be generated from the drawing based on each pen up value. The bit-string will then be hashed using a one-way hash function before storing in a system. For an authorised verification, users are required to redraw the image or figure which can produce the same hash value as stored in the system within an acceptable tolerance preset by the system (Refer to Figure 1).

According to previous studies [20, 21, 22], the DAS scheme is able to increase user memorability by enabling the users to draw the images or figures based on their familiarity rather than remember any kind of meaningless and unfamiliar alphanumeric string. Besides, these studies [20, 21, 22] mentioned that the DAS scheme is able to provide better security protection against attackers due to its ability to derive a secret key to encrypt and decrypt a user's password before storing the password into a device. As a result, the user's password or the encrypted content can be protected from attackers even if the device falls into the attackers' hands. Based on the raw size testing result obtained from [11], it was shown that the password space for the DAS scheme with the number of passwords length ≥12 is already greater than the password space of a textual password since it only consists of 8 characters or less as constructed from the printable ASCII codes ($95^8 \approx 2^{53}$) [11].

However, [20, 21, 22] noted several limitations in the DAS scheme: (1) There is still a risk for the attackers to gain access to the device if the attackers obtained a copy of the stored secret, and, brute force attacks can be launched by trying all possible combinations of grid coordinates. (2) The scheme is vulnerable to shoulder surfing attack if a user accesses the system in public environments. The password keystrokes of a user can also be recorded and used later by the attacker to gain access to the device. The password keystrokes of a user can be recorded and used by an attacker to gain access to the device. (3) Supported by cognitive studies and literature [9, 19], users are inclined to create centred and symmetrical passwords to ease their memorability. This behaviour has increased the tendency for attackers to identify the users' password. (4) Drawing a diagonal line and identifying a starting point from any oval shape figure using the DAS scheme itself can be a challenge for the users. (5) Difficulties might arise when the user chooses a drawing which contains strokes that pass too close to a grid-line, thus, the scheme may not be able to distinguish which cell the user is choosing [20, 21, 22]. (6) The scalability of the DAS scheme is restricted by small cells' size (5x5 grid cells) that further sacrifices other aspects, such as ease of inputting passwords, restricts freedom of choosing passwords as well as reduces the memorable password space and its security level [20, 21, 22].



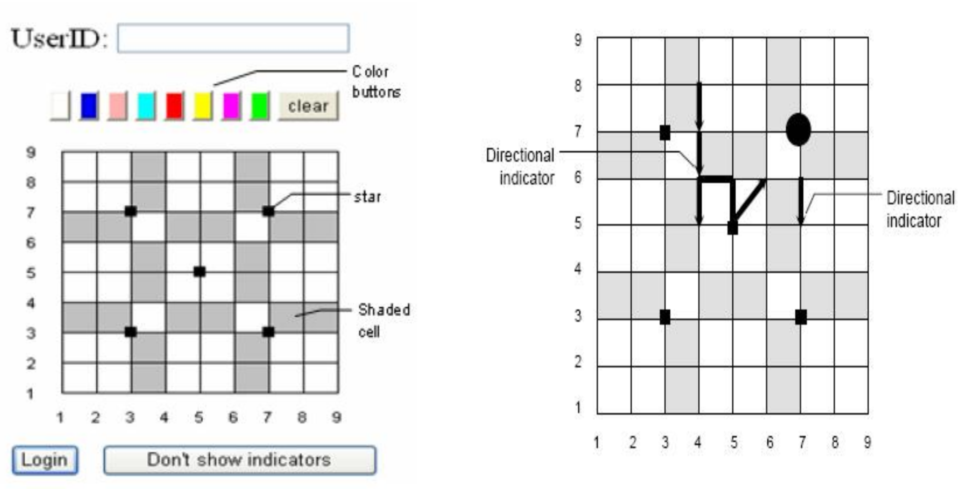
a) A Multi-Grid Password Example

b) A Multi-Grid Template

Fig. 2: Multi-Grid DAS Scheme (adapted from [7])

The Multi-Grid DAS scheme has been proposed by Konstantinos Chalkias, Anastasios Alexiadis, and George Stephanides in 2006 (Refer to Figure 2 (a) and (b)). The Multi-Grid DAS scheme enhanced the DAS scheme by enabling the users to draw their images or figures on a different grid cell size. The users are given an option to choose a predefined Multi-Grid template to draw their password and the final password produced by the scheme can be composed from several internal grids. According to [7], the purpose of proposing the different grid cell size is to reduce users from creating passwords which are centred. In the Multi-Grid DAS scheme, users are allowed to focus on a single internal grid or a nested grid. As a result, an attacker has to use even harder massive brute-force techniques to find the password used due to the various neighbouring cells utlized [7].

From the survey results carried out in [7], the Multi-Grid DAS scheme managed to reduce the shift errors issue made by the users. The results, however, left the ordering error unchanged. From this aspect, it was proven that users still have difficulty memorising the correct order of their drawn passwords.



a) Pass-Go Scheme GUI

b) Indicators

Fig. 3: Pass-Go Scheme (adapted from [23, 24])

In 2006, inspired by Go (an old Chinese chess game), Hai Tao has proposed a scheme named Pass-Go (Refer to Figure 3 (a)). According to [23, 24], Pass-Go is an enhanced version of the DAS scheme based on a coordinate system with 9x9 grid cells. In the Pass-Go scheme, a user is required to select or touch on the intersections of the grid cells instead of cells when creating a password. In this scheme, users can create passwords using only dot indicator [23]. A dot indicator will appear when one intersection point is selected (or clicked) and a line indicator will appear when two or more intersections are touched continuously (Refer to Figure 3 (b)). However, an intersection (dot or line) can only be created if a user is able to select the intersection within an acceptable sensitive area. A matrix which consists of an intersection coordinate will be generated after each dot or line indicator has been created. The generated coordinates will then be hashed and used as the password verification and authentication.

According to [21, 23, 24], the Pass-Go scheme is able to achieve stronger security and better usability compared to DAS scheme. Users of the Pass-Go scheme are able to draw a shape more freely compared to DAS scheme. A different colour scheme, star and shaded cells have been used as a cue in the Pass-Go scheme to increase the usability and memorability of a user. Apart from that, the analysis result obtained from [23, 24] proved that the Pass-Go scheme (Pass-Go-5) with 5x5 grid cells offers larger password space as compared to the DAS scheme.

Despite the advantages, the Pass-Go scheme does have some limitations such as: (1) Users will get used to creating weak passwords that tend to be either symmetrical or centred. (2) When trying to prevent shoulder surfing attack, users might face difficulty in creating passwords once they choose sensitive areas to be invisible. This is because users will not know if their password has been successfully selected until the dot or line indicator appears. (3) There is a learning curve for users to practise using the Pass-Go scheme before they are able to draw lines without making any unintentional errors.

