Chapter 1 Introduction

1.1 Background

Traditionally, passwords have been used as an authentication method to identify users who are attempting to gain access to a computer system. Passwords that are formed using printable ASCII characters (such as strings of letters and digits) are known as alphanumeric passwords, and were first introduced in the 1960s (Sobrado & Birget, 2002). The alphanumeric passwords are effective when they are too complicated to be deduced or predicted. From the security aspect, a password should consist of a string of eight or more random characters, including case sensitive characters such as uppercase and lowercase alphabetic characters, digits, and special characters. A password that is formed using random characters contains no meaningful content and must be memorised by rote, but rote learning is a weak way of remembering (Rundus, 1971). Hence, many users tend to forget their passwords, and with the number of passwords per user becoming increasingly more common, the rate of forgetfulness has also increased (Moncur & Lepalâtre, 2007).

Many users have difficulty in remembering a password that is long, and appears to be randomly formed (Narender, Babu, & Mohan Rao, 2010). Limitations of the human memory often cause users to choose passwords that are easy to remember such as common words that are used daily, or those found in a dictionary. Unfortunately, common word passwords are easy to predict and they can be cracked by the use of malicious software, for example, in small dictionary attack. In this method of attack, an individual uses several tools to crack passwords by automatically testing all the words that occur in dictionaries or public directories (Feldmeier & Karn, 1989). In his study, Klein (1990) reported that the small dictionary attack has been successful in cracking about 25% of 14,000 passwords using a dictionary with only 3 million entries (approximately 21.5 bits).

Threats from a software security breach could range from the very mild to be very disastrous (Azzazi & Sheikh, 2007). Therefore, the alphanumeric passwords are no longer secure enough to protect the computer systems effectively especially when the number of security threats and improper practices by users are becoming more rampant. As a result, the picture-based password was proposed as an alternative to alphanumeric password to improve password memorability, and security (Biddle, Chiasson, & Van Oorschot, 2009).

1.2 Motivation

A preliminary study was conducted on 100 computer-literate students from the Faculty of Computer Science and Information Technology (FCSIT), University of Malaya, Malaysia, for the purpose of identifying the pattern of use of the alphanumeric password. Table 1.1, Figure 1.1, and Figure 1.2 summarise the results from the study on the aspect of usage of the different categories of alphanumeric passwords, the number of different passwords used by users for accessing all services, and the alphanumeric passwords change frequency, respectively. The results show that: 88% of the users do not use strong passwords; 55% of the users use the same passwords for accessing all services; and 90% of the users only change their passwords after three months (one semester is approximately four and a half months).

Table 1.1: Usage of the Different Categories of Alphanumeric Passwords

Password category	Constitutions of alphanumeric passwords	Computer Users (%)
Weak	Only letters	25%
	Only numbers	15%
	Only keyboard symbols	0%
Moderate	Letters and keyboard symbols	3%
	Numbers and keyboard symbols	5%
	Letters and numbers	40%
Strong	Letters, numbers and keyboard symbols	12%

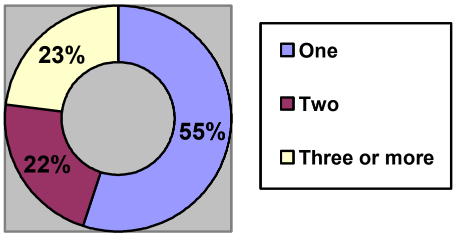


Figure 1.1: Number of Different Passwords Frequently Used for Accessing All Services

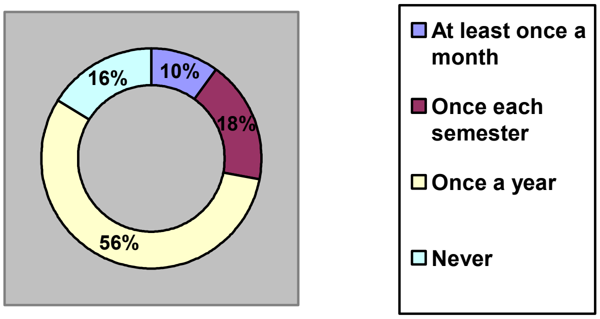


Figure 1.2: Alphanumeric Passwords Change Frequency

From the findings of this preliminary study, it is clear that based on the pattern of use, alphanumeric passwords have weaknesses, and are vulnerable to hacking and other forms of attacks to crack the passwords. Thus, the picture-based password authentication system was proposed as an alternative to alphanumeric password to improve password memorability and, thus, usability and also to make it less vulnerable to guessing attacks (Biddle et al., 2009).

The picture-based password authentication system was first introduced in 1996 (Blonder, 1996). Over the years, various picture-based password systems had been proposed to exploit the use of pictures or images for user authentication. However, they are still vulnerable to shoulder-surfing security threat like the alphanumeric passwords. Shoulder-surfing is a very common security threat against most of the picture-based password authentication systems. Shoulder-surfing happens when (Sobrado & Birget, 2002; Lashkari, Zakaria, Salleh, & Farmand, 2009):

- an attacker directly watches a user during the login process
- a security camera films a user during the login process
- an electromagnetic pulse scanner monitors the keyboard or the mouse activities or inputs during the login process
- Trojan login screen software captures the passwords as they are being entered by the user during the authentication processes.

Using the above methods, shoulder-surfing attackers are able to observe and reproduce the same password that is being drawn or being identified by a legitimate user in picture-based password authentication systems. Needless to say, to have a user's password cracked or become known to an attacker is a very serious security breach and can lead to untold damage. All efforts must be made to counter such shoulder-surfing threats. This also provided the motivation to carry out this research to mitigate shoulder-surfing attack in picture-based password authentication systems.

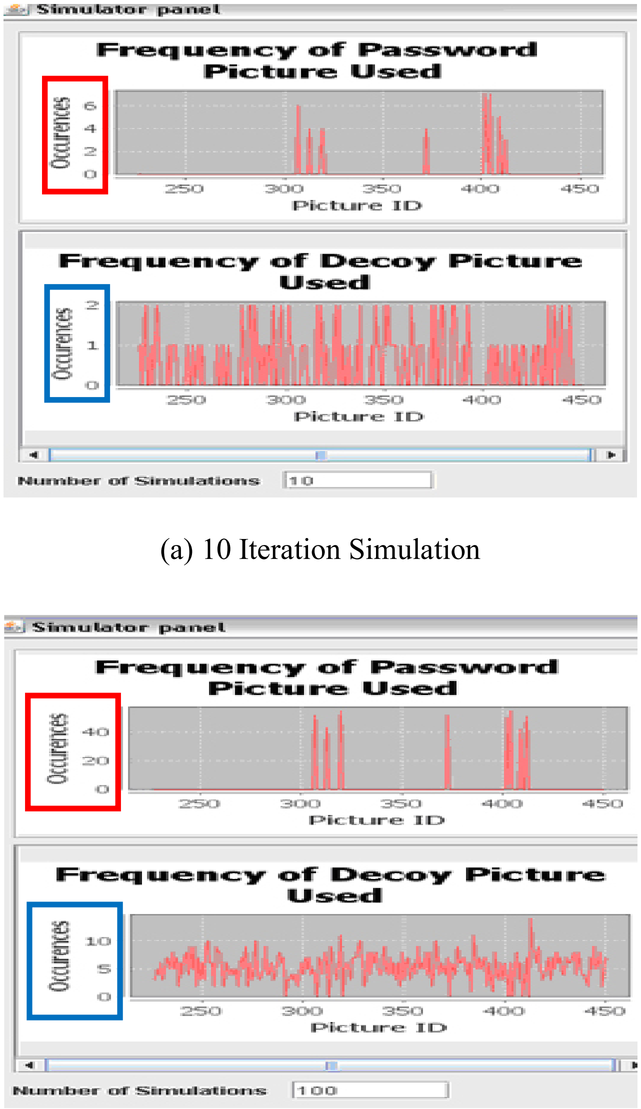
1.3 Statement of Problem

Picture-based password authentication systems have a drawback – they are more vulnerable to shoulder-surfing attacks than alphanumeric passwords (Lashkari et al., 2009). Shoulder-surfing has exacerbated the problems for systems that use picture-based password because of their visual interface (Gao, Ren, Chang, & Aickenlin, 2010). The problem arises from the picture-based password login processes, because shoulder-surfing attackers can observe the users inputting their passwords and later reproduce the passwords. Some password authentication systems such as Pass-Go use a hide function method that enables users to secure the password drawn during the whole authentication process to resist shoulder-surfing attacks. It is important to ensure that all the activities of an authentication process are secure, and this is an effective way to prevent shoulder-surfing attack. However, the Pass-Go method has serious flaws during the login process and can be an obstacle to users as they have no clue whether their password was correctly keyed in.

Other systems – such as Triangle system (Sobrado & Birget, 2002), Movable Frame system (Sobrado & Birget, 2002), Special Geometric Configuration system (Sobrado & Birget, 2002), and Scalable Shoulder-Surfing Resistant Textual-Graphical Password Authentication Scheme (S3PAS) system (Zhao and Li, 2007) – were proposed to mitigate shoulder-surfing attack by deploying a special method that enables the users to login using the pass-objects instead of the secret pass-objects (password). Pass-objects are decoy objects that can be used to login into a secure system (Man et al, 2003). Previous studies show that it is more difficult for the attackers to shoulder-surf and guess the password by using pass-objects compared with secret pass-objects (Sobrado & Birget, 2002; Zhao & Li, 2007). Zhao and Li concluded that the attackers have no clue on which pass-objects to be used for login because the pass-objects can only be determined dynamically based on the secret pass-objects in each challenge set. However, the distribution of the secret pass-objects and the number of pass-objects used have become an issue as they can affect the security of a system. For example, if the distribution of the secret pass-objects is relatively large and the number of pass-objects used is relatively high, there is very high likelihood of the attackers gaining access into the system by randomly selecting an object. On the other hand, if the distribution of the secret pass-objects is relatively small and the number of pass-objects used is relatively low, the users might have difficulty in identifying the correct pass-objects to login. Unfortunately, no further research was carried out on the distribution of the secret pass-objects and the optimum number of pass-objects to be used after the aforementioned method was proposed.

Recently, a new security threat known as Frequency of Occurrence Analysis (FOA) attack, had been identified. FOA is a method for identifying the rate of recurrence of a set of picture images generated by a secure system. FOA occurs only in a searchmetric picture-based password authentication system where users are required to search a number of password pictures among the other distracter pictures from a challenge set. An offline simulation is used by an attacker to observe and analyse the frequency of occurrence of a set of generated pictures. Thereafter, the attacker is able to identify the password pictures used by increasing the number of iterations of the simulation because the uniform randomisation algorithm used by the searchmetric picture-based password authentication systems tends to select the password pictures used when compared with the other distracter pictures.

An offline FOA attack simulation tool was developed using Java programming to illustrate the aforementioned claim. The algorithm used in Visual Identification Protocol Version 3 (VIP3), one of the searchmetric picture-based password systems proposed by De Angeli, Coventry, Johnson and Renaud (2005), has been modelled and used as an example to demonstrate the FOA attack. The simulation result (Figure 1.3) shows that the password pictures created by the user can be identified easily because the password pictures produce obvious peaks compared with the other distracter pictures. As a result, a shoulder-surfing attacker can make an educated guess based on the highest frequency of occurrences of the selected pictures when mounting an attack.



Number of Simulations 10

(a) 10 Iteration Simulation

Number of Simulations 100

(b) 100 Iteration Simulation

The password pictures used have higher occurrences compared with the other distracter pictures in Figure 1.3(a). The result is more obvious when the number of iteration increases, as shown in Figure 1.3(b).

Figure 1.3: An Off-line FOA Attack Simulation and Its Observation Result

Passwords are expected to comply with two fundamentally contradictory requirements – it must be easy to memorise, and yet it has to be secure (Wiedenbeck, Waters, Birget, Brodskiy, & Memon, 2005b). Therefore, it is crucial to ensure that the proposed system makes it easy for users to memorise and identify the password or pass-objects during the authentication processes. Hence, studies on various cued techniques used in helping users to memorise their passwords were carried out to address the memorability issue.

1.4 Statement of Objective

The aim of this research is to mitigate shoulder-surfing attack against picture-based passwords. The word "mitigate" in this context is to reduce the effect and success rate of shoulder-surfing attacks. In order to achieve the aim, the set objectives are as follows:

1. To propose falsifying authentication methods to mitigate shoulder-surfing attack. The methods include the use of: (a) penup event and neighbouring connectivity; (b) partial password selection and metaheuristic randomisation algorithm.

2. To design and implement the proposed falsifying authentication methods, specifically related to the picture-based password authentication clusters.

3. To evaluate the capability of the proposed methods in mitigating shoulder-surfing attack.

4. To evaluate the capability of the metaheuristic randomisation algorithm in preventing FOA attack (only for the searchmetric cluster).

1.5 Scope of the Research

In order to ensure that this research can achieve its set objectives within the stipulated timeframe, it is necessary to define the scope of the research, which are:

i. The evaluation of the functionalities of the prototypes is mostly done using standalone systems because extensive evaluations of the prototype of the proposed systems are costly.

ii. The study on usability, in terms of the cued techniques used to aid users in memorising their passwords is carried out using standalone systems.

The following are not within the scope of this research due to the time constraint of achieving the main objective which has been stated in section 1.4:

i. Other standalone system security threats such as keystroke logging, hotspots, dictionary attack, and brute-force attack.

ii. Other types of online security threats such as phishing, pharming, man-in-the-middle, man-in-the-browser, and spyware.

iii. Other types of shoulder-surfing methods/tools such as hardware-based methods (use hardware/tool to prevent shoulder-surfing), pressure-based methods (use pressure as one of the parameters to draw a password), Brain-Computer Interface (BCI) technology (use brain signal as one of the parameters to draw a password), and the gaze method (use eye tracking as one of the parameters to draw a password).

iv. Any hybrid password authentication systems that use biometric-based methods or the aforementioned methods.

v. Usability testing in terms the time taken for users to login into the proposed systems.

1.6 Significance of the Research

A new security threat known as Frequency of Occurrence Analysis (FOA) attack was identified and its counter-measure was proposed. To retain the randomness when selecting a password, a uniform randomisation algorithm is also adapted for the proposed method. However, the idea of recycling the old distracter pictures in the previous challenge set was proposed to increase the frequency of occurrence of the distracter pictures to overcome the FOA attack. A counter-measure that utilises metaheuristic randomisation algorithm was proposed and used to reselect the old distracter pictures in the previous challenge set.

The discovery of the FOA attack has provided researchers the opportunity to gain experience and better knowledge about such security threat. Researchers will be to make more-well-informed decisions when proposing new systems, especially in searchmetric picture-based password.

More significantly, this research has contributed to better knowledge on mitigating shoulder-surfing attack on picture-based passwords using falsifying authentication methods. Two falsifying authentication methods have resulted from this research:

(i) penup event and neighbouring connectivity manipulation

(ii) partial password selection and metaheuristic randomisation algorithm.

The first method is based on the idea of bypassing the nearest neighbour from one intersection point to another to trick the attackers when drawing a password in a G×G grid cells (G is the size of the grid) environment. Another method was proposed to increase the probability of incorrect password guessing by the attacker. It involves holding the mouse click long enough before manoeuvring the mouse to another intersection point to create a ‘flawed’ keystroke or penup event.

The second method is based on the idea of partial password selection and metaheuristic randomisation algorithm. It must be noted that only selected password pictures (partial password) are used in each challenge set, hence, the proposed method is able to confuse the attackers from identifying the correct password pictures and their sequence. Thus, an attacker mounting an FOA attack to shoulder-surf the password will not succeed.

1.7 Organisation of Thesis

This thesis consists of nine chapters. Chapter 1 presents a brief background information on alphanumeric password and its drawbacks. The aim, objectives, and scope of the research are also defined. This chapter also presents the significance of the research, and highlights two falsifying authentication methods that have resulted from the research.

Chapter 2 provides a review of the literature pertinent to the study. It covers current knowledge and significant research findings relating to picture-based passwords. These include picture-based password authentication security threats, generic classification of authentication systems, locimetric, drawmetric, searchmetric and their hybrid authentication system classifications.

Chapter 3 describes the research methodology adopted for the research to achieve the research objectives. The details regarding to the procedures involved are explained according to the following sequence: Proposed Falsifying Authentication Methods and Cued Recall Methods, System Design and Implementation, Testing, Evaluation and

Documentation. This chapter also presents the data gathering method and instrument used in the various systems development phases.

Chapter 4 discusses the first proposed system – the Background Pass-Go (BPG) system. This chapter begins with an introduction followed by the discussion of the BPG system architecture. The first falsifying authentication method that uses penup event and neighbouring connectivity manipulation to mitigate shoulder-surfing attack is presented. The upload background picture function and colour scheme used in the BPG system to help to improve users' memorability are then discussed. A use case diagram of the BPG system is presented to give an overview of the proposed method, and its functional requirements. The database design of BPG is presented followed by the chapter summary.

Chapter 5 discusses the second proposed system – the enhanced BPG system. This chapter discusses the architecture of the enhanced BPG system. To improve the users' memorability, the grid line scaling function and loose authentication method are proposed. The use case diagram of the enhanced BPG system is presented and used to discuss the additional functional requirements of the enhanced BPG system. The database design of the enhanced BPG system is presented followed by the chapter summary.

Chapter 6 discusses the third proposed system – the Visual Identification Protocol Professional (VIP Pro) system. This chapter discusses the architecture of the VIP Pro system. The second falsifying method that uses partial password selection and metaheuristic randomisation algorithm is presented. The use case diagram of the system is presented and used to discuss the functional requirements of the VIP Pro system. The database design of the VIP Pro system is then presented. Finally, a chapter summary concludes the chapter.

Chapter 7 discusses the analysis and testing of each of the proposed systems. The discussion focuses on the analysis and testing of the features in each of the proposed systems – the BPG system, the enhanced BPG system, and the VIP Pro system, respectively. The details of the testing are presented. Finally, a chapter summary is presented.

Chapter 8 discusses the results of the analyses and testing of each of the proposed systems. The synthesis result and the password space analysis of each proposed system are then presented. A summary is presented at the end of this chapter.

Chapter 9 discusses the outcomes of the research and how the research objectives have been met. The contribution of the research outcomes is then discussed, followed by suggestions on aspects of picture-based password authentication for research to be undertaken in future. The final remarks of the research are presented at the end of this chapter.

Chapter 2 Literature Review

2.1 Introduction

This chapter reviews the pertinent literature on the current problems and challenges of picture-based password systems. Information was gathered from various sources such as books, journals, conferences proceedings and websites. This chapter begins by reviewing the literature on the security threats related to the picture-based password authentication systems. Related work on various authentication systems such as the locimetrics, drawmetrics, searchmetrics and their hybrid authentication systems are explained, analysed and synthesised.

2.2 Security Threats in Picture-Based Password

A picture-based password authentication system must offer sufficient security protection against some common attacks to meet its primary goal (Biddle et al., 2009). It is important to have a good understanding of the different types of security threats against the picture-based password authentication system with the intention that researchers will be more mindful of such threats when proposing new systems or any counter-measures. The password authentication security threats can be categorised as: Surveillance Approach; Password Guessing and Cracking; Malicious Software (malware); and Social Engineering attacks (refer to Figure 2.1).

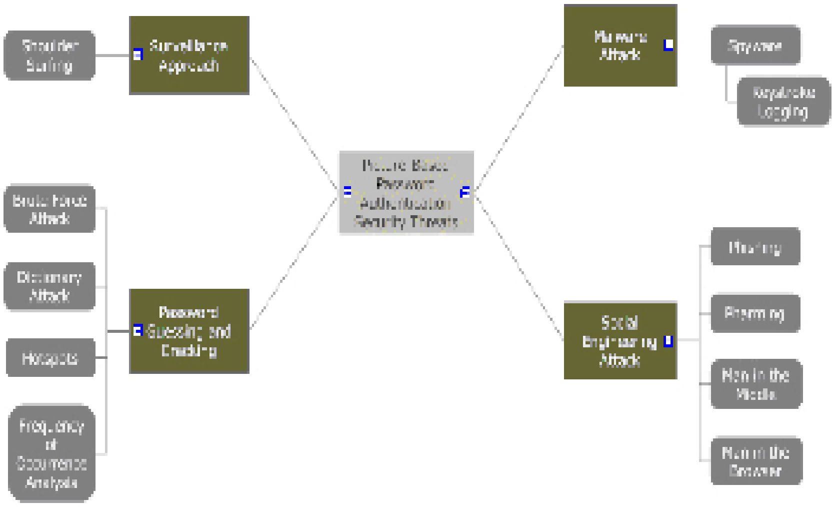


Figure 2.1: Picture-Based Password Security Threats Classification

2.2.1 Surveillance Approach

In the Surveillance Approach attack, the behaviour of an authorised user, object or process within a secure system is monitored or recorded. Shoulder-surfing has been classified as a Surveillance Approach attack.

Shoulder-surfing is a process of password theft through surreptitious monitoring. Shoulder-surfing attack occurs through direct observation techniques, such as looking over someone's shoulder to get passwords, PINs, and other sensitive personal information (Lashkari et al., 2009). Besides direct observation of a user during login, shoulder-surfing also happens when a security camera films a user, or when an electromagnetic pulse scanner monitors the keyboard and the mouse, or when Trojan login screens capture the passwords being entered by the user (Sobrado & Birget, 2002). Subsequently, the attacker is able to use the captured password to gain access to a system as a legitimate user although he is not authorised to do so.

2.2.2 Malware Attack

Malware refers to a security threat that uses any malicious software to gain access to a secure system (Biddle et al., 2009). Spyware is an example of malware attack (Peter, Karen, & Joseph, 2005). If a computer system has been infected by a spyware, valuable data or information will be gathered and sent to the parties who installed the spyware.

Keystroke logging or key logging software is an example of spyware. A keystroke logging spyware can record a user's keystrokes made on the keyboard. The recorded data can be analysed and evaluated by an attacker in order to find out or crack a user's password.

2.2.3 Password Guessing and Cracking

Password Guessing and Cracking refers to an act of gaining access to a secure system or network through guessing or cracking the password. Brute-Force, Dictionary, Hotspots and Frequency of Occurrence Analysis (FOA) attacks fall into this category.

In a brute-force attack, one or several software will be used by an attacker to try out all possible combinations of a user's password until he (attacker) is able to gain access to a secure system (Biddle et al., 2009).

A dictionary attack is a method of breaking into a secure system by systematically trying out all the words in an exhaustive list as a password (Biddle et al., 2009). In the picture-based password authentication context, a dictionary attack is always used with hotspots attack to gain access to a secure system.

Hotspots refer to areas of a picture that are more probable than other areas for users to click on (Biddle et al., 2009). A hotspots database can be developed to analyse and identify click points in a picture. In this way, an attacker can launch a hotspots dictionary attack to obtain the user's passwords.

Frequency of Occurrence Analysis (FOA) attack is a newly-discovered security threat, which uses a technique for identifying the rate of recurrence of a set of images generated by a secure system. As mentioned in the problem statement section at Chapter 1, FOA occurs only in the searchmetric picture-based password authentication system where users are required to search a number of secret password pictures from among the other distracter pictures from a challenge set. Because of the uniform randomisation algorithm used, the searchmetric picture-based password authentication systems tend to select the password pictures used when compared with the other distracter pictures. Thus, attackers are able to launch an offline FOA simulation attack to observe, analyse and identify the secret password pictures used by a user by increasing the number of iteration during the simulation. When the attacker has successfully identified the secret password pictures used, he can launch a password guessing attack as well as shoulder-surfing attack to gain access to the system as a legitimate user.

2.2.4 Social Engineering Attack

Social Engineering refers to a method of obtaining or attempting to obtain confidential information by deceiving legitimate users into revealing secure information. Phishing, Pharming, Man-in-the-Middle, and Man-in-the-Browser fall into this category (Biddle et al., 2009).

Phishing and pharming are two types of threats, which deceive unsuspecting users into clicking on links to fake websites and, in the process, giving up their usernames, passwords, and other personal information (Biddle et al., 2009). This could have grave consequences, and could lead to financial fraud and even identity theft. Unlike phishing, where users click on links in e-mails and are taken to the fake site, pharming compromises the Domain Name Services (DNS) and automatically redirects users who are attempting to login to a legitimate website to a fraudulent site (Biddle et al., 2009). What is more alarming is that pharming can reroute many thousands of Internet users at a time, thus, can have potentially huge adverse impact on computer security (Biddle et al., 2009). With phishing, the attacker scams one person at a time, whereas, in pharming, an attacker scams a large group of users, simultaneously.

The Man-in-the-Middle threat uses the phishing method to trick users from clicking on a link to login into their bank through a Man-in-the-Middle phishing proxy site (Biddle et al., 2009). However, the users have no knowledge that they have been tricked because they have actually passed through to the real website.

The Man-in-the-Browser (MITB) attack is a variation of the Man-in-the-Middle attack (Biddle et al., 2009). During a MITB attack, a malware will be installed; it will be interjected between a user and a web browser. Once the MITB has been launched, the malware will modify the transaction data issued by the user, without any knowledge of the user.

Several security threats were discussed in the previous sections. In this thesis, however, the focus is on proposing counter-measures to mitigate shoulder-surfing attack and to prevent FOA attack. A generic classification of the authentication system is discussed in the following section followed by the analysis and synthesis of the related work.

2.3 Password Authentication

An authentication system can be classified into token-based, biometric-based, and knowledge-based systems (Xiaoyuan, Ying, & Owen, 2005; Hayashi, Christin, Dhamija, & Perrig, 2008). In the token-based authentication system, a token or an object, such as a key card, RFID card, bank card or a smart card, is used as an instrument for authorised verification. It means that anyone who obtains a valid token can immediately gain access to resources regardless of whether or not he is an authorised user. To overcome this drawback, the biometric-based authentication system was introduced.

The biometric-based authentication system uses personal and physiological characteristics of an authorised user such as fingerprints, iris, speech, and facial recognition to perform verification. It is undeniable that a biometric-based authentication system is more secure compared with the token-based authentication system in terms of identifying the legitimate user's identity. However, the biometric-based authentication system 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 systems perform slowly and are often highly unreliable for making correct identification (Xiaoyuan et al., 2005). For example, most voice authentication systems produce high error rates when tested in a noisy environment while the facial recognition systems are sensitive to variations in lighting conditions during verification, and fingerprint readers can be deceived by fake fingerprints (Matsumoto, Matsumoto, Yamada, & Hoshino, 2002). As a result, the knowledge-based authentication system was developed.

In the knowledge-based authentication system, a user uses 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 and colour, as passwords and PINs (De Angeli et al., 2005). Some of the reasons for the wide acceptance of the knowledge-based authentication system are that the authentication process is fast, and it produces an acceptable rate of accuracy, when compared with the biometric-based system. In addition, most knowledge-based authentication systems do not require the users to undergo long or intensive training session during the first deployment of the system when compared with the biometric-based authentication systems (Hayashi et al., 2008).

The knowledge-based authentication system can be divided into two main categories: text-based password, and picture-based password. Text-based password uses alphanumeric characters as passwords or PINs. However, because of the emphasis on maintaining very high security level as advocated in various reports (Bishop, 1990; Carlton, Taylor, & Wyszynski, 1988; Jobusch & Oldehoeft, 1989b; Klein, 1990; Menkus, 1998), several policies and good password practices for text-based password have been suggested (Jobusch & Oldehoeft, 1989b; Menkus, 1998; Bishop, 1991a; Bishop, 1991b; Jobusch & Oldehoeft, 1989a). In this research, the main focus is on the picture-based password authentication system. Therefore, text-based password will not be discussed further.

The picture-based password authentication system was pioneered in 1996 by Greg Blonder who also holds US patent 5559961 for the system. Over the years, various picture-based password systems have been proposed to exploit the use of pictures or images for user authentication. In 2005, De Angeli et al. (2005) proposed a cluster of three categories (locimetrics, drawmetrics, and cognometrics) for classifying picture-based password authentication. The terminology and description for cognometrics, locimetrics, and drawmetrics were expanded by Moncur and Lepalâtre (2007) and the cognometrics terminology was revised to searchmetrics by Renaud and De Angeli in 2009.

Many researchers are still trying to standardise the terminology used (Xiaoyuan et al, 2005; De Angeli et al., 2005; Biddle et al., 2009). In order to incorporate the existing picture-based password authentication systems, De Angeli et al. proposed a more generic classification approach, which was revised by Renaud and De Angeli (2009) and subsequently adopted and expanded (refer to Figure 2.2).

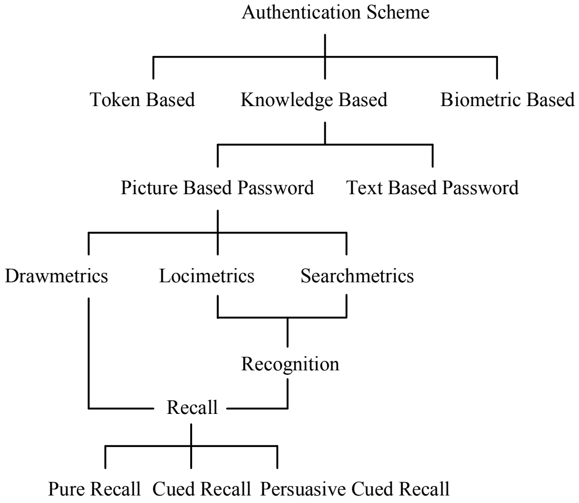


Figure 2.2: Authentication System Classification Tree

2.4 Related Work

This section discusses the related work on picture-based passwords which are pertinent to this research. The strengths and weaknesses of each picture-based password authentication system being reviewed are discussed. Besides, an initiative has been taken to classify the reviewed picture-based password authentication systems into Locimetrics, Drawmetics, Searchmetrics and the related hybrid cluster. At the end of each classification, a synthesis of the cluster is presented.

2.4.1 Locimetrics Authentication System

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 (De Angeli et al., 2005; Moncur & Lepalâtre, 2007; Renaud & De Angeli, 2009). Blonder (1996) adopted the idea and initiated a picture-based password system, which requires users to identify and select one or more predetermined positions from a predetermined image in a particular order, before they are allowed to gain access to a secure system (refer to Figure 2.3). However, Blonder's system had one major drawback – users cannot click arbitrarily on the background (Hafiz, Abdullah, Ithnin, & Mammi, 2008). Therefore, the password space of the system was limited and restricted to the size of the object image. This restriction increases the vulnerability of the system to shoulder-surfing, guessing, and brute-force attacks. However, Blonder contended that the purpose of implementing such restriction is to prevent users from having difficulty in identifying their passwords due to the system's tolerance and the users' memorability issues.

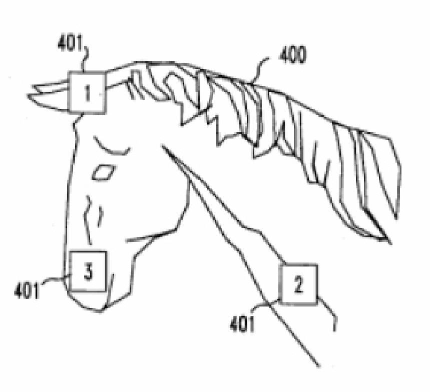


Figure 2.3: Blonder System (adapted from Tao, 2006)

visKey was the first product to use the patented visual Key technology in 1999. visKey is a recall-based[1] authentication system, which was commercialised by SFR Company, Germany (Tao & Adams, 2008). It was designed for small mobile devices such as PDA and pocket PC. Besides, pictures in JPEG, GIF, PNG and BMP formats can be stored in the device storage to allow users to initialise the password by choosing the pictures as the cue background. The visKey system consists of defined spots and their sequence. To enter a password correctly, a user has to tap the same spots in the same sequence as was done during the password setup process (refer to Figure 2.4).

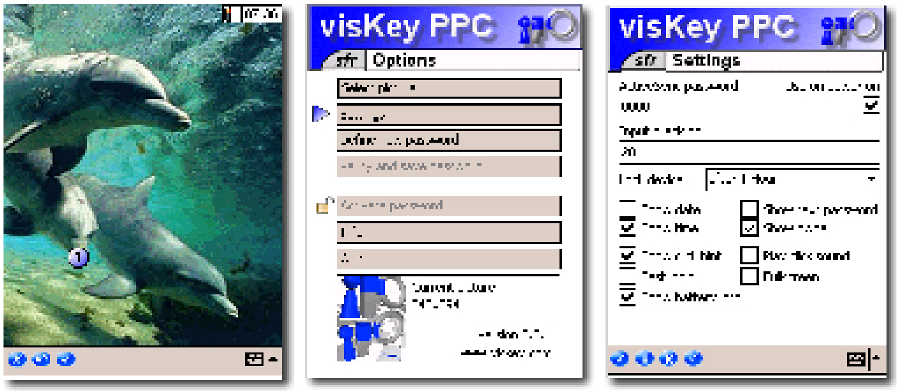


Figure 2.4: visKey System (adapted from visKey, 2005)

[1] Recall-based: A technique which requires a user to reproduce something – can be a drawing or repeating a selection that the user created or selected earlier during the registration phase (Sabzevar & Stavrou, 2008; Xiaoyuan et al., 2005).

As in Blonder's system, it is often difficult to tap on the exact spots in visKey. This is due to the tolerance setting of the system. However, in this system, users are able to personalise and predefine the size of the tolerance area. Thus, setting the size of the tolerance area has become a challenging issue in the visKey system because the input precision must be set precisely as it can directly influence the security and usability of the system. For example, the system is easily cracked if the setting of the input precision is too large. On the other hand, if the setting of the input precision is too small, users will have difficulty in entering a password. With regard to the password space, Tao and Adam (2008) suggested that a pragmatic setting of parameters with a four-spot visKey can offer relatively almost 1 billion combinations (approximately 30 bits) and it is comparable to the password space of a textual password, which is composed of five alphanumeric characters ($\log_2 65^5 \approx 30$). However, Tao and Adam recommended that the visKey system should use more spots (i.e., 8 spots) for a password to be able to resist offline attacks such as brute-force attack. Nevertheless, visKey is still vulnerable to shoulder-surfing attack.

Passlogix V-Go is a commercial security solution provided by Passlogix Inc in 2002 (Wiedenbeck et al., 2005b). According to Wiedenbeck et al. (2005b), Passlogix V-Go is an enhanced system of the Blonder system. It uses a technique, known as "repeating a sequence of actions", that allows a user to create a picture-based password by navigating through an image sequentially (Hafiz et al., 2008). Subsequently, users can select their background images showing various environments such as bathroom, bedroom, kitchen, stock trade, and even cocktail lounge. A user needs to click and/or drag a series of objects with the background image as his/her password (refer to Figure 2.5). For example, in the cocktail lounge, users are allowed to choose their favourite liquor and mix it with other drinks to become cocktails. In addition, users are required to choose the objects in the correct sequence in order to get authenticated.

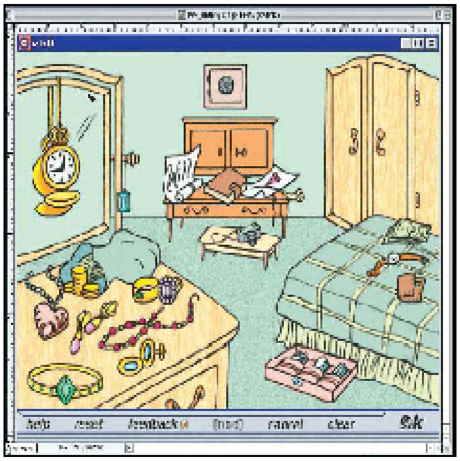


Figure 2.5: Passlogix V-Go System (adapted from Hafiz et al., 2008)

Passlogix V-GO authentication system is easier to memorise and more fun to use (Hafiz et al., 2008). Nevertheless, there are several drawbacks such as: the system is vulnerable to shoulder-surfing attack; the size of the password space is small; limited types of cocktails/objects that one can choose such as brandy, whiskey or wine to be mixed together; thick boundaries are defined in order to detect whether an object is clicked using a mouse. Therefore, the passwords are somehow predictable.

Birget, Hong, & Memon (2003; 2006) enhanced Blonder's system by introducing the MultiGrid Discretization method, which allows users to create and click on any point inside a background image. Moreover, the proposed system allows users to upload their own images besides using the default collection of images provided by the system. For verification, the user is still required to click within a predetermined tolerance distance of the originally chosen spots/points before they are allowed access to the secure system.

Subsequently, Birget et al. (2006) together with Wiedenbeck et al. (2005b) proposed a more superior system called PassPoints in 2005 (refer to Figure 2.6). They contended that the PassPoints system allows any image to be used and does not need artificial predefined click regions with well-marked boundaries. This means that a password can be created by choosing any sequence of points in the image arbitrarily. To login, the users have to click on a spot that is close to the chosen click points within the tolerance distance of between 0.25 and 0.50 cm (Wiedenbeck, Waters, Birget, Brodskiy, & Memon, 2005a).