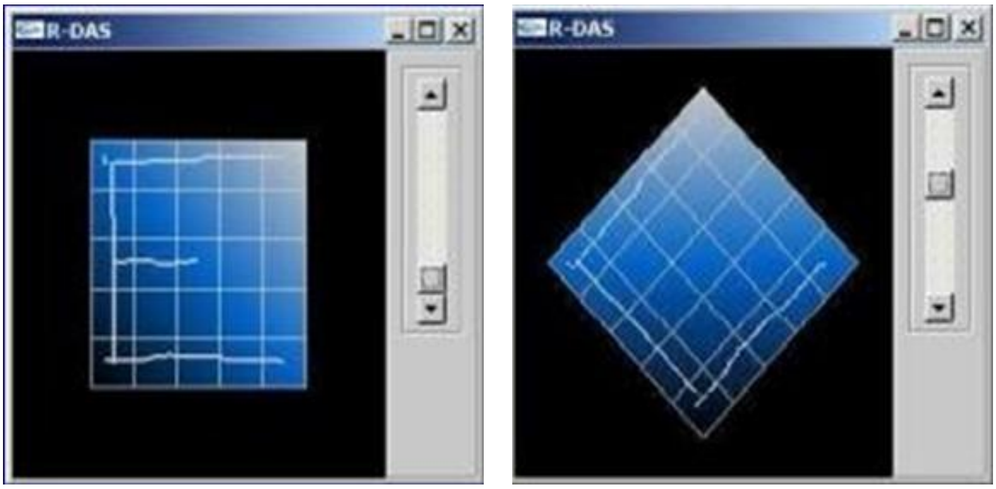


Fig. 4: DAS with Rotation Scheme (adapted from [6])

In 2007, Saikat Chakrabarti, George V. Landon and Mukesh Singhal, proposed another hybrid method called DAS with Rotation (R-DAS) which allows users to rotate the canvas of a drawn password on the z-axis in clockwise or anticlockwise motion (Refer to Figure 4). According to [20, 21, 22], R-DAS inherited all DAS scheme features in addition to extra rotation angles (clockwise direction: 45, 90, 135, 180, 225, 270, 315 and 360 degrees, anticlockwise direction: -45, -90, -135, -180, -225, -270, -315 and -360 degrees). Based on the analysed result from [29], R-DAS not only increases the full password space, but also increases the predictable password space corresponding to the number of components (strokes). With the aid of rotation technique and full password space utilisation, the R-DAS scheme is able to provide greater security than the DAS scheme if both schemes are using an identical grid size (i.e. with 5x5 grid cells). However, the R-DAS scheme faces a bigger challenge compared to the DAS scheme in terms of memorability aspect due to the extra rotation angle information that has to be memorised by the users [20, 21, 22]. To date, there are no findings on the memorability of the R-DAS scheme.

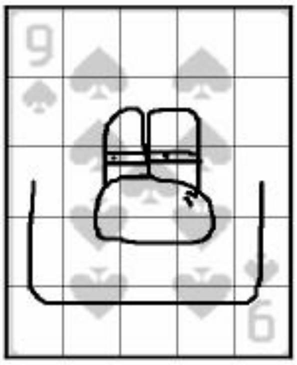


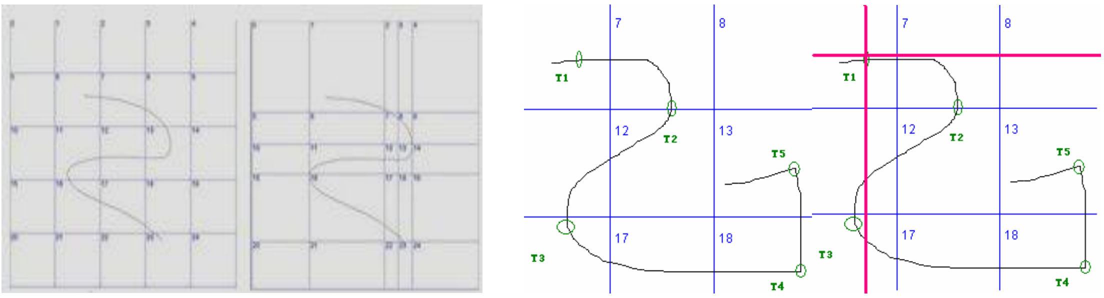
Fig. 5: Background Draw a Secret Scheme (adapted from [9])

In 2007, Paul Dunphy and Jeff Yan from Newcastle University proposed a scheme named Background Draw a Secret (BDAS). The mechanism of the BDAS scheme is exactly the same as the DAS scheme except with an aid of a background image superimposed over the blank DAS grid (Refer to Figure 5).

According to [9, 20, 21, 22], the advantages of superimposing a background over the blank DAS grid is to (1) help the users achieve better memorability, (2) alleviate problems such as difficulty in identifying a password starting point, (3) encourage the users to draw a more complicated password with larger stroke count or length, and (4) dissuade the users from creating a password which has less symmetrical or centre cognitive behaviour.

However, BDAS scheme may encounter issues and challenges such as (1) maintaining and managing the capacity of the data storage as the scheme enables a user to upload unlimited background images in various sizes.

In terms of (2) performance and (3) the quality of the background image used, the system downloading time will be unnecessarily extended for a dedicated user if the background image used by the user is sufficiently large. On the other hand, if the background image used is sufficiently distorted due to low quality image resolution, a user might have difficulty in creating his/her password. As a result, the user might create a symmetrical or centre password as in the DAS scheme which defeats the purpose of the BDAS scheme. Furthermore, (4) BDAS scheme is not able to resist shoulder surfing security threats.



a) Dynamic Grid b) Grid Transformation

Fig. 6: Qualitative Draw A Secret Scheme (adapted from [15])

Di Lin and his colleagues proposed Qualitative Draw A Secret (QDAS) in 2007. QDAS is an enhanced scheme for DAS and it works the same way as in DAS scheme [15]. According to Lin et al., (2007), the QDAS scheme deployed a different encoding mechanism for each keystroke produced by the users. An integer index was predefined and assigned to each grid cell. Each password produced by a user consists of the starting stroke in a grid cell together with the sequence of qualitative direction changes in the stroke relative to the grid [15]. (A qualitative direction change is denoted by the authors as a direction change when a line indicator crosses over a grid cell boundary.) In order to be authorised, a user is required to recreate the password which manages to fabricate the correct grid index value and the correct order of qualitative direction change.

To increase the level of protection against shoulder surfing attack, the QDAS scheme deploys a masking mechanism named dynamic grid transformations throughout the process of the password creation phase. To generate the dynamic grid, a set of turning points for a stroke is calculated. The coordinate of the stroke will then be used to form two perpendicular lines that intersect at the current turning point. The formation of the two perpendicular lines that intersect at the next turning point are carried out until a 5x5 grid cells is produced (Refer to Figure 6 (a)).

In order to prevent users from producing a password or stroke which has no turning point, the QDAS scheme has randomly identified four random points from the stroke and performed the aforementioned dynamic grid transformations. The dynamic grid transformations method is able to increase the size of the password to an acceptance level if a user is creating a small or undersized password (Refer to Figure 6 (b)).

Based on the preliminary empirical study conducted by [15], QDAS scheme is able to achieve better outcomes compared to the DAS scheme in terms of usability and shoulder surfing resistance. However, the result obtained by the authors is not as significant due to the small sampling size used (i.e., only 10 subjects was used to evaluate QDAS scheme towards DAS scheme). The study also failed to obtain a positive outcome for memorability testing.

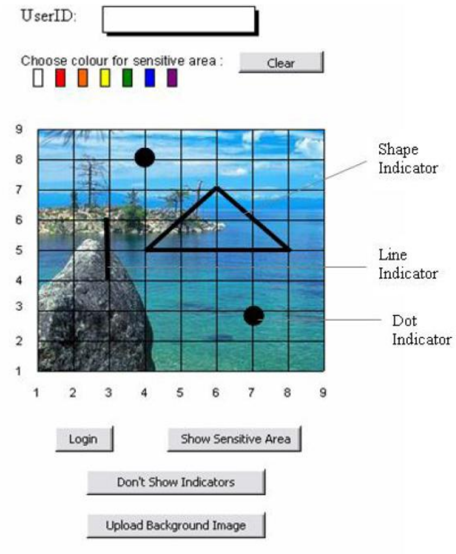


Fig. 7: Background Pass-Go (adapted from [22])

[22] proposed a Background Pass-Go (BPG) scheme in 2008 (Refer to Figure 7.). According to the study, the development of the BGP scheme was inspired by the DAS, Pass-Go and BDAS schemes. The main difference between the BPG scheme and the Pass-Go scheme is that the BPG scheme enables users to personalise their background picture that works as a cue in achieving better user memorability. Moreover, the personalised background picture feature used enables users to avoid creating weak passwords with symmetrical or centred elements. In this scheme, the server does not keep a copy of users' background picture but it is available at the client's side. This allows users to use any picture to his/her liking from the local hard drive or portable storages. Moreover, intruders or attackers are not able to launch hotspots analysis attack since they have no information about the background image used. However, any image used by a user has its particular areas that "draw the eye" or that are preferable to each user [28]. As a result, BPG is possible to encounter hotspots attack if the background image has been obtained by the attackers.

In regards to the aspect of sensitive area when creating the passwords, BPG scheme uses slightly smaller sensitive area size, 0.30×d (d is the side length of a grid cell), for drawing its indicators. However, the BPG scheme is still using the same shoulder surfing prevention method as in the Pass-Go scheme where users might face difficulty in creating a password once they choose the sensitive areas to be invisible.

Table 1 shows the synthesis result for the drawmetric research. From the table, it shows that only the Pass-Go scheme and the BPG scheme are able to prevent shoulder surfing security threats. As mentioned previously, the idea of resisting the challenge of shoulder surfing attack by securing entire activities of an authentication process might be useful to actually prevent the shoulder surfing attack. As a trade-off, however, this will definitely decrease user memorability. As a result, falsifying the authentication process to the shoulder surfing attacker is likely to provide a better option to alleviate or reduce the shoulder surfing attack. Thus, a novel shoulder surfing resistance mechanism that utilises pen up event and neighbouring connectivity manipulation was proposed.

Table 1: Synthesis Results

Drawmetrics Authentication Scheme		**Password Space**	**Memorability**	**Shoulder Surfing Attack**
Pure Recall	Draw A Secret	▪ Infinite password space However, the password space is dependent on the number of keystroke produced by a user.	▪ Depends on the keystroke produced by a user. ▪ Easy if uses i) less strokes and ii) centred and symmetry drawing. ▪ Difficult if uses i) more and complex strokes and ii) non-centred and symmetry drawing.	×
	Multi-Grid DAS	▪ Infinite password space ▪ However, it has larger password space compared to DAS scheme The password space is dependent on the number of keystroke produced by a user.	▪ Same as DAS scheme although a drawing produced by a user is less centred and symmetry.	×
	DAS with Rotation	▪ Same as DAS scheme	▪ Depends on the keystroke produced by a user. ▪ However, the user memorability level will be reduced compared to DAS scheme due to the fact that a user is required to remember extra rotation parameters used.	×
	Qualitative Draw A Secret	▪ Same as DAS scheme	▪ Depends on the keystroke produced by a user. ▪ However, the user memorability level declined compared to DAS scheme [15].	×
Cued Recall	Background Draw a Secret	▪ Same as DAS scheme	▪ Depends on the keystroke produced by a user. ▪ However, the user memorability level will be increased compared to DAS scheme due to the implementation of the cue background image technique [9].	×
	Pass-Go	▪ Larger password space compared to DAS scheme [23] ▪ Infinite password space However, the password space is dependent on the number of keystroke produced by a user.	▪ Depends on the keystroke produced by a user. ▪ Different colour scheme, star and shaded cells have been used as a cue in Pass-Go scheme to increase the usability and memorability of a user. ▪ Easy if uses i) less strokes ii) centred and symmetry drawing. ▪ Difficult if uses i) more and complex strokes and ii) non-centred and symmetry drawing.	√ Using hide function However, users will have difficulty identifying the password since it is invisible
	BPG	▪ larger password space compared to Pass-Go scheme ▪ Infinite password space However, the password space is dependent on the number of keystroke produced by a user.	▪ Depends on the keystroke produced by a user. ▪ Easy if uses fewer strokes. However, BPG scheme is able to minimise the centred and symmetrical drawing with the aid of the personalised background image feature. ▪ Difficult if uses more and complex strokes ▪ Uses different colour scheme and personalised background image features as cue techniques to increase the usability and memorability of a user.	√ Same As Pass-Go scheme

3.0 PROPOSED METHOD

Figure 8 shows the GUI Design of the revised BPG scheme. In order to strengthen the user memorability and increase the challenge of shoulder surfing attack, the majority of components of the BPG scheme except the cue colour scheme and the encoding mechanism have been revised.

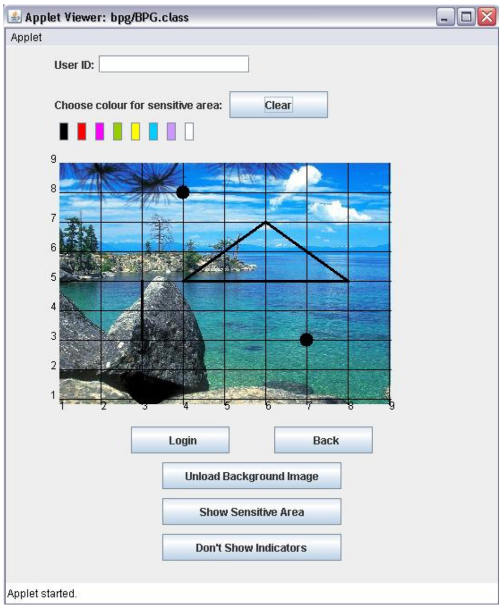


Fig. 8: Revised Background Pass-Go GUI Design

3.1 Cue Colour Scheme

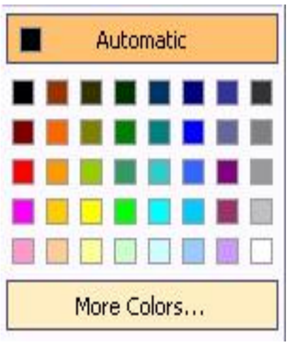


Fig. 9: Font Colour Scheme in the Microsoft Office Word 2003

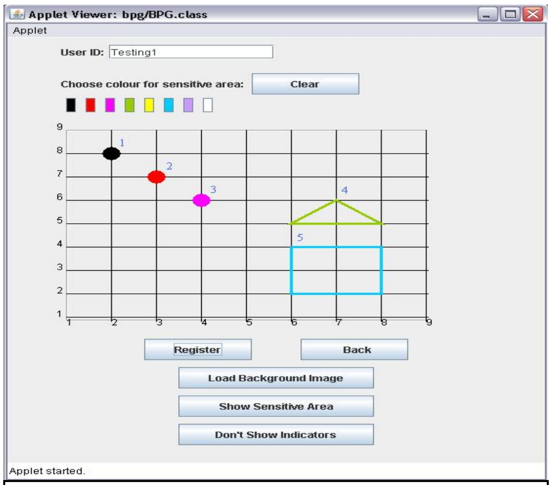
As an important element in Human Visual Sensory (HVS) system, colour not only can be used as a significant factor to strengthen the security, but also as a cue to help improve user memorability [24]. There are 40 colours identified in Microsoft Office Word 2003 (as indicated in Figure 9). The reason for choosing this colour scheme is that all computers in the Faculty of Computer Science and Information Technology (FCSIT), University of Malaya (UM), Malaysia, are equipped with Microsoft Office Word 2003 since 2005. This is considered to be one of the important factors for doing the research. As the survey result showed, all 250 participants are familiar with the colour scheme used in Microsoft Office Word 2003. In order to model and enhance the Pass-Go and the BPG schemes for achieving better user memorability, a brand new colour scheme was identified based on the survey result. Eight colours were identified based on the order of highest user preferences and their RGB (red, green and blue) values presented in Table 2. As in the BPG scheme, black colour was selected as the default colour. To create a password, a user was allowed to use at least one to a maximum of eight colours. The generated RGB values were included in the revised BPG password encoding processes.