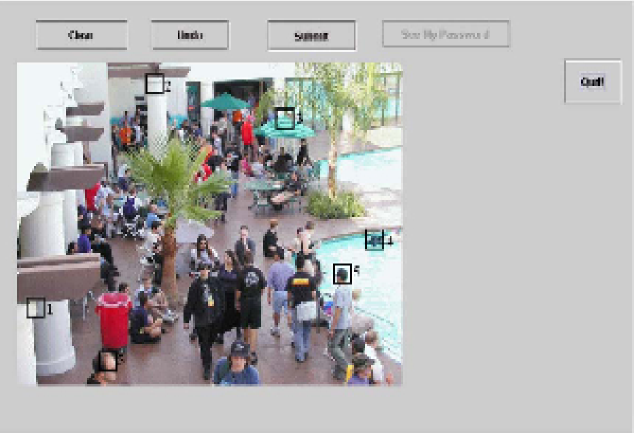


Figure 2.6: PassPoints System (adapted from Wiedenbeck et al., 2005b)

One of the advantages of PassPoints is that it is able to overcome the limitations of the Blonder's system – needing simple, artificial images, and predefined regions. Besides, PassPoints is a much more secure system when compared with the alphanumeric passwords, and the Blonder system because of its larger password space (Wiedenbeck et al., 2005a).

However, PassPoints has some disadvantages such as: it takes significantly longer time to input the picture-based passwords; it identifies only certain important points on an image, rather than areas, and the user has to click relatively close to all those points to input the correct password to gain access to the system; it is likely that the participants will feel frustrated when their password inputs are often close to the acceptable tolerance level but still lie outside of it; users have problems in handling a multi-PassPoints image. In addition, the attackers are often able to guess PassPoints password correctly because of the image "hotspots". As a result, an attacker can launch a hotspots dictionary attack to crack the user's passwords; and, it is vulnerable to shoulder-surfing attack.

Chiasson, van Oorschot, and Biddle (2007) proposed a system, known as Cued Click Points (CCP), which is an enhanced system of PassPoint. The development of the CCP system was inspired by PassPoints, Passfaces, and Story systems (Passfaces and Story systems will be discussed in the following section). In the CCP system, users are required to click on a single point in a sequence of five images for authentication rather than clicking on five points on a single image, as implemented in the PassPoints system. In the CCP system, the image that is shown is determined by the location of the previously entered click-point except the initial image. However, each click in CCP system will result in displaying the next-image even though an invalid point has been clicked (refer to Figure 2.7).

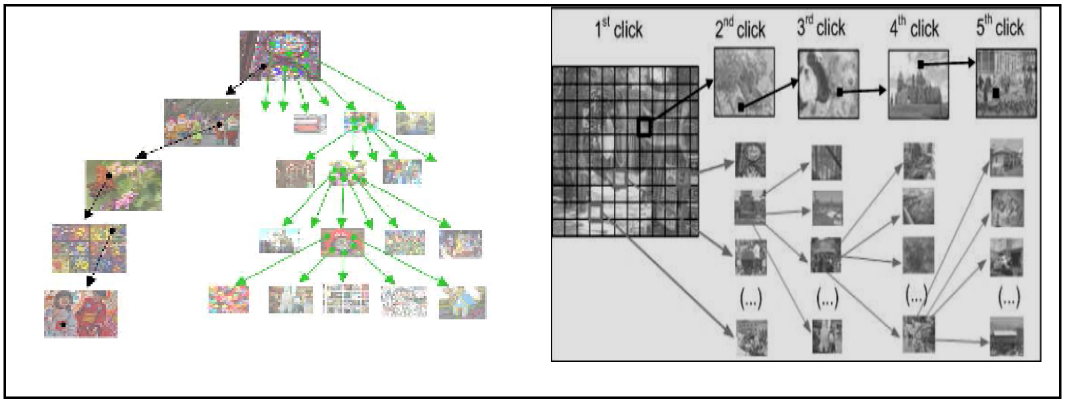


Figure 2.7: Cued Click-Points System (adapted from Chiasson et al., 2007; Chiasson et al., 2008b)

Therefore, Chiasson et al. (2007) claimed that the CCP system is able to: improve resistance to shoulder-surfing attack; improve the users' memorability and alleviate the problem of memorising the sequence of the click-points implemented in PassPoints by providing an implicit feedback which is useful only to legitimate users, because a wrong click will lead to an incorrect path. However, hotspots are still an issue in the CCP system during password creation because there is still the possibility that an attacker would make proportionally more effort to gain confidential information (Chiasson, Forget, & Biddle, 2008a). Besides, resisting shoulder-surfing attack is still an issue using the CCP system.

Forget, Chiasson, and Biddle (2007) adopted the CCP system as a base system and proposed a new system, known as Persuasive Cued Click-Points (PCCP). During the password creation process in the PCCP system, a hotspot analysis will be carried out by the system to identify a viewport positioned randomly outside the hotspot tolerant boundary (refer to Figure 2.8 (a) - (b)).

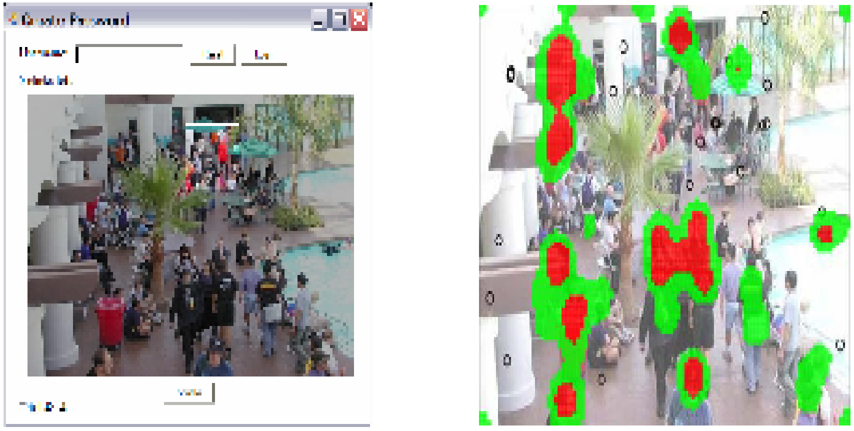
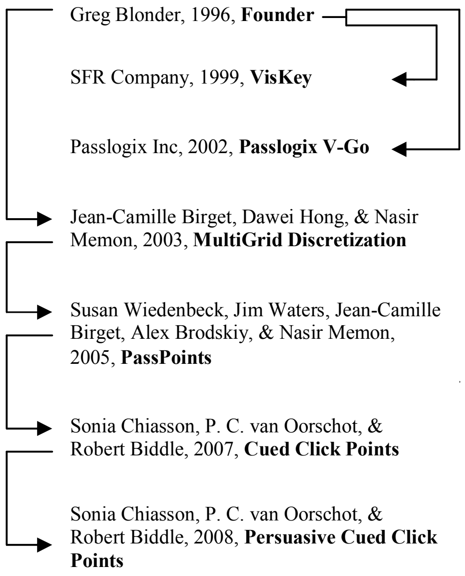

(a) Viewport Highlighting (b) Aggregated Hotspots Analysis

Figure 2.8: Persuasive Cued Click-Points System (adapted from Forget et al., 2007)

The purpose of positioning the viewport randomly rather than specifically is to avoid known hotspots, and at the same time, to prevent attackers from improving guesses by using the formation of new hotspots. According to Forget et al. (2007), the size of the viewport offers a variety of distinct points but covers only an acceptably small fraction of all possible points. It is recommended that users select a click-point within the highlighted viewport. They can, however, reshuffle the viewport or identify their favourite click-point located outside the viewport by using the PCCP system (Chiasson et al., 2008b). Based on their study, Forget et al. expressed that the viewport feature in the PCCP system is beneficial in educating users to create a more secure password during the password creation process. The click-point distribution across users will be more randomly dispersed and will not form new hotspots when the viewport is applied. However, the PCCP system is defenceless against shoulder-surfing attack. With regard to memorability, users might have difficulty in remembering unfamiliar click-points identified with the aid of the viewport.

An initiative was undertaken to organise the locimetric picture-based password systems according to the year of their establishment and their referred systems (refer to Figure 2.9). This effort was aimed at providing a better perspective of the systems being reviewed from the aspects of their evolution and the enhancement methods used. Researches on picture-based password systems have benefited from this initiative, and researchers can use the organisation chart to propose better systems.


Greg Blonder, 1996, **Founder**
SFR Company, 1999, **VisKey**
Passlogix Inc, 2002, **Passlogix V-Go**
Jean-Camille Birget, Dawei Hong, & Nasir Memon, 2003, **MultiGrid Discretization**
Susan Wiedenbeck, Jim Waters, Jean-Camille Birget, Alex Brodskiy, & Nasir Memon, 2005, **PassPoints**
Sonia Chiasson, P. C. van Oorschot, & Robert Biddle, 2007, **Cued Click Points**
Sonia Chiasson, P. C. van Oorschot, & Robert Biddle, 2008, **Persuasive Cued Click Points**

Note: An arrow and its direction are used to denote an enhancement of the system by other researchers.

Figure 2.9: Organisation Chart of Locimetrics Authentication Systems

A synthesis table of the locimetrics authentication systems has been established to improve the new systems being proposed (refer to Table 2.1). The table shows that resisting shoulder-surfing security threat is an issue that is still receiving much attention. The table also shows that researchers have proposed a better system to improve the password space for locimetrics authentication cluster. However, the improved system has resulted in a reduction in the users' memorability level. To improve the user memorability level, various cued techniques can be used. The concept of cued recall techniques was introduced in 2005 by Wiedenbeck et al. (2005b). According to Dirik, Memon, and Briget (2007), a system which utilises cued recall techniques will offer a framework of hints, context, and cues to help users to reproduce their passwords or to help them to make the reproduction more accurate. At the same time, a group of researchers advocated educating users to create stronger passwords by using persuasive method. It is logical to expect that even a good system can be vulnerable to security threats if a user creates a weak password. It is important to note that all the systems that had been reviewed are vulnerable to shoulder-surfing attack. It is, therefore, not surprising that many research efforts have been focused on finding ways to mitigate shoulder-surfing attack. This is also the main focus of this study.

Table 2.1: Synthesis of Locimetrics Authentication Systems

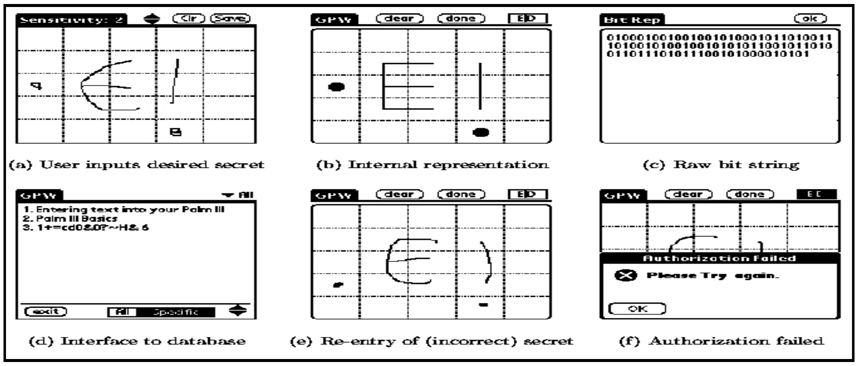
Locimetrics Authentication System		Password Space	Memorability	SS	FOA
Cued Recall	Blonder	▪ Small ▪ Depends on the object and tolerant value used in a picture. ▪ Generic Password Space: N^k (Xiaoyuan et al., 2005) (N is the tolerant units of an object in a picture; K is the number of locations to be clicked on.)	▪ Easy to remember.	×	N/A
	visKey	▪ Small but larger than the Blonder system. ▪ Depends on the tolerant value used in a picture. ▪ Generic Password Space: N^k (Xiaoyuan et al., 2005) (N is the tolerant units of an object in a picture; K is the number of locations to be clicked on (include tolerant value).)	▪ Depends on where users pointed at. ▪ Easy but more difficult to remember compared with the Blonder system.	×	N/A
	Passlogix V-Go	▪ Smaller than the Blonder system. ▪ Depends on the number of object used in a picture. ▪ Generic Password Space: N^k (Xiaoyuan et al., 2005) (N is the number of object in a picture; K is the number of password object to be clicked on.)	▪ Easy to remember.	×	N/A
	MultiGrid Discretization	▪ Large ▪ Generic Password Space: N^k (Xiaoyuan et al., 2005) (N is the number of pixels of a picture, K is the number of locations to be clicked on (include tolerance value).)	▪ Can be difficult to remember. ▪ Depends on where users pointed at. ▪ More difficult than visKey system.	×	N/A
	PassPoints			×	N/A
Cued Recall	Cued Click Points	▪ Large but smaller than PassPoints system. ▪ Generic Password Space: $\sum_{i=1}^{5}(N_i)^k$ N is the number of pixels of a picture. K is a location to be clicked on (includes tolerance value).	▪ Easier to remember compared with the PassPoints system. ▪ Can still be difficult to remember. ▪ Depends on where users pointed at.	×	N/A
Persuasive Cued Recall	Persuasive Cued Click-Points	▪ Large ▪ Generic Password Space: N^k (N is the number of pixels of a picture, K is the number of locations to be clicked on (includes tolerance value).)	▪ More difficult to remember than PassPoints system.	×	N/A

Key:
SS: Shoulder-Surfing Attack
FOA: Frequency of Occurrence Analysis
× : vulnerable to
√ : invulnerable to
N/A : Not Applicable

2.4.2 Drawmetrics Authentication System

In the drawmetric authentication system, users are required to draw a preset outline figure on a grid (De Angeli et al., 2005; Moncur & Lepalâtre, 2007). The position, sequence, as well as the visual appearance of a redrawing, are then used as the analysis metrics for users' verification.

Jermyn, Mayer, Monrose, Reiter, and Rubin (1999) proposed a well-known drawmetrics system, Draw A Secret (DAS) – which is a pure recall picture-based password system (De Angeli et al., 2005). According to Dirik et al. (2007), in the pure recall picture-based password systems, a user is required to reproduce his/her password without being given any hints or cues. During the password creation process, users are allowed to create their password by drawing a free-form image or other figures on a grid. The underlying algorithm for the DAS system involves storing the coordinates of the 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 penup value. The bit-string will then be hashed using a one-way hash function before storing it in a system. For an authentication verification, users are required to redraw the image or figure which can produce the same hash value as that stored in the system, within an acceptable tolerance preset by the system (refer to Figure 2.10).



(a) User inputs desired secret

(b) Internal representation

```
01000100100100101000101101001 1
10100101001001010101100101101 0
011011101011100101000010101
```

(c) Raw bit string

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

(d) Interface to database

(e) Re-entry of (incorrect) secret

Please Try again.

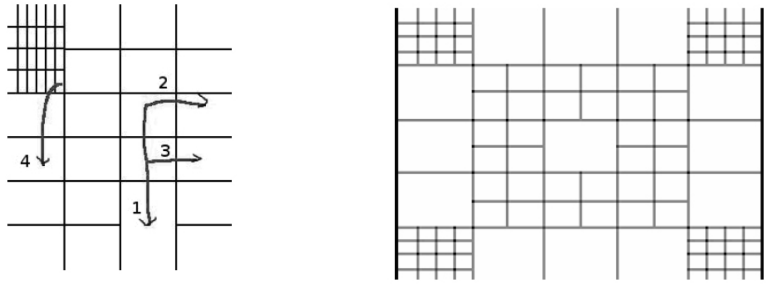
(f) Authorization failed

Figure 2.10: Draw A Secret System (adapted from Jermyn et al., 1999)

Some advantages of the DAS system include: able to increase users' memorability by enabling the users to draw the images or figures based on their familiarity rather than by remembering any kind of meaningless and unfamiliar alphanumeric string; able to provide better security protection against attackers because of its ability to derive a secret key to encrypt and decrypt a user's password before storing the password into a device. Therefore, the user's password or the encrypted content can be protected from attackers even if the device falls into the attackers' hands; and based on the raw size testing result obtained from Jermyn et al. (1999), it was shown that the password space in the DAS system with password length ≥12 is already greater than the password space of a textual password as it only consists of 8 characters or less as constructed from the printable ASCII codes ($95^8 \approx 2^{53}$).

The DAS system has some limitations, which include: brute-force attacks can be launched by trying all possible combinations of the grid coordinates if the attackers had obtained a copy of the stored secret; it is vulnerable to shoulder-surfing attack. The password keystrokes of a user can be recorded and used by the attacker to gain access to the device; findings from cognitive studies show that users are inclined to create centred and symmetrical passwords to make them easier to remember, but this makes it easy for attackers to identify the users' password (Dunphy & Yan, 2007; Nali & Thorpe, 2004); drawing a diagonal line and identifying a starting point from any oval shape figure using the DAS system can itself be a challenge for the users; if the user chooses a drawing which contains strokes that pass too close to a grid-line, the DAS system may not be able to identify the cell the user chooses; the scalability of the DAS system is restricted by the small cell size (5x5 grid cells) and this leads to difficulty in inputting passwords, restriction in choosing passwords freely, reduction in the memorable password space, and reduction in the overall security level.

The Multi-Grid DAS system proposed by Chalkias, Alexiadis, and Stephanides in 2006 is an enhancement of the DAS system (refer to Figure 2.11 (a) - (b)). It allows users to draw their images or figures on different grid cell sizes. The users are allowed to choose a predefined Multi-Grid template to draw their password, but the final password produced by the system can be composed from several internal grids. The purpose of having different grid cell sizes is to reduce the users' tendency to create passwords that are centred. In this system, users are also allowed to focus on a single internal grid or a nested grid. Thus, an attacker has to use even more complex and massive brute-force techniques to find out the password used by a user because of the various neighbouring cells used.



(a) A Multi-Grid Password Example (b) A Multi-Grid Template

Figure 2.11: Multi-Grid DAS System (adapted from Chalkias et al., 2006)

Based on the results of their study using the Multi-Grid DAS, Chalkias et al. (2006) reported a reduction in the shift errors made by the users. However, the ordering errors remained the same. This shows that users still have difficulty in memorising the correct order of their drawn passwords. Similar to the DAS system, the Multi-Grid DAS system is also vulnerable to shoulder-surfing attack.

Chakrabarti, Landon, and Singhal (2007) proposed another hybrid method called the DAS with Rotation (R-DAS). R-DAS allows users to rotate the canvas of a drawn password on the z-axis in a clockwise or an anticlockwise motion (refer to Figure 2.12). R-DAS has inherited all the features of the DAS system and, in addition, it has the 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).

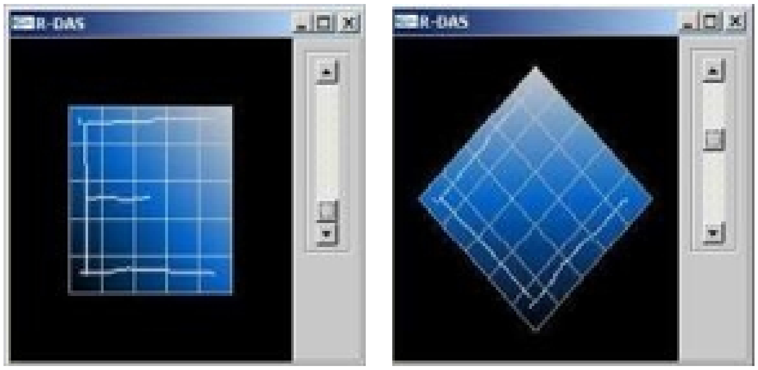


Figure 2.12: DAS with Rotation System (adapted from Chakrabarti et al., 2007)

Based on the result of the analyses conducted by Brostoff and Sasse (2000), it is found that R-DAS not only increases the full password space, but it also increases the predictable password space corresponding to the number of components (strokes). Using the rotation technique and the full password space, the R-DAS system provides better security when compared with the DAS system, if both systems use the same grid size (i.e., 5x5 grid cells).

However, the R-DAS system has some short-comings when compared with the DAS system. These include: the extra rotation angle information has to be memorised by the users; it is likely that users will still create centred and symmetrical password to make it easier for them to remember, and dispense with the need to remember the rotation angles; the R-DAS system is vulnerable to shoulder-surfing attack if the system is open to public access.

Dunphy and Yan (2007) from Newcastle University proposed the Background Draw a Secret (BDAS) system, which works exactly in the same way as the DAS system, except that it is aided by a background image superimposed over the blank DAS grid (refer to Figure 2.13).

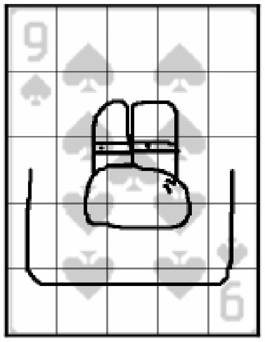


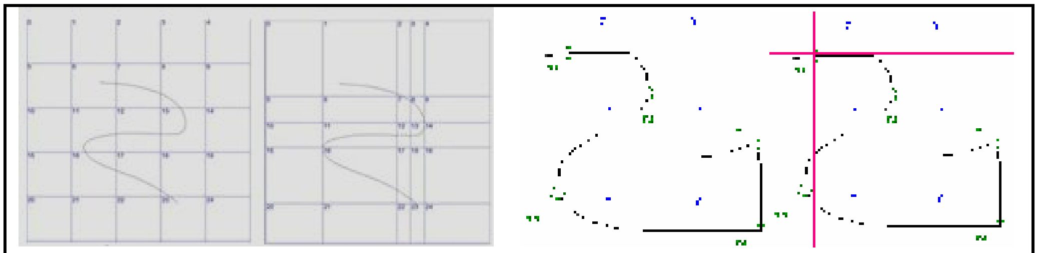
Figure 2.13: Background Draw a Secret System (adapted from Dunphy and Yan, 2007)

The advantages of superimposing a background over the blank DAS grid are to: make it easier for users to remember; alleviate problems such as difficulty in identifying a password starting point; encourage the users to draw a more complicated password – having more strokes, or longer password length; and discourage the users from creating a password which is less symmetrical or less centred.

However, the BDAS system has some drawbacks, and these include: the need to maintain and manage the data storage capacity optimally as the system allows a user to upload an unlimited amount of background images of various sizes; depending on the quality of the background image, the system downloading time will be unnecessarily long if a large background image is used; if the background image used is distorted due to low image resolution, a user might have difficulty in creating his password, thus, the user might create a symmetrical or centred password as in the DAS system, and this would defeat the purpose of the BDAS system; and, the BDAS system is vulnerable to shoulder-surfing security threats.

Lin, Dunphy, Olivier, and Yan (2007) proposed the Qualitative Draw A Secret (QDAS) in 2007. QDAS is an enhanced version of the DAS system and, thus, both work in the same way. However, the QDAS system uses a different encoding mechanism for each keystroke made by the users. An integer index is predefined and assigned to each grid cell. Each password consists of the starting stroke in a grid cell together with the sequence of the qualitative direction changes in the stroke relative to the grid. A qualitative direction change happens when a line indicator crosses over a grid cell boundary. In order to be authenticated, a user is required to recreate the password, which will then manage the fabrication of 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 system uses a masking mechanism – dynamic grid transformations – for the password creation process. 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 will continue until 5x5 grid cells are produced (refer to Figure 2.14 (a)).



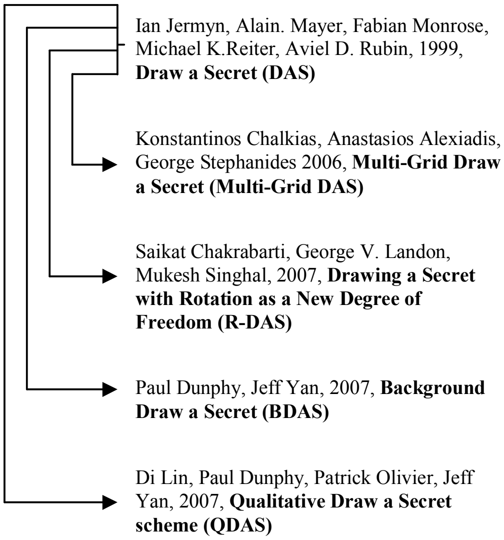
(a) Dynamic Grid (b) Grid Transformation

Figure 2.14: Qualitative Draw A Secret System (adapted from Lin et al., 2007)

In order to prevent users from producing a password or stroke that has no turning point, the QDAS system will randomly identify four random points from the stroke and perform the aforementioned dynamic grid transformations. This will increase the size of the password to an acceptable level if a user is creating a small or undersized password (refer to Figure 2.14 (b)).

Based on the results of the study conducted by Lin et al. (2007), the QDAS system produces better outcomes when compared with the DAS system in terms of usability, and resistance to shoulder-surfing attack. However, the findings from the study have no true significance because of the small sample size comprising only 10 subjects. The study also failed to show that the QDAS system can help to improve memorability.

An initiative was undertaken to organise the drawmetrics picture-based password systems according to the year of their establishment and their referred systems (refer to Figure 2.15). The figure shows that many researchers have proposed drawmetrics systems based on the DAS system. The DAS system is a pure recall system and a user is required to reproduce his password without being given any hint or cue. Therefore, most of the researchers have concentrated on making improvement to the users' memorability rather than the security aspect of the drawmetrics authentication cluster.


Ian Jermyn, Alain. Mayer, Fabian Monrose, Michael K.Reiter, Aviel D. Rubin, 1999, **Draw a Secret (DAS)**
Konstantinos Chalkias, Anastasios Alexiadis, George Stephanides 2006, **Multi-Grid Draw a Secret (Multi-Grid DAS)**
Saikat Chakrabarti, George V. Landon, Mukesh Singhal, 2007, **Drawing a Secret with Rotation as a New Degree of Freedom (R-DAS)**
Paul Dunphy, Jeff Yan, 2007, **Background Draw a Secret (BDAS)**
Di Lin, Paul Dunphy, Patrick Olivier, Jeff Yan, 2007, **Qualitative Draw a Secret scheme (QDAS)**

Note: An arrow and its direction are used to denote an enhancement of the system by other researchers.

Figure 2.15: Organisation Chart of Drawmetrics Authentication Systems

Table 2.2 is a synthesis table of the drawmetrics authentication system. It shows that most of the systems being reviewed are aimed at improving the users' memorability. The upload background and multi-grid methods have been proposed to aid the users in memorising and remembering their passwords. These two methods can also be used to reduce the tendency of users to create centred and symmetrical passwords (Chalkias et al., 2006; Dunphy & Yan, 2007). However, as stated earlier, all the systems being reviewed are vulnerable to shoulder-surfing attack. Again, this reinforces the need to develop methods that are able to mitigate shoulder-surfing attacks. This is also the main focus of this study.

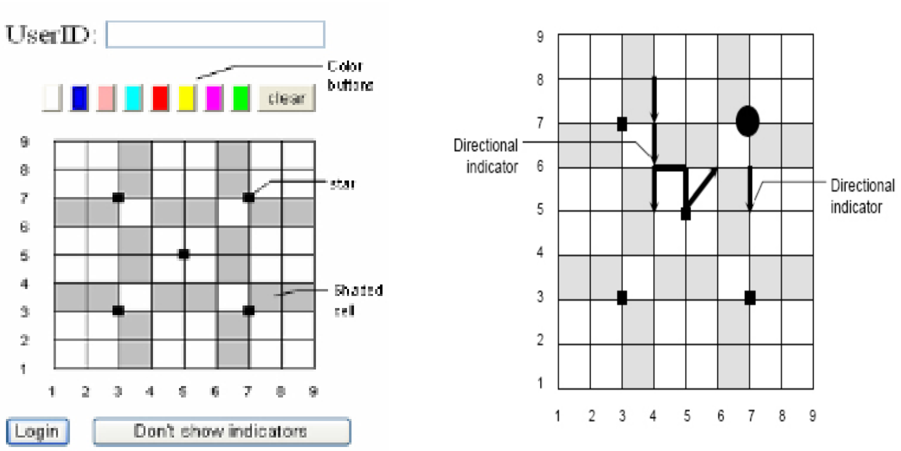
Table 2.2: Synthesis of Drawmetrics Authentication Systems

Drawmetrics Authentication System		**Password Space**	**Memorability**	**SS**	**FOA**
Pure Recall	Draw a Secret (DAS)	▪ Unlimited password space However, the password space is dependent on the number of keystrokes made by a user.	▪ Depends on the number of keystrokes made by a user. ▪ Easy to memorise if i) less strokes used and ii) centred and symmetrical drawing. ▪ Difficult to memorise if i) more and complex strokes used and ii) drawing is not centred and not symmetrical.	×	N/A
	Multi-Grid DAS	▪ Unlimited password space ▪ However, it has larger password space compared with the DAS system The password space is dependent on the number of keystroke produced by a user.	▪ Same as DAS system although the drawing produced by a user is less centred and symmetrical.	×	N/A
	DAS with Rotation	▪ Same as the DAS system	▪ Depends on the number of keystrokes made by a user. ▪ However, the user's memorability level is reduced compared with the DAS system because the user has to remember extra rotation parameters used.	×	N/A
	Qualitative Draw A Secret	▪ Same as the DAS system	▪ Depends on the number of keystrokes made by a user. ▪ However, the user's memorability level declines compared with the DAS system (Lin et al., 2007).	×	N/A
Cued Recall	Background Draw a Secret	▪ Same as the DAS system	▪ Depends on the number of keystrokes made by a user. ▪ However, the user's memorability level increases compared with DAS system due to the implementation of the cued background image technique (Dunphy & Yan, 2007).	×	N/A

Key:
SS: Shoulder-Surfing Attack
FOA: Frequency of Occurrence Analysis
× : vulnerable to
√ : invulnerable to
N/A : Not Applicable

2.4.3 Locimetrics and Drawmetrics Hybrid Authentication System

Inspired by Go (an old Chinese chess game), Tao (2006) proposed the Pass-Go system (refer to Figure 2.16 (a)). Pass-Go is an enhanced version of the DAS system based on a coordinate system with 9x9 grid cells (Tao, 2006; Tao & Adams, 2008). A user has to select or touch on the intersections of the grid cells instead of the cells when creating a password. Users can create passwords using only the dot indicator, which explains why the Pass-Go system is classified under the hybrid category of the locimetrics and drawmetrics systems. A dot indicator will appear when an intersection point is selected (or clicked), and a line indicator will appear when two or more intersections are touched continuously (refer to Figure 2.16 (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 consisting 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 for password verification and authentication.



(a) Pass-Go System GUI (b) Indicators

Figure 2.16: Pass-Go System (adapted from Tao, 2006; Tao & Adams, 2008)

There are some advantages of the Pass-Go system: it provides a higher level of security and better usability when compared with the DAS system (Tao, 2006; Tao & Adams, 2008); it prevents shoulder-surfing attack by using the hide indicators function; users can draw a shape more freely when compared with the DAS system; cued methods such as different colour schemes, star, and shaded cells are used to increase the usability of the system, and improve the memorability of the user; and, the use of 5x5 grid cells offers larger password space when compared with the DAS system.

However, the Pass-Go system has some limitations: users will get used to creating weak passwords that tend to be either symmetrical or centred; when trying to prevent shoulder-surfing attack, users might face difficulty in creating passwords if they choose the indicators to be 'invisible' because they will not know if their password has been successfully selected until the dot or line indicator appears; users have to learn and practise the use of the Pass-Go system before they are able to draw lines without making any unintentional errors.

Figure 2.17 shows the hybrid authentication system organisation chart for the locimetrics and drawmetrics systems. It is clear that Pass-Go is the only system to be categorised into this hybrid category because it allows the users to create their passwords by using only dot indicator or the mixture of dot and line indicators.

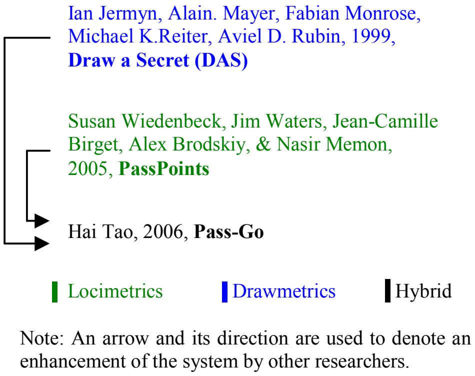

Ian Jermyn, Alain. Mayer, Fabian Monrose, Michael K.Reiter, Aviel D. Rubin, 1999, **Draw a Secret (DAS)**
Susan Wiedenbeck, Jim Waters, Jean-Camille Birget, Alex Brodskiy, & Nasir Memon, 2005, **PassPoints**
Hai Tao, 2006, **Pass-Go**
Locimetrics
Drawmetrics
Hybrid
Note: An arrow and its direction are used to denote an enhancement of the system by other researchers.

Figure 2.17: Hybrid Authentication System Organisation Chart for Locimetrics and Drawmetrics Systems

A synthesis table of the locimetrics and the drawmetrics hybrid authentication systems has been established (refer to Table 2.3). Reports in the literature strongly indicate the increasing shoulder-surfing attacks on these systems. Tao (2006) proposed an effective method to prevent attackers from shoulder-surfing the passwords of users by using the hide indicators function. However, this method will cause difficulty to the users when they are creating their passwords because the passwords drawn will also not be visible to them as well as the attackers. This study will propose methods that are able to falsify the authentication process rather than securing the whole authentication process to prevent shoulder-surfing attack. The concept of falsifying the authentication process in this context is referring to the process of using indirect tricks to confuse the attackers with the intention that the changes of making an invalid login will be increased. The importance of this method is to mislead the attackers from obtaining the correct passwords or pass-objects used. Only by implementing the proposed methods, the attackers will have no clue which passwords or pass-objects were used by the users during login processes although their passwords have been shoulder-surfed. In addition, relevant cued methods will be explored to improve the users' memorability and to impress upon them on the need to create stronger passwords by avoiding creating a centred and symmetrical password.

Table 2.3: Synthesis of Locimetrics and Drawmetrics Hybrid Authentication System

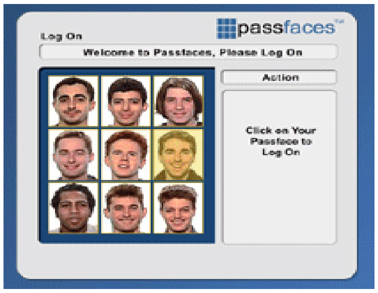
Locimetrics and Drawmetrics Hybrid Authentication System		**Password Space**	**Memorability**	**SS**	**FOA**
Cued Recall	Pass-GO	▪ Bigger password space when compared with the DAS system (Tao, 2006) ▪ Unlimited password space However, the password space is dependent on the number of keystrokes made by a user.	▪ Depends on the number of keystrokes made by a user. ▪ Different colour schemes, star, and shaded cells have been used as a cue in Pass-Go system to increase usability, and improve the memorability of a user. ▪ Easy to remember if i) less strokes used, and ii) password is centred and symmetrical. ▪ Difficult to remember if i) more and complex strokes used, and ii) password is not centred and not symmetrical. ▪ Causes difficulty to users if indicators or keystrokes are hidden when preventing shoulder-surfing attack.	√ Using hide indicators function However, users will have difficulty when identifying the password as it is invisible	N/A

Key:
SS: Shoulder-Surfing Attack
FOA: Frequency of Occurrence Analysis
× : vulnerable to
√ : invulnerable to
N/A : Not Applicable

2.4.4 Searchmetrics and Its Hybrid Authentication Systems

The term cognometric was used by the Real User Corporation to denote the measurement of the innate cognitive abilities of the human brain when users are going through the authentication process (De Angeli, Coventry, Johnson, & Coutts, 2003). Renaud and De Angeli revised the terminology to searchmetric in 2009, to represent the process of identifying or searching a number of ‘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 in a challenge set (Dirik et al., 2007; Moncur & Lepalâtre, 2007; Renaud & De Angeli, 2009). Passfaces™ is one of the earliest systems to use the searchmetrics approach in the picture-based password.

Passfaces™ is a commercial product of the Passfaces Corporation, first introduced in 2000 (Passfaces™, 2005). During the password creation process, each Passfaces™ user is required to select four human face pictures for his/her password portfolio. Throughout the authentication process, one human face picture will be selected from the user portfolio together with eight distracter human face pictures so as to form a grid of nine human face pictures (refer to Figure 2.18). In order to gain access into a Passfaces™ system, a user is required to click on the correct human face picture in four continuous attempts. In order to increase the security level against the detection of keystroke logging and packet-sniffing attacks, a randomised mechanism is applied to alter the order of the human face pictures within each grid in each attempt.