Table 2: Colour Code and Its RGB Value

Colour	RGB value
⬛	[0,0,0]
🟥	[255,0,0]
🟪	[255,0,255]
🟩	[153,204,0]
🟨	[255,255,0]
🟦	[0,204,255]
🟪	[204,153,255]
⬜	[255,255,255]

3.2 Encoding Scheme

The revised BPG scheme uses a slightly different encoding scheme as compared to the BPG scheme and the Pass-Go scheme. A password produced by the revised BPG scheme consists of a sequence of intersections. Each intersection fabricates the encoding of (x,y,[r,g,b]) where the values of x and y respectively refer to the two-dimensional coordinate pair of the intersection that exists in the G×G grid cells (G is the size of the grid used) and the [r,g,b] refer to the red, green and blue colour components of the predefined colour scheme used in the revised BPG scheme. In order to indicate a penup event, the symbol {} is used. Thus, the revised BPG encoding scheme can be denoted as $\sum_{(x,y)\in[1..G]\times[1..G]}(x,y,[r,g,b]) \in \{\}$. Figure 10 shows the password encoding generated by the revised BPG scheme.



Applet Viewer: bpg/BPG.class

Applet

User ID: Testing1

Choose colour for sensitive area:

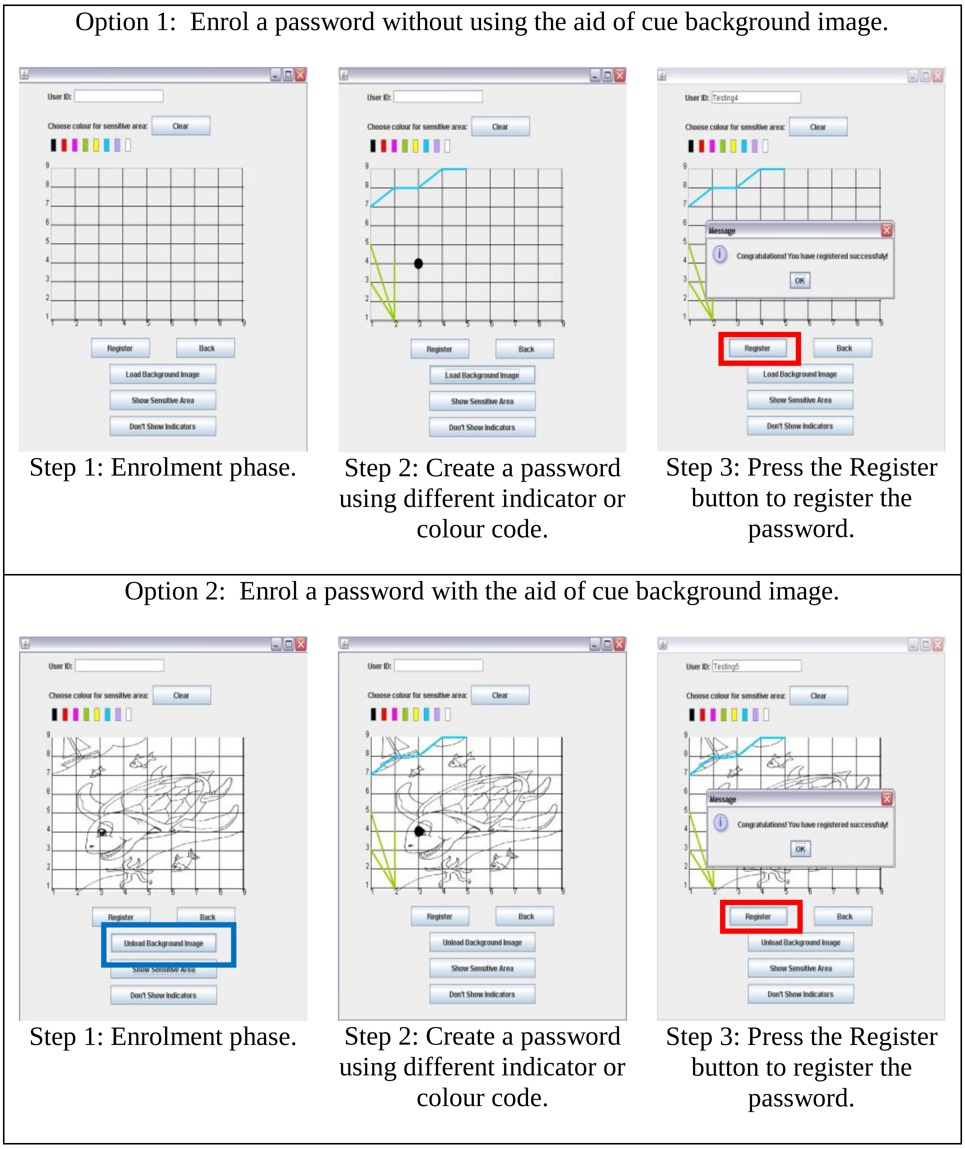
Applet started.

(2,8,[0,0,0])(3,7,[255,0,0])(4,6,[255,0,255])\{(7,6,[153,204,0])(6,5,[153,204,0])(7,5,[153,204,0])(8,5,[153,204,0])(7,6,[153,204,0])}{(6,4,[0,204,255])(6,3,[0,204,255])(6,2,[0,204,255])(7,2,[0,204,255])(8,2,[0,204,255])(8,3,[0,204,255])(8,4,[0,204,255])(7,4,[0,204,255])(6,4,[0,204,255])}

Fig. 10: Password Encoding for the revised BPG Scheme

3.3 ENROLMENT AND AUTHENTICATION

Initially, as in the BPG scheme, the revised BPG requires the users to create their passwords using dots, lines and shape indicators or a mixture of these. Users are allowed to personalise their colour code when drawing their password. After the users confirm the password, a set of password encoding is generated. The generated password encoding is hashed and stored in the database at the end of the enrolment phase. Figure 11 shows the password enrolment phase for the revised BPG scheme. Details of the indicator creation can be obtained from [21 and 22].



Option 1: Enrol a password without using the aid of cue background image.

Step 1: Enrolment phase.

Step 2: Create a password using different indicator or colour code.

Step 3: Press the Register button to register the password.

Option 2: Enrol a password with the aid of cue background image.

Step 1: Enrolment phase.

Step 2: Create a password using different indicator or colour code.

Step 3: Press the Register button to register the password.

User ID: Testing4

User ID: Testing5

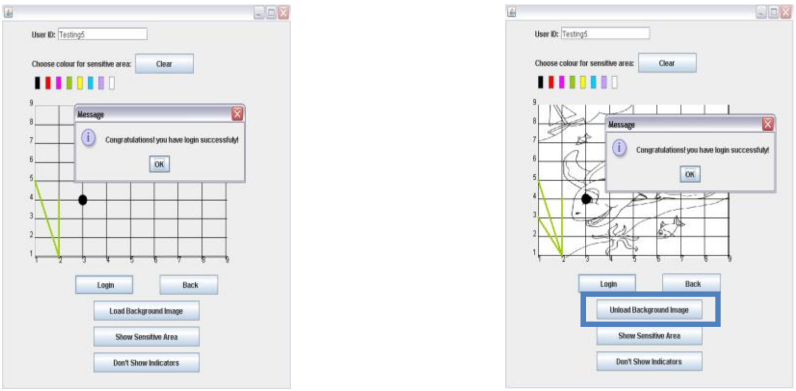
Message

Congratulations! You have registered successfully!

Fig. 11: Password Enrolment Phase

For authentication, users are required to identify the correct colour code together with the correct sequence order of the indicators used during the enrolment phase before they are allowed to gain access to the system. Users are also able to hide a part of, or the whole, password created without revealing the sensitive areas (as shown in Figure 12). If a user fails to be authenticated after three continuous attempts, his/her account will be blocked by the system. Figure 13 shows the enrolment and authentication flow chart for the revised BPG scheme.

Hide a part of the password using “Hide Function” during authentication phase.