Welcome to Passfaces, Please Log On

Click on Your Passface to Log On

Figure 2.18: Passfaces™ System (adapted from Passfaces™, 2005)

Based on the results of a users' study, Brostoff and Sasse (2000) concluded that the Passfaces™ passwords are easier to remember when compared with the textual passwords. However, in their study, Davis, Monrose, & Reiter (2004) found that the Passfaces™ system has several limitations such as: limited password spaces; psychological effects and biases which can greatly influence a user to choose a predictable password; unpleasant login experience for certain users due to the predefined human face pictures generated by the Passfaces™ system; face-blind (a disorder which affects a person's ability to tell faces apart) problem; vulnerable to FOA attack, and vulnerable to shoulder-surfing attack.

In order to address the above short-comings in Passfaces and particularly, to overcome the face-blind problem, Dhamija and Perrig (2000) proposed the Déjà Vu system in 2000. Déjà Vu is a picture-based recognition password, which uses non-describable abstract pictures that are generated on-the-fly from stored seed values (refer to Figure 2.19). The Déjà Vu system consists of three processes: portfolio creation, training, and authentication processes. During the portfolio creation process, a user is required to identify a set of pictures which will be used as the password for system authentication. After creating a portfolio, the user has to go through a training session to familiarise himself with the pictures used and to improve the memorability. During the authentication process, a $n_i \times n_j$ (n_i: number of row, n_j: number of column) grid picture-based authentication challenge set, which consists of several random pictures from the user's portfolio together with other distracter or decoy pictures chosen from the system, will be formed. The user then selects the pictures that belong to his/her portfolio in order to gain access to the system.

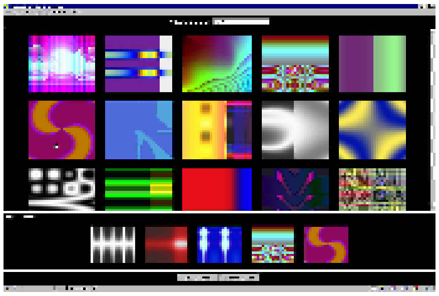


Figure 2.19: Déjà Vu System (adapted from Dhamija & Perrig, 2000)

However, storing the seeds on the server of the Déjà Vu system makes it vulnerable to several security threats such as guessing attack and shoulder-surfing attacks. An attacker could launch a brute-force attack by trying all combination of the picture selections in the challenge set because of the limited password space allocated by the Déjà Vu system. Moreover, if an attacker knows the user very well, then the attacker might make an educated guessing attack on the system by guessing what pictures the user might have in his portfolio. Similar to the Passfaces™ system, the Déjà Vu system is vulnerable to FOA and shoulder-surfing attacks. The password used by a user can easily be stolen or obtained by an attacker if the login process has been recorded.

Sobrado and Birget (2002) proposed a series of three picture-based password systems in 2002 to overcome the shoulder-surfing problem. The authors called the first system a triangle system. During the registration process, a user is required to select three pass-objects (secret pass-objects), which work as a clue for the triangle system. For authentication, the user is required to find the three secret pass-objects and click within the region of an invisible triangle or the convex hull of the pass-objects that is formed by the three secret pass-objects (refer to Figure 2.20).

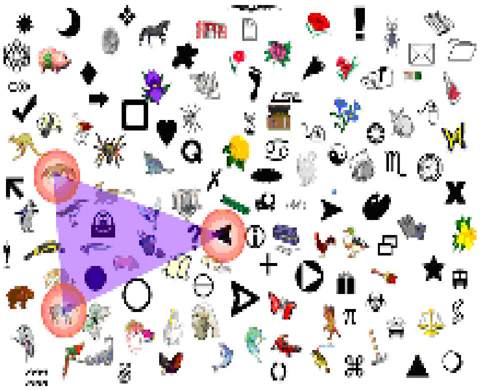


Figure 2.20: Triangle System (adapted from Sobrado & Birget, 2002)

Xiaoyuan et al. (2005), and Sobrado and Birget (2002) suggested that the number of objects used can be a few hundreds or a few thousands in order to make the password difficult to be guessed. Moreover, by increasing the number of objects, the triangle system also decreases the possibility of brute-force attack because an attacker would require extra effort. Additionally, allowing the user to click within the convex hull, as implemented in the triangle system, is an effective way to resist shoulder-surfing attack. A shoulder-surfing attacker will not have any clue as to which pass-objects have been used by a user to gain access to the system, even if the authentication process has been recorded.

However, there are some drawbacks of this system. Increasing the number of objects will cause the display screen to become congested and cluttered. Users will have difficulties in searching for the secret pass-objects if the number of objects used is relatively large. On the other hand, if the number of objects used is relatively small, the size of the convex hull formation will become larger, thus, making the system easier to crack or guess. As a result, distributing the three secret pass-objects has become an issue of concern as it can affect the size of the convex hull formation. Unfortunately, no further research has been carried out on the distribution of the secret pass-objects.

The second system, the movable frame system, was also proposed by Sobrado and Birget in 2002. The movable frame system is similar to the triangle system, and it also requires a user to recognise pre-selected secret pass-objects. However, it involves only two secret pass-objects, while the third object is placed in the movable frame. In order to be authenticated, a user is required to move or rotate the frame until the locations of all the pass-objects are aligned in a row with the assistance of the two secret pass-objects (refer to Figure 2.21).

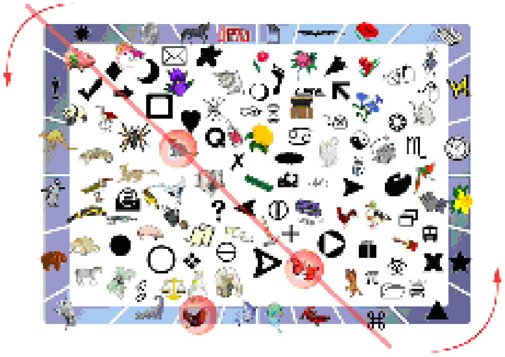


Figure 2.21: Movable Frame System (adapted from Sobrado and Birget, 2002)

In order to increase its usability among the users, Sobrado and Birget suggested that the users practise more on rotating the frame. However, rotating the frame repeatedly is time-consuming and causes the authentication process to be slow as there are too many non-pass-objects involved (Xiaoyuan et al., 2005; Hafiz et al., 2008).

Sobrado and Birget (2002) also proposed the third system – the Special Geometric Configuration system. This system inherits the features of the two the previous methods and thus performs at a higher level of complexity by using four pass-objects, which work as two invisible lines to create an intersection point (refer to Figure 2.22). In order to be authenticated, a user is required to click on the pass-objects that fall inside the convex quadrilateral region (the intersection point).

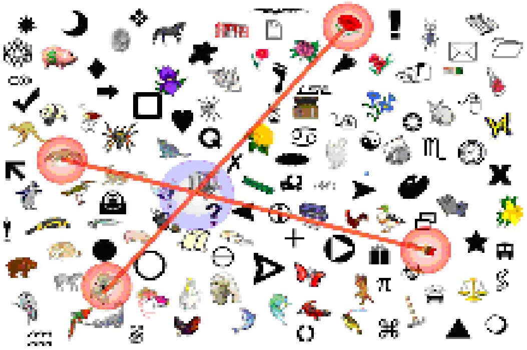
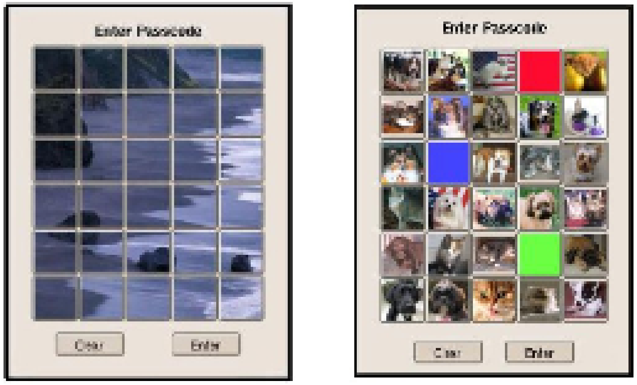


Figure 2.22: Special Geometric Configuration System (adapted from Sobrado and Birget, 2002)

The password space allocated by the Special Geometric Configuration system is dependent on the number of pass-objects used in the system. The system is able to resist shoulder-surfing attack because the pass-objects of a user is dynamically chosen in every single attempt. However, no further research has been carried out to determine the optimum number of pass-objects to be used. Moreover, no usability testing has been conducted either by the authors or by other researchers on the system.

Jansen, Gavrila, Korolev, Ayers, and Swanstrom (2003) proposed the Picture Password system in 2003. The system is a 5×6 grid picture-based authentication system designed especially for mobile devices such as PDAs. During the password creation process, a user is required to identify a sequence of pictures within the three predefined themes (i.e., Cats & Dogs theme, and Sea & Shore theme) as his/her password (refer to Figure 3(a) - (b)). The authentication process for the Picture Password system is dependent on the need of the system. For example, a user can be requested to identify his/her password using an eight-entry picture sequence or using two pictures during the system authentication process. The security level solely relies on the system itself. However, the user is still required to recognise and identify the correct pictures and their correct sequence in order to be authenticated.



(a) Sea and Shore Theme (b) Cats and Dogs Theme

Figure 2.23: Picture Password System (adapted from Jansen et al., 2003)

The Picture Password system can allocate a larger password space by increasing the size of the grid. However, it is still vulnerable to brute-force attack and a user's password can still be observed and learned by an attacker if the login process has been recorded. As a result, the Picture Password system is still not able to resist the guessing and the shoulder-surfing attacks. Besides, the Picture Password system is also vulnerable to other security threats such as keystroke logging attack because of the static and fixed locations of all the pictures used in all authentication attempts. The Picture Password system will also face an FOA attack if it uses a uniform randomisation algorithm to select the secret password and the decoy pictures.

Man, Hong and Mathews (2003) developed the Where Is Waldo (WIW) system in 2003 (refer to Figure 2.24). In the WIW system, a user is required to select a number of pictures as pass-objects. Each pass-object has two perturbations (variants) and each perturbation is associated with a unique code (Xiaoyuan et al., 2005). During the authentication process, the user has to go through several scenes, and each scene consists of a few pass-objects and perturbations, which are randomly generated by the system. The user then has to input a string of unique code corresponding to the pass-object variants, which appear in the scene as well as a code indicating the relative location of the pass-objects with reference to an eye-shape icon at the centre of the system. To confuse a shoulder-surfing attacker and other attackers, the WIW system uses a mechanism that generates perturbations on non-pass-objects which are similar to those perturbations on pass-objects.

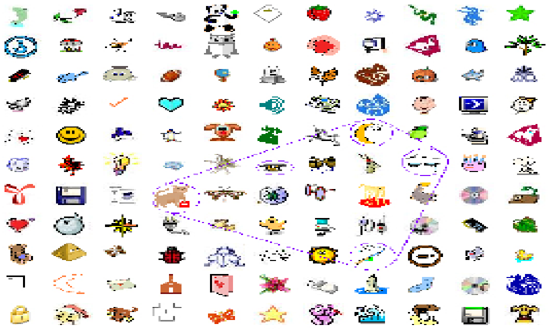


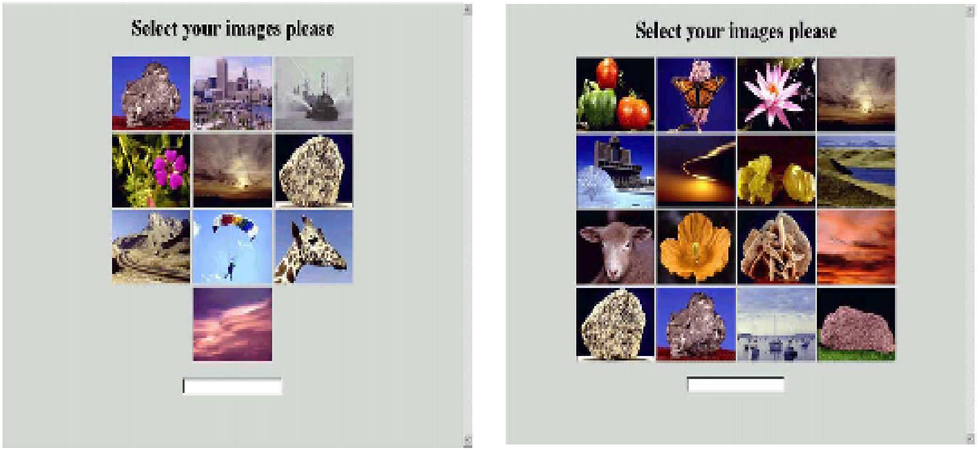
Figure 2.24: Where Is Waldo (WIW) System (adapted from Man et al, 2003)

There are some advantages of the WIW system: it can improve the user's memorability by allowing him to select the number of pass-objects to be used. However, the authentication process will be more complex if the user chooses a large number of pass-objects. This is because the number of passwords that have to be memorised by a user increases proportionally for every number of pass-object used. On the other hand, if the user chooses a small number of pass-objects, there is high likelihood of security threats such as guessing or brute-force attacks on the password. However, the WIW system is able to resist shoulder-surfing attack as the users are required to input the unique codes instead of clicking on the pass-objects during the login process. In this way, there is no threat from the shoulder-surfing attackers.

De Angeli et al. (2003) introduced a series of Visual Identification Protocol (VIP) systems in 2003. All the VIP systems use the pictorial concept in place of the PIN numbers commonly used in Automatic Teller Machine (ATM), for authentication. The pictures used in the VIP systems can be clustered into nine semantic categories: flowers; animals; rocks; landscapes; humans; vegetables; buildings; skies; and, boats.

In the first VIP system (VIP1), a user has to select a sequence of four pictures out of ten pictures in the same position at each authentication attempt. At every authentication attempt, the pictures from the user's selected categories and a new set of distracter pictures will be extracted from the visual database. To login, the user has three attempts to identify the correct picture. This is similar to logging in at the ATM machine, which also allows a user only three attempts to enter the correct PIN. However, for all authentication processes, there is no reshuffling of the pictures and their locations in the grid. This makes the VIP1 system vulnerable to keystroke logging attack. The VIP1 system is also vulnerable to FOA attack because of the uniform randomisation algorithm used when selecting the secret passwords and the decoy pictures. In addition, the VIP1 system is vulnerable to shoulder-surfing attacks because the passwords selected by the user can be observed by shoulder-surfing attackers.

The second VIP system (VIP2) differs from the VIP1 system because in the VIP2 system, the four pictures forming the authentication code are displayed randomly around the visual keypad at the beginning of each authentication attempt (De Angeli et al., 2005). However, in order not to disclose any clue about the authentication code, the same visual configuration will be displayed if a failed authentication is detected. Hence, the VIP2 system is able to prevent keystroke logging attack. However, the VIP2 system is still vulnerable to FOA attack and shoulder-surfing attack (refer to Figure 2.25 (a) for the VIP1 and VIP2 graphical user interfaces).



(a) VIP1/VIP 2 Interface

(b) VIP3 Interface

Figure 2.25: Visual Identification Protocol (VIP) Systems (adapted from De Angeli et al., 2005)

The third VIP system (VIP3) uses a different mechanism in password identification and generation. A user is required to create a portfolio that has eight pictures selected from the nine predefined semantic categories. However, to prevent replication of the categories of the code items displayed in the current challenge set, only four pictures from the portfolio will be randomly used together with another 12 distracter pictures, which will be selected randomly from the remaining categories so as to form a 4×4 grid cells picture-based authentication system (refer to Figure 2.25 (b)). To avoid accidental disclosure of the authentication code, the same visual configuration will be displayed if an invalid authentication has been detected. On the other hand, a user is required to identify the four pictures used from the portfolio in the correct sequence before he/she can gain access into the system.

De Angeli et al. (2005) claimed that all the systems in the VIP series help in making it easier for users to memorise their passwords. However, those systems in their VIP series are still vulnerable to guessing attack because of the small password space used in the VIP1, and VIP2 systems, (which has a maximum of 104 possibilities in sequence) and the VIP3 system (which has a maximum of 1820 possibilities in sequence). Nevertheless, the VIP2 and VIP3 systems are able to improve the resistance to keystroke logging attack by using the random positions and random picture selections from the user's portfolio, as mentioned earlier. The four-choose-eight password selection mechanism used in the VIP3 system makes a user's password secure against attacks, even though the login process has been recorded. Thus, the VIP3 system is better at preventing shoulder-surfing attack when compared with the other two systems in the VIP series. Nevertheless, the shoulder-surfing threat cannot be totally resolved because the VIP3 system is vulnerable to FOA attack (refer to the demonstration in section 1.3).

Figure 2.26 shows the graphical user interface for the Story system. An evaluation of the Story system and the Passfaces™ system was carried out by Davis et al. (2004). The findings showed that the Story system has the same authentication mechanism as the Passfaces™ system. During the password selection process, the users select a sequence of pictures from nine predefined categories (animals, cars, women, food, children, men, objects, nature, and sports) rather than using only human faces from different races. However, each of the images selected must be derived from a distinct category of the image types. Based on the evaluation results, Davis et al. concluded that the Story system is better in improving the users' memorability when compared with the Passfaces™ system. This is because the Story system users are able to create a chronological story based on the selected pictures. However, both the Story system and Passfaces™ system use the same mechanism for authentication. Therefore, the Story system is also vulnerable to brute-force, guessing, shoulder-surfing, and FOA attacks.

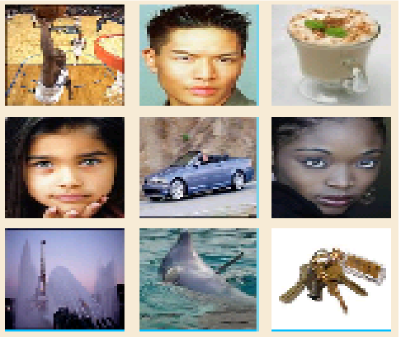
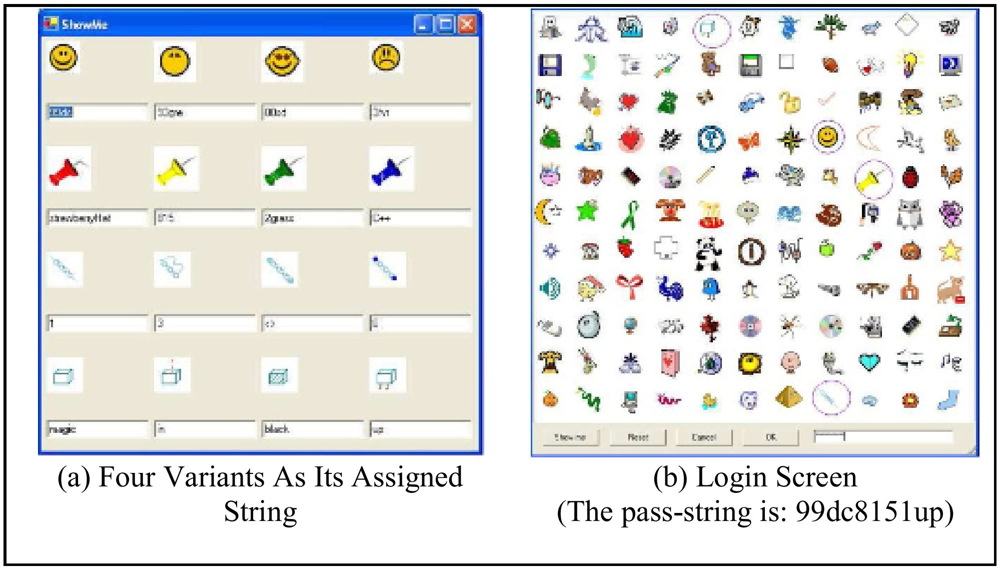


Figure 2.26: Story System (adapted from Davis et al., 2004)

In 2004, Hong et al. proposed the Pict-O-Lock system which was an improved system of the WIW system. In this system, *n* icons are used during the login process and a user is required to select *k* pass-icons. Each *n* icon has *m* variants, and the user is required to assign a string for each variant, respectively (refer to Figure 2.27 (a)). The *k* value and the *m* value can be personalised by each user, while the *n* value is predefined by the system.



[illegible] | 33one | [illegible] | [illegible]

strawberryHat | 815 | 2grass | C++

1 | 3 | <> | [illegible]

magic | in | black | up

(a) Four Variants As Its Assigned String

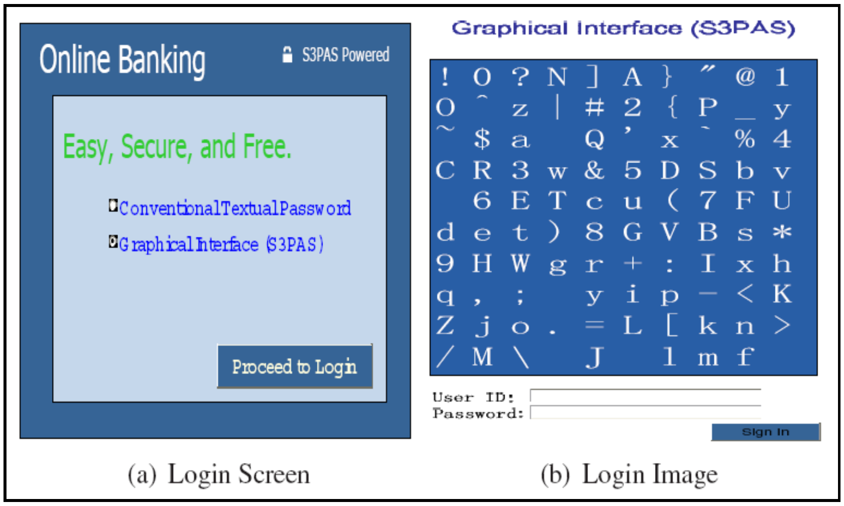
(b) Login Screen
(The pass-string is: 99dc8151up)

Figure 2.27: Pict-O-Lock System (adapted from Hong et al., 2004)

During the authentication process, the user has to identify the variants, which have been randomly generated by the system together with the sequence of the pass-icons used. The user then has to recall each string associated with the generated variant and the result of the concatenated string formed will be used as a pass-string for the authorisation process in the Pick-O-Lock system (refer to Figure 2.27 (b)).

Hong et al. stated that the design of the variants help to improve the memorability of users. They also claimed that the Pick-O-Lock system is able to resist spyware and shoulder-surfing attacks by using their proposed mechanism. In addition, FOA attacks hardly occur because of the large number of pass-icons used.

The password space for the Pick-O-Lock system is *mk*. Obviously, if the *k* value and the *m* value used by a user are sufficiently large, the Pick-O-Lock system will in turn allocate a password space that is also sufficiently large. However, if a large value is assigned for each *k* and each *m*, the user might have difficulty in memorising all the strings used to associate with the variants. The user must not forget a single string used or his login process will fail. Thus, users are advised to assign a string which acts as a cue to associate with each variant.



Online Banking

S3PAS Powered

Easy, Secure, and Free.

□ Conventional Textual Password

☒ Graphical Interface (S3PAS)

Proceed to Login

(a) Login Screen

Graphical Interface (S3PAS)

!	O	?	N	]	A	}	″	@	1
O	ˆ	z	|	#	2	{	P	_	y
~	$	a		Q	’	x	ˋ	%	4
C	R	3	w	&	5	D	S	b	v
	6	E	T	c	u	(	7	F	U
d	e	t	)	8	G	V	B	s	*
9	H	W	g	r	+	:	I	x	h
q	,	;		y	i	p	–	<	K
Z	j	o	.	=	L	[	k	n	>
/	M	\		J		l	m	f	

User ID:

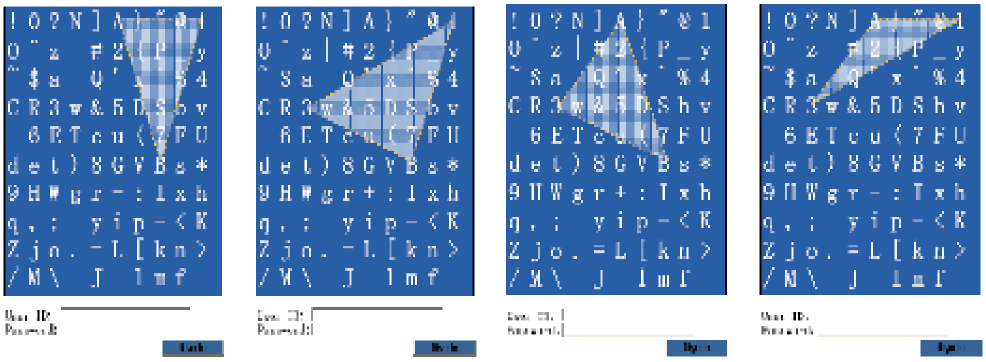
Password:

Sign In

(b) Login Image

Figure 2.28: Scalable Shoulder-Surfing Resistant Textual-Graphical Password Authentication Scheme (S3PAS) System (adapted from Zhao and Li, 2007)

Figure 2.28 shows the S3PAS system proposed by Zhao and Li in 2007. The development of the S3PAS system was inspired by the work of Sobrado and Birget (2002). Before a user is able to login, he is required to identify a set of characters to be the password. The password must have a minimum length of three characters. Users are allowed to use the same character again to form his password. During the authentication process, the password or the set of characters is grouped into three-character groups, recursively, and the user is required to identify each session password that consists of any character within the convex hull that is formed by the triangular shape of the three-character groups. For example, if a user has selected “A1B3” as his original password, he is required to identify the session passwords within the convex hull that is formed by the triangular shape of “A1B”, “1B3”, “B3A” and “3A1” (refer to Figure 2.29).



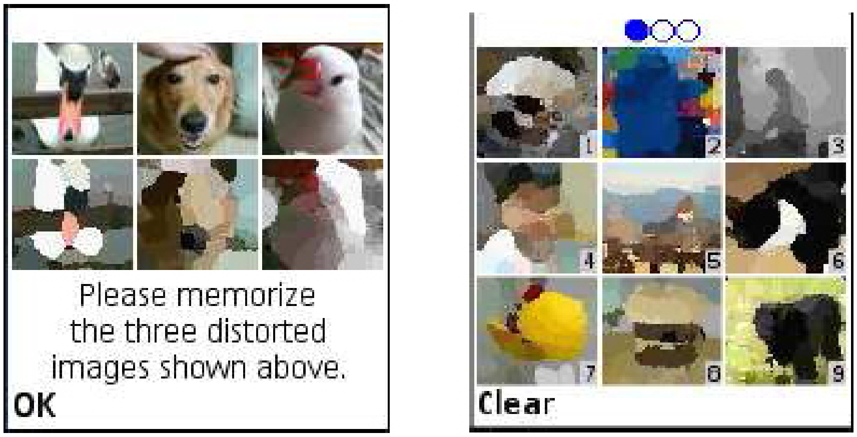
(a) pass-triangle △A1B (b) pass-triangle △1B3 (c) pass-triangle △B3A (d) pass-triangle △3A1

Figure 2.29: S3PAS Session Password Determination (adapted from Zhao and Li, 2007)

The users are allowed to click on the login image or use the keyboard to input the session passwords. Besides, Zhao and Li (2007) claimed that the S3PAS is able to resist shoulder-surfing attack because a shoulder-surfing attacker does not have any clue which password or characters have been used by a user to gain access to the system even if the authentication process has been recorded. Moreover, Zhao and Li used a fixed login image with 94 characters to reduce the complexity associated with the number of characters used. In order to increase the resistance to brute-force attack, Zhao and Li suggested that a user will be given a brand new login image with random scatter characters if a user fails to identify the session password every *I* (i.e., *I* = 10) times. In addition, they also suggested that in order to address the issue of redundant character, users can click on an invisible line that are formed by two redundant characters (i.e., A1A) or an invisible circle that is formed by three redundant characters (i.e., AAA).

However, there was no mention about the length and radius of the invisible line and circle formation, respectively. Besides, there will be an issue regarding the distribution of the original password used if the convex hull size is relatively small as no algorithm is used in the S3PAS system to identify a reasonable size of the convex hull used (i.e., A#2). Moreover, because of the memorability issue, users may write down their original password when trying to create a group of three characters recursively before identifying the session passwords.

Inspired by the Déjà Vu and the Passfaces™ systems, Hayashi et al. (2008) proposed the Use Your Illusion system in 2008. There are three processes in the Use Your Illusion system. During the portfolio creation process, a user is required to choose three pictures as his password. After creating the password, a distorted mechanism will be applied to the chosen pictures. The three original pictures together with the distorted pictures are then displayed side-by-side during the priming process (refer to Figure 2.30 (a)). The user is required to go through a short training in order to familiarise himself and improve his memorability of the pictures used in the portfolio. During the authentication process, a 3×3 grid picture-based authentication challenge set, which consists of nine distorted pictures, will be formed. The user is required to identify one of his passwords in the 3×3 grid cells in three consecutive attempts before he can be authorised to access the system (refer to Figure 2.30 (b)).



Please memorize
the three distorted
images shown above.

(a) Three Password Images and Its Distorted Images

(b) A Challenge Set of Images

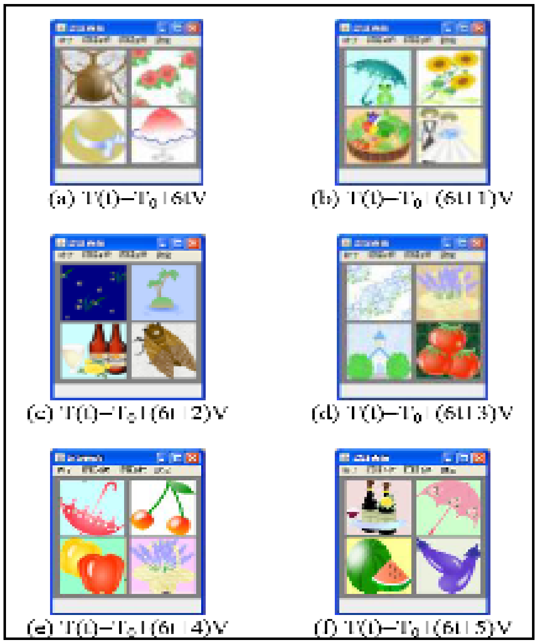
Figure 2.30: Use Your Illusion System (adapted from Hayashi et al., 2008)

In the Use Your Illusion system, it is difficult to revert mentally towards a degraded picture without having any prior knowledge of the original picture. As a result, Hayashi et al. claimed that their system can provide a strong line of defence against access by an impostor. Apart from that, users can use the system to personalise their portfolio by uploading their preferred pictures rather than using the predefined pictures. Compared with the Déjà Vu system, the Use Your Illusion system is better in enhancing users' memorability because abstract pictures are used and they are semantically meaningful to the users.

However, the password space used by the Use Your Illusion system is as small as that in the Passfaces™ system. As a result, an attacker can launch a brute-force attack or guessing attack by attempting all combinations of the picture selections in the challenge set. The Use Your Illusion system is vulnerable to both shoulder-surfing and FOA attacks if the login process has been recorded, or a uniform algorithm is used.

Nevertheless, Hayashi et al. claimed that the system has been successful in preventing brute-force, guessing, and shoulder-surfing attacks.

Takumi, Yuko, and Masakatsu (2009) proposed the Temporal Indirect Image-Based Authentication (TI-IBA) system in 2009 (refer to Figure 2.31). The TI-IBA system consists of two processes: registration process, and authentication process. During the registration process, users are required to identify *P* number of pictures as his pass-images. During the authentication process, a set of *N* slide-shows will be generated according to the system presettings. There will be a set of *M* pictures in each slide-show. The pass-images will be inserted into one of the slide-shows and each image of each slide-show will take *t* seconds to change from one image to another. In order for a user to be authenticated, he needs to observe and click on the slide-show that consists of his pass-images. To prevent users from overlooking his pass-images, a *Q* repetition cycle is implemented to repeat the rotation of the images in all the slide-shows.



(a) $T(t)-T_0+6tV$

(b) $T(t)-T_0+(6t+1)V$

(c) $T(t)-T_0+(6t+2)V$

(d) $T(t)-T_0+(6t+3)V$

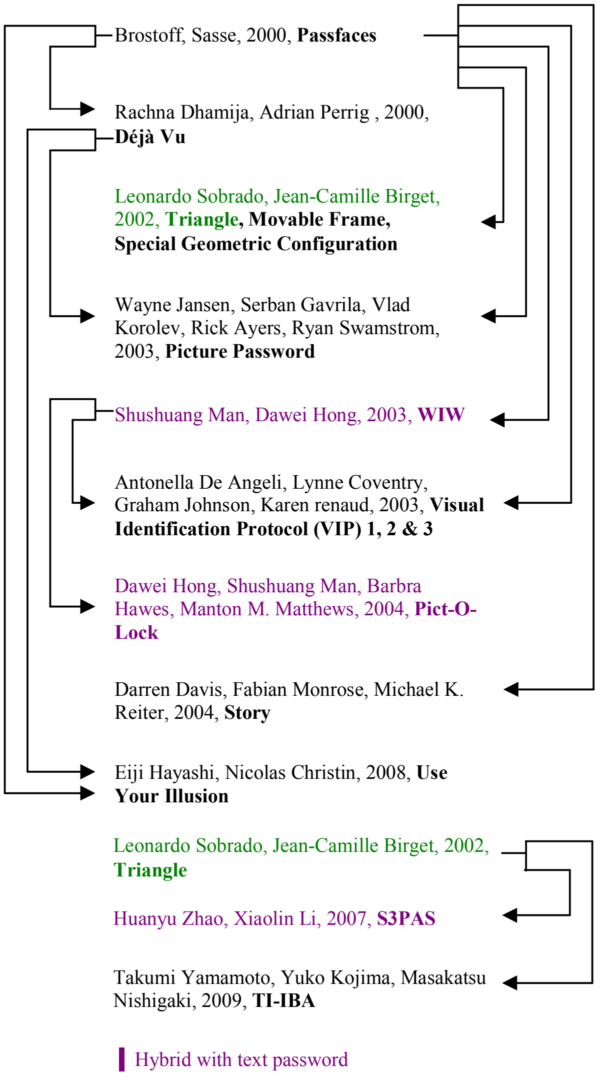
(e) $T(t)-T_0+(6t+4)V$

(f) $T(t)-T_0+(6t+5)V$

Figure 2.31: Temporal Indirect Image-Based Authentication (TI-IBA) (adapted from Takumi et al., 2009)

The results from studies using the TI-IBA system showed better improvement in the users' ability in memorising their password, when compared with the Triangle system. However, Takumi et al. admitted that the TI-IBA system is vulnerable to shoulder-surfing, guessing, and brute-force attacks. One of the reasons for this is that the underlying algorithm is vulnerable to guessing attack. For example, it is clear that an attacker has a high probability of guessing the correct slide-show (one out of *N* slide-shows) that consists of the pass-images used by an authorised user, although the attacker does not need much information about which pictures are the pass-images. Besides, the TI-IBA system will be open to FOA attack if it uses the uniform randomisation algorithm to select the secret password and the decoy pictures.

Figure 2.32 shows the organisation chart of the searchmetrics and its hybrid authentication systems. It is evident that most of the systems have evolved from the Passfaces™ system. In addition, hybrid systems, which make use of both text-based password and picture-based password, have been proposed.


Brostoff, Sasse, 2000, Passfaces
Rachna Dhamija, Adrian Perrig , 2000, Déjà Vu
Leonardo Sobrado, Jean-Camille Birget, 2002, Triangle, Movable Frame, Special Geometric Configuration
Wayne Jansen, Serban Gavrila, Vlad Korolev, Rick Ayers, Ryan Swamstrom, 2003, Picture Password
Shushuang Man, Dawei Hong, 2003, WIW
Antonella De Angeli, Lynne Coventry, Graham Johnson, Karen renaud, 2003, Visual Identification Protocol (VIP) 1, 2 & 3
Dawei Hong, Shushuang Man, Barbra Hawes, Manton M. Matthews, 2004, Pict-O-Lock
Darren Davis, Fabian Monrose, Michael K. Reiter, 2004, Story
Eiji Hayashi, Nicolas Christin, 2008, Use Your Illusion
Leonardo Sobrado, Jean-Camille Birget, 2002, Triangle
Huanyu Zhao, Xiaolin Li, 2007, S3PAS
Takumi Yamamoto, Yuko Kojima, Masakatsu Nishigaki, 2009, TI-IBA
▌ Hybrid with text password

Note: An arrow and its direction are used to denote an enhancement of the system by other researchers.

Figure 2.32: Organisation Chart of Searchmetrics and Its Hybrid Authentication Systems

There have been several suggestions to increase the number of pass-icon/object/picture used in a system to enlarge the password space. However, the notion of increasing the number of pass-icon/object/picture used in a system is not an appropriate move solely for the purpose of enlarging the password space of a system as this can give rise to problems for a user in visualising and memorising the combination or the number of pass-icon/object/picture used. Therefore, ensuring security for all the activities in the authentication process or falsifying the authentication process is still the better way of reducing shoulder-surfing attacks despite the fact that the password space of a proposed system is relatively small.

With regard to FOA attack, most of the systems reviewed (except for Triangle, Movable Frame, Special Geometric Configuration and the hybrid systems) are vulnerable to the FOA attack because of the uniform randomisation algorithm used (see Table 2.4). Therefore, it is important to develop methods to prevent FOA attacks.

On the need to improve users' memorability, various cued techniques such as story line, object variants, and chronological effect have been identified as the value-added elements for improving the users' memorability in the searchmetric authentication cluster.

Table 2.4: Synthesis of Searchmetric Authentication Systems

Searchmetrics Authentication System			Password Space	Memorability	SS	FOA
Recognition	Pure Recall	Passfaces™	▪ Generic Password Space: N^K (Xiaoyuan et al., 2005) N is the total number of pictures generated at each round, K is the number of attempts.	▪ Easy to remember ▪ Difficult to remember if a user has face-blind problem.	×	×
		Déjà Vu	▪ Generic Password Space: $\frac{N!}{K!(N-K)!}$ (Xiaoyuan et al., 2005) N is the total number of pictures generated at each round, K is the number of password pictures used during an authentication process.	▪ Easy to remember	×	×
		Triangle	▪ Generic Password Space: $\frac{N!}{K!(N-K)!}$ (Xiaoyuan et al., 2005) N is the total number of picture objects generated at each round, K is the number of pass-objects used during an authentication process.	▪ Easy to remember but more difficult than Passfaces™ and the Déjà Vu systems. ▪ Difficult to search the secret pass-objects if the number of objects used is relatively large.	√	N/A
		Movable Frame			√	N/A
		Special Geometric Configuration			√	N/A
		Picture Password	▪ Generic Password Space: $\left(\frac{N!}{(N-K)!}\right)^J$ N is the total number of pictures generated at each round, K is the number of password pictures used during an authentication process, J is the number of attempts.	▪ Easy to remember	×	× if uniform algorithm is used
		VIP1	▪ Generic Password Space: N^K N is the total number of pictures generated at each round, K is the length of the password.	▪ Easy to remember	×	×
		VIP2		▪ Easy to remember	×	×
		VIP3	▪ Generic Password Space: $\frac{N!}{(N-K)!}$ N is the total number of pictures generated at each round, K is the number of selected password pictures.	▪ Easy to remember but more difficult than VIP1 and VIP2	√	×
		Use Your Illusion	▪ Generic Password Space: N^K N is the total number of distorted pictures generated at each round, K is the number of attempts.	▪ Easy to remember ▪ Easier to remember when compared with Déjà Vu system (Hayashi et al., 2008)	×	×

Key:
SS: Shoulder-Surfing Attack
FOA: Frequency of Occurrence Analysis
× : vulnerable to
√ : invulnerable to
N/A : Not Applicable

Table 2.4: Synthesis of Searchmetric Authentication Systems (continued)

Searchmetrics Authentication System			Password Space	Memorability	SS	FOA
Recognition	Pure Recall	S3PAS	▪ Generic Password Space: $\frac{94}{K!(94-K)!}$ K is the number of session passwords used during an authentication process.	▪ Easier to remember when compared with the Triangle system. ▪ Users may write down their original password when trying to create a group of three characters recursively before identifying the session passwords. ▪ Difficult in identifying the invisible line and circle formation as no information about the length of the line, or radius of the circle is given.	√	N/A
		TII-BA	▪ Generic Password Space: $\frac{1}{N}$ *N* is the number of slide-shows used during an authentication process. *K* is the number of perturbations used	▪ Easier to remember as compared to Triangle system.	×	× if uniform algorithm is used
	Cued Recall	Story	▪ Same as Passfaces™	▪ Easy to remember ▪ Able to create a chronological story based on the selected pictures. ▪ Easier to remember as compared to the Passfaces™ system (Davis et al., 2004)	×	× if uniform algorithm is used
		Where Is Waldo	▪ Generic Password Space: $\left(\left(\frac{N!}{(N-K)!}\right)\times 94^{J_i}\right)^L$ *N* is the number of icons generated at each round. *K* is the number of perturbations used. J_i is a unique code for each perturbation. A unique code is formed from a string of 94 printable characters (excluding space). *L* is the number of attempts.	▪ Difficult to remember ▪ Users have to identify the perturbations which have been randomly generated by the system together with the sequence of the icons used and the respective unique code for each perturbation.	√	N/A
		Pict-O-Lock	▪ Generic Password Space: $\left(\frac{N!}{(N-K)!}\right)\times 94^{J_i}$ *N* is the total number of variants generated, *K* is the number of variants used. J_i is the length of the password for each variant. There are 94 printable characters excluding space.	▪ Difficult to remember but easier than WIW system because a user is required to authenticate in a single attempt. ▪ Users have to identify the variants which have been randomly generated by the system together with the sequence of the pass-icons used and the respective string used for each variant.	√	N/A

Key:
SS: Shoulder-Surfing Attack
FOA: Frequency of Occurrence Analysis
× : vulnerable to
√ : invulnerable to
N/A : Not Applicable

2.5 Summary

This chapter provides a review of the literature pertinent to the study. Various picture-based password authentication security threats were studied and categorised into: Surveillance Approach; Password Guessing and Cracking Approach; Malicious Software (malware); and Social Engineering attacks. Various picture-based password systems – locimetric, drawmetric, searchmetric systems, and their hybrid authentication clusters – have been reviewed to learn more about their strengths, weaknesses, and the underlying concepts of each system. The reviewed systems have also been evaluated and compared vis-a-vis their vulnerability to security threats, the password space, and the features for improving users' memorability. In general, the results of the analyses indicate that users' memorability and security are the main issues that must be considered when developing a better picture-based password authentication system. From the information gathered from the literature, many of the reviewed systems are vulnerable to shoulder-surfing and FOA attacks. To prevent shoulder-surfing attack, it is important to ensure the security of all the activities of an authentication process. However, this method will give rise to problems for users because the passwords drawn or identified are invisible to the users as well as the attackers. Thus, falsifying the authentication process was proposed, as it is an effective method for mitigating the shoulder-surfing attacks. The importance of proposing the methods that are able to falsify the authentication process is to trick or mislead the attackers from obtaining the correct passwords or pass-objects used. By doing so, the attackers will have no clue which passwords or pass-objects were used by the users during login processes although their passwords have been shoulder-surfed. FOA attack is a newly-discovered security threat, which uses a technique for identifying the rate of recurrence of a set of images generated by a secure system. Many searchmetrics picture-based password systems are vulnerable to FOA attacks because they use a uniform algorithm to select the secret password and the decoy pictures. Hence, one of the main objectives of this study is to propose a method that is able to prevent FOA attack, and at the same time, be able to retain the randomness of the secret password and the decoy pictures. In creating passwords, users are expected to comply with two fundamentally contradictory requirements – the password must be easy to memorise, and yet it has to be secure (Wiedenbeck et al., 2005b). Therefore, it is crucial to ensure that the proposed system makes it easy for users to memorise and identify theirs password during the authentication process. The next chapter describes the methodology used in the study.

Chapter 3 Methodology

3.1 Introduction

This chapter describes the methods used in the research to achieve the research objectives, mentioned in Chapter 1. The details of the data gathering techniques, the instruments used, and data analysis techniques are presented. The last section concludes this chapter with a chapter summary.

3.2 Approaches to Research

Figure 3.1 shows the research methodology framework of this research. An analysis of the features of the various picture-based password authentication systems was carried out based on information gathered from the literature review. The results from the analysis give a better understanding and more accurate perspective of the developments and current issues in picture-based password authentication systems. The information also provides direction for this research, and aids in formulating the following objectives:

1. To propose falsifying authentication methods to mitigate shoulder-surfing attack. The methods include the use of: (a) penup event and neighbouring connectivity; (b) partial password selection and metaheuristic randomisation algorithm.

2. To design and implement the proposed falsifying authentication methods, specifically related to the picture-based password authentication clusters.

3. To evaluate the capability of the proposed methods in mitigating shoulder-surfing attack.

4. To evaluate the capability of the metaheuristic randomisation algorithm in preventing FOA attack (only for the searchmetric cluster).

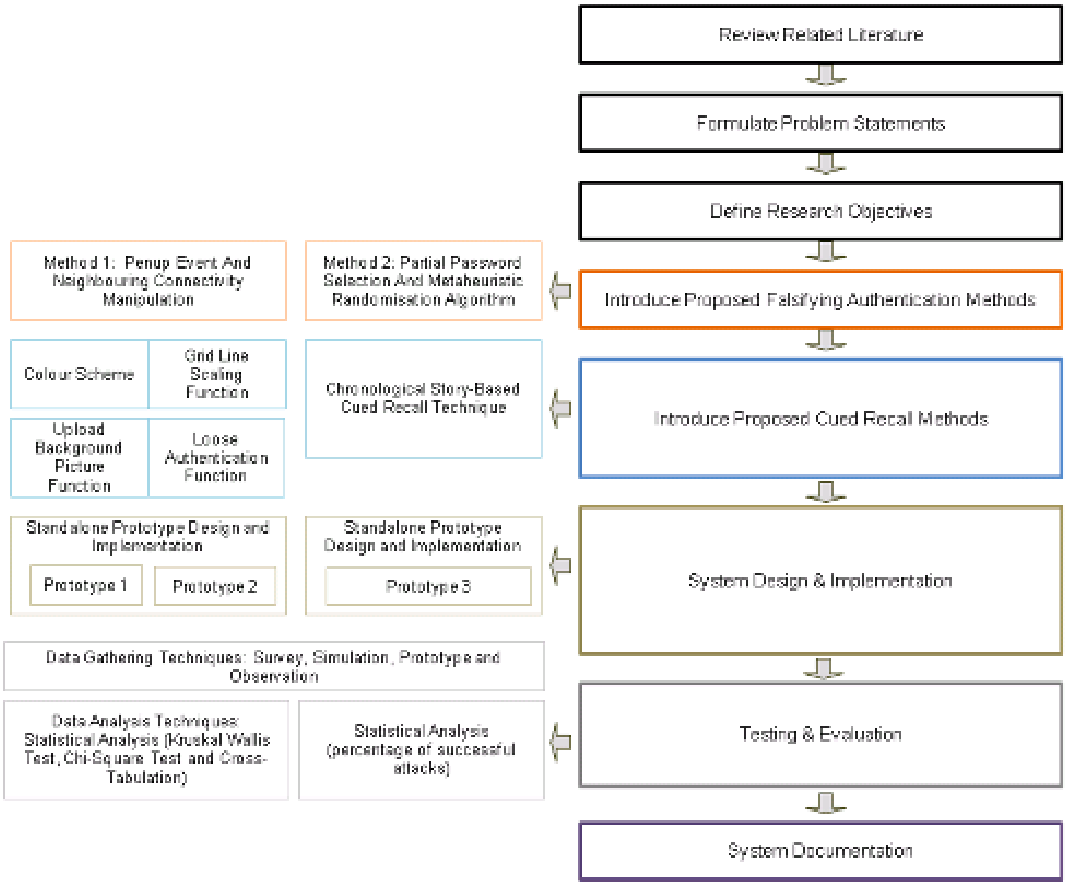

Review Related Literature
Formulate Problem Statements
Define Research Objectives
Method 1: Penup Event And Neighbouring Connectivity Manipulation
Method 2: Partial Password Selection And Metaheuristic Randomisation Algorithm
Introduce Proposed Falsifying Authentication Methods
Colour Scheme
Grid Line Scaling Function
Upload Background Picture Function
Loose Authentication Function
Chronological Story-Based Cued Recall Technique
Introduce Proposed Cued Recall Methods
Standalone Prototype Design and Implementation
Prototype 1
Prototype 2
Standalone Prototype Design and Implementation
Prototype 3
System Design & Implementation
Data Gathering Techniques: Survey, Simulation, Prototype and Observation
Data Analysis Techniques: Statistical Analysis (Kruskal Wallis Test, Chi-Square Test and Cross-Tabulation)
Statistical Analysis (percentage of successful attacks)
Testing & Evaluation
System Documentation

Figure 3.1: Research Methodology Framework

3.2.1 Proposed Falsifying Authentication Methods and Cued Recall Methods

To achieve the first objective, it is important to propose methods that can mitigate shoulder-surfing attack. The following two falsifying authentication methods have been are proposed:

i. penup event and neighbouring connectivity manipulation

ii. partial password selection and metaheuristic randomisation algorithm.

The first method, above, is designed to deceive the shoulder-surfing attackers, and this is done by using the concept of bypassing the nearest neighbour from one intersection point to another to trick the attackers when drawing a password in a G×G grid cells environment (G is the size of the grid used). Another trick is used to increase the probability of the attackers guessing the password incorrectly. This is done by holding the mouse click long enough before manoeuvring the mouse to another intersection point to create a 'flawed' keystroke or penup event. However, both tricks can only be applied to the drawmetrics cluster or the locimetrics and drawmetrics hybrid cluster, which allows users to draw their passwords on the grid cells. The first falsifying authentication method was incorporated in the encoding scheme of our first proposed Background Pass-Go (BPG) system. Besides, an upload background picture function and a new colour scheme feature were designed and implemented in the BPG system to make it easy for users to memorise their password.

To improve the users' memorability, the enhanced Background Pass-Go (enhanced BPG) system was proposed. An extra grid line scaling function and a loose authentication method were designed and implemented in the enhanced BPG system to improve the users' memorability.

To apply the method to the searchmetrics cluster, the second falsifying authentication method, which uses the concept of selecting partial password pictures instead of a fixed number of password pictures or all the password pictures that were identified by a user during the enrollment (password registration) process, was proposed. The proposed technique was integrated with the metaheuristic randomisation algorithm to prevent FOA attack. The partial password selection and metaheuristic randomisation algorithm are modelled and implemented in the third proposed system – the Visual Identification

Protocol Professional (VIP Pro). A chronological story-based cued recall technique has been proposed to make it easy for the users to memorise their passwords.

3.2.2 System Design and Implementation

To achieve the second research objective, the proposed techniques were transformed into workable systems before they were used as a tool to gather data or feedback from respondents who were invited to evaluate the effectiveness of the proposed methods in mitigating shoulder-surfing attack, and in preventing FOA attack, respectively. There are two stages in the transformation process – system design stage, and implementation stage.

In the system design stage, all the activities which are involved with the transformation of the requirements can be presented using use case diagrams, flowcharts, and pseudocodes. The two proposed falsifying authentication methods – penup event and neighbouring connectivity manipulation method, and partial password selection and metaheuristic randomisation algorithm method – were designed. The system design stage also involves the GUI design, database design, and specific functional design.

In the implementation stage, open source software such as MySQL and Java were used as the database management system, and the scripting language, respectively, of the proposed systems.

NetBeans IDE (Integrated Development Environment) was used as the design and development tool for the proposed systems. The authentication algorithms were written using the Java programming language, and MySQL database was used to store the relevant data of the developed systems.

A prototype for each proposed system was developed in a standalone mode. However, the development of each prototype also involves separate GUI (Graphical User Interface) design, database design, functional requirements design and non-functional requirements design for each prototype, based on the set objectives. Each prototype was iteratively fine-tuned and tested until it achieves the set objectives.

3.2.3 Testing and Evaluation

To achieve the third objective, the two proposed falsifying authentication methods were evaluated. Table 3.1 shows the data gathering techniques used in evaluating the capability of the proposed methods in mitigating shoulder-surfing attack. A case study was conducted to investigate the behaviours of the shoulder-surfing attackers as well as to test the capability of the proposed falsifying authentication methods in mitigating shoulder-surfing attack, under natural conditions.

Table 3.1: Data Gathering Techniques Used to Evaluate the Capability of the Proposed Techniques in Mitigating Shoulder-Surfing Attack

No.	Title	Data Gathering Technique	Method	Information Obtained
1	Shoulder-Surfing Attack I	Case Study	Quantitative	User attempts and the shoulder-surfing results using BPG system
2	Shoulder-Surfing Attack II	Case Study and Interview	Quantitative and Qualitative	User attempts and the shoulder-surfing results using VIP Pro system User feedback on the shoulder-surfing method used

3.2.3.1 Shoulder-Surfing Attack I

The purpose of this case study is to:

i. evaluate the capability of the first proposed falsifying authentication method – utilising penup event and neighbouring connectivity manipulation – in mitigating shoulder-surfing attack.

A sample size of 30 it is often suggested will produce an approximately normal sampling distribution (Smith & Wells, 2006). Thus, the sample size which is at least 30 or more was used in this case study to evaluate the proposed method in mitigating shoulder-surfing attack. In order to test and verify whether the proposed method can successfully mislead a shoulder-surfing attacker from identifying and obtaining the correct password of a user, a case study involving 100 participants was conducted in the Faculty of Computer Science & Information Technology (FCSIT), University of Malaya, Malaysia. An authorised user with username *testing2* along with the following password encoding was generated using the proposed system:

{(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 3.2 shows the password created using the above-mentioned password technique.

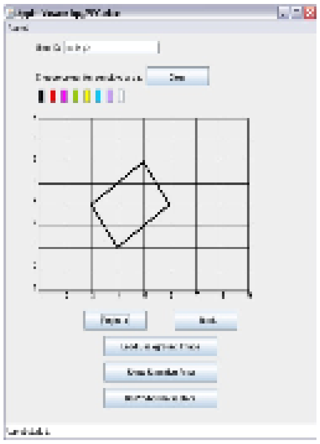


Figure 3.2: A Password Created Using the Predefined Password Encoding Technique

To determine whether the varying competency levels or gender of the participants will affect the result, the participants were categorised into either postgraduate or undergraduate students, and according to their gender.

Initially, all the participants were grouped in a group of five. Ten groups of postgraduate students were further grouped according to their gender: male (Group No. 1, 2, 3, 4 and 5), and female (Group No. 6, 7, 8, 9 and 10). Another 10 groups of undergraduate students were also further grouped according to their gender: male (Groups No. 11, 12, 13, 14 and 15), and female (Groups No. 16, 17, 18, 19 and 20). The participants were then briefed on their roles, and they witnessed a demonstration of the login process. Every group of shoulder-surfing attackers was allowed three consecutive attempts to identify, discuss, and guess the password of a user named *testing2*. Hints on the methods used to mitigate shoulder-surfing (such as the neighbouring connectivity and penup event) would only be given if the attackers had failed to login at the first attempt. The password encoding activities generated by the attackers in each attempt were collected and analysed.

Table 3.2 shows the techniques used for data analysis. Several statistical analysis techniques such as Kruskal Wallis test were used to evaluate the capability of the proposed systems in mitigating shoulder-surfing attack. Other statistical analysis methods such as Chi-Square test, and cross-tabulation were used to determine the association between the different entities of the gathered data such as the participants' academic level or gender.

The following formula was proposed to calculate the password spaces produced by the proposed systems for different lengths of the password:

$$\sum_{i=1}^{L_{\max}} 8 \times G^2 \times (8 \times G^2 + (G^2 - 1))^{i-1} \qquad (1)$$

where L_{max} is the number of strokes used in creating a password, and G is the size of the grid.

The purpose of calculating the password spaces is to determine the vulnerability of the proposed system. By increasing the password spaces, more password patterns can be drawn. Therefore, it follows that increasing the password spaces of a system correspondingly reduces the probability of attackers guessing a user's password in a shoulder-surfing attack.

Table 3.2: Data Analysis Techniques Used to Evaluate the First Proposed Method (Penup Event and Neighbouring Connectivity Manipulation)

No.	Purpose	Data Analysis Technique	Information Obtained
1	Evaluate the capability of the first proposed falsifying authentication method in mitigating shoulder-surfing attack.	Statistical Analysis (Kruskal Wallis test, Chi-Square test, and Cross-tabulation)	Statistical results on the shoulder-surfing attacks. The association between the entities of the gathered data (such as participants' academic level or gender).
2	Evaluate the password space produced by BPG and the enhanced BPG systems.	Using a Mathematical Equation (1)	Password space information for different password lengths.

3.2.3.2 Shoulder-Surfing Attack II

The purpose of this case study is to:

i. evaluate the capability of the second proposed falsifying authentication method – utilising partial password selection and metaheuristic randomisation algorithm – in mitigating shoulder-surfing attack.

Similarly, the sample size which is at least 30 or more was used in this case study to evaluate the proposed method in mitigating shoulder-surfing attack. In this case study, 73 participants were randomly picked to perform the shoulder-surfing attacks. The participants were categorised into three groups – expert, normal, and control groups. The expert group comprised 30 participants who had taken the computer security subject or are currently conducting research in computer security at the FCSIT, University of Malaya, Malaysia. The normal group comprised 38 participants randomly identified from among members of the public during the Seoul International Invention Fair, Korea. The control group comprised five randomly-picked undergraduate students of the FCSIT, University of Malaya, Malaysia. All participants were briefed on their role as attackers, before they began their attacks. Each shoulder-surfing attacker was allowed three consecutive attempts to guess an authorised user's password after they have witnessed a successful login demonstration. An attacker who fails to be authenticated after the third attempt, would be blocked by the system.

An unstructured interview was conducted with the participants right after the case study to obtain additional feedback from them. The following open-ended questions were used to solicit information on the attack method used by each participant:

i. What was your first impression when you were making the attack?

ii. What was your attacking method? (i.e., guessing?)

iii. Did you use the identified password that I used during the demonstration to make the attack or did you use other pictures as well?

iv. What strategies did you use when you noticed that the password pictures used in the demonstration were not the same as those in the challenge set?

Table 3.3 shows the data analysis techniques used in the evaluation. A statistical analysis of the percentage of successful attacks will give a good indication of the capability of the proposed system in mitigating shoulder-surfing attack. The permutations (^nP_r) method was used to determine the password length produced by the proposed system, and this was compared with that of the benchmark system.

Table 3.3: Data Analysis Techniques Used to Evaluate the Second Proposed Method (Partial Password Selection and Metaheuristic Randomisation Algorithm)

No.	Purpose	Data Analysis Technique	Information Obtained
1	Evaluate the capability of the second proposed falsifying authentication method in mitigating shoulder-surfing attack.	Statistical Analysis (percentage of successful attacks)	Statistical results of the shoulder-surfing attacks.
2	Identify the password space produced by the VIP Pro system.	Permutation (^nP_r) method	Password space information for different password lengths.

To achieve the fourth objective, an offline FOA Java simulation was used to evaluate the capability of the proposed method – utilising the metaheuristic randomisation algorithm – in preventing FOA attack. Table 3.4 shows the data analysis technique used to determine the parameters used and to evaluate the capability of the proposed method in preventing FOA attack. Some parameters such as number of secret passwords used ($|X|$), number of partial secret passwords used ($|J|$), and metaheuristic range ($\overset{j_{n..m}}{R_i}$), were determined and tested. Initially, the permutations (${}^{n}P_{r}$) method was used to determine the cardinality of X. The cardinality of J and the metaheuristic range ($\overset{j_{n..m}}{R_i}$) were determined using the offline FOA Java simulation and its observation results. After finalising the parameters, the offline FOA Java simulation and its observation results were used to determine the capability of the proposed method in preventing offline FOA attack by comparing the occurrence of suspicious pictures with the secret password pictures generated using the proposed method.

Table 3.4: Data Analysis Techniques Used to Evaluate the Capability of the Proposed Method in Preventing FOA Attack

No.	**Purpose**	**Data Analysis Technique**	**Information Obtained**
1	Identify the suitable range to be used for the parameter ($|X|$) in VIP Pro system.	Permutation (${}^{n}P_{r}$) method	Information about the number of selection based on different x values. Determine the significant interval for x.
2	Identify the suitable range to be used for the parameter ($|J|$) in VIP Pro system.	Simulation and Observation	The frequency of occurrence of the secret password pictures and other decoy pictures simulation results using different j secret passwords. Observation results based on the simulated results. Determine the significant interval for j.

Table 3.4: Data Analysis Technique Used to Evaluate the Capability of the Proposed Method in Preventing FOA Attack (continue)

No.	Purpose	Data Analysis Technique	Information Obtained
3	Identify the suitable metaheuristic range, $R_i^{j_{n..m}}$, to be used in VIP Pro system. n and m refer to the minimum and maximum number of secret passwords, respectively, used during authentication, and R_i is the reused decoy pictures interval with $i \in \boldsymbol{N_0}$.	Simulation and Observation	The frequency of occurrence of the secret password pictures and other decoy pictures simulation results using different n, m and i values. Observation results based on the simulated results. Determine the significant value for n, m and i respectively. Determine the metaheuristic range for $R_i^{j_{n..m}}$.
4	Evaluate the effectiveness of the metaheuristic randomisation algorithm in preventing offline FOA attack.	Simulation and Observation	Comparison of occurrence of suspicious pictures with the secret password pictures of the proposed system. Observation results based on the simulated results.

The cued recall methods were used in the testing and evaluation of the size of the indicator used, colour scheme preferences, background image effect, story line cued recall technique, and grid line scaling. Table 3.5 shows the data analysis techniques used in the aforementioned testing and evaluation processes. The survey questionnaire was chosen as one of the data gathering instruments because a large sample can be collected in a relatively short time. In addition, it also allows generalization to be made about the demography of the population being studied (Greenfield, 2001). On the other hand, the prototype was chosen as one of the data gathering techniques because the users' feedback on the usefulness of the proposed cued recall methods can only be obtained after a complete prototype with the related cued recall method have been successfully implemented. Direct observation was also used because observation of the behaviour of the users and other feedback from them can only be obtained when a test is conducted.

Table 3.5: Data Analysis Techniques Used to Evaluate the Capability of the Proposed Methods in Helping Users to Improve the Memorability

No.	Title	Data Gathering Technique	Method	Information Obtained
1	Survey on Colour Usage	Survey	Quantitative	Users' feedback on their preferred colours.
2	Sensitive Area Testing	Prototype and Observation	Quantitative and Qualitative	Optimal size for sensitive area.
3	Survey on Usability Part I	Prototype and Survey	Quantitative	Users' feedback on the usefulness of uploaded background picture in aiding users' memorability. User information such as gender and academic background. Users' feedback on the usefulness of grid line scaling feature in aiding users' memorability.
4	Survey on Usability Part II	Survey	Quantitative	Users' feedback on the difficulties in memorising the password, before using chronological story-based cued recall technique. Users' feedback on the usefulness of chronological story-based cued recall technique in aiding users' memorability.

3.2.3.3 Survey on Colour Usage

Colour is an important element of the Human Visual Sensory (HVS) system, as it is a significant factor not only in strengthening security, but also as a cue to help improve users' memorability (Tao & Adams, 2008). Therefore, a survey on colour usage was conducted to:

i. identify the users' preferred colour scheme to be used in the prototype.

There are 40 colours available in Microsoft Office Word. The reason for choosing this colour scheme is that since 2005, Microsoft Office Word 2003 had been installed in all computers in the FCSIT, University of Malaya, Malaysia. The survey instrument consists of a two-page questionnaire containing five questions (refer to Appendix B). These questions were formulated from interval data and nominal data types. The first two questions are used to obtain a participant's personal information such as age, and gender. The information is needed to determine whether the gender and age of the participants have any influence on the colour scheme used in the prototype. The third and fourth questions enquire about the participants' familiarity in the use of Microsoft Office Word and its accompanying colour scheme. The last question requires participants to choose their preferred colours (maximum of 10 colours). Table 3.6 shows the data type of each question in the questionnaire.

Table 3.6: Colour Usage Survey Questions and the Data Type

Question	Definition	Data Type
1	Age Group	Interval Data
2	Gender	Nominal Data
3	Familiarity with Microsoft Office Word	Nominal Data
4	Familiarity with the colour scheme in Microsoft Office Word	Nominal Data
5	User's preferred colour scheme	Nominal Data

Before conducting the survey, each question was checked and revised by the supervisor to avoid any ambiguity, and to ensure that the response options are mutually exclusive, which means they do not overlap with one another. The revised questionnaire was then used in a pilot test involving 10 participants, to verify its reliability as an instrument to achieve the intended objectives. Following the pilot testing, the questionnaire was randomly distributed to 250 participants in the FCSIT, University of Malaya, Malaysia. The returned questionnaires were checked for completeness, before the data were inputted and analysed.

3.2.3.4 Sensitive Area Testing

The purpose of this testing is to:

i. identify the optimal size of the sensitive area used in the proposed system.

To produce approximately normal sampling distribution, the sample size which is at least 30 or more must be used. This testing involved 250 participants who were randomly picked from among the students from the FCSIT, University of Malaya, Malaysia. The participants were briefed on the use of the prototype – they were taught the method to create their password using the following radius size: 0.10×d, 0.15×d, 0.20×d, 0.25×d, 0.30×d, 0.35×d, and 0.40×d (where d is the side length of a grid cell), with and without the assistance of the "show/hide indicators" function.

All participants were given three consecutive attempts to login into the proposed hybrid drawmetric and locimetric prototype by using grids of different radius sizes, with and without the assistance of the "show/hide indicators" function. Each participant was observed as he made an attempt to access the system. The attempts were recorded as either "successful" or "failure", for this sensitive area test.

3.2.3.5 Survey on Usability Part I

The purpose of this survey is to:

i. evaluate the effectiveness of the proposed upload background picture feature in aiding users' memorability.
ii. evaluate the effectiveness of the proposed grid line scaling feature in aiding users' memorability.
iii. evaluate the effectiveness of the proposed loose authentication feature in aiding users' memorability.

The survey instrument is a three-page hybrid-format questionnaire, which contains seven questions (refer to Appendix C). The questionnaire contains both fixed-format questions and free-format questions. There are two data types – nominal data and ordinal data.

Before conducting the survey, a sequence of case-by-case scenarios were demonstrated to each participant on the use of the following proposed features:

i. upload background picture feature
ii. grid line scaling feature
iii. loose authentication feature.

Table 3.7 shows the usability survey questions and their data type. Survey Questions 1 - 2 are used to elicit information on the academic level and the gender of each participant, respectively. This is aimed at determining whether the academic level and gender of the participants have any effect on the features being evaluated. The third question was designed to find out whether a participant has knowledge of the picture-based password.

Questions 4 - 6 are used to gather information relating to the usefulness of the cued background feature, grid line scaling feature, and loose authentication feature in aiding users to remember their passwords. Question 7 is used to determine whether the participants know about shoulder-surfing attack. Ordinal data type was used in Question 4 - 6. The participants answer Questions 4 - 6 using a five-point scale (from 'strongly disagree' to 'strongly agree').

Table 3.7: Survey on Usability Part I: Questions and Their Data Type

Question	Definition	Data Type
1	Current highest academic qualification	Nominal Data
2	Gender	Nominal Data
3	Knowledge about graphical authentication	Nominal Data
4	Usefulness of upload background picture feature in aiding users' memorability	Ordinal Data
5	Usefulness of grid line scaling feature in aiding users' memorability	Ordinal Data
6	Usefulness of loose authentication feature in aiding users' memorability	Ordinal Data
7	Knowledge about shoulder-surfing attack	Nominal Data

Before conducting the survey, each question was checked and revised by the supervisor to avoid any ambiguity and to ensure that the response options are mutually exclusive. The revised questionnaire was then used in a pilot test that involved 5 participants to verify its reliability as an instrument to achieve the objectives. Following the pilot testing, the questionnaire was randomly distributed to 30 participants in the FCSIT, University of Malaya, Malaysia. The returned questionnaires were checked for completeness – i.e., all the questions, especially the open-ended questions, have been answered – before the data were inputted and analysed.

3.2.3.6 Survey on Usability Part II

The purpose of this survey is to:

i. evaluate the effectiveness of the proposed chronological story-based cued recall technique in aiding users' memorability.

A proposed searchmetric prototype and a paper-based questionnaire are the two data gathering instruments used in the survey. The participants were first asked to use the proposed prototype to identify the secret pictures for their password. Subsequently, each participant was required to reproduce the secret pictures that he/she had selected in the correct sequence by using his/her own recall method. They would then be taught how to memorise their password using the chronological story-based cued recall technique. In this technique, each participant creates a story by linking each secret picture that he/she had selected according to their sequence. A questionnaire survey was later conducted to obtain the users' feedback on the effectiveness of the proposed technique.

Table 3.8 shows the Part II usability survey questions and their data type. There are two data types – nominal data and ordinal data. Questions 1 - 2 are used to gather information on the participants' academic level and their gender, respectively. This is aimed at determining whether the academic level and the gender of the participants have any effect on the feature being evaluated. Question 3 is used to find out whether a participant has knowledge of the picture-based password authentication. Question 4 is used to determine whether the participants have difficulty in memorising their passwords in the past, using their own recall method. Question 5 asks participants about the effectiveness of the proposed chronological story-based cued recall technique in assisting them in memorising their passwords. Ordinal data type was used in Question

5, and the participants answer the question using a five-point scale (from ‘strongly disagree’ to ‘strongly agree’).

Table 3.8: Survey on Usability Part II: Questions and Their Data Type

Question	Definition	Data Type
1	Academic level	Nominal Data
2	Gender	Nominal Data
3	Knowledge about graphical authentication	Nominal Data
4	Users’ feedback on memorability before using chronological story-based cued recall technique	Nominal Data
5	The effectiveness of chronological story-based cued recall technique in aiding users’ memorability	Ordinal Data

Before conducting the survey, each question was checked and revised by the supervisor to avoid any ambiguity and to ensure that the response options are mutually exclusive. The revised questionnaire was then used in a pilot test, that involved 5 participants, to verify its reliability as an instrument to achieve the intended objectives. Following the pilot testing, the questionnaire was randomly distributed to 32 participants in the FCSIT, University of Malaya, Malaysia. The returned questionnaires were checked for completeness – i.e., all the questions, especially the open-ended questions, have been answered – before the data were inputted and analysed.

3.2.4 Documentation

At the end of this research, all the procedures involved, and the findings obtained were documented in this thesis. Some of the experiences gained such as those relating to: the design and implementation the of proposed systems; the techniques used in mitigating shoulder-surfing attack; FOA and the counter-measures; and the results of statistical analyses and the significant findings; have been published as articles in several academic journals, and in conferences proceedings. The VIP Pro software has been copyrighted, and a patent has been filed on the VIP Pro algorithm used in preventing FOA, and in mitigating shoulder-surfing attacks.

3.3 Summary

This chapter discussed the methodology adopted for this research. A research methodology framework was proposed as an approach to achieve the research objectives. The details regarding the procedures involved in the proposed research methodology are explained according to the following sequence: Proposed Falsifying Authentication Methods and Cued Recall Methods, System Design and Implementation, Testing, Evaluation, and Documentation. The data gathering method and instrument used in the various system development phases are explained in detail. The next chapter presents the system design and implementation of the first proposed system, the Background Pass-Go (BPG) system.

Chapter 4 Design and Implementation of Background Pass-Go

4.1 Introduction

This chapter discusses the system architecture design of the first proposed system – Background Pass-Go (BPG) – a falsifying authentication method that uses penup event and neighbouring connectivity manipulation to mitigate shoulder-surfing attack. A use case diagram is used to illustrate the functional requirements of the proposed system. There are two main processes in the proposed system – the enrollment process, and the verification process. The shoulder-surfing mitigation method is discussed together with the enrollment process. The design and implementation of the enrollment process and the verification process together with their sub-functions are also discussed with the aid of the GUI (Graphical User Interface), pseudocode, and flow charts. The last section of the chapter discusses the database design of the proposed system.

4.2 BPG System Architecture

The Background Pass-Go (BPG) system is a single-tier architecture system or it can be referred to as a standalone system. In a standalone system, all the essential system components exist on a single machine and are available only to the user physically working on that machine (Riordan, 1999). BPG was programmed using Java 2 Platform Standard Edition (J2SE), and developed using Java Plug-in technology (Java Applet) bundled with Java Runtime Environment (JRE). JRE provides developers of legacy OLE/COM/ActiveX containers such as Word or Visual Basic, the ability to embed and use portable JavaBeans components in the same way as they would embed and use platform-specific OLE/COM/ActiveX components, previously (Sun Microsystems, Inc., 2009). MySQL database is a freeware, and is used to store the relevant data or transactions produced by the users and the system. Figure 4.1 shows the BPG system architecture.