User ID: Testing5

Choose colour for sensitive area:

Message

Congratulations! you have login successfuly!

a) without cue background image

b) with cue background image

Fig.12: Login Using “Hide Sensitive Areas Function”

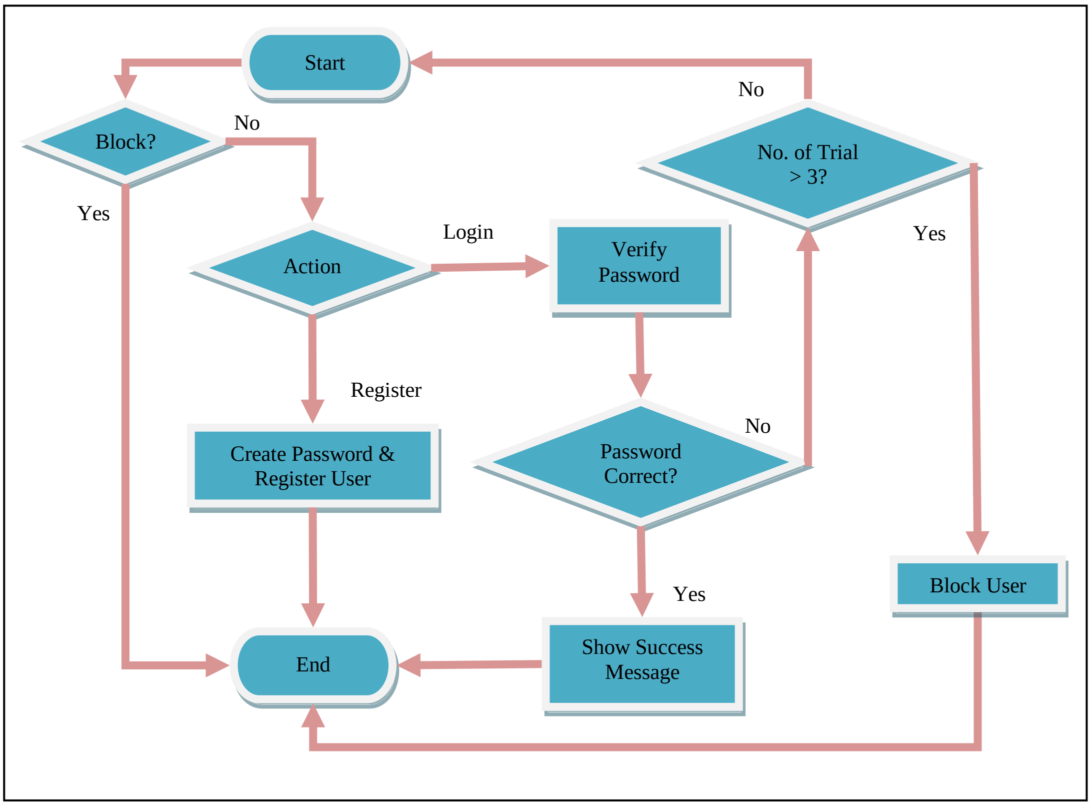


Fig.13: Revised BPG Flow Chart

4.0 SHOULDER SURFING ANALYSIS AND PRELIMINARY RESULT

In order to test and verify whether the revised BPG scheme is able to mislead a shoulder surfing attacker from identifying and obtaining the correct password of a user, a test consisting of 100 participants was carried out in the FSCIT, UM. In a group of five, the participants were instructed to perform the shoulder surfing attack task. In order to identify whether varying competency levels or gender will affect the result, the participants were classified based on postgraduate, undergraduate students and their gender.

To prove this concept, a case study was conducted, as follows: 10 groups of postgraduate students were identified and grouped according to male (Group No. 1, 2, 3, 4 and 5) and female groups (Group No. 6, 7, 8, 9 and 10). Another 10 groups of undergraduate students were assigned to the following groups, respectively (Male groups: No. 11, 12, 13, 14 and 15. Female groups: No. 16, 17, 18, 19 and 20). An authorised user with username *testing2* along with the following password encoding was generated:
{(3,5,[0,0,0])(5,7,[0,0,0])(6,5,[0,0,0])}{(6,5,[0,0,0])(5,4,[0,0,0])(4,3,[0,0,0])(3,5,[0,0,0])}.

Figure 14 shows the GUI for the password created using the above-mentioned password encoding.

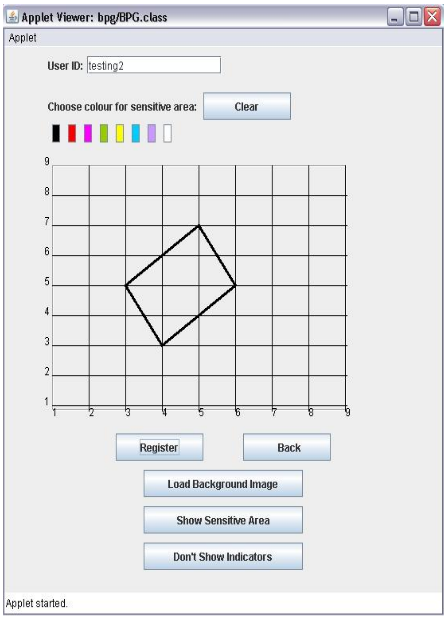

User ID: testing2

Fig. 14: A Password Created Using the Predefined Password Encoding

After finalising the students into groups, the role of the identified students were explained before a demonstration of the login process was done. Each shoulder surfer group was given three continuous attempts to identify, discuss and guess the password used by the user named *testing2*. Hints such as the neighbouring connectivity and penup event used would only be given if, and only if, the attackers failed to login at the first attempt.

To measure the percentage of password accuracy produced by the attackers, an online demo fuzzy approximate comparison of two text segments produced by [25] was adopted. The reasons for adopting the online demo fuzzy approximate comparison are because 1) it is free, 2) it has the required features such as percentage differences required for non-parametric analysis and 3) it is able to perform fuzzy approximate comparison for the password encoding produced by the proposed scheme. According to [25], the online demo fuzzy approximate comparison is able to provide statistical testing result with coefficient value of 76% for natural language matching. However, this coefficient value (i.e., produced by any of the approximate string matching algorithm) does not affect the testing results as the BPG encoding does not have any natural language element (the revised BPG encoding consists of only numbers and seven symbols such as [ ] ( ) { } and ,). The discussion on approximate string matching algorithms is outside the scope of this paper and will not be discussed any further.

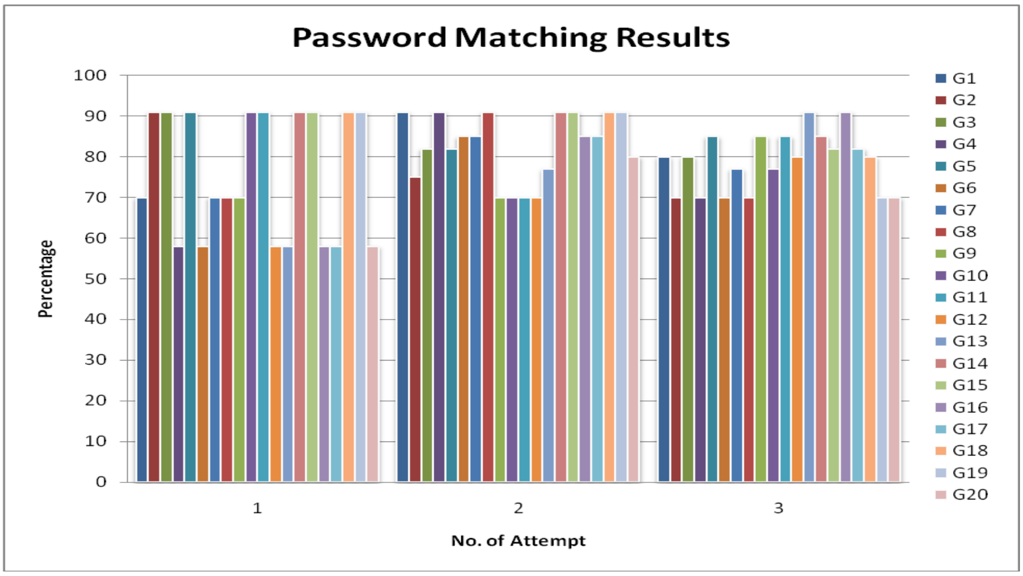


Fig. 15: Percentage Password Matching Results

Figure 15 shows the percentage of password matching results obtained from the attackers in three continuous attempts. It shows that none of the attackers were able to shoulder surf and guess the password used primarily because the attackers were not able to identify and obtain the correct penup events and the neighbouring connectivity among the indicators used. Figure 16 shows several password encoding examples produced by the attackers.