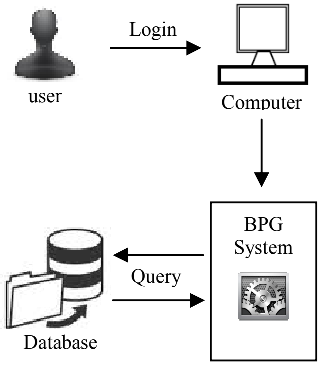


Figure 4.1: BPG System Architecture

4.3 BPG Use Case Diagram

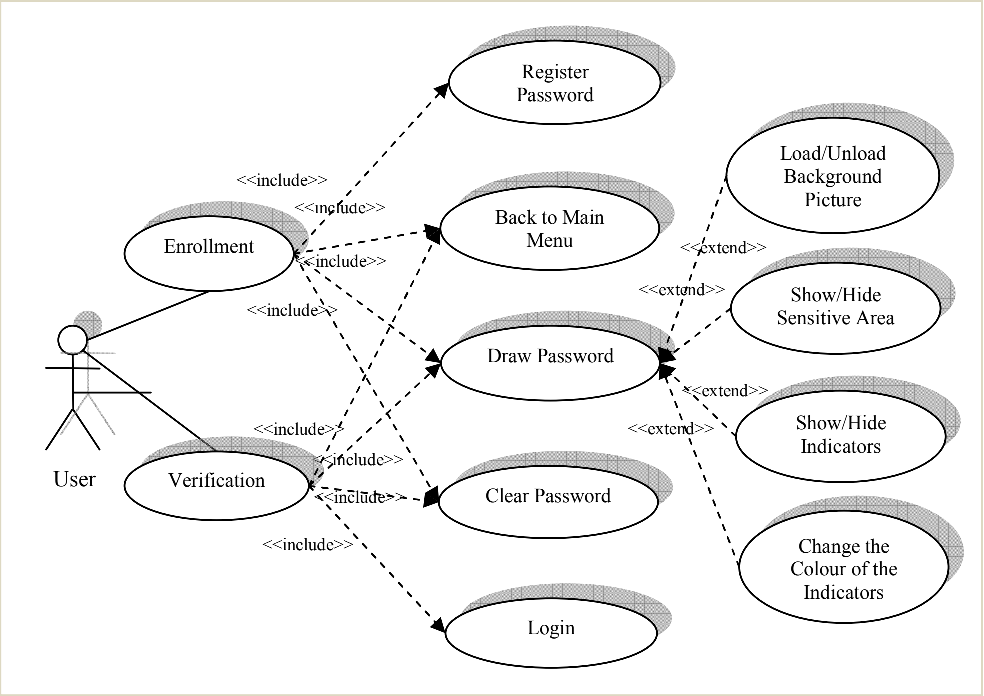


Figure 4.2: Background Pass-Go Use Case Diagram

Figure 4.2 shows the use case diagram for BPG. The use case diagram is used to identify the interactions between the proposed system and the users. In the use case diagram, the use cases or processes are drawn as an oval shape whereas the actors or the users are represented as stick figure. The compulsory procedure is shown using the <<include>> relationship whereas the <<extend>> relationship indicates the optional procedure for the BPG processes. There are two main processes in BPG – enrollment process, and verification process.

4.3.1 Enrollment Process

The enrollment procedure consists of four sub-functions, as follows:

i. Draw Password

ii. Register Password

iii. Clear Password

iv. Back to Main Menu.

4.3.1.1 Draw Password

To register a password in the BPG system, users are required to choose an ID as a username and draw their passwords using dots, lines, and shape indicators or a mixture of these. To draw a password, a user is required to select or touch the intersections rather than the cells. The idea of utilising intersections is taken from the Pass-Go system. An intersection is a point that does not have an area. Therefore, in theory, it is almost impossible for a user to select an intersection without an error tolerance mechanism. Thus, a sensitive area has to be identified to solve the aforementioned problem. A sensitive area is an area surrounding each intersection (Tao, 2006; Tao & Adams, 2008). By implementing the sensitive area, users are allowed to click on an intersection point within a specific error tolerance area. The sensitive areas are sensitive to the interaction with an input device such as a mouse click. Thus, clicking any point inside a sensitive area will be deemed to be the same as clicking on the exact corresponding intersection point.

There are 9×9 intersection points in the BPG system. A user can use the intersection points together with the predefined sensitive area to create three types of indicator such as dot, line, and shape indicators, as shown in Figure 4.3. The dot and line indicators are the basic indicators used to show the intersections and grid lines that correspond most closely to the input trace, while the shape indicator can be formed by using several line indicators. A dot indicator will only appear when one intersection is selected (or clicked), whereas, a line indicator will appear only when two or more intersections are selected continuously. The pseudocode for the implementation of the intersection points and the indicators in the BPG system are shown in Figure 4.4 and Figure 4.5, respectively.

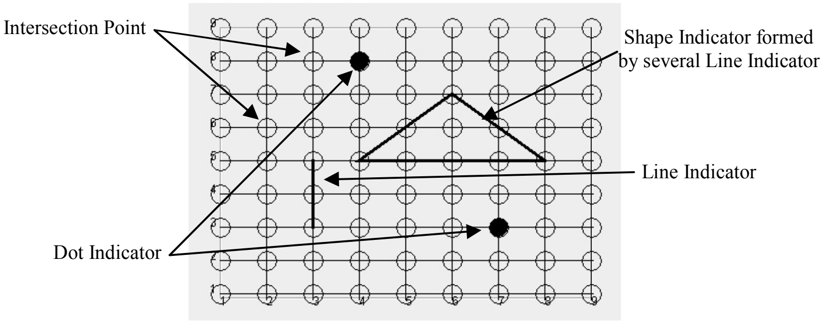


Figure 4.3: Intersection Points and Indicators Design

```
Set xOffset = x offset to grid
Set yOffset = y offset to grid

Add gridCellHeight to yOffset
FOREACH gridRow
      DrawLine horizontalLine
      Add cellHeight to yOffset
END FOREACH

Set xOffset = x offset to grid
Set yOffset = y offset to grid
Add cellWidth to xOffset
FOREACH gridRow
      DrawLine verticalLine
      Add cellWidth to xOffset
END FOREACH
```

Figure 4.4: Pseudocode for Intersection Points Implementation

```
PROCEDURE drawIndicators
      CALL drawClickPoints
      CALL drawLines
END PROCEDURE

PROCEDURE drawClickPoints

      FOREACH visibleClickPoints
            Get color of point
            Draw point
      END FOREACH
END PROCEDURE


PROCEDURE drawLines
      FOREACH visibleLine
            Get line points
            Set i to 0
            FOR totalPoint -1
                  Draw line with point i and point i+1
                  Increment i
            END FOR

      END FOREACH
END PROCEDURE
```

Figure 4.5: Pseudocode for Indicators Implementation

In the Pass-Go system, users are restricted 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 $(x+1, y+1)$ (refer to Figure 4.6).

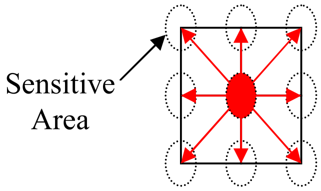


Figure 4.6: Eight-Nearest-Neighbour Connectivity

In the proposed system, the connectivity was expanded from one intersection (x, y) point to another point within the set of $(x \pm i, y \pm i)$ neighbours, where $i = \{0, 1, 2, \ldots, G-1\}$ and G is the size of the grid (refer to Figure 4.7).

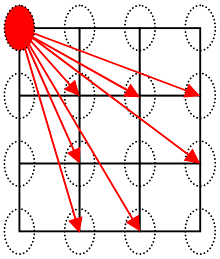
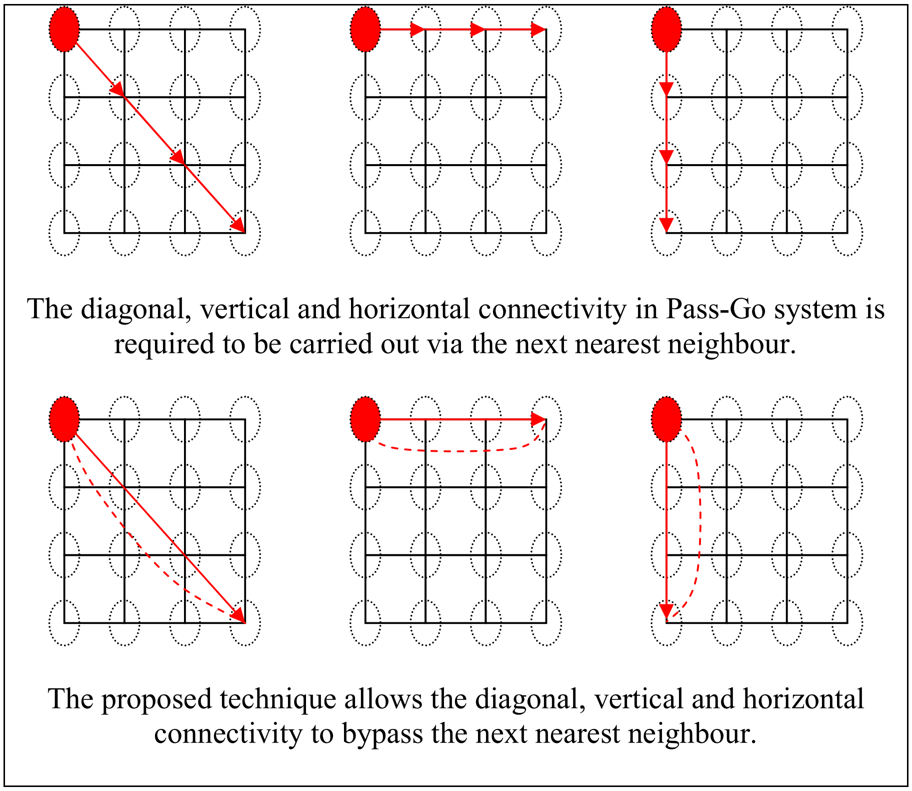


Figure 4.7: Proposed Neighbour Connectivity

Moreover, in the proposed system, the diagonal, vertical and horizontal connectivity are carried out by bypassing the next nearest neighbour instead of via the conventional way (refer to Figure 4.8).



The diagonal, vertical and horizontal connectivity in Pass-Go system is required to be carried out via the next nearest neighbour.

The proposed technique allows the diagonal, vertical and horizontal connectivity to bypass the next nearest neighbour.

Figure 4.8: Neighbour Connectivity Comparisons

Thus, more password patterns can be drawn using the proposed system, and this in turn, directly increases the difficulty level for the attackers to guess the correct password.

To increase the probability for the attackers to predict the password wrongly, another technique is used. It involves holding the mouse click long enough before manoeuvring the mouse to another intersection point to create a 'flawed' keystroke or penup event. To demonstrate the aforementioned technique, let A be denoted as (x,y) and B as the other coordinate that A is interested to connect with (refer to Figure 4.9).

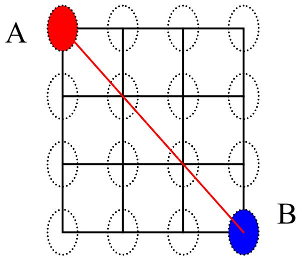


Figure 4.9: Penup Event Demonstrations

To draw a diagonal line from A to B using only the penup event, the proposed technique allows a user to use one penup, two penups or up to *n* penups. For example, if a user uses only one penup event to draw a diagonal line from A to B, the coordinate pairs produced by the proposed technique is denoted as follows: (x,y)(x+1,y-1)(x+2,y-2)(x+3,y-3) (refer to Figure 4.10).

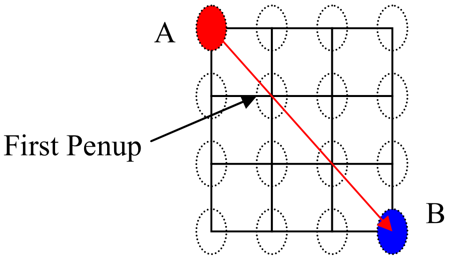


Figure 4.10: Draw a Line with One Penup Event

If two penup events are used, there are two probabilities that the user can manipulate the penup event in this specific case (refer to Figure 4.11). A new coordinate grouping method has been proposed to identify the penup events. Figure 4.11 (a) shows that the first penup event is connected to the coordinate (x,y) and (x+1,y-1). The coordinate grouping for the first penup is denoted as (x,y)(x+1,y-1). For the second penup event, the coordinates involved are (x+1,y-1), (x+2,y-2), and (x+3,y-3). Therefore, the coordinate grouping for the second penup is denoted as (x+1,y-1)(x+2,y-2)(x+3,y-3). In Figure 4.11 (b), the coordinate grouping for the first penup event and the second penup event are denoted as (x,y)(x+1,y-1)(x+2,y-2) and (x+2,y-2)(x+3,y-3), respectively.

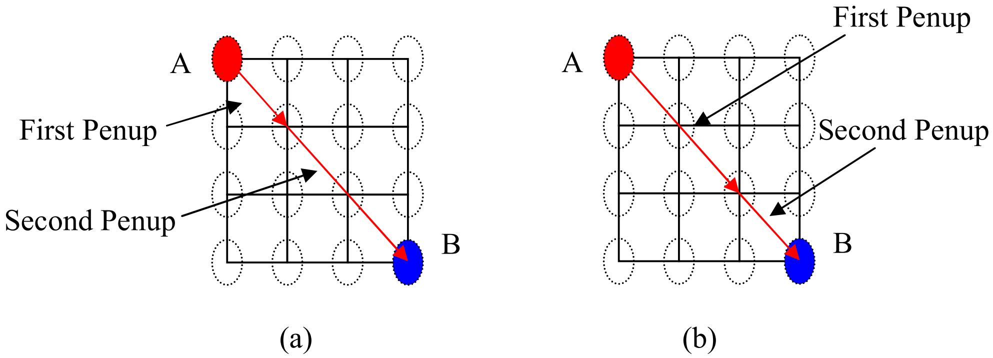


Figure 4.11: Draw a Line with Two Penup Events

Similarly, if a user uses three penup events to draw a line from A to B, the coordinate grouping for the first, second, and third penup are denoted as (x,y)(x+1,y-1), (x+1,y-1)(x+2,y-2), and (x+2,y-2)(x+3,y-3), respectively (refer to Figure 4.12).

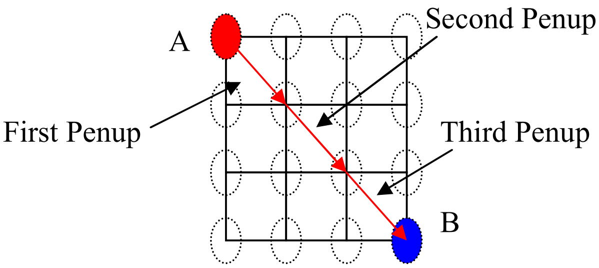


Figure 4.12: Draw a Line with Three Penup Events

Thus, the above shows that the proposed technique can also increase the probability of the indicators connectivity, which directly increases the difficulty level for the attackers to guess the password correctly.

Subsequently, both proposed techniques (penup event and neighbouring connectivity manipulation) were used simultaneously to increase the number of patterns when connecting two or more coordinates. For example, in Figure 4.13, different coordinate groupings are produced when a nearest neighbour is bypassed. The coordinate grouping for the first penup produced is denoted as (x,y)(x+2,y-2), instead of (x,y)(x+1,y-1)(x+2,y-2), and the second penup produced is denoted as (x+2,y-2)(x+3,y-3).

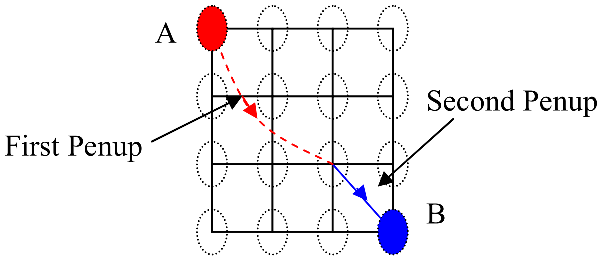
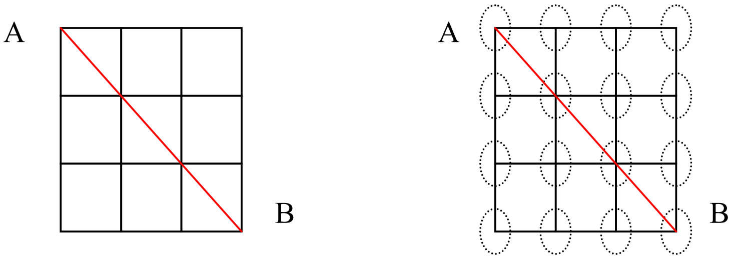


Figure 4.13: Penup Event and Neighbouring Connectivity Manipulation

To confuse the attackers, especially the shoulder-surfing attackers, in an actual implementation, the visual effect of connecting A to B will show that only a single line is used regardless of how many penup events and neighbouring connectivity manipulation have been used (refer to Figure 4.14).



(a) without the illustration of the sensitive area

(b) with the illustration of the sensitive area

Figure 4.14: Visualisation Effect

Moreover, in actual implementation, the connectivity between the coordinates is allowed to overlap. For example, in Figure 4.15, the coordinate grouping for the first penup produced is denoted as (x,y)(x+2,y-2), and the second penup produced is denoted as (x,y) (x+3,y-3). However, the visual effect of connecting A to B is still the same, as shown in Figure 4.14.

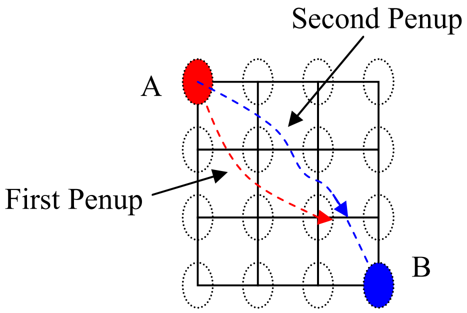


Figure 4.15: Overlapped Penups

The proposed falsifying authentication method that uses penup event and neighbouring connectivity manipulation is fabricated as two-dimensional coordinate pair in the proposed encoding scheme in the Register Password process. Subsequently, the draw password sub-function comprises four extended sub-functions, as follows:

i. Change the Colour of the Indicators

ii. Load/Unload Background Picture

iii. Show/Hide Sensitive Area

iv. Show/Hide Indicators.

4.3.1.1.1 Change the Colour of the Indicators

As an important element of the Human Visual Sensory (HVS) system, colour, has been used, not only as a significant factor to strengthen security, but also as a cue to help improve the users' memorability (Tao & Adams, 2008). To improve their memorability, users are allowed to assign different colour codes when drawing an indicator in BPG system. Eight colours were identified based on the users' ranked preferences obtained using a survey, and their RGB (red, green and blue) values presented in Table 4.1.

Table 4.1: The Identified Colours and Their RGB Values

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]

Black was selected as the default colour. Users can select their preferred colours by clicking on the corresponding colour buttons, as shown in Figure 4.16. To create a password, users can use at least one to a maximum of eight colours. Figure 4.17 shows the pseudocode for the implementation of the colour scheme in the BPG system.

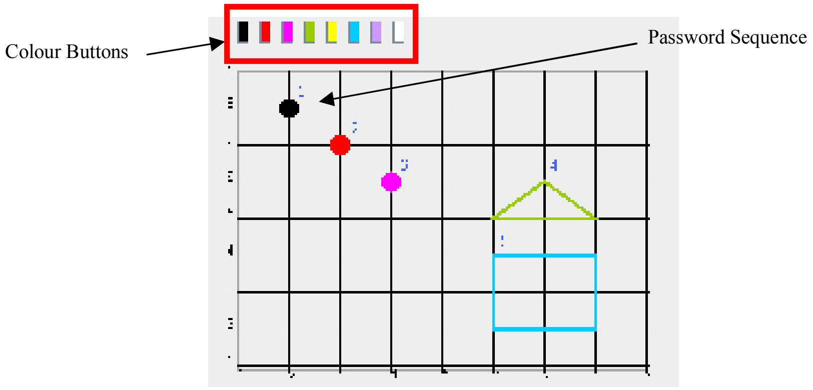


Figure 4.16: A BPG Password Instance Using Colours as a Cue

```
PROCEDURE createButtonColors
      Set buttonsColors[0] with RGB value (0,0,0);
      Set buttonsColors[1] with RGB value (255,0,0);
      Set buttonsColors[2] with RGB value (255,0,255);
      Set buttonsColors[3] with RGB value (153,204,0);
      Set buttonsColors[4] with RGB value (255,255,0);
      Set buttonsColors[5] with RGB value (0,204,255);
      Set buttonsColors[6] with RGB value (204,153,255);
      Set buttonsColors[7] with RGB value (255,255,255);
END PROCEDURE
```

Figure 4.17: Pseudocode for Colour Scheme Implementation

4.3.1.1.2 Load/Unload Background Picture

Besides changing the colour, users can also use the upload background picture function to help them in memorising their password. The upload background picture function allows users to personalise their background image and superimpose it onto the BPG system. With this feature, users are able to remember where they started drawing their passwords or which parts of the image background contain their passwords. In other words, instead of having to remember the coordinate pairs of the passwords, the users can remember their passwords better by recalling which part of the image background they had clicked. Figure 4.18 and Figure 4.19 show the upload background image function and its pseudocode, respectively.

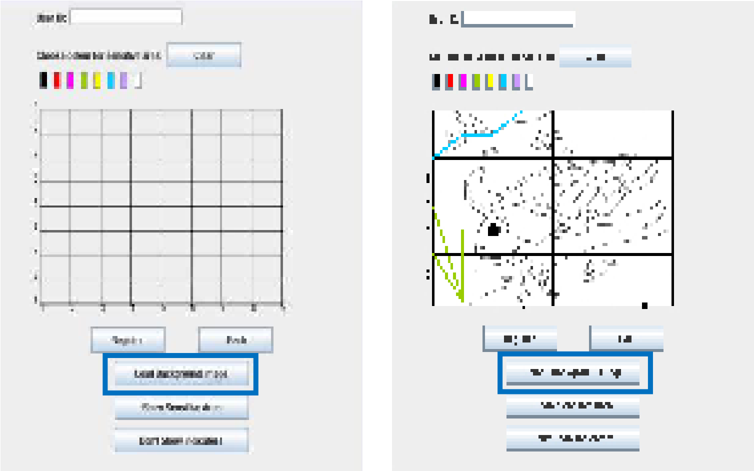


Figure 4.18: Load/Unload Background Picture Function

```
PROCEDURE LoadUnloadImage
      IF isLoadImage = true
            Prompt choose file box
            Load image to memory
            Display image at background
      ELSE
             Unload image from background
      END IF

      Set isLoadImage to inverse of isLoadImage
END PROCEDURE
```

Figure 4.19: Pseudocode for Load/Unload Background Picture Implementation

4.3.1.1.3 Show/Hide Sensitive Area

Users can use the “show/hide sensitive area” function to connect or draw the indicators more precisely. When this feature is activated, all the sensitive areas in the BPG system will be revealed. This feature enables the users to draw more challenging passwords such as connecting two indicators beyond the eight-nearest-neighbour connectivity, discussed in the previous section. The “show/hide sensitive area” function and its pseudocode are shown in Figure 4.20 and Figure 4.21, respectively.

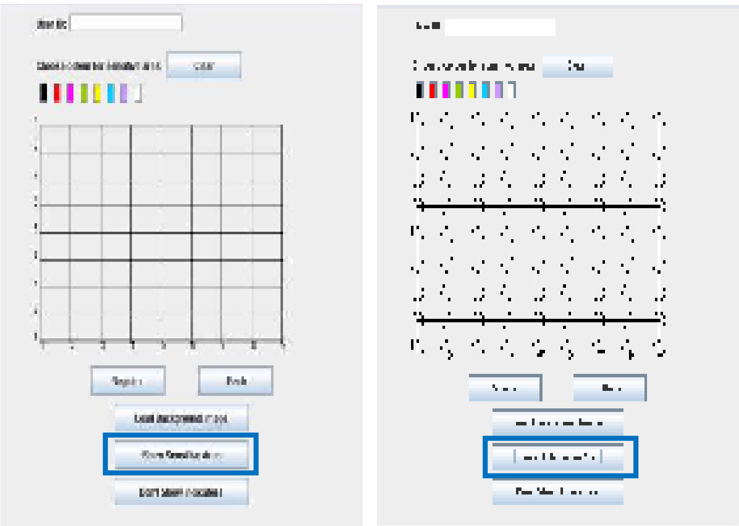


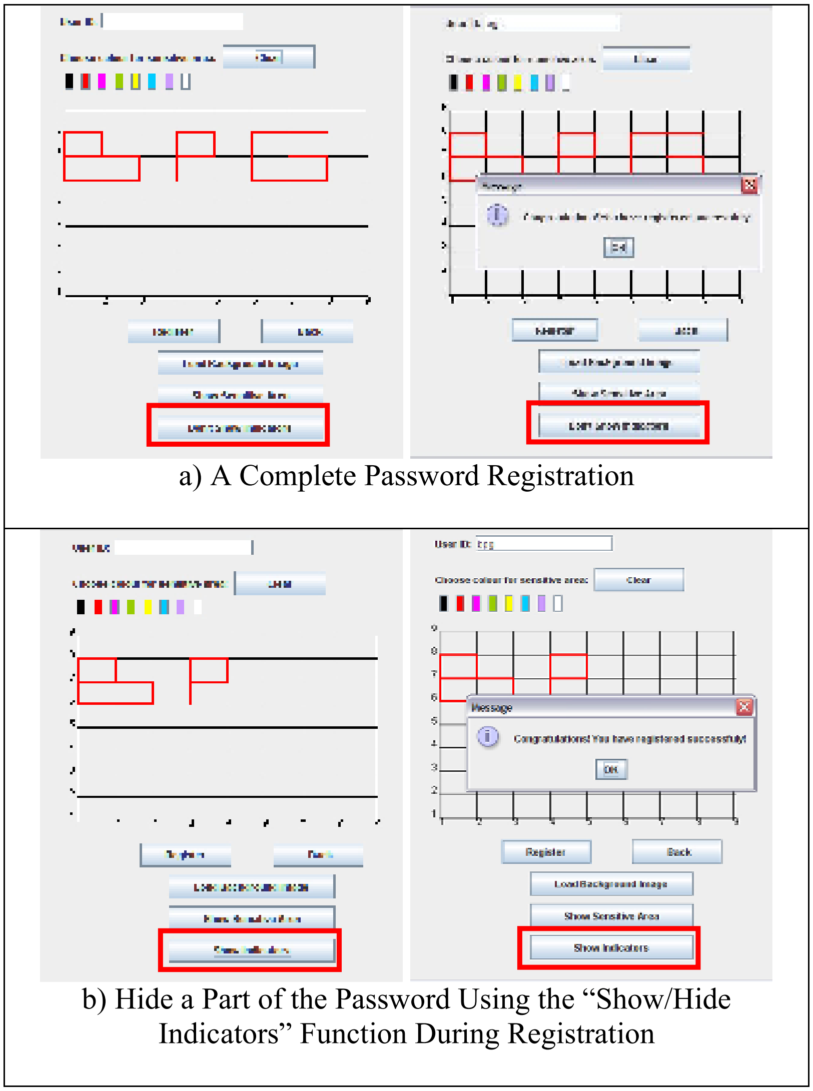
Figure 4.20: Show/Hide Sensitive Area Function

```
PROCEDURE RevealSensitiveArea
      IF is isConcealed = true
            Display Sensitive Area
      ELSE
            Hide Sensitive Area
      END IF

      Set isConcealed to inverse of isConcealed

END PROCEDURE
```

Figure 4.21: Pseudocode for Show/Hide Sensitive Area Implementation

4.3.1.1.4 Show/Hide Indicators

To prevent shoulder-surfing attack, users are allowed to conceal all or a part of the drawn password by using the “show/hide indicators” function – the drawn indicators will be invisible. Thus, this function provides an extra layer of protection against shoulder-surfing attack because the correct indicator connectivity and the penup events used can be hidden totally or partially. Figure 4.22 shows the “show/hide indicators” function, and Figure 4.23 shows its implementation pseudocode.



User ID:

Choose colour for sensitive area:

Message

Congratulations! You have registered successfully!

a) A Complete Password Registration

b) Hide a Part of the Password Using the “Show/Hide Indicators” Function During Registration

Figure 4.22: An Instant of a Login Process Using the “Show/Hide Indicators” Function

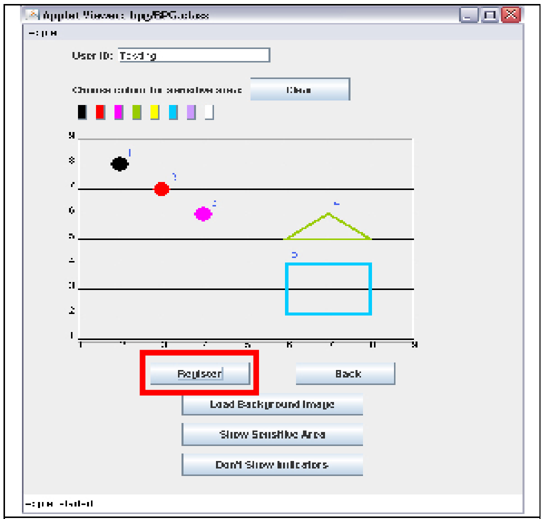
```
PROCEDURE addIndicator
      IF(showIndicator)
            Add to visible indicators list
      END IF

      Add to all indicators list
END PROCEDURE
```

Figure 4.23: Pseudocode for “Show/Hide Indicators” Implementation

As mentioned in the problem statement section in Chapter 1, it is important to ensure that all the activities of an authentication process are secure, as this is an effective way to prevent shoulder-surfing attack. This includes the use of the “show/hide indicators” function. However, implementing such measures gives rise to a problem for the users in the login process. They have no clue as to whether their password was correctly drawn. Despite this drawback, the “show/hide indicators” function is incorporated in the BPG system only as an optional feature for users who need the extra layer of security.

4.3.1.2 Register Password

After a user has drawn a password, a sequence of intersections is produced. Each intersection fabricates the encoding of (x,y,[r,g,b]) where the values 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 [r,g,b] refers to the red, green and blue colour components of the predefined colour scheme used in the BPG system. The symbol {} is used to indicate a penup event. Thus, the BPG encoding scheme can be denoted as $\sum_{(x,y)\in[1..G]\times[1..G]}(x,y,[r,g,b]) \in \{\}$. Figure 4.24 shows the password encoding generated by the BPG system, and Figure 4.25 shows the pseudocode for the implementation of the BPG encoding scheme.



User ID: Testing

(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])}

Figure 4.24: Example of a Password Encoding Generated by the BPG System

```
Set pass to empty string
FOREACH clickPoints
      Set pos to position click point
      Get colour of click point
      Append to pass, "(" + pos + "," + colourName + ")"
END FOREACH

FOREACH lines
      Get line colour
      Append to pass, "{"
            FOREACH point in line
                Set pos to position of point
                Append to pass, "(" + pos + "," + colourName + ")"
            END FOREACH
      Append to pass, "}"
return pass;
```

Figure 4.25: Pseudocode for BPG Encoding Scheme Implementation

In order to ensure the integrity of the authentication information, a MD5 hashing algorithm was applied to hash the password created by a user. The hashed password will be kept in a database and subsequently used in the verification process. Figure 4.26

shows an example of a BPG password produced after hashing, and Figure 4.27 shows the pseudocode of its implementation.

Password Produced Before Hashing (refer to Figure 4.23):
(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])}

Password Produced After Hashing: 7932cd3cc2e672828c485c48e7bc9c4d

Figure 4.26: Password Hashing Feature

```
Get md5 hashing implementation
Process input string
Return result
```

Figure 4.27: Pseudocode for Password Hashing Implementation

4.3.1.3 Clear Password

If the users intend to redraw their passwords, they can use the clear password function to remove all the previously drawn passwords. Figure 4.28 and Figure 4.29 show the clear password function GUI screenshot and its pseudocode, respectively.

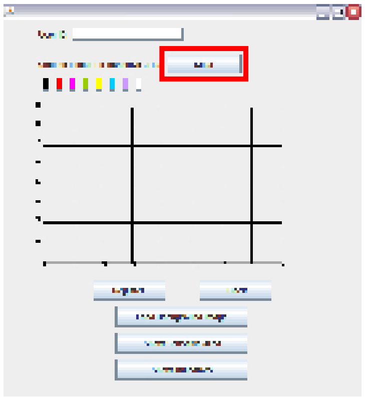


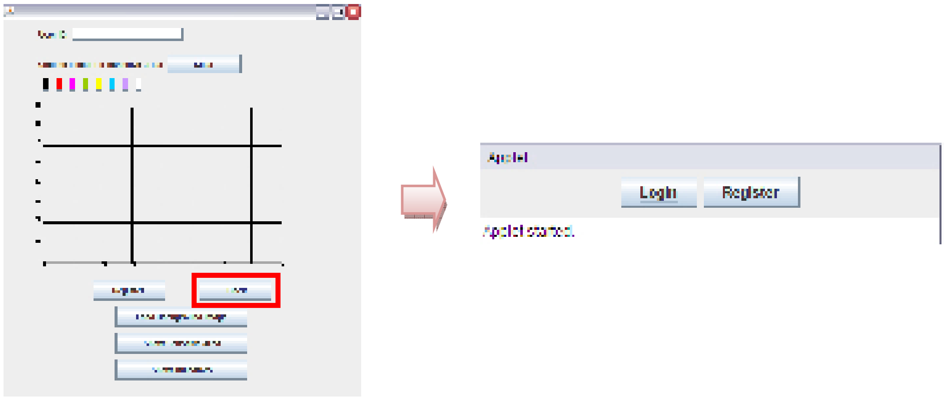
Figure 4.28: Clear Password Function

```
PROCEDURE clear

      Clear all mouse clicks
      Clear mouse clicks’ colours
      Clear lines
      Clear lines' colours

END PROCEDURE
```

Figure 4.29: Pseudocode for Clear Password Implementation

4.3.1.4 Back to Main Menu

The users can use the back function, as shown in Figure 4.30, to go back to the main menu. Figure 4.31 shows the pseudocode for implementing the back to main menu function.



Applet started.

Figure 4.30: Back Function GUI

```
PROCEDURE back

      close current panel
      open MainManu Panel

END PROCEDURE
```

Figure 4.31: Pseudocode for Back Function Implementation

4.3.1.5 System Flow of the Enrollment Process

Figure 4.32 shows the system flow of the password enrollment process in the BPG system. As an initial step, the users are required to draw their passwords. They are allowed to personalise their colour code and background picture when drawing their passwords. They are also permitted to use the “show sensitive area” function to assist them in drawing their passwords. The users are also able to hide a part of, or the whole password created by using the hide indicators function. After a user has confirmed his password, a set of password encoding will be generated. The generated password encoding is hashed and stored in the database at the end of the enrollment process.

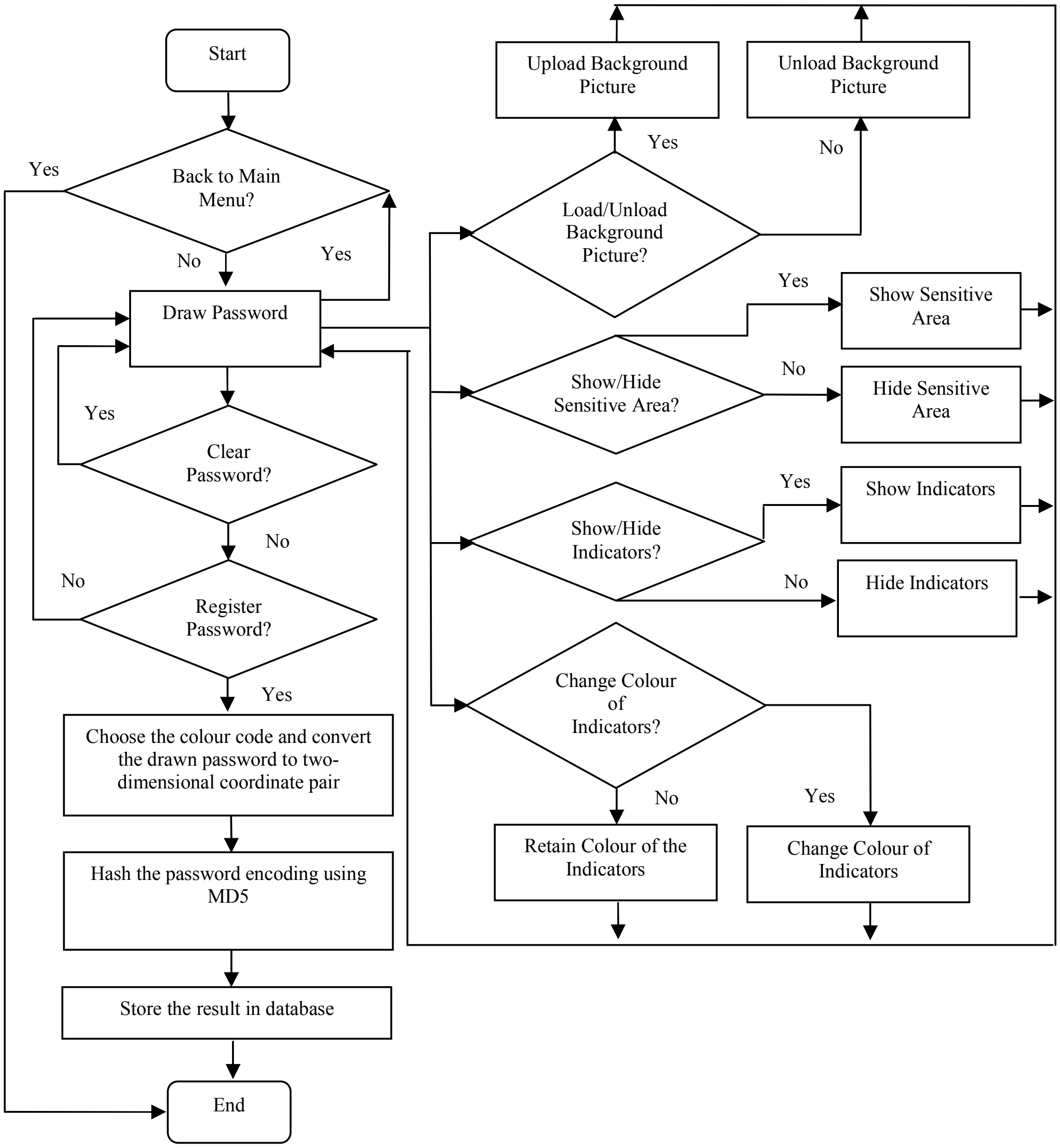

Start
Back to Main Menu?
Yes
No
Yes
Draw Password
Yes
Clear Password?
No
No
Register Password?
Yes
Choose the colour code and convert the drawn password to two-dimensional coordinate pair
Hash the password encoding using MD5
Store the result in database
End
Upload Background Picture
Unload Background Picture
Yes
No
Load/Unload Background Picture?
Yes
Show Sensitive Area
Show/Hide Sensitive Area?
No
Hide Sensitive Area
Yes
Show Indicators
Show/Hide Indicators?
No
Hide Indicators
Change Colour of Indicators?
No
Yes
Retain Colour of the Indicators
Change Colour of Indicators

Figure 4.32: System Flow of the Enrollment Process

4.3.2 Verification Process

The verification process consists of four sub-functions, which are as follows:

i. Draw Password

ii. Clear Password

iii. Back to Main Menu

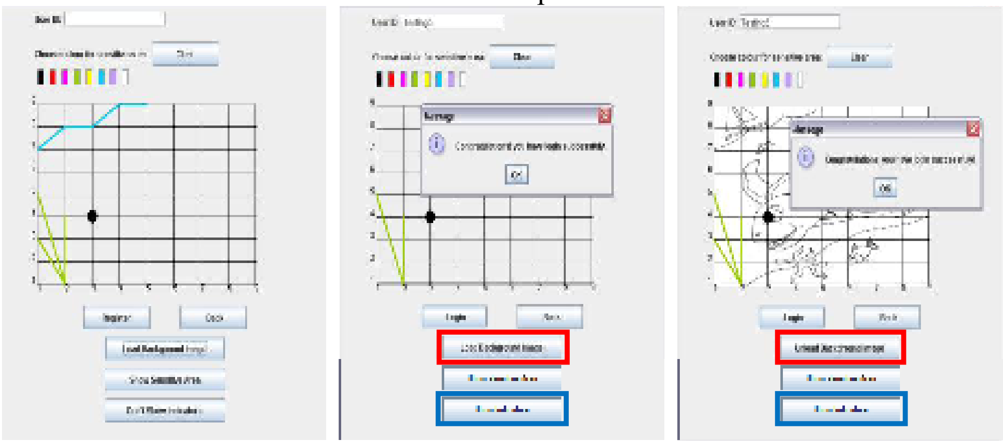
iv. Login.

The draw password function, the clear password function, and the back to main menu function, work exactly in the same way as in the enrollment process.

4.3.2.1 Login

To login, users are required to identify the correct colour code together with the correct sequence of the indicators used during the enrollment process. However, the users are allowed to use the upload background picture function to assist them in drawing the password. Besides using the proposed falsifying authentication method, the users can hide a part of, or the whole password created without revealing the indicators, as shown in Figure 4.33. After the users have drawn their passwords, a string that consists of the password encoding will be produced. A hashing algorithm will be applied to hash the password. The hashed password will then be compared with the registered password in the database. If a user fails to be authenticated after three consecutive attempts, his/her account will be blocked by the proposed system. Figure 4.34 and Figure 4.35 show the login function pseudocode, and a sample of the login historical data recorded in the database, respectively.

Hide a part of the password using “show/hide indicators” function during authentication process.



(a) Sample Password

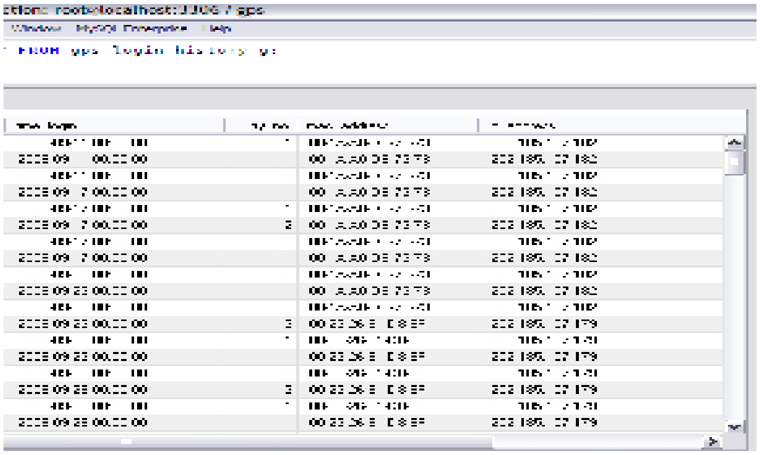
(b) Login without cue background image

(c) Login with cue background image

Figure 4.33: Login using Show/Hide Indicator Function

```
PROCEDURE login

      Get pass from user
      Process pass with MD5
      Open database and retrieve IS_LOCKED record

      IF(IS_LOCKED != 1)
            Open database and retrieve PASSWORD record
            IF(MD5(pass)= PASSWORD)
                  Display Welcoming Message
            ELSE
                  Update TRIAL_NO by adding 1
                  Update TIME_LOGIN record
                  Update MAC_ADDRESS record
                  Update IP_ADDRESS record
                  Display Wrong Password or ID Message

                  IF(TRIAL_NO >= 3)
                        Update IS_LOCKED = 1
                  END IF
            END IF
      ELSE
            Display Blocking Message
      END IF

END PROCEDURE
```

Figure 4.34: Pseudocode for Login Function



ction: root@localhost:3306 / gps
Window MySQL Enterprise Help

```
FROM gps_login_history g;
```

Figure 4.35: Sample Login Data

4.3.2.2 System Flow of the Verification Process

Figure 4.36 shows the system flow of the password verification process of the BPG system. Initially, the proposed system will verify whether a user has been blocked by the system. If the user has been blocked, he/she cannot login into the system. If the user is registered with the system, he/she will be required to produce the correct password keystrokes and in the correct order before he/she is allowed access into the system. The user is allowed to personalise his/her colour code and background picture when drawing his/her password. Besides, the user can use the show sensitive area function to assist him/her in drawing the password. The user can also hide a part of, or the whole password created by using the hide indicators function (instead of using the proposed falsifying authentication method). After a user has confirmed his/her the password, a set of password encoding is generated. The generated password encoding is hashed and compared with the registered password in the database. If the user password is authenticated, a welcoming message will be displayed. If the user fails to be authenticated, he/she will be given another two attempts to be authenticated. The user will be blocked by the proposed system if he/she fails to be authenticated after the third attempt.

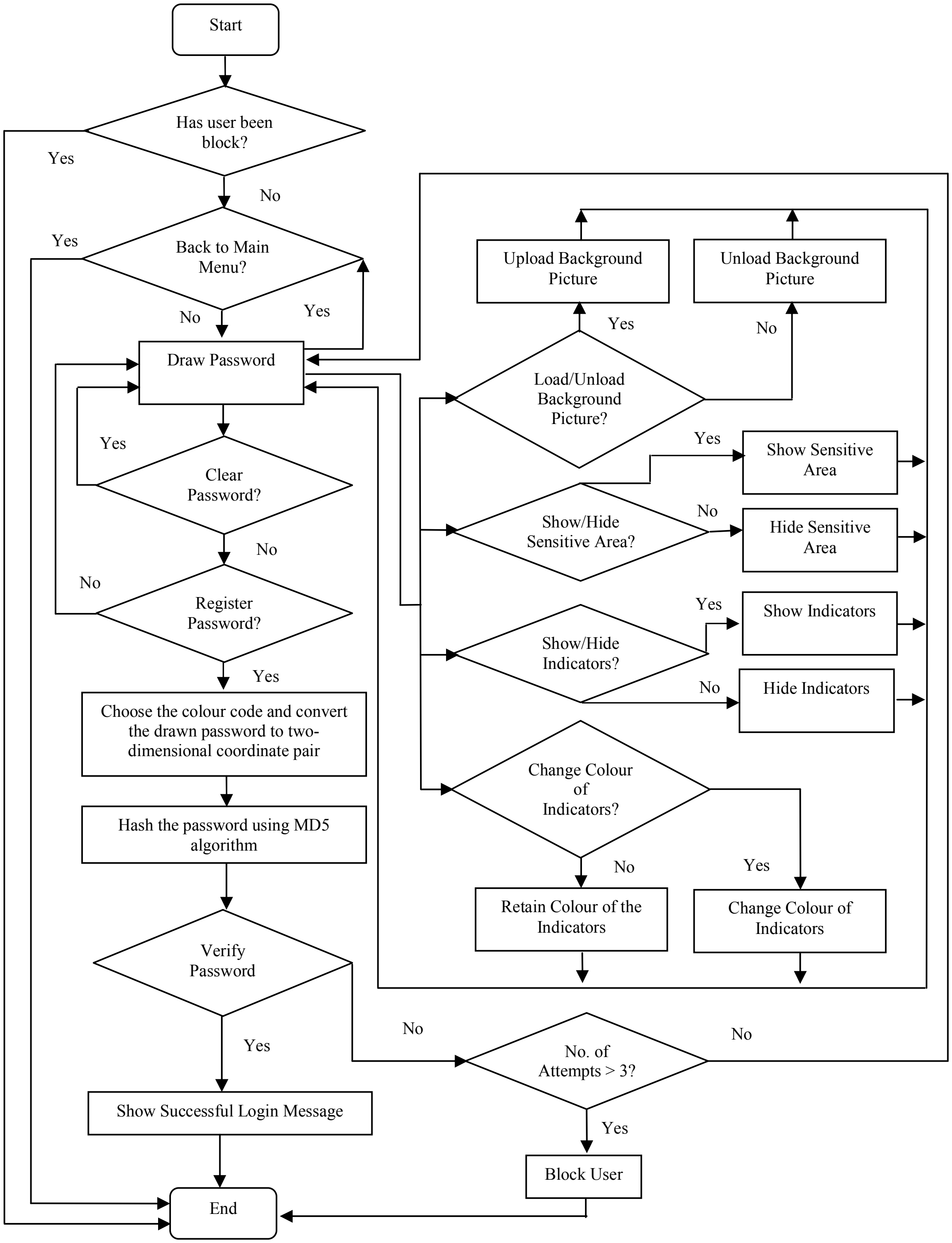

Start
Has user been block?
Yes
No
Back to Main Menu?
Yes
No
Yes
Draw Password
Clear Password?
Yes
No
Register Password?
No
Yes
Choose the colour code and convert the drawn password to two-dimensional coordinate pair
Hash the password using MD5 algorithm
Verify Password
Yes
Show Successful Login Message
End
No
No. of Attempts > 3?
Yes
Block User
No
Upload Background Picture
Unload Background Picture
Yes
No
Load/Unload Background Picture?
Yes
Show Sensitive Area
Show/Hide Sensitive Area?
No
Hide Sensitive Area
Yes
Show Indicators
Show/Hide Indicators?
No
Hide Indicators
Change Colour of Indicators?
No
Yes
Retain Colour of the Indicators
Change Colour of Indicators

Figure 4.36: System Flow of the Verification Process

4.4 Database Design

Table 4.2: BPG Metadata

Field Name	Data Type	NULL	Key	Description
USERNAME	varchar(256)	NO	PRI	User-defined name
PASSWORD	Longtext	NO	-	stores 128 bits MD5 hashing values
IS_LOCKED	tinyint(1)	NO	-	0: unlock, 1: lock
TRIAL_NO	int(10) unsigned	NO	-	number of FAILED login attempts
TIME_LOGIN	Datetime	NO	-	indicates the last login date and time
MAC_ADDRESS	varchar(45)	NO	-	stores user's MAC address
IP_ADDRESS	varchar(45)	NO	-	stores user's IP address

Table 4.2 shows the metadata of the BPG system. Seven fields have been defined for the BPG system – *USERNAME*; *PASSWORD*; *IS_LOCKED*; *TRIAL_NO*; *TIME_LOGIN*; *MAC_ADDRESS;* and *IP_ADDRESS*. The *USERNAME* is a user-defined name used by the proposed system to identify each user. The *PASSWORD* field is used to store the user's password in a 128-bit variable-length message produced by the MD5 hashing algorithm. The *IS_LOCKED* field is used as an indicator by the proposed system to identify whether a user has been blocked or has not been blocked by the system. The *TRIAL_NO*, *TIME_LOGIN*, *MAC_ADDRESS,* and *IP_ADDRESS* fields are used to record the number of unsuccessful login attempts, user last login date, and time when failure occurred, the MAC Access Control (MAC) address and Internet Protocol (IP) address of the computer used by the user, when failure occurred, respectively.

4.5 Summary

The BPG system was presented in this chapter. It is a standalone system developed using Java programming language, and MySQL was used as the database to store the transaction data produced by the users and the proposed system. The use case diagram of the BPG system was presented and used to discuss the functional requirements of the BPG system. The two main processes in the BPG system: enrollment process, and verification process were presented. The sub-functions of the enrollment process and verification process – drawn password function; register password function; clear password function; back to main menu function; and login function – were discussed in detail with the help of the GUI, pseudocode, and flow charts. The first falsifying authentication method that uses penup event and neighbouring connectivity manipulation to mitigate shoulder-surfing attack was then presented. The “show/hide indicators” function which allowed the user to hide a part of, or the whole password instead of using the proposed falsifying authentication method was also discussed. Discussion was then focused on the upload background picture function, and the colour scheme used in the BPG system to help to improve users’ memorability. To improve users’ memorability, an enhanced BPG system was developed. The new features for the enhanced BPG system will be presented in the following chapter.

Chapter 5 Design and Implementation of Enhanced Background Pass-Go

5.1 Introduction

The BPG system was enhanced with the aim of improving the users' memorability. The main difference between the enhanced BPG system and the original BPG system is that an extra grid line scaling function and a loose authentication method were added to the enhanced BPG system to assist the users in memorising their passwords. In this chapter, the enhanced BPG system architecture design as well as its use case diagram are discussed. The additional functional requirements and the database design are also discussed. A chapter summary is presented in the last section of this chapter.

5.2 Enhanced BPG System Architecture

The enhanced BPG is a single-tier architecture system and was programmed using J2SE and developed using Java Plug-in technology (Java Applet). MySQL database was used to store the relevant data or transactions produced by the users and the proposed system. Figure 5.1 shows the enhanced BPG system architecture.

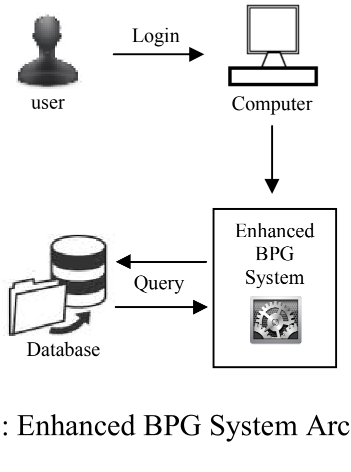


Figure 5.1: Enhanced BPG System Architecture

5.3 Enhanced BPG Use Case Diagram

Figure 5.2 shows the use case diagram of the enhanced BPG system. The enrollment process and the verification process are also the two main processes in the enhanced BPG system. The sub-functions of the enhanced BPG system are presented in the diagram and the additional extended functions are highlighted in red.

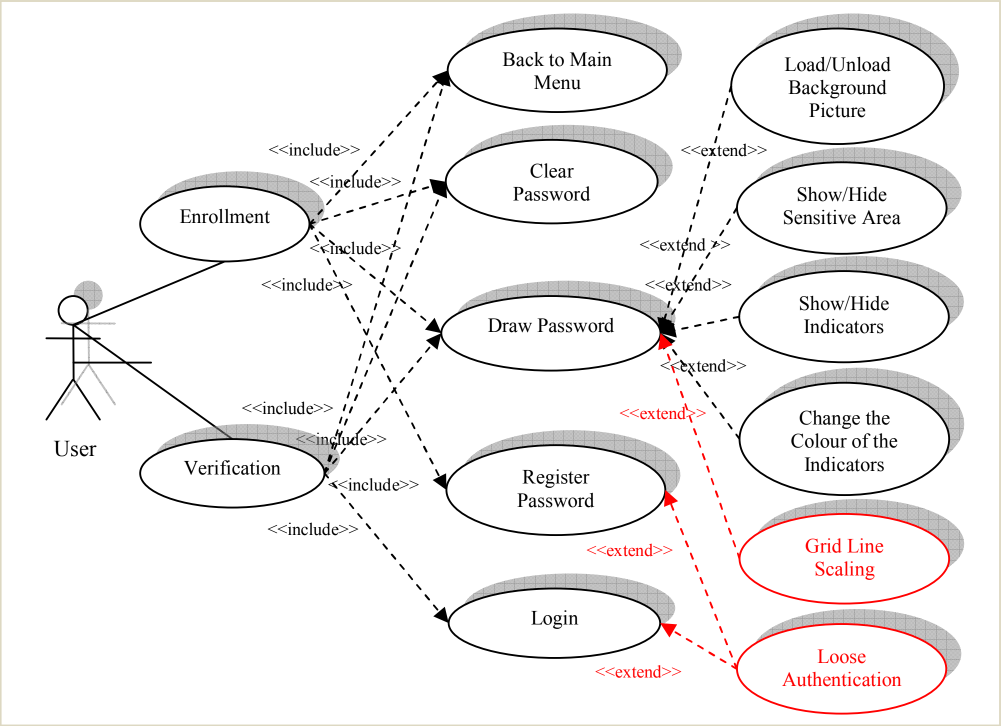


Figure 5.2: Enhanced BPG Use Case Diagram

5.3.1 Enrollment Process

The enrollment process of the enhanced BPG system consists of four sub-functions, which are as follows:

i. Draw Password

ii. Clear Password

iii. Back to Main Menu

iv. Register Password.

The draw password function, the clear password function, and the back to main menu function work exactly in the same way as the corresponding functions in the BPG system. However, in the draw password process, the users use the grid line scaling function to assist them in drawing their passwords.

5.3.1.1 Draw Password

The draw password sub-function consists of five extended sub-functions, which are as follows:

i. Change the Colour of the Indicators
ii. Load/Unload Background Picture
iii. Show/Hide Sensitive Area
iv. Show/Hide Indicators
v. Grid Line Scaling Function.

The first four extended sub-functions work exactly in the same way as the corresponding functions of the BPG system. To register a password in the enhanced BPG system, the user is required to choose an ID as a username and draw the password using dot, line, and shape indicators or a mixture of these indicators. Apart from using the first four extended sub-functions, a user can also use the grid line scaling function to draw his passwords.

5.3.1.1.1 Grid Line Scaling Function

Figure 5.3 shows the proposed grid line scaling feature. Two scroll bars are used to control the grid line scaling function in the enhanced BPG system. However, a user can only manipulate the grid lines by scaling up to 25 lines each due to the large predetermined indicator size. When the grid line has been scaled to more than 25 lines (either vertically or horizontally), the users might have difficulty in identifying the correct password because the dot indicator produced by the enhanced BPG system is relatively small and difficult to be seen and clicked (refer to Figure 5.4).

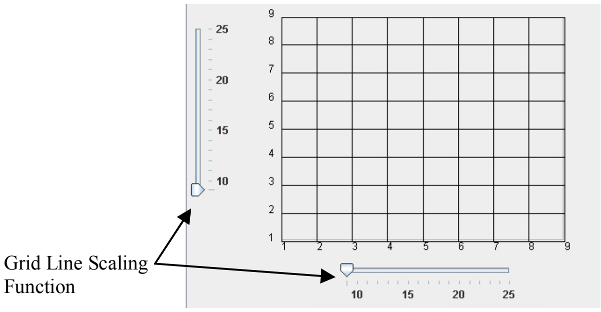
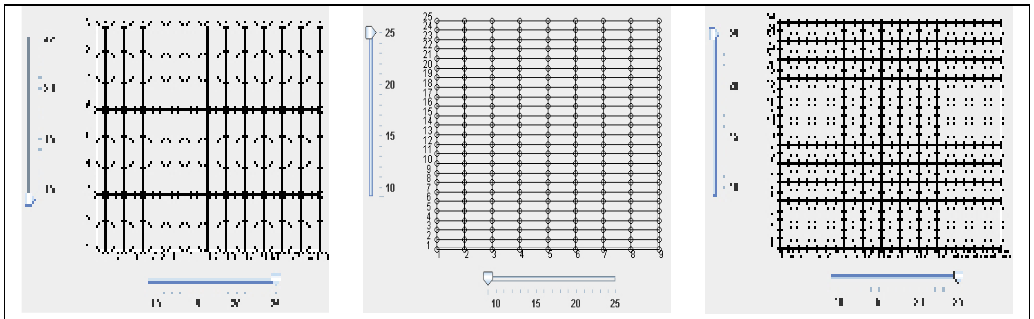


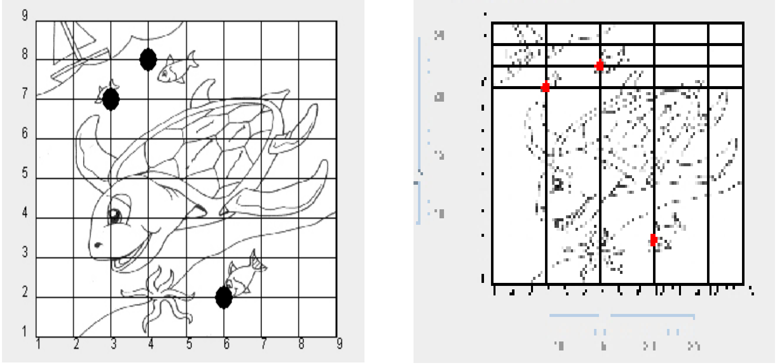
Figure 5.3: Grid Line Scaling Feature



a) Horizontal Scaling b) Vertical Scaling c) Maximum Scaling

Figure 5.4: Maximum Scaling Feature

The purpose of using the grid line scaling function is to allow the users to draw and identify more preferred points to be used as their passwords. Figure 5.5 illustrates the usability of the grid line scaling function in terms of its usefulness and flexibility in helping the users in memorising their passwords. If the users intend to use the chosen points (eyes of the fishes) from a preferred background as their password in the BPG system, they are required to draw and memorise those points by using the adjacent coordinates, which are relatively close to the chosen points. However, in the enhanced BPG system, the users can use the grid line scaling function to scale to the chosen points. Therefore, it is possible that the users can remember their passwords better as the chosen points can be identified more easily and more accurately. Figure 5.6 shows the pseudocode of the grid line scaling function implementation in the proposed system.



(a) The adjacent coordinates must be memorised if the chosen points (eyes of the fishes) are used in the original BPG system.

b) The chosen points can be identified more easily using the grid line scaling function in the enhanced BPG system.

Figure 5.5: The Usability of the Grid Line Scaling Function

```
PROCEDURE createRowSlider
      Create slider
      Add slider to user interface
      If slider is dragged, recalculate the sensitive areas
END PROCEDURE

PROCEDURE createColSlider
      Create slider
      Add slider to user interface
      If slider is dragged, recalculate the sensitive areas
END PROCEDURE
```

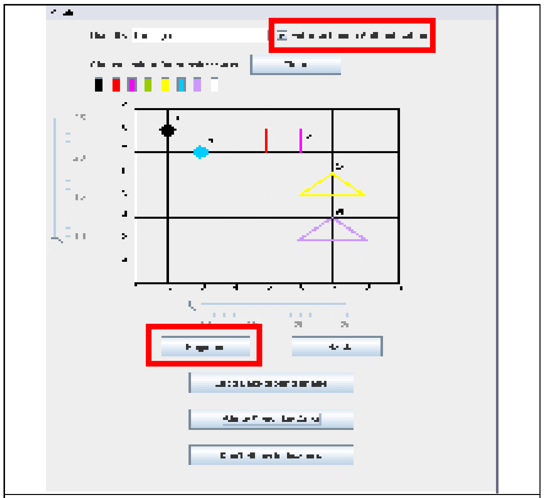
Figure 5.6: Pseudocode for Grid Line Scaling Implementation

5.3.1.2 Register Password

The register password function works exactly in the same way as the corresponding functions in the original BPG system. After a user has drawn a password, a sequence of intersections will be produced and converted using the following encoding scheme: $\sum_{(x,y)\in[1..G]\times[1..G]}(x,y,[r,g,b]) \in \{\}$. The system will verify whether the loose authentication method has been applied before encrypting the converted encoding using the MD5 hashing algorithm. Finally, the encrypted data will be stored into the database.

5.3.1.2.1 Loose Authentication

The loose authentication method is an additional function of the enhanced BPG system to assist users in memorising their passwords. This function allows users to use the sequence of dot indicators followed by the sequence of line indicators or vice versa, to perform the authentication besides using the actual sequence of order, which is used in the BPG system. To illustrate the loose authentication method, a password was created and its encoding was generated, as shown in Figure 5.7.



Password Sequence:
black dot indicator, blue dot indicator, red line indicator, pink line indicator, yellow triangle line indicator, purple triangle line indicator

Generated Password Encoding:
(2,8,[0,0,0])(3,7,[0,204,255]){(5,8,[255,0,0])(5,7,[255,0,0])}{(6,8,[255,0,255])(6,7,[255,0,255])}{(6,6,[255,255,0])(5,5,[255,255,0])(6,5,[255,255,0])(7,5,[255,255,0])(6,6,[255,255,0])}{(6,4,[204,153,255])(5,3,[204,153,255])(6,3,[204,153,255])(7,3,[204,153,255])(6,4,[204,153,255])}

Figure 5.7: A Sample Password and the Encoding Generated of the Enhanced BPG System

Let:

$$\text{D(x,y[r,g,b])} = \sum_{(x,y)\in[1..G]\times[1..G]}^{n_1}(x,y,[r,g,b]) \qquad (2)$$

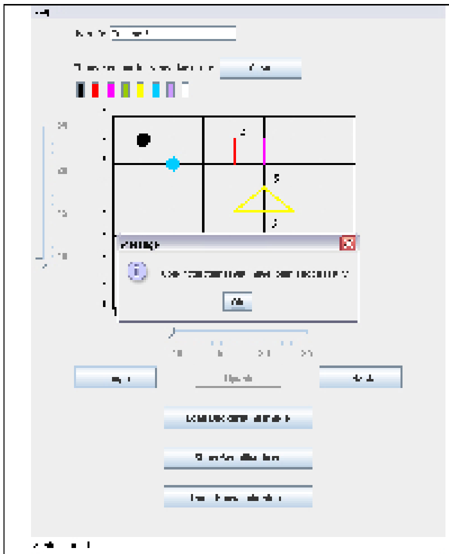
n_1 is the total number of dot indicators used in the sequence for the password.

$$\text{L(x,y[r,g,b])} = \sum_{(x,y)\in[1..G]\times[1..G]}^{n_2}(x,y,[r,g,b]) \in \{\} \qquad (3)$$

n_2 is the total number of line indicators used in the sequence for a password and {} represents the penup event.

As mentioned earlier, in order to produce an acceptable password using the loose authentication method, the sequence of the combination of the dot indicators and the line indicators is not important as long as the relationship between equations (2) and (3) holds: For example, a user is required to identify the black dot indicator (2,8,[0,0,0]) before the blue dot indicator (3,7,[0,204,255]) in order to verify the correct dot indicators. With the line indicators, the red line indicator, {(5,8,[255,0,0])(5,7,[255,0,0])} must be identified, to be followed by the pink line indicator {(6,8,[255,0,255])(6,7,[255,0,255])}, the yellow triangle line indicator, {(6,6,[255,255,0])(5,5,[255,255,0])(6,5,[255,255,0])(7,5,[255,255,0])(6,6,[255,255,0])}, and finally the purple triangle line indicator {(6,4,[204,153,255])(5,3,[204,153,255])(6,3,[204,153,255])(7,3,[204,153,255])(6,4,[204,153,255])}.

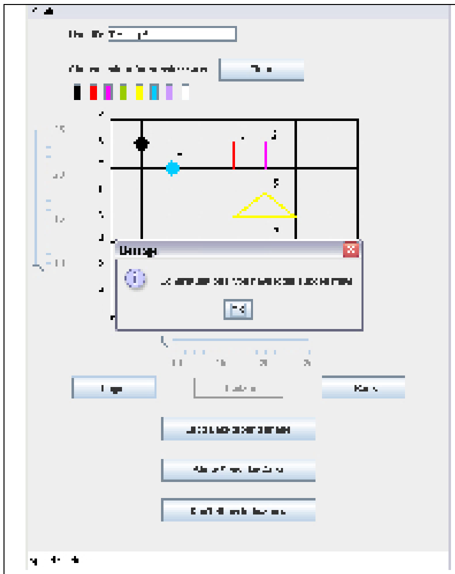
Figures 5.8 - 5.10 show the sample password instances that can be used and the pseudocode for the implementation, if the loose authentication method is enabled, respectively.



Password Sequence:
black dot indicator, red line indicator, blue dot indicator, pink line indicator, yellow triangle line indicator, purple triangle line indicator

Generated Password Encoding:
(2,8,[0,0,0]),{(5,8,[255,0,0])(5,7,[255,0,0])},(3,7,[0,204,255]),{(6,8,[255,0,255])(6,7,[255,0,255])},{(6,6,[255,255,0])(5,5,[255,255,0])(6,5,[255,255,0])(7,5,[255,255,0])(6,6,[255,255,0])},{(6,4,[204,153,255])(5,3,[204,153,255])(6,3,[204,153,255])(7,3,[204,153,255])(6,4,[204,153,255])}

Figure 5.8: Loose Authentication Password and its Encoding: Example I



Password Sequence:
red line indicator, pink line indicator, black dot indicator, blue dot indicator, yellow triangle line indicator, purple triangle line indicator

Generated Password Encoding:
{(5,8,[255,0,0])(5,7,[255,0,0])},{(6,8,[255,0,255])(6,7,[255,0,255])},(2,8,[0,0,0]),(3,7,[0,204,255]),{(6,6,[255,255,0])(5,5,[255,255,0])(6,5,[255,255,0])(7,5,[255,255,0])(6,6,[255,255,0])},{(6,4,[204,153,255])(5,3,[204,153,255])(6,3,[204,153,255])(7,3,[204,153,255])(6,4,[204,153,255])}

Figure 5.9: Loose Authentication Password and its Encoding: Example II

```
Set pass to empty string
IF inSequence
      FOREACH passwordDrawing
            Get password for the drawing
            Append the password to pass
      END FOREACH
ELSE
      Clone a copy of the passwordDrawing, passwordDrawingClone
      Sort the passwordDrawingClone so that clicks are sorted infront
      FOREACH passwordDrawing
            Get password for the drawing
            Append the password to pass
      END FOR EACH
END IF
```

Figure 5.10: Pseudocode for Loose Authentication Implementation

5.3.1.3 System Flow of the Enrollment Process

Figure 5.11 shows the system flow of the password enrollment process for the enhanced BPG system. The new process flows are shown as red broken lines. As an initial step, the users are required to draw their passwords. They are allowed to personalise their colour code, background picture, and grid scaling line, when drawing their password. Besides, the users can use the show sensitive area function to assist them in drawing their passwords. They can also choose to hide a part of, or the whole password, by using the hide indicators function instead of using the proposed falsifying authentication method. The users are required to indicate whether they want to enable the loose authentication function before registering their passwords. After the password has been confirmed, a set of password encoding will be generated. The password encoding is hashed and stored in the database at the end of the enrollment process.

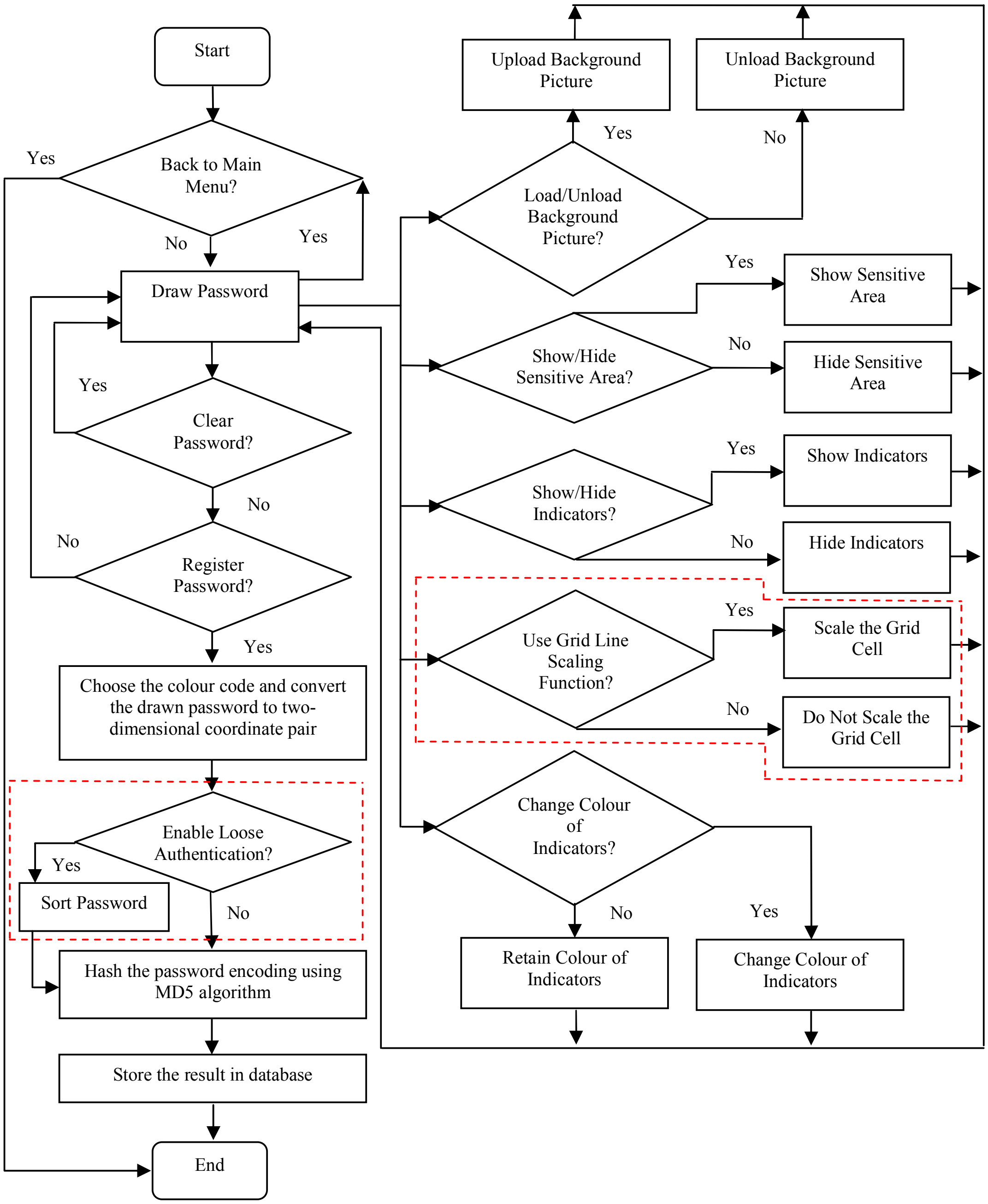

Start
Back to Main Menu?
Yes
No
Yes
Draw Password
Yes
Clear Password?
No
No
Register Password?
Yes
Choose the colour code and convert the drawn password to two-dimensional coordinate pair
Enable Loose Authentication?
Yes
Sort Password
No
Hash the password encoding using MD5 algorithm
Store the result in database
End
Upload Background Picture
Unload Background Picture
Yes
No
Load/Unload Background Picture?
Yes
Show Sensitive Area
No
Show/Hide Sensitive Area?
Hide Sensitive Area
Yes
Show Indicators
Show/Hide Indicators?
No
Hide Indicators
Yes
Scale the Grid Cell
Use Grid Line Scaling Function?
No
Do Not Scale the Grid Cell
Change Colour of Indicators?
No
Yes
Retain Colour of Indicators
Change Colour of Indicators

Figure 5.11: System Flow of the Enrollment Process

5.3.2 Verification Process

The verification procedure consists of four sub-functions, which are as follows:

i. Draw Password

ii. Clear Password

iii. Back to Main Menu

iv. Login.