i) A password encoding that has less penup event compared to the correct password:
{(3,5,[0,0,0])(4,6,[0,0,0])(5,7,[0,0,0])(6,5,[0,0,0])(5,4,[0,0,0])(4,3,[0,0,0])(3,5,[0,0,0])}

ii) A password encoding that has correct penup events but wrong neighbouring connectivity:
{(3,5,[0,0,0])(4,6,[0,0,0])(5,7,[0,0,0])}{(5,7,[0,0,0])(6,5,[0,0,0])(5,4,[0,0,0])(4,3,[0,0,0])(3,5,[0,0,0])}

ii) A password encoding that has more penup events compared to the correct password:
{(3,5,[0,0,0])(4,6,[0,0,0])}{(4,6,[0,0,0])(5,7,[0,0,0])}{(5,7,[0,0,0])(6,5,[0,0,0])}{(6,5,[0,0,0])(5,4,[0,0,0])}{(5,4,[0,0,0])(4,3,[0,0,0])}{(4,3,[0,0,0])(3,5,[0,0,0])}

Fig. 16: Incorrect Password Encoding Produced by the Attackers

During the login demonstration, several tricks were carried out, such as: 1) faking or pretending to create a penup event by holding the mouse click in a sufficiently long manner before manoeuvring the mouse to another intersection points, as well as, 2) bypassing the nearest neighbour connectivity from one intersection point to another. These tricks eventually increased the probability for the attackers to guess the password incorrectly. From the observation result, the attacker with a higher competency level created more password patterns once hints about the penup event and the nearest neighbour connectivity information were given. However, neither the postgraduate nor the undergraduate participants were able to obtain the correct password. Thus, the password encoding produced by the revised BPG scheme was able to mislead a shoulder surfing attacker from identifying and obtaining the correct password used by an authorised user.

In order to identify whether competency levels or gender affects the result of the proposed method, an in-depth analysis was carried out based on the percentage match results generated from SPSS tool. A homogeneity testing was carried out and its correspondence hypothesis structured as follows:

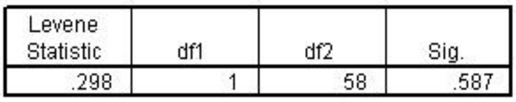
H_o^1: $\sigma^2_{G(postgraduate)} = \sigma^2_{G(undergraduate)}$

(Assume that the variance among postgraduate group and undergraduate group are equal.)

H_1^1: $\sigma^2_{G(postgraduate)} \neq \sigma^2_{G(undergraduate)}$

(Assume that the variance among postgraduate group and undergraduate group are not equal.)

Table 3: Homogeneity Testing Result



Levene Statistic	df1	df2	Sig.
.298	1	58	.587

The purpose of constructing the homogeneity testing was to identify a suitable testing method (parametric or non-parametric) to be used for the verification mentioned above. From Table 3, the result of the homogeneity test was abortive due to the p-value produced (0.587) being greater than 0.05. That is, the variance of percentage matches among the postgraduate and the undergraduate groups were not equal to each other. This phenomenon also indicates that the level of competency between both groups is not significant.

The percentage matches shown in the distribution graph (as in Figure 17) is a left skewed graph. Hence, a non-parametric test, such as Kruskal Wallis or Mann Whitney, is more appropriate for the aforementioned verification process.

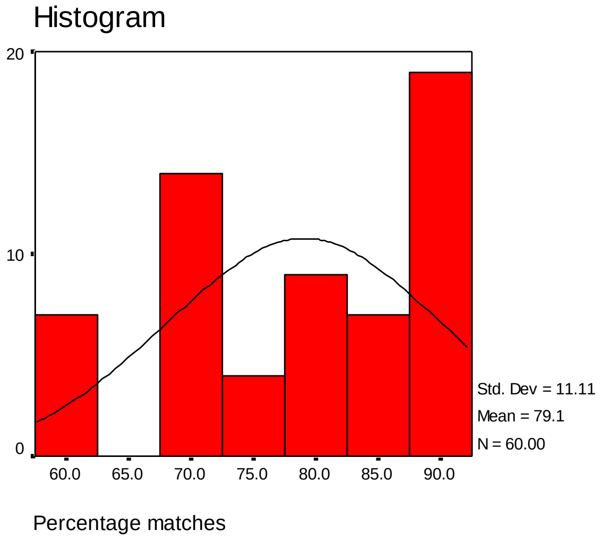


Fig.17: Distribution Testing Result

A Kruskal Wallis test was carried out and its correspondence hypothesis is structured as follow:

H_o^2: $\bar{x}_{G(postgraduate)} = \bar{x}_{G(undergraduate)}$; $\bar{x}$: mean

(There is no difference between the mean of percentage matches among postgraduate group and undergraduate group)

H_1^2: $\bar{x}_{G(postgraduate)} \neq \bar{x}_{G(undergraduate)}$

(There is a difference between the mean of percentage matches among postgraduate group and undergraduate group)

Table 4: Postgraduate and Undergraduate Kruskal Wallis Test Result

Ranks

	Competency Level	N	Mean Rank
Percentage matches	Postgraduate Undergraduate Total	30 30 60	28.43 32.57

Test Statistics(a,b)

	Percentage matches
Chi-Square	.883
df	1
Asymp. Sig.	.347

a Kruskal Wallis Test
b Grouping Variable: Competency Level

From Table 4, the result shows that the p-value produced (0.347) is greater than 0.05. This indicates that the outcome of the hypothesis test does not reject H_o^2 at 5% significance level. Therefore, it shows no difference in mean percentage matches between the postgraduate and the undergraduate groups. This confirms that even with different competency levels, the revised BPG encoding was able to mislead shoulder surfing attackers from identifying and obtaining the correct password.

In order to identify whether gender affects the result of the proposed method, the following hypotheses were structured:

H_o^3: $\bar{x}_{G(Male)} = \bar{x}_{G(Female)}$

(There is no difference between the mean percentage matches among male group and female group)

H_1^3: $\bar{x}_{G(Male)} \neq \bar{x}_{G(Female)}$

(There is a difference between the mean percentage matches among male group and female group)

H_o^4: $\bar{x}_{G(Postgraduate\_Male)} = \bar{x}_{G(Postgraduate\_Female)}$

(There is no difference between the mean percentage matches among male postgraduate group and female postgraduate group)

H_1^4: $\bar{x}_{G(Postgraduate\_Male)} \neq \bar{x}_{G(Postgraduate\_Female)}$

(There is a difference between the mean percentage matches among male postgraduate group and female postgraduate group)

H_o^5: $\bar{x}_{G(Undergraduate\_Male)} = \bar{x}_{G(Undergraduate\_Female)}$

(There is no difference between the mean percentage matches among male undergraduate group and female undergraduate group)

H_1^5: $\bar{x}_{G(Undergraduate\_Male)} \neq \bar{x}_{G(Undergraduate\_Female)}$

(There is a difference between the mean of percentage matches among male undergraduate group and female undergraduate group)

Table 5: Gender Kruskal Wallis Test Result

Ranks

	Gender	N	Mean Rank
Percentage matches	Male	30	33.33
	Female	30	27.67
	Total	60	

Test Statistics(a,b)

	Percentage matches
Chi-Square	1.660
df	1
Asymp. Sig.	.198

a Kruskal Wallis Test
b Grouping Variable: Gender

Table 6: Gender Kruskal Wallis Test Result of Postgraduate Students

Ranks

	Gender	N	Mean Rank
Percentage matches	Male	15	17.57
	Female	15	13.43
	Total	30	

Test Statistics(a,b)

	Percentage matches
Chi-Square	1.745
df	1
Asymp. Sig.	.187

a Kruskal Wallis Test
b Grouping Variable: Gender

Table 7: Gender Kruskal Wallis Test Result of Undergraduate Students

Ranks

	Gender	N	Mean Rank
Percentage matches	Male	15	16.40
	Female	15	14.60
	Total	30	

Test Statistics(a,b)

	Percentage matches
Chi-Square	.338
df	1
Asymp. Sig.	.561

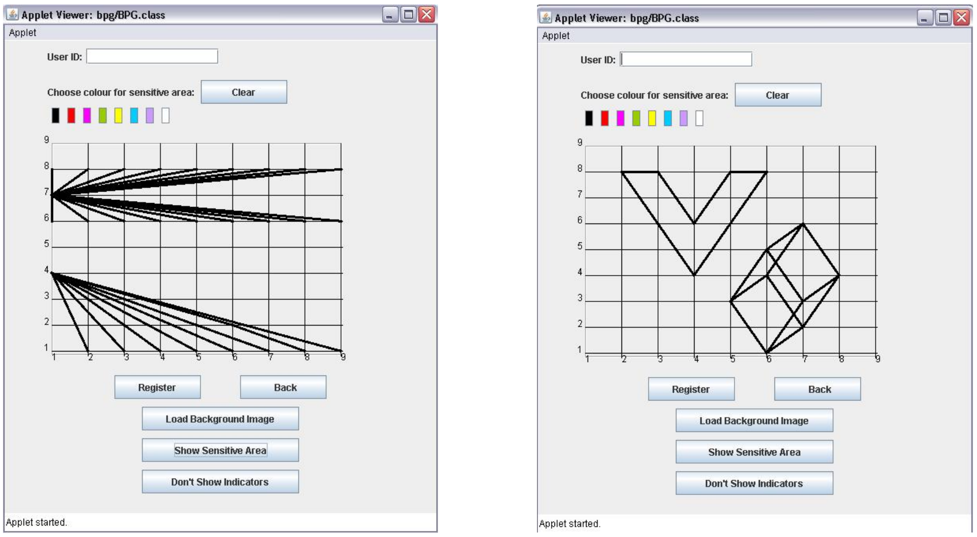
a Kruskal Wallis Test
b Grouping Variable: Gender

From the results shown in Table 5, 6 and 7, the p-values produced (0.198, 0.187, 0.561) are greater than 0.05, i.e., the outcome of the hypothesis test does not reject H_o^3, H_o^4 and H_o^5 at 5% level of significance, respectively. Thus, the aforementioned phenomena indicate that there are no differences between mean percentage matches among different gender even within each postgraduate and undergraduate group. In other words, the revised BPG encoding was able to mislead shoulder surfing attackers from identifying and obtaining the correct password used even if the shoulder surfing attackers are of different sexes.

5.0 ENCODING SCHEME AND PASSWORD SPACE ANALYSIS

The length of a password generated by the revised BPG scheme is the total number of indicators with two-dimensional coordinate pairs excluding the penups. Alternatively, it can be denoted as $\sum_{(x,y)\in[1..G]\times[1..G]}^{n}(x,y,[r,g,b])$ $\in$ {} where n is the total number of indicators and {} represent the penup event. As in the Pass-Go and BPG schemes, the revised BPG scheme was able to produce an infinite password space. In terms of the connectivity of a line indicator, the revised BPG scheme enabled users to connect from one intersection (x, y) point to another within the set of $(x \pm i, y \pm i)$ neighbours, where i = {0, 1, 2, …, 8}.

The previous line indicator connectivity analysis shows that the revised BPG scheme was able to fully utilise the G×G grid whereas, on the contrary, the Pass-Go and BPG schemes restricted the users to connecting an intersection (x, y) point only up to its eight nearest neighbour cells, as follows: (x-1, y-1), (x-1, y), (x-1, y+1), (x, y-1), (x, y+1), (x+1, y-1), (x+1, y) and (x+1, y+1). Thus, the revised BPG scheme not only is able to produce more password spaces, but users who undergo the revised scheme are able to draw more lines and shapes compared to other schemes. Figure 18 shows the lines and shapes samples which can be produced in the revised BPG scheme.



a) Line Indicators with No Nearest Neighbour Connection Restriction

b) Instances of Shapes That Cannot Be Drawn Using The Pass-Go Scheme

Fig. 18: Lines and Shapes Samples Which Can be Produced Exclusively by the Revised Scheme

5.1 Password Length

The password length of the revised BPG scheme can be denoted as $\left[\sum_{i=1}^{L_{\max}} i(G \times G)\right] \times NumberOfColours$ where L_{max} is the number of strokes used in creating a password, G is the size of the grid used in the revised BPG scheme and *NumberOfColours* is the number of colours available. A stroke can be created from multiple coordinate pairs such as a line or shape indicator. As such, the multiple coordinate pairs within a penup event are only considered as one stroke count in the password length calculation. Table 8 shows the password space comparison between BPG, Pass-Go and the revised BPG schemes. As shown, the revised BPG scheme has larger password spaces compared to other schemes. Moreover, it also shows that the password space for the revised BPG scheme increased exponentially as the number of strokes increased (see Figure 19).

Table 8: Comparison of Password Space

L_{max}	1	2	3	4	5	6	7	8	9	10
Pass-Go-9 (adapted from [23, 24])	6	13	19	26	32	39	45	52	58	64
Coloured Pass-Go-9 (adapted from [23, 24]) and BPG Scheme	9	19	28	37	47	56	65	75	84	94
Revised BPG	81	243	567	1215	2511	5103	10287	20655	41391	82863

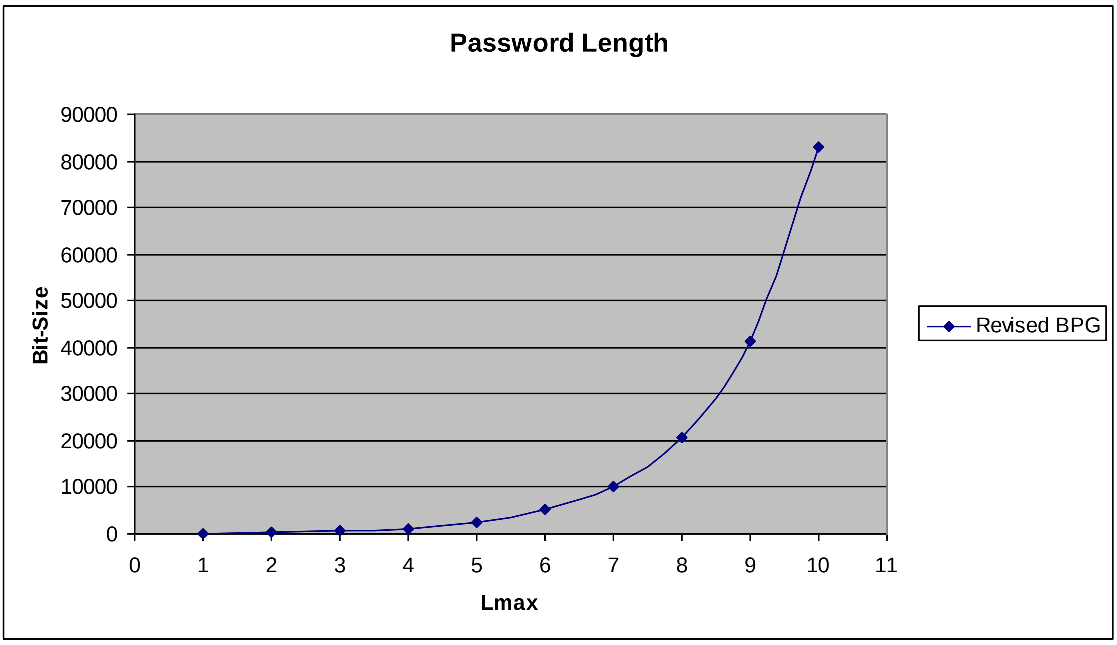


Fig. 19: Revised BPG Password Length

6.0 DISCUSSION

The proposed scheme utilises penup event and neighbouring connectivity manipulation to prevent shoulder surfing attacks. The analysis result shows that the proposed method was able to prevent the aforementioned attack. Besides, the testing result also shows that the competency level and sex of the attackers did not exert a statistically significant influence on the proposed method in preventing shoulder surfing attacks. This is due to the ability of the proposed method to falsify the drawn password during the authentication process. In addition, the proposed method was able to decrease the probability of password to be guessed by significantly improving the password length. However, due to the fact that the number of intakes at FSCIT, UM, Malaysia is approximately 200 people per year (for both undergraduate and postgraduate students), the sample size used was limited.