The draw password function, the clear password function, and the back to main menu function work exactly in the same way as the corresponding functions in the enrollment process.

5.3.2.1 Login

During the login process, the system will verify whether the users have enabled the loose authentication function. If the users have enabled the function, they can proceed to identify the correct password keystrokes, and the sequence for the dot indicators, and the line or shape indicators, separately. If the users have not enabled the loose authentication function, they are required to re-produce the correct password keystrokes and their sequence (similar to that of the enrollment process) before they are allowed access into the system.

The users can use the upload background picture function to assist them in drawing the password. Besides using the proposed falsifying authentication method, the users can use the “show/hide indicators” function to hide a part of, or the whole password created by them. After the users have drawn their passwords, a string, which is the password encoding, will be generated. The password encoding will be hashed, and the hashed password will then be compared with the registered password in the database. If a user fails to be authenticated after three consecutive attempts, his/her account will be blocked by the proposed system.

5.3.2.2 System Flow for Verification Process

Figure 5.12 shows the system flow of the password verification process of the enhanced BPG system. The new process flows are shown in red broken lines. As an initial step, the proposed system will verify whether a user has previously been blocked by the system. If the user has been blocked, he/she cannot use the system to login. The proposed system will then verify whether the user has enabled the loose authentication function. If the feature has been enabled, the user will proceed to identify the correct password keystrokes and the sequence for the dot indicators and the line indicators or the shape indicators, separately. If the user has not enabled the loose authentication function, he is required to produce the correct password keystrokes and the sequence (i.e., exactly as was done during the enrollment process) before he/she is allowed access into the system. The user is allowed to personalise his/her colour code and the background picture when drawing his/her password. Besides, the user can use the grid line scaling function, and the show sensitive area function to assist him/her when drawing the password. The user can also hide a part of, or the whole password, by using the hide indicators function instead of using the proposed falsifying authentication method. After the user has confirmed the password, a set of password encoding is generated. The generated password encoding is hashed using a hashing algorithm. The hased password is then compared with the registered password in the database. If the user has been successfully authenticated, a welcoming message will be displayed. If the user has not been authenticated, her/she will be allowed another two attempts to be authenticated. If the user fails to be authenticated after the third attempt, he/she will be blocked from accessing the system.

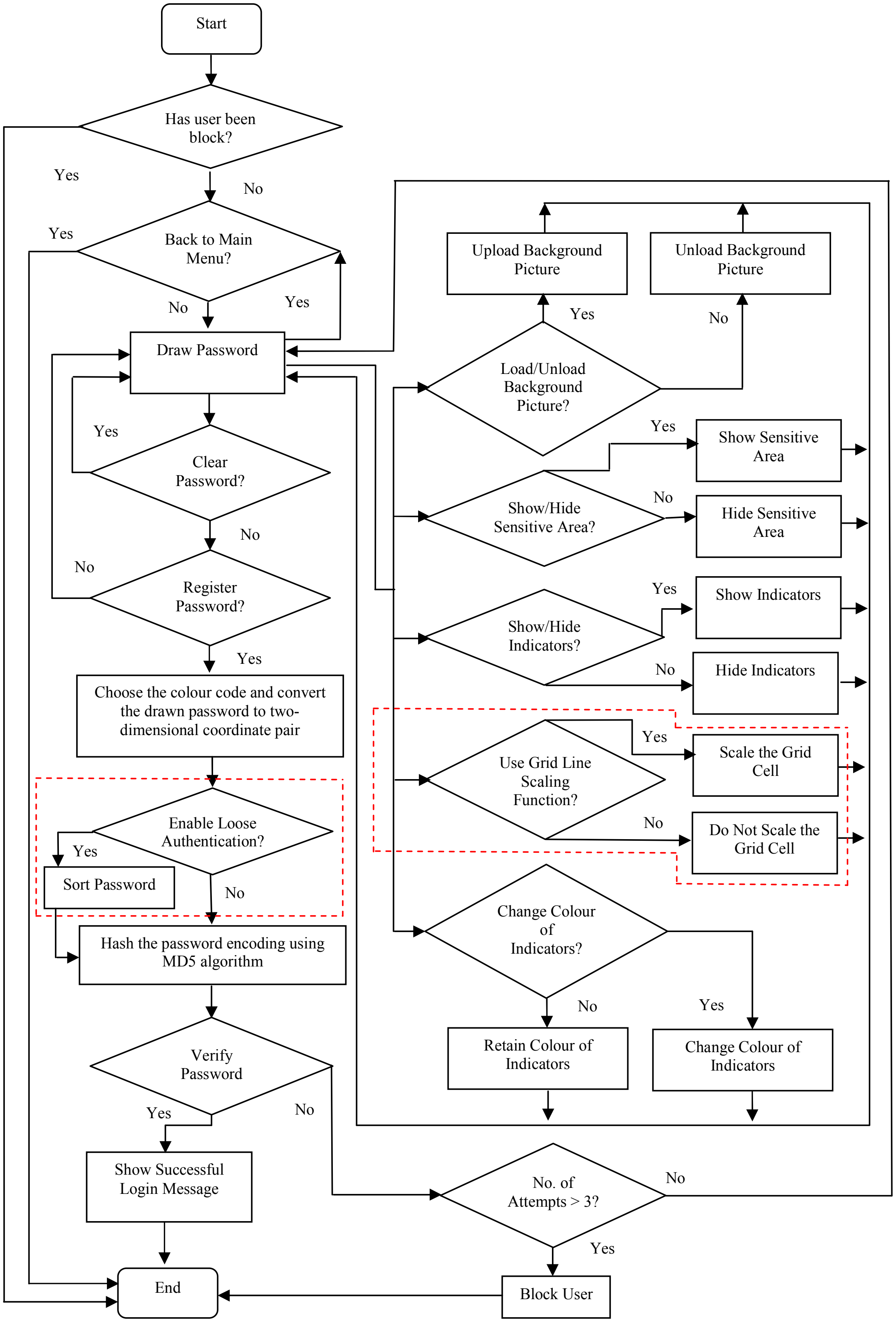

Start
Has user been block?
Yes
No
Back to Main Menu?
Yes
No
Yes
Draw Password
Yes
Clear Password?
No
No
Register Password?
Yes
Choose the colour code and convert the drawn password to two-dimensional coordinate pair
Enable Loose Authentication?
Yes
Sort Password
No
Hash the password encoding using MD5 algorithm
Verify Password
Yes
No
Show Successful Login Message
End
Upload Background Picture
Unload Background Picture
Yes
No
Load/Unload Background Picture?
Yes
Show Sensitive Area
Show/Hide Sensitive Area?
No
Hide Sensitive Area
Yes
Show Indicators
Show/Hide Indicators?
No
Hide Indicators
Yes
Use Grid Line Scaling Function?
Scale the Grid Cell
No
Do Not Scale the Grid Cell
Change Colour of Indicators?
No
Yes
Retain Colour of Indicators
Change Colour of Indicators
No. of Attempts > 3?
No
Yes
Block User

Figure 5.12: System Flow of the Verification Process

5.4 Database Design

Table 5.1 shows the metadata of the enhanced BPG system. Except for the LOOSE_AUTH field, all the other fields in the enhanced BPG metadata are similar to the corresponding fields of the BPG metadata. The additional field, LOOSE_AUTH, is used to indicate whether a user has applied the "loose authentication" function.

Table 5.1: Enhanced BPG Metadata

Field Name	Data Type	NULL	Key	Description
USERNAME	varchar(256)	NO	PRI	user-defined name
PASSWORD	Longtext	NO	-	stores 128 bits MD5 hashing values
IS_LOCKED	tinyint(1)	NO	-	0: unlock, 1: lock
TRIAL_NO	int(10) unsigned	NO	-	number of FAILED login attempts
TIME_LOGIN	Datetime	NO	-	indicates the last login date and time
MAC_ADDRESS	varchar(45)	NO	-	stores user's MAC address
IP_ADDRESS	varchar(45)	NO	-	stores user's IP address
LOOSE_AUTH	tinyint(1)	NO	-	0: does not enforce loose authentication method, 1: enforce loose authentication method

5.5 Summary

The enhanced BPG system was presented in this chapter. The system architecture for the enhanced BPG system was discussed. The use case diagram of the enhanced BPG system was presented and used to discuss the functional requirements of the enhanced BPG system. The two main processes in the BPG system: enrollment process, and verification process were presented. Most of the functions in the enhanced BPG system are similar to that to the BPG system, except for the additional grid line scaling function, and the loose authentication function, which were added to assist the users in memorising their passwords. Two scroll bars are used to control the grid line scaling operation in the enhanced BPG system. The loose authentication feature is an alternative authentication method used in the enhanced BPG system. This chapter also described the functionality of the additional grid line scaling function, and the loose authentication function. The database design of the enhanced BPG system was then presented. The next chapter presents the third proposed system – the Visual Identification Protocol Professional (VIP Pro) system.

Chapter 6 Design and Implementation of Visual Identification Protocol Professional

6.1 Introduction

The Visual Identification Protocol Professional (VIP Pro) system has been proposed to complete the picture-based password authentication cluster (searchmetric cluster). The development of the VIP Pro system has been inspired by the visual identification protocol authentication series proposed by De Angeli et al. (2003; 2005). In this chapter, the VIP Pro system architecture design and its use case diagram are discussed. There are two main processes in the VIP Pro system – the enrollment process, and the verification process. The design and implementation of the enrollment process and the verification process together with their sub-functions are discussed, and illustrated with screenshots of the graphical user interfaces, pseudocodes, and flow charts. A counter-measure that uses metaheuristic randomisation algorithm is proposed to prevent Frequency of Occurrence Analysis (FOA) attack. A falsifying authentication method that uses partial password selection and metaheuristic randomisation algorithm is proposed to mitigate shoulder-surfing attack. The details of the proposed methods are described in the verification process. The database design of the proposed system is also presented. The last section presents the chapter summary.

6.2 VIP Pro System Architecture

VIP Pro is a standalone application and was programmed using J2SE, and developed using Java Plug-in technology (Java Applet). MySQL database was used to store the relevant data and transactions produced by the users and the system. Figure 6.1 shows the system architecture for the VIP Pro system.

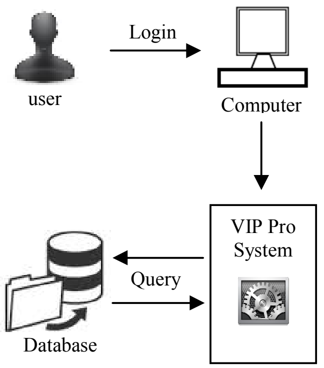


Figure 6.1: VIP Pro System Architecture

6.3 VIP Pro Use Case Diagram

Figure 6.2 shows the use case diagram for the VIP Pro system. There are two main processes in the VIP Pro system – the enrollment process, and the verification process.

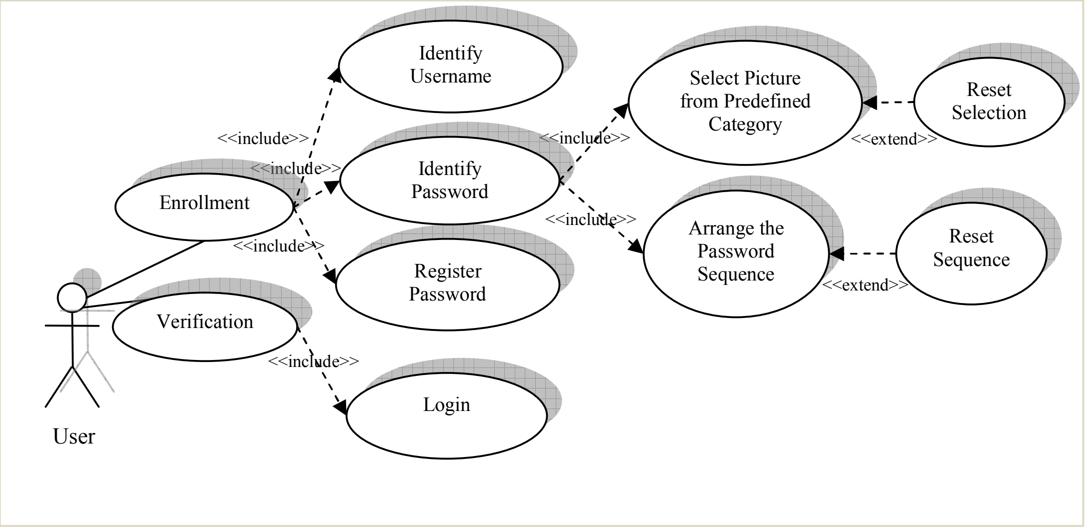


Figure 6.2: VIP Pro System Use Case Diagram

6.3.1 Enrollment Process

The enrollment procedure for the VIP Pro system consists of three sub-functions, as follows:

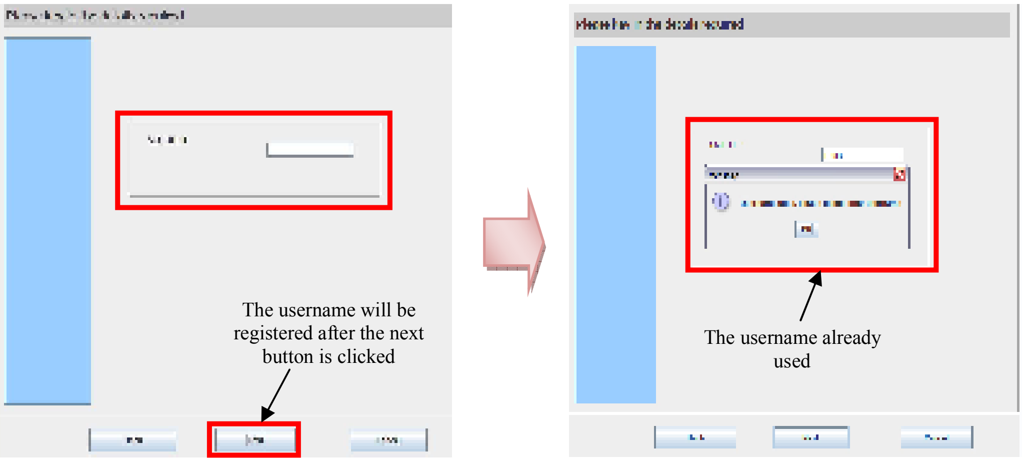
i. Identify Username

ii. Identify Password

iii. Register Password.

6.3.1.1 Identify Username

Initially, users are required to choose a suitable username. The username is a unique identifier for identifying a user in the proposed system. The system will notify the user if a username has already been used. Figure 6.3 and Figure 6.4 show the graphical user interface (GUI) and the pseudocode of the "identify username" function.



The username will be registered after the next button is clicked

The username already used

Figure 6.3: Identify Username GUI

```
PROCEDURE getUserName

      Set userName to NULL
      Get userName
      Open database and retrieve username from users table
      IF (username = userName)
            Prompt username already used
      END IF

END PROCEDURE
```

Figure 6.4: Pseudocode for the Identify Username Implementation

6.3.1.2 Identify Password

The identify password sub-function consists of two sub-functions, which are as follows:

i. Select Picture from Predefined Category

ii. Arrange Password Sequence.

6.3.1.2.1 Select Picture from Predefined Category

Figure 6.5 shows the GUI of the feature of the "select picture from predefined category" function. There are nine semantic categories – flowers; animals; rocks; landscapes; humans; vegetables; buildings; skies; and boats – which are modelled after the categories defined by De Angeli et al. (2003). These were adopted as the predefined categories in the VIP Pro system. The users are required to register a set of secret password pictures, $X \in x_1, x_2, x_3 \ldots x_{|X|}$, selected from the predefined categories, as their password. They are allowed to select the pictures from a single category or a mixture of pictures from different categories. However, the total number of pictures selected must be within the domain of $8 \leq |X| \leq 16$. The justification for the cardinality of $|X|$ is presented in Chapter 7. Figure 6.6 shows the implementation pseudocode of the "select picture from predefined category" function.

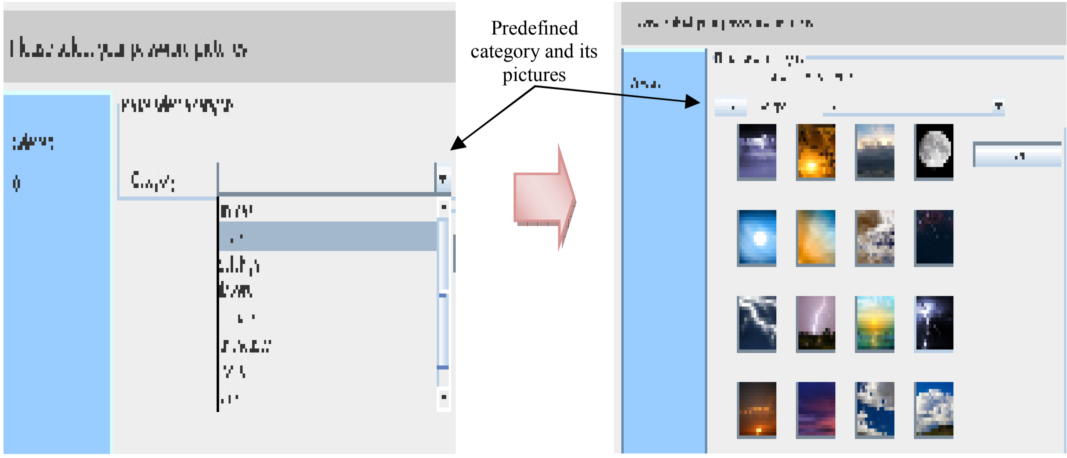


Figure 6.5: Select Picture from Predefined Category

```
PROCEDURE identifyCategory

      Clear GridPanel
      Get CategoryName
      Open database and retrieve pictures from CategoryName
      Arrange Pictures in GridPanel according to PictureID

END PROCEDURE
```

Figure 6.6: Pseudocode for Select Picture from Predefined Category Function and Its Respective Pictures Implementation

The select picture function has the following extended sub-function:

i. Reset Selection

6.3.1.2.1.1 Reset Selection

This function allows users to reset or undo their picture selection, as shown in Figure 6.7. Following this, the users can repack another set of new pictures as their password. Figure 6.8 shows the reset selection implementation pseudocode.

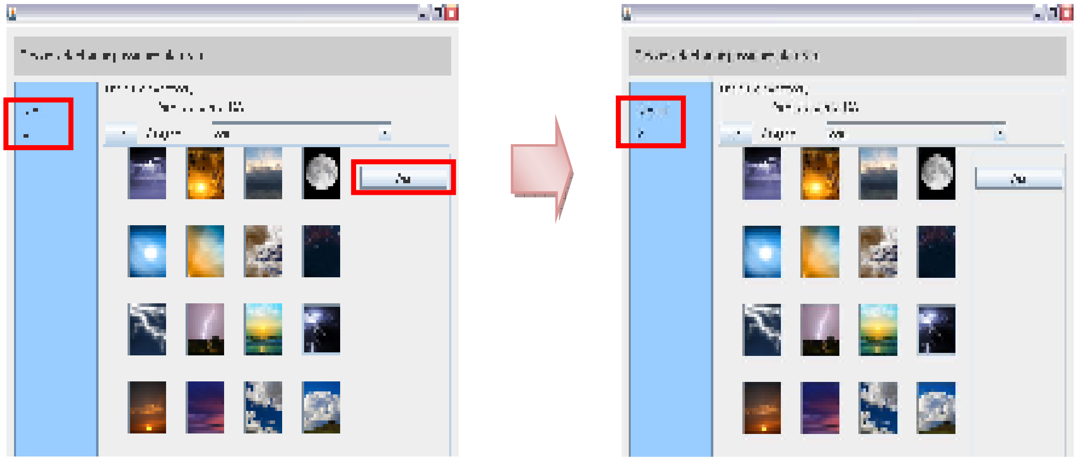


Figure 6.7: Reset Selection Feature

```
PROCEDURE resetPicture

      Set selected counter to 0
      Set SelectedPitureID to NULL

END PROCEDURE
```

Figure 6.8: Pseudocode for Reset Selection Implementation

6.3.1.2.2 Arrange Password Sequence

After the users have selected their pictures, they are required to determine the password sequence using each of the selected pictures. They have to click on the selected pictures (shown within the red broken line box in Figure 6.9) and the password sequence is then shown on the right-hand panel (refer to the blue broken line box in Figure 6.9). Figure 6.10 shows the selected password sequence implementation pseudocode.

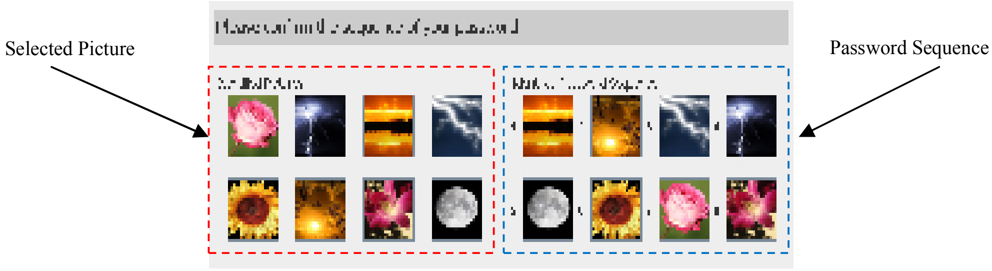


Figure 6.9: Identify Password Sequence

```
FOREACH clickPass
      Get PictureID and assign to pass
      Arrange pass in GridPanel
      Append to pass

END FOREACH
```

Figure 6.10: Pseudocode for Identify Password Sequence Implementation

The “arranged password sequence” function has the following extended sub-function:

i. Reset Password Sequence

6.3.1.2.2.1 Reset Password Sequence

This function allows users to reset their existing password sequence. Pressing the ‘Clear’ button, as shown in Figure 6.11, will cause the existing selected password sequence to be removed. Following this, the users are required to click on the identified pictures (shown within the red broken line box) and re-determine the new password sequence. Figure 6.12 shows the reset password sequence implementation pseudocode.

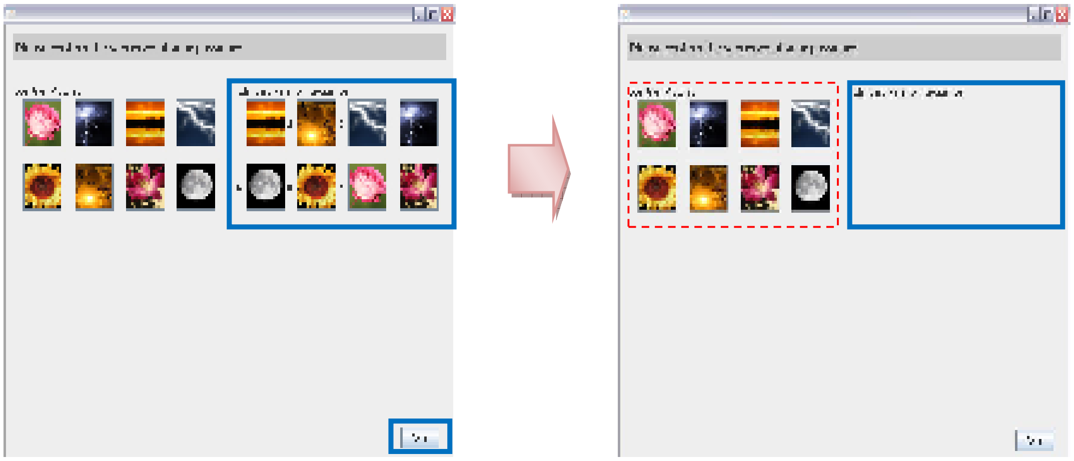


Figure 6.11: Reset Password Sequence Function

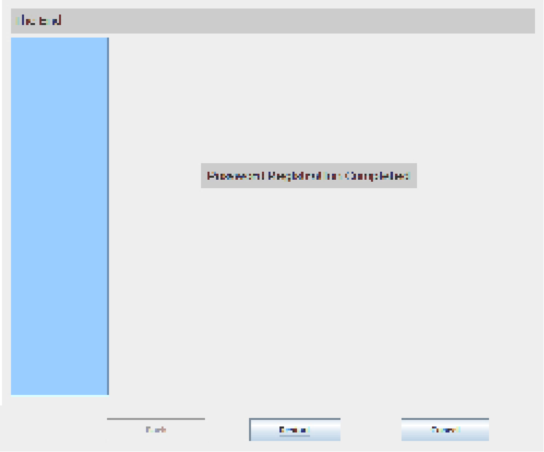
```
PROCEDURE resetPassSeq

      Clear GridPanel
      Set pass to NULL

END PROCEDURE
```

Figure 6.12: Pseudocode for Reset Password Sequence Implementation

6.3.1.3 Register Password

After the user has confirmed the password sequence, the picture ID is then arranged according to the selected password sequence. The arranged picture IDs are encrypted using the MD5 algorithm, and the encypted password is finally stored in the database.

Figure 6.13 and Figure 6.14 show the final screenshot of the GUI of the registration process and its implementation pseudocode, respectively.



Password Registration Completed

Figure 6.13: Registration Password Completion GUI

```
PROCEDURE register

      Get pass
      Process pass with MD5
      Open database and insert pass into database

END PROCEDURE
```

Figure 6.14: Pseudocode for Registration Password Implementation

6.3.1.4 System Flow for Enrollment Process

Figure 6.15 shows the system flow of the password enrollment process of the VIP Pro system. As an initial step, the users are required to create their password by selecting pictures from the predefined categories. They must also decide on the password sequence after selecting their preferred pictures. The users are allowed to reselect their favourite pictures and password sequence before registering their password. After the password has been confirmed, the picture IDs are arranged according to the selected password sequence and then encrypted using the MD5 algorithm. The encrypted password is finally stored in the database at the end of the enrollment process.

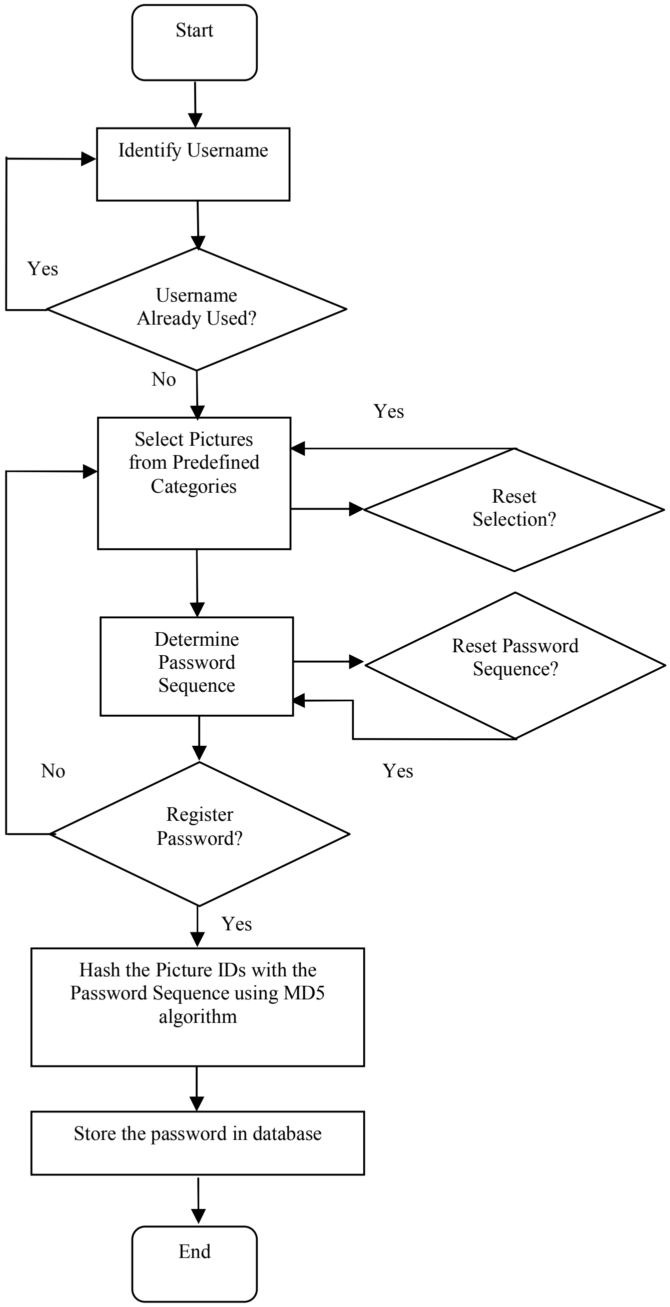

Start
Identify Username
Yes
Username Already Used?
No
Yes
Select Pictures from Predefined Categories
Reset Selection?
Determine Password Sequence
Reset Password Sequence?
No
Yes
Register Password?
Yes
Hash the Picture IDs with the Password Sequence using MD5 algorithm
Store the password in database
End

Figure 6.15: System Flow of the Enrollment Process

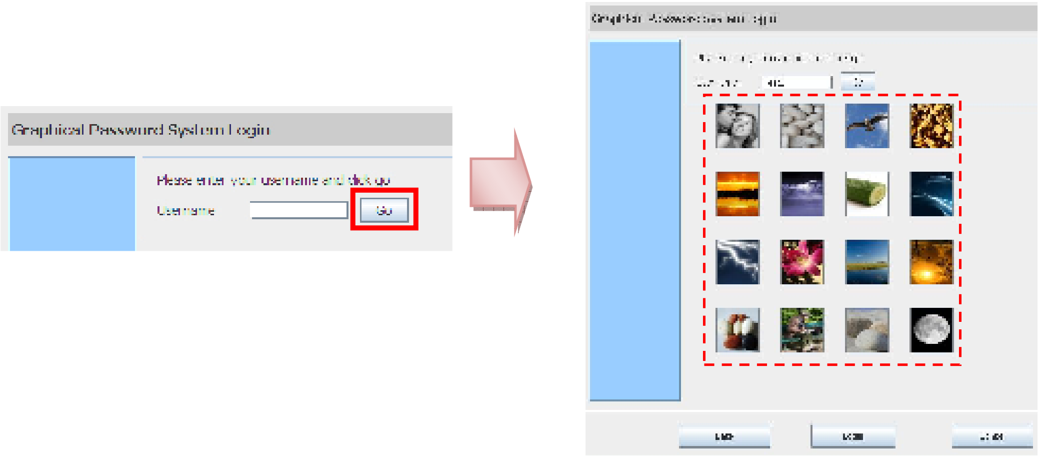
6.3.2 Verification Process

The verification process has the following sub-function:

i. Login

6.3.2.1 Login

During the login process, a user is required to key in his/her username. A set of 16 pictures (in a 4×4 grid) will be generated as a challenge set after the user has submitted the username to the system when he/she clicks on the 'Go' button (refer to Figure 6.16). A different set of partial password pictures is used in each challenge set to mitigate shoulder-surfing attacks. To retain randomness, a uniform randomisation algorithm is used to select the partial secret password pictures, $J \in j_1, j_2, j_3 \ldots j_{|J|}$, from X where $4 \leq |J| \leq 5$. The remaining pictures in the challenge set comprised k decoy pictures selected from (N – $|X|$) using the uniform randomisation algorithm (N is the total sample pictures used in the proposed system). The justification for the cardinality of $|J|$ is presented in Chapter 7.



Graphical Password System Login

Please enter your username and click go

Username

Figure 6.16: Challenge Set Generation GUI

To login into the system, the users must first identify the correct sequence of the partial password pictures generated by the proposed VIP Pro system. The proposed falsifying authentication method in the VIP Pro system can successfully confuse the shoulder-surfing attackers from identifying the correct password pictures and their sequence because only partial password pictures are used and there is no fixed number of the partial password pictures to be determined in each challenge set.

If the users fail to identify their password in the first attempt, the uniform randomisation algorithm is used to select a brand new set of partial secret password, $J_{new} \in j_1, j_2, j_3 \ldots j_{|J_{new}|}$, from X where $4 \leq |J_{new}| \leq 5$. The FOA attack can be prevented by recycling the old distracter pictures in the previous challenge set to increase the frequency of occurrence of the distracter pictures. In the proposed system, the metaheuristic randomisation algorithm (MRA) is used to randomly identify and reuse a set of decoy pictures which have been selected in the previous attempt. The total number of pictures produced in the second attempt can be denoted as the summation of J_{new} secret passwords, $P_A(k)$ of decoy pictures from the previous attempt and $P_B(N - |X| - k)$ new decoy pictures from the remaining sampling pool, where N is the total number of sample pictures used in the sampling pool, k is the number of decoy pictures used in the previous attempt, P_A is the probability of decoy pictures used in the previous attempt where it has the metaheuristic distribution range of $\overset{j_{4..5}}{R_4} - \overset{j_{4..5}}{R_7}$ and P_B is the probability of new decoy pictures with $P_B = 1 - P_A$. The metaheuristic distribution range notation, $\overset{j_{n..m}}{R_i}$, and the distribution range used in the proposed system are discussed in Chapter 7. Figure 6.17 shows the sample password pictures used by a user and Figures 6.18 - 6.19 illustrate the use of the proposed method in selecting the password pictures and the decoy pictures in the first and second challenge sets, respectively.

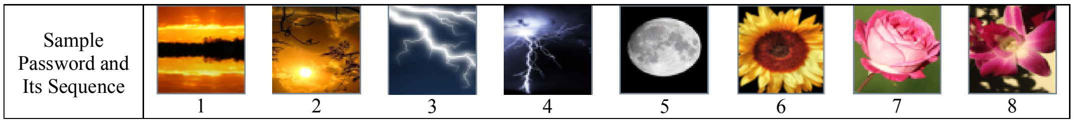
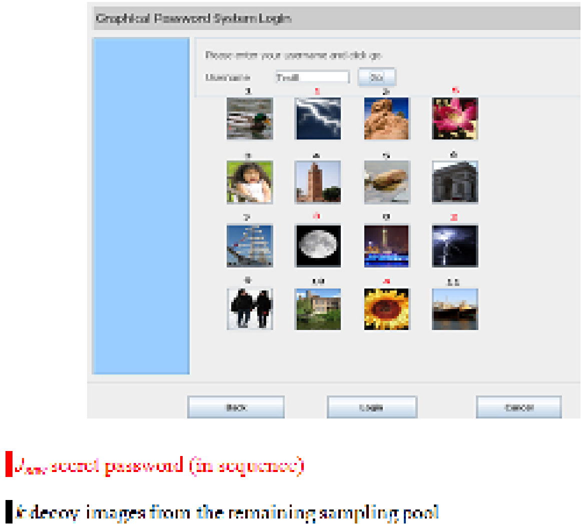
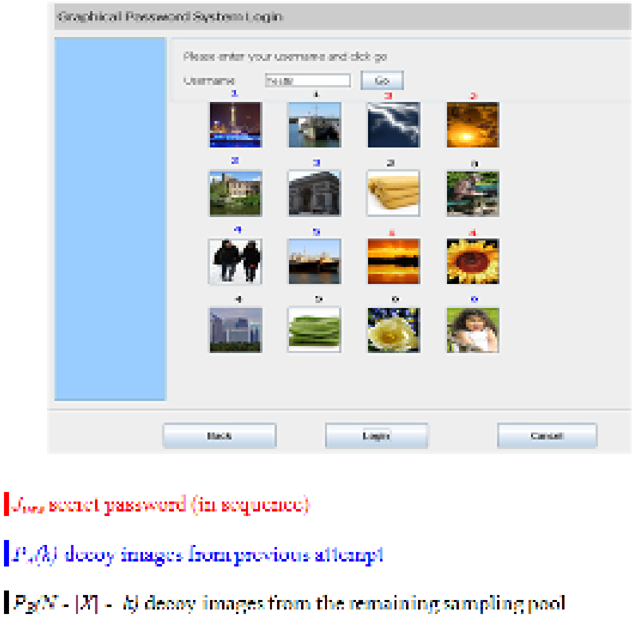


Figure 6.17: Sample Password



Graphical Password System Login
Please enter your username and click go
Username
Go
Back
Login
Cancel
J_{new} secret password (in sequence)
k decoy images from the remaining sampling pool

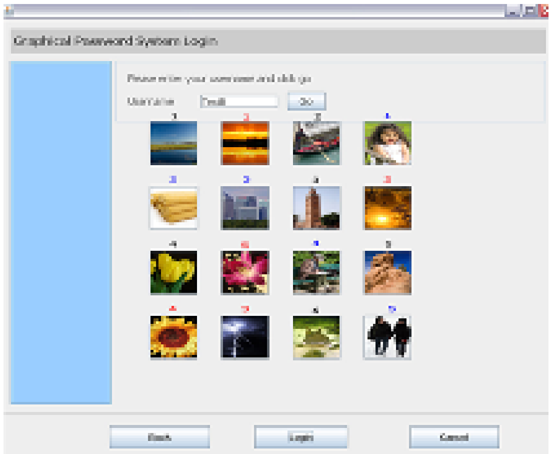
Figure 6.18: Initial Challenge and Its Generated Pictures



Graphical Password System Login
Please enter your username and click go
Username
Go
Back
Login
Cancel
J_{new} secret password (in sequence)
$P_A(k)$ decoy images from previous attempt
$P_B(N - |X| - k)$ decoy images from the remaining sampling pool

Figure 6.19: Second Attempt and Its Generated Pictures

If the users are unable to identify their passwords after two consecutive attempts, the same proposed mechanism is used to select the password and decoy pictures. Similarly, a new set of partial passwords, J_{new}, is first identified using the uniform randomisation algorithm. The MRA is then used to identify and reuse the decoy pictures, which have been generated during the second login attempt. Finally, the remaining pictures are filled with a completely new set of decoy pictures which have been identified from the sampling pool of pictures of the proposed system. The total number of pictures produced in the third attempt can be denoted as the summation of J_{new} partial passwords, $P_A(P_A(k) + P_B(N - |X| - k))$ of decoy pictures from the second attempt, and $P_B(N - |X| - (P_A(k) + P_B(N - |X| - k)))$ new decoy pictures from the remaining sampling pool, where P_A and P_B have the probability distribution range of $\overset{j_{4..5}}{R_4} - \overset{j_{4..5}}{R_7}$ and $\overset{j_{4..5}}{R_3} - \overset{j_{4..5}}{R_6}$, respectively. The metaheuristic distribution ranges used in the proposed system, are discussed in Chapter 7. Figure 6.20 and Figure 6.21 show the propagation process of the third attempt and the pseudocode for the proposed method, respectively.


Graphical Password System Login
Please enter your username and click go
UserName
Test
Go
Back
Login
Cancel

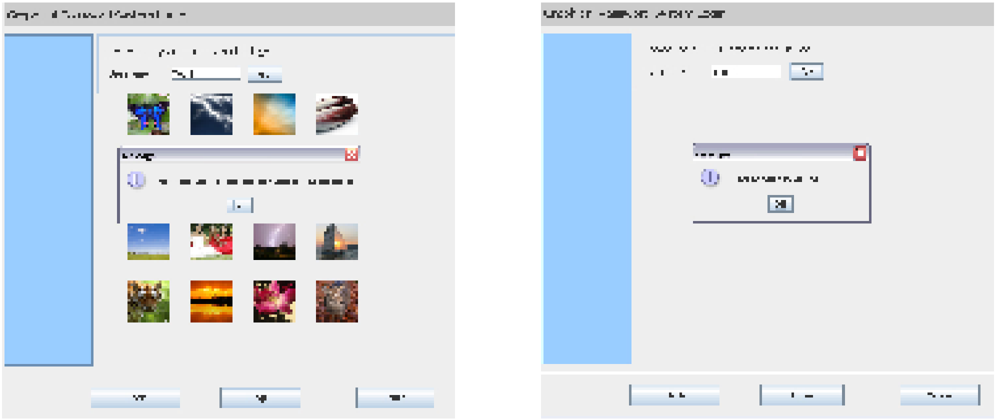
J_{new} secret password (in sequence)
$P_A(P_A(k) + P_B(N - |X| - k))$ decoy images from previous attempt
$P_B(N - |X| - (P_A(k) + P_B(N - |X| - k)))$ decoy images from the remaining sampling pool

Figure 6.20: Final Attempt and the Pictures Generated by the Proposed System

```
Get Min and Max password used for authentication
Retrieve passwords
Randomise the amount of password to be used

FOR i=0 to the amount of password to be used
      Uniform randomise the password image from the password set
      Add to the returnSet
END FOR

IF feedback feature enabled
Get Min and Max decoy reuse parameters (metaheuristic distribution)
Randomise the amount of reused decoy images based on metaheuristic
distribution
      FOR i=0 to the amount of reused decoy images
            Uniform random the password image from the previous set
            Add to the returnSet
      END FOR
END IF

allPass = CALL GetAllPasswords function

Calculate seed from day month and year and user
Rearrange allPass using uniform randomisation with the seed

FOR i = returnSet size till totalImage

      randNum = randomise a standard normal distribution num

      Calculate index from randNum
      Extract picture from allPass using index
      Add to the returnSet
END FOR
```

Figure 6.21: Pseudocode for the Proposed Falsifying Authentication Method (Partial Password Selection and Metaheuristic Randomisation Algorithm)

A block mechanism is implemented to limit the number of accesses. The block mechanism can increase the level of protection against password guessing attacks. A user is allowed three attempts to login into the proposed system. The Internet Protocol (IP) address and the Media Access Control (MAC) address of a computer are recorded if a user fails to be authenticated for login after three consecutive attempts, even though each attempt at login is done on different days. Once the IP and the MAC addresses have been recorded, the user can no longer gain access into the proposed system. The screenshot of the GUI, and the pseudocode for the block function are shown in Figure 6.22 and Figure 6.23, respectively.



(a) the user is informed that his account is blocked after the third trial

(b) the user can no longer access the proposed system

Figure 6.22: Block Function

```
IF login failed
      Increment total login attempts
       IF login attempts >= total permissible attempts
            Set account locked
       END IF
      Save total login attempts
END IF
```

Figure 6.23: Pseudocode for Block Function

6.3.2.2 System Flow for Verification Process

Figure 6.24 shows the system flow of the password verification process of the VIP Pro system. The system will first verify whether a user has been blocked by the system. If the user has been blocked, he/she cannot use the system to login. If the user has not been blocked, the system will verify the password pictures selected by the user. Once the user has confirmed the password, the IDs of the selected pictures are hashed and compared with the registered password in the database. If the user is successfully authenticated, a welcoming message will be displayed. If the user fails to be authenticated, he/she will be allowed another two attempts to be authenticated. If the users still fails to be authenticated after the third attempt, he/she will be blocked by the system.

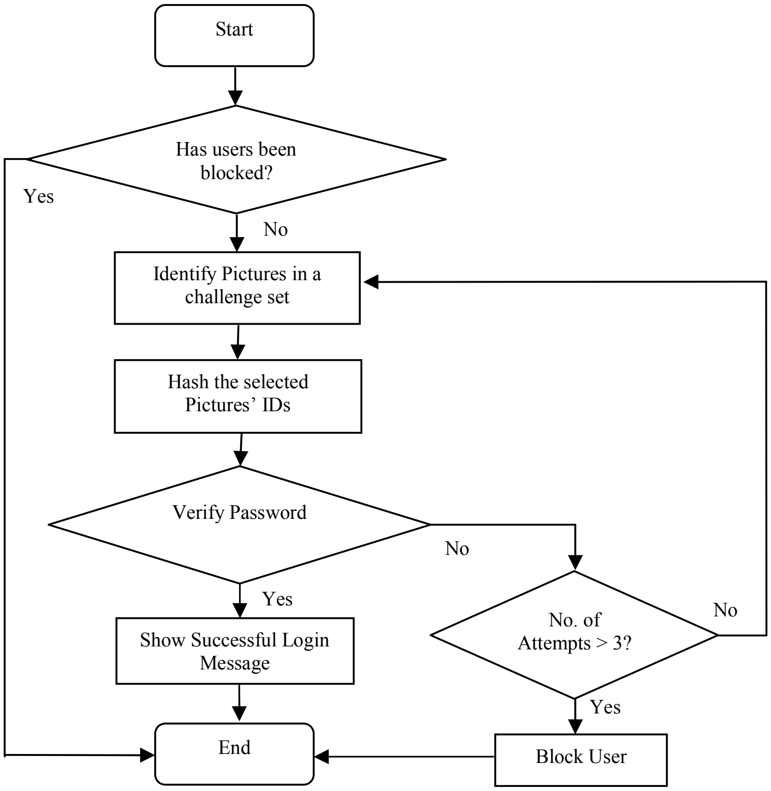

Start
Has users been blocked?
Yes
No
Identify Pictures in a challenge set
Hash the selected Pictures' IDs
Verify Password
No
Yes
Show Successful Login Message
No. of Attempts > 3?
No
Yes
End
Block User

Figure 6.24: System Flow of Verification Process

6.4 Database Design

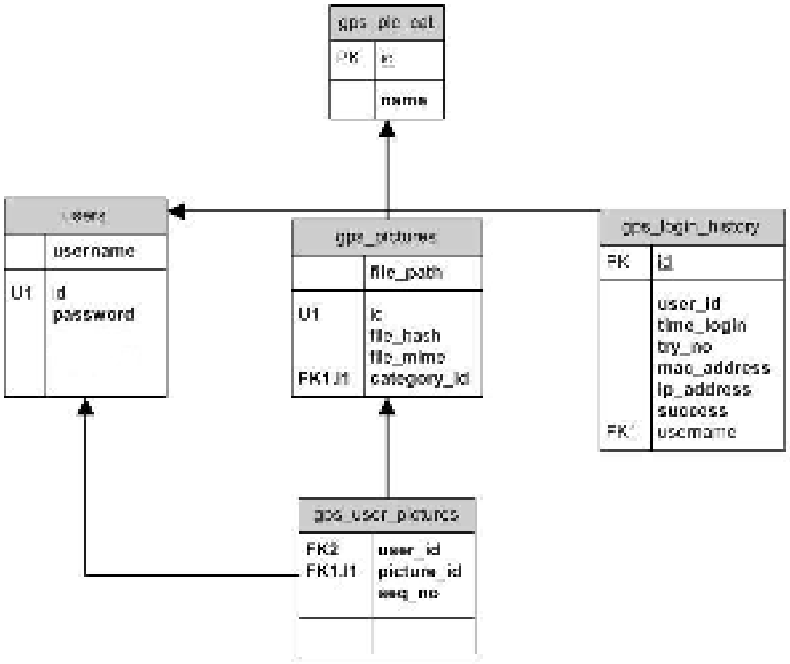


Figure 6.25: VIP Pro Relational Database Diagram

Table 6.1: VIP Pro Metadata

Table Name	Field Name	Data Type	NULL	Key	Description
gps_pic_cat	id	int(10) unsigned	NO	PRI	Unique identifier for the table
gps_pic_cat	name	varchar(45)	NO	-	Category name
gps_pictures	id	int(10) unsigned	NO	PRI	Unique identifier for the table
gps_pictures	file_path	varchar(255)	NO	-	Stores the path of each picture used
gps_pictures	category_id	int(10) unsigned	NO	-	Determines the category of each picture
users	id	int(10) unsigned	NO	PRI	Unique identifier for the table
users	username	varchar(45)	NO	UNI	Unique username defined by a user
users	password	varchar(45)	NO	-	User's password
gps_user_pictures	user_id	int(10) unsigned	NO	PRI	A match with the id field of the users' table
gps_user_pictures	picture_id	int(10) unsigned	NO	PRI	A match with the id field of the gps_pictures table
gps_user_pictures	seq_no	varchar(45)	NO	PRI	Stores information on the password sequence
gps_login_history	id	int(10) unsigned	NO	PRI	Unique identifier for the table
gps_login_history	user_id	int(10) unsigned	NO	-	Stores user's id
gps_login_history	time_login	datetime	NO	-	Stores the date when a user fails to login
gps_login_history	try_no	int(10) unsigned	NO	-	Number of failed attempts
gps_login_history	mac_address	varchar(45)	NO	-	Stores information on MAC address
gps_login_history	ip_address	varchar(45)	NO	-	Stores information on IP address
gps_login_history	success	tinyint(1)	NO	-	0: Indicates failure 1: Indicates success

Figure 6.25 and Table 6.1 show the metadata, and the relational database diagram for the VIP Pro system, respectively. There are five tables in the database – *gps_pic_cat*; *gps_pictures*; *users*; *gps_user_pictures*; and *gps_login_history* tables. The *gps_pic_cat* table is used to store information on the category of each picture used. There are two fields in the *gps_pic_cat* table – the *id* field and the *name* field. The *id* field is set as a unique identifier for the table, and the *name* field indicates the name of the category to which the pictures belong.

The *gps_pictures* table is used to store the details of the pictures. There are three fields in the *gps_pictures* table – *id*, *file_path*, and *category_id*. The *id* field is used as the primary key of the table. The *file_path* and the *category_id* fields are used to store the path, and the category of each picture, respectively.

The *users* table is used to store the login information of the user. The *users* table consists of the *id*, *username*, and *password* fields. The *id* field is used as the primary key of the *users* table. The user-defined username and the password are stored in the *username* and *password* fields, respectively.

The *gps_user_pictures* table is an intermediate reference table that is produced after the normalisation process. The *gps_user_pictures* table has three fields – *seq_no, user_id*, and *picture_id* fields. The *seq_no* field is used to store the password sequence information for each registered user. In order to identify a registered user, a referential integrity rule is applied. The *user_id* and *picture_id* fields are used as the foreign key for matching the *id* in both the *users* and the *gps_pictures* tables, respectively.

The *gps_ login_history* table is used to monitor and maintain the access rights of a user. There are seven fields in the *gps_login_history* table – *id*, *user_id*, *time_login*, *try_no*, *success*, *mac_address*, and *ip_address* fields. The *id* field is a unique identifier for the table. The *user_id*, *time_login,* and *try_no* fields are used to monitor the information of a user, the date, and the number of attempts that the user has made to access the system, respectively. If the user succeeds in gaining access to the system, the value “1” will be assigned to the *success* field, otherwise the value “0” will be assigned to the *success* field. If the value at the *try_no* field is 3, the MAC address and IP address of the user will be recorded in the *mac_address* and *ip_address* fields, respectively. Following this, the user who is associated with the recorded MAC address or IP address, will be blocked from accessing the system.

6.5 Summary

The VIP Pro system was presented in this chapter. The architecture of the VIP Pro system was discussed. The use case diagram of the system was presented and used to discuss the functional requirements of the system. The two main processes – the enrollment process, and the verification process – were then presented. The sub-functions of the enrollment process such as identify username and password, and register password were discussed in details. The second falsifying method that uses partial password selection and metaheuristic randomisation algorithm was presented in the verification process. The database design of the VIP Pro system was then presented. The next chapter presents the data analysis and testing of the all the proposed methods.

Chapter 7 Analysis and Testing

7.1 Introduction

This chapter discusses the analysis of the results of the case studies, using the proposed methods to mitigate shoulder-surfing attacks, and FOA attacks. It also discusses the use of the cued methods to improve users' memorability. Testing was conducted on all the methods developed, and the details on the testing on the BPG system, the enhanced BPG system, and the VIP Pro system, are presented, respectively. A chapter summary is presented in the last section.

7.2 Analysis and Testing of the BPG System

This section discusses the analysis and testing of the BPG system with respect to its use in improving users' memorability, and in mitigating shoulder-surfing attacks. The following four aspects of the BPG system were tested:

i. Shoulder-Surfing Mitigation

ii. Sensitive Area

iii. Colour Scheme

iv. Upload Background Picture Feature.

7.2.1 Shoulder-Surfing Mitigation

A case study was conducted to verify the capability of the first proposed falsifying authentication method that uses penup event and neighbouring connectivity manipulation in mitigating shoulder-surfing attack. To produce an approximately normal sampling distribution a sampling size of 30 or more is required to be used. Thus, this case study was carried out in the FCSIT, University of Malaya, Malaysia, and involved 100 participants. The participants were divided in groups of five, and instructed to perform shoulder-surfing attacks. The participants were also categorised into postgraduate and undergraduate students, as well as their gender. This was done to evaluate whether the competency level of the undergraduate and postgraduate students, as well as do their gender, could affect the results of the case study.

In the case study, 10 groups of postgraduate students comprising 5 male groups (Groups G1 - G5) and 5 female groups (Groups G6 - G10), respectively, were involved. Another 10 groups of undergraduate students were similarly assigned: 5 male groups (Groups G11 - G15); and 5 female groups (Groups G16 - G20). An authorised user with the login details: username: *testing2*; generated password encoding: {(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]) }, was also selected for the case study. Figure 7.1 shows the GUI for the password created from the above-mentioned password encoding.

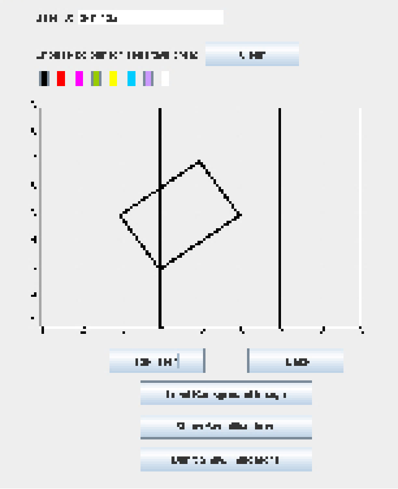


Figure 7.1: A Password Created from the Predefined Password Encoding

The participants were briefed on their role in the case study. They were also given a demonstration of the login process. Each shoulder-surfer group (attackers) was allowed three attempts to identify, discuss, and guess the password used by the user *testing2*.

Hints on the neighbouring connectivity, and penup event used, would only be given if the attackers failed to login at the first attempt.

To measure the percentage of password guessed correctly (password matching) by the attackers, an online approximate string pattern matching tool produced by Textolution (2009) was used. The tool was used because: i) it is free; ii) it has the required features such as percentage differences required for non-parametric analysis; and iii) it is able to perform approximate string pattern matching for the password encoding produced by the proposed system. The online tool provides 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 because the BPG encoding does not have any natural language element (the BPG encoding consists of only numbers and seven symbols: [ ] ( ) { } and ,). The use of approximate string matching algorithms, is beyond the scope of this research and will not be discussed further.

Figure 7.2 shows the percentage of password matching resulting from the attacks made by the shoulder-surfing attackers. It shows that none of the attackers were able to shoulder-surf and guess the password correctly, mainly because they were not able to identify and obtain the correct penup events, and the neighbouring connectivity among the indicators. Figure 7.3 shows several password encoding examples produced by the attackers.

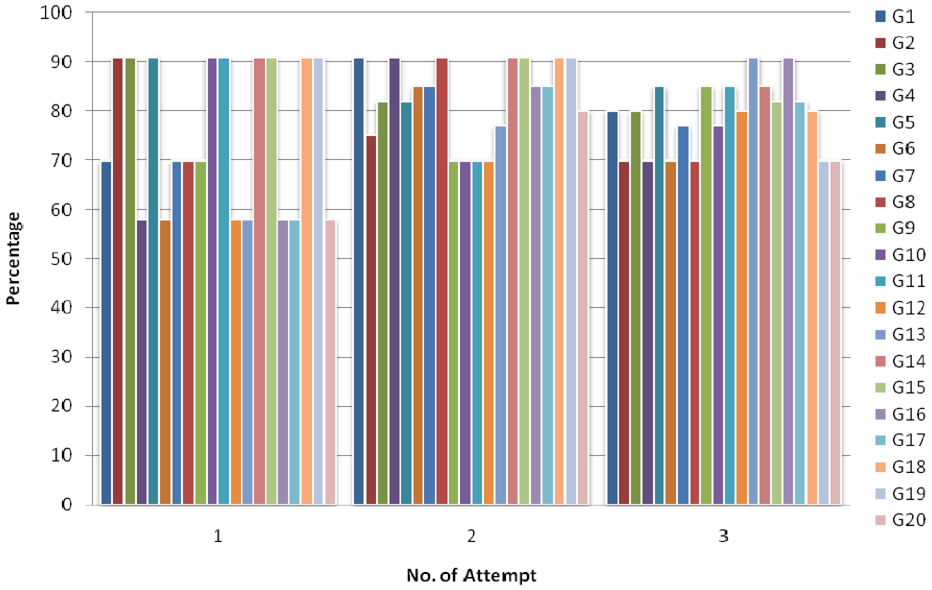


Figure 7.2: Percentage Password Matching Results

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])}

iii) 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])}

Figure 7.3: Incorrect Password Encoding Produced by the Attackers

During the demonstration of the login process, some tricks were used, such as: i) faking or pretending to create a penup event by holding the mouse click long enough before manoeuvring the mouse to another intersection point, and, ii) bypassing the nearest neighbour connectivity from one intersection point to another. These tricks increase the probability of the attackers in guessing the password incorrectly. The results showed that attackers with a higher competency level (postgraduate students) created more password patterns, when they were given hints on the penup event, and the nearest neighbour connectivity information. However, neither the postgraduate nor the undergraduate student participants were able to guess the correct password. Thus, the password encoding produced by the BPG system had been effective in misleading a shoulder-surfing attacker from identifying and guessing the password of an authorised user.

An in-depth analysis was made on the percentage match results generated by the SPSS tool to determine whether the participants' competency level or their gender can affect the results produced by the proposed method. The distribution graph of the percentage matches is a left-skewed graph (see Figure 7.4). Hence, a non-parametric test, such as Kruskal Wallis test or Mann Whitney test, would be more appropriate for the verification process.

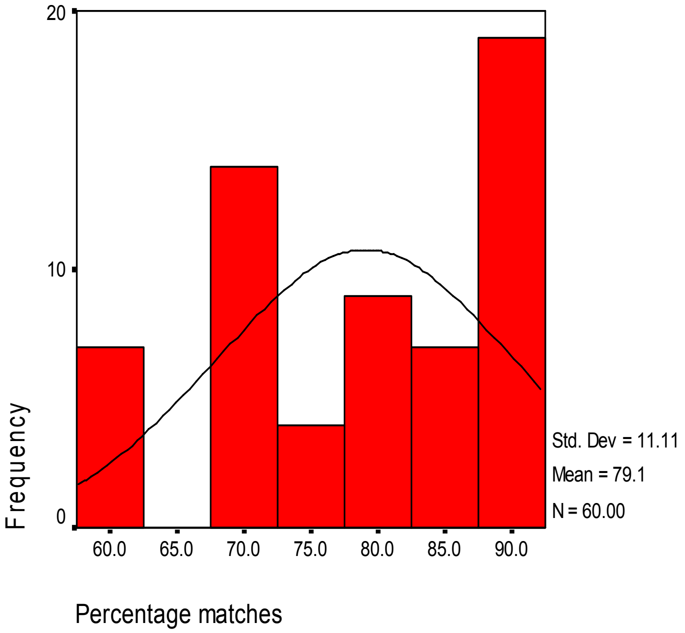


Figure 7.4: Distribution Testing Result

A Kruskal Wallis test was carried out and its corresponding hypothesis was formulated as follows:

H_o^1: $\tilde{x}_{G(postgraduate)} = \tilde{x}_{G(undergraduate)}$; $\tilde{x}$: median

(There is no difference in the median of percentage matches between the postgraduate student group and the undergraduate student group).

H_l^1: $\tilde{x}_{G(postgraduate)} \neq \tilde{x}_{G(undergraduate)}$

(There is a difference in the median of percentage matches between the postgraduate student group and the undergraduate student group).

Table 7.1 shows that the p-value of 0.347 is greater than 0.05. The result of the hypothesis test indicated not to reject H_o^1 at 5% significance level. This means that there is no difference in median percentage matches between the postgraduate student group and the undergraduate student group. This confirms that the BPG encoding algorithm has been effective in misleading shoulder-surfing attackers, regardless of their competency level, from identifying and guessing the correct password.

Table 7.1: Comparison of the Kruskal Wallis Test Results between the Prosgraduate Student Group and the Undergraduate Student Group

Ranks

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

Test Statistics(a,b)

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

a Kruskal Wallis Test
b Grouping Variable: Competency Level

In order to determine whether gender affects the results produced by the proposed method, the following hypotheses were formulated:

H_o^2: $\tilde{x}_{G(Male)} = \tilde{x}_{G(Female)}$

(There is no difference in the median percentage matches between the male group and the female group).

H_1^2: $\tilde{x}_{G(Male)} \neq \tilde{x}_{G(Female)}$

(There is a difference in the median percentage matches between the male group and the female group).

H_o^3: $\tilde{x}_{G(Postgraduate\_Male)} = \tilde{x}_{G(Postgraduate\_Female)}$

(There is no difference in the median percentage matches between the male postgraduate group and the female postgraduate group).

H_1^3: $\tilde{x}_{G(Postgraduate\_Male)} \neq \tilde{x}_{G(Postgraduate\_Female)}$

(There is a difference in the median percentage matches between the male postgraduate group and the female postgraduate group).

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

(There is no difference in the median percentage matches between the male undergraduate group and the female undergraduate group).

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

(There is a difference in the median of percentage matches between the male undergraduate group and the female undergraduate group).

Tables 7.2 - 7.4 show that the p-values (0.198, 0.187, 0.561) are greater than 0.05, i.e., the results of the hypothesis test indicated not to reject H_o^2, H_o^3, H_o^4 at 5% level of significance, respectively. Thus, the results of the above analyses indicated that there are no differences in median percentage matches among the two genders even within each postgraduate or undergraduate group. In general, the BPG encoding was effective in misleading shoulder-surfing attackers, regardless of their gender, from identifying and guessing the correct password.

Table 7.2: Comparison of the Kruskal Wallis Test Result Obtained by the Male and the Female Participants

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 7.3: Comparison of the Kruskal Wallis Test Result Obtained by the Male and the Female Participants (for 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 7.4: Comparison of the Kruskal Wallis Test Result Obtained by the Male and the Female Participants (for Undergraduate Students)

Ranks

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

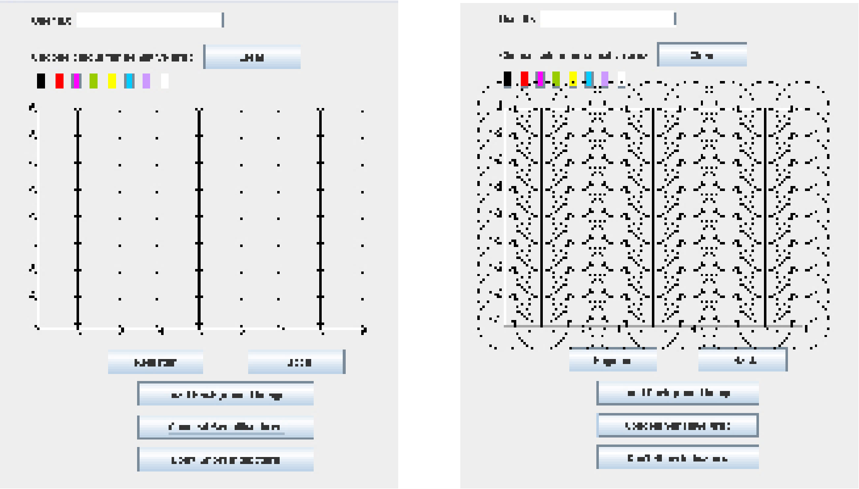
Test Statistics(a,b)

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

a Kruskal Wallis Test
b Grouping Variable: Gender

7.2.2 Sensitive Area

The shape and size of the sensitive areas in the BPG system must be predefined before an indicator can be created. A few factors have to be considered before identifying the size of the sensitive area for the BPG system. Undoubtedly, the larger the size of a sensitive area used, the easier it is for a user to select an intersection in the BPG system. However, clicking on the neighbouring intersections can become a problem if the pre-determined size of the sensitive area is relatively large. Figure 7.5 shows the implication of using a relatively small and a relatively larger sensitive area.



(a) Sensitive Area with Relatively Small Radius Size

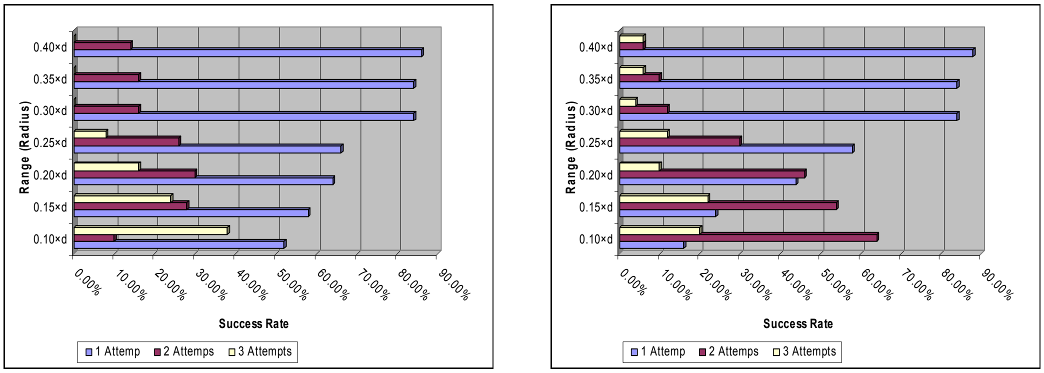
(b) Sensitive Area with Relatively Large Radius Size

Figure 7.5: Sensitive Area Design

It is therefore crucial to identify an optimal size for the sensitive area in the proposed system. In order to provide higher security protection against shoulder-surfing attack and to prevent a high number of invalid password input problems among registered users, round circle sensitive areas with a radius of 0.30×d (d is the side length of a grid cell) are implemented in the BPG system. The main reason for proposing a radius of 0.30×d is based on the result of the heuristic testing, and on the feedback from 250 survey participants, who were randomly selected from the FCSIT, University of

Malaya, Malaysia. The participants were briefed on the use of the BPG system, and were taught to create their password using radius of 0.10×d, 0.15×d, 0.20×d, 0.25×d, 0.30×d, 0.35×d and 0.40×d, with and without the assistance of the “show/hide indicators” function.

Figure 7.6 shows the statistics on the rate of success in accessing the system based on the trial results made by the participants, with and without the use of the “show/hide indicators” function. The results show that, a relatively high percentage of decline occurred in both approaches after the reduced range of radius 0.30×d. On the other hand, more than 80% of the respondents were able to access the BGP system using the radius of 0.30×d, 0.35×d, and 0.40×d, for both with and without the “show/hide indicators” function. However, the success rate in accessing the system, with and without the guidance of the “show/hide indicators” function, for radius 0.40×d, and 0.35×d is relatively small compared with that for radius 0.30×d. The success rate is approximately 2.38% and 7.14% higher when using radius of 0.40×d compared with radius of 0.30×d, using and without using the “show/hide indicators” function, respectively. However, there is no significant difference between the range of radius 0.35×d and radius 0.30×d when applying the “show/hide indicators” function. In order to enforce higher security protection against shoulder-surfing attack and with smaller sensitive area, and to achieve more than 80% success rate in accessing the system, a sensitive area range of radius 0.30×d was proposed for the BPG system. Figure 7.7 shows the sensitive area used in the proposed system.



(a) Successful Access Rate Using The Show Indicators Function

(b) Successful Access Rate Without Using The Show Indicators Function

Figure 7.6: Successful Access Rate Results

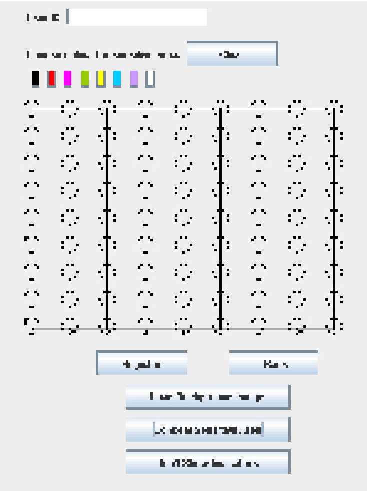


Figure 7.7: Proposed Sensitive Area with the Radius Size of 0.30×d

7.2.3 Colour Scheme

Colour is an important element of the Human Visual Sensory (HVS) system, as it is a significant factor not only in strengthening security, but also as a cue to help improve users' memorability (Tao & Adams, 2008). Therefore, a survey was conducted to identify the users' preferred colour scheme to be used in the BPG system. The survey instrument consists of a two-page questionnaire containing five questions (refer to Appendix B). These questions were formulated from interval data and nominal data types. The questionnaire was randomly distributed to 250 participants in the FCSIT, University of Malaya, Malaysia. Figure 7.8 shows the 40 colours used in the survey. Of the participants, 52% were female students, and 48% were male students. There were 12 males who were in the 25 - 34 years age group, while the rest of the male participants and all the female participants were in the 18 - 24 years age group. The survey results showed that all the participants were familiar with the colour scheme used. Following this, a completely new colour scheme was proposed for the BPG system based on the users' feedback on their most preferred colours. The new colour scheme was proposed in order to model and to enhance the Pass-Go system (benchmark system) to improve users' memorability. Figure 7.9 shows the number of participants who chose each colour, as their preferred colour, while Table 7.5 lists the top 10 most preferred colours. The eight most preferred colours identified from the survey results, were used in the BPG system. Only the top eight colours were selected because there is a significant difference in the number of survey participants who chose the 8th highest preferred colour (71.6% of participants) and those who chose the 9th highest preferred colour (57.6% of participants). This indicated that the 9th highest preferred colour was not a popular colour among the participants, generally.

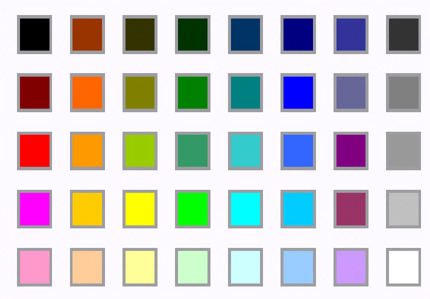


Figure 7.8: Colour Scheme Adopted from Microsoft Office Word 2003

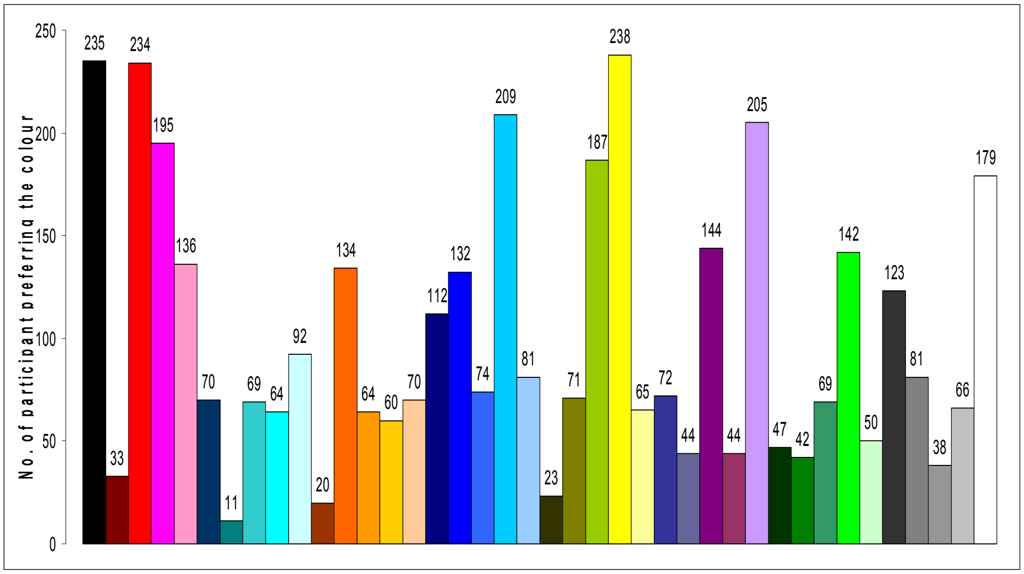


Figure 7.9: Survey Result on Colour Usage

Table 7.5: Top 10 Preferred Colours

Colour	RGB values	Percentage (%) of participants preferring the colour
🟨	[255,255,0]	95.2
⬜	[0,0,0]	94.0
🟥	[255,0,0]	93.6
🟦	[0,204,255]	83.6
🟪	[204,153,255]	82.0
🟪	[255,0,255]	78.0
🟩	[153,204,0]	74.8
⬛	[255,255,255]	71.6
🟪	[128,0,128]	57.6
🟩	[0,255,0]	56.8

7.2.4 Upload Background Picture Feature

A survey was conducted to determine whether the proposed upload background picture function can help the users in memorising their password. The survey instrument is a three-page hybrid-format questionnaire that contains seven questions (refer to Appendix C). The questionnaire contains both fixed-format questions and free-format questions. There are two data types – nominal data and ordinal data. In this particular case, an ordinal data type was used in the questionnaire to determine the usability of the upload background picture feature. To produce an approximately normal sampling distribution, the survey involved 30 participants who were randomly identified from among the students of the FCSIT