7.0 FUTURE WORK AND CONCLUSION

In summary, this paper presents a novel shoulder surfing resistance mechanism that utilises penup event and neighbouring connectivity manipulation in the revised Background Pass-Go scheme. The analysis and preliminary results show that the proposed mechanism was able to significantly resist shoulder surfing attack and produce larger password space compared to other schemes. To improve user memorability, a set of new cue colour schemes was proposed. In future, further research can be done on various cued techniques to improve user memorability along with relevant countermeasure techniques for combating other security threats. Furthermore, more tests and pool samples can be used during the analysis stage.

REFERENCES

[1] A. De Angeli, L. Coventry, G. Johnson, K. Renaud, Is A Picture Really Worth A Thousand Words? Exploring the Feasibility of Graphical Authentication Systems, *International Journal of Human-Computer Studies*, 63(1-2), 2005, pp. 128-152.

[2] M. Bishop, Password Checking Techniques, *Proceedings of the Second Workshop on Computer Security Incident Response*, pp. IV-D-1:4, 1990.

[3] M. Bishop, Metrics for Comparing Authentication Systems, *Proceedings of the Third Workshop on Computer Incident Handling*, pp. G-11-1:10, 1991.

[4] Bishop, M. Password management, *Digest of Papers Compcon Spring*, San Francisco, California, pp. 167-169, 1991.

[5] S. F. Carlton, J. W. Taylor, J. L. Wyszynski, Alternate Authentication Mechanisms, *Eleventh National Computer Security Conference Proceedings*, National Bureau of Standards/ National Computer Security Center, 1988, pp. 333-338.

[6] S. Chakrabarti, G. V. Landon, M. Singhal, Graphical Passwords: Drawing a Secret with Rotation as a New Degree of Freedom, *Proceedings of the Fourth IASTED Asian Conference on Communication Systems and Networks*, Phuket, Thailand, 2007, pp. 561-173.

[7] K.Chalkias, A. Alexiadis and G. Stephanides, A Multi-Grid Graphical Password Scheme, *Proceedings of the Sixth International Conference on Artificial Intelligence and Digital Communications*, Thessaloniki, Greece, 2006, pp. 80-90.

[8] A. E. Dirik, N. Memon, J. C. Birget, Modeling User Choice in the PassPoints Graphical Password Scheme, *Proceedings of the 3rd symposium on Usable privacy and security*, Pittsburgh, USA, 2007, pp. 20-28.

[9] P. Dunphy, and J. Yan, Do Background Images Improve "Draw A Secret" Graphical Passwords*? Proceedings of the 14th ACM conference on Computer and communications security, Session: Authentication and passwords*, Alexandria, Virginia, USA, 2007, pp. 36-47.

[10] E. Hayashi, N.Christin, R. Dhamija, and A. Perrig, Use Your Illusion: Secure Authentication Usable Anywhere, *Proceedings of the Fourth Symposium on Usable Privacy and Security*, Pittsburgh, PA, USA, 2008, pp. 35-45.

[11] I. Jermyn, A.Mayer, F. Monrose, M. K. Reiter, A. D. Rubin, The Design and Analysis of Graphical Passwords, *Proceedings of the 8th Conference on USENIX Security Symposium*, Washington, District of. Columbia, 1999, pp. 1-1.

[12] D. L. Jobusch, A. E. Oldehoeft, A Survey of Password Mechanisms: Weaknesses and Potential Improvements, Part 1, *Computers and Security*, 8(7), 1989, pp. 587-603.

[13] D. L. Jobusch, A. E. Oldehoeft, A Survey of Password Mechanisms: Weaknesses and Potential Improvements, Part 2, *Computers and Security*, 8(8), 1989, pp. 675-689.

[14] D. V. Klein, Foiling the cracker: A survey of, and improvements to, password security, *Proceedings of the 2nd USENIX Security Workshop*, 1990, pp. 5-14.

[15] D. Lin, P. Dunphy, P. Olivier, J. Yan, Graphical Passwords & Qualitative Spatial Relations, *Proceedings of the 3rd Symposium, On Usable Privacy and Security*, Pittsburgh, USA, 2007, pp. 161-162.

[16] T. Matsumoto, H. Matsumoto, K. Yamada, S. Hoshino, Impact of Artificial Gummy Fingers on Fingerprint Systems, *Proceedings SPIE: Optical Security and Counterfeit Deterrence Techniques IV*, Yokohama, Japan, vol. 4677, 2002, pp. 275-289.

[17] B. Menkus, Understanding the use of passwords, Computers and Security, 78(2), 1998, pp. 132-136.

[18] W. Moncur, G. Lepalâtre, Pictures at the ATM: Exploring the Usability of Multiple Graphical Passwords, *Proceedings of the SIGCHI conference on Human factors in computing systems*, San Jose, California, USA, 2007, pp. 887-894.

[19] D. Nali, J. Thorpe, Analyzing User Choice in Graphical Passwords. *Technical Report*, School of Information Technology and Engineering, University of Ottawa, Canada, 2004.

[20] L. Y. Por, X. T. Lim, Issues, Threats and Future Trend for GSP, *Proceedings of The 7th WSEAS International Conference on Applied Computer & Applied Computational Science (ACACOS '08)*, Hangzhou, China, 2008, pp. 627-633.

[21] L. Y. Por, X. T. Lim Multi-Grid Background Pass-Go, *Journal of WSEAS Transactions on Information Science & Applications*, 5(7), 2008, pp. 1137-1148.

[22] L. Y. Por, , X. T. Lim, M. T. Su, F. Kianoush, The Design and Implementation of Background Pass-Go Scheme Towards Security Threats, *Journal of WSEAS Transactions on Information Science and Applications*, 5(6), 2008, pp. 943-952.

[23] H. Tao, Pass-Go, a New Graphical Password Scheme, *Master Dissertation Report*, Ottawa, Canada, 2006.

[24] H. Tao, C. Adams, Pass-Go: A Proposal to Improve the Usability of Graphical Passwords, *International Journal of Network Security*, vol. 7, no. 2, 2008, pp. 273-292.

[25] Textolution. Clear Solution for Fuzzy Tasks [Online Demo], SoftComplete Development, Available from: < *http://www.textolution.com/fuzzysearch_demo.asp*>, [Accessed 20 April 2009].

[26] S. Xiaoyuan, Z. Ying, G. S. Owen, Graphical Passwords: A Survey, 21st Annual Computer Security Applications Conference, *IEEE Computer Society Washington*, DC, USA, 2005, pp. 463-472.

[27] K. Renaud, A. De Angeli, Visual Passwords: Cure-All or Snake-Oil?, *Communications of the ACM*, 52(12), 2009, pp. 135-140.

[28] K. Renaud, A. De Angeli, My password is here! An investigation into Visuo-Spatial Authentication Mechanisms, *Interacting with Computers*, 16(6), 2004, pp. 1017-1041.

[29] S. Brostoff, M. A. Sasse, Are Passfaces More Usable than Passwords: A Field Trial Investigation, *Proceedings of Human-Computer Interaction, Springer*, Sunderland, United Kingdom, 2000, pp. 405-424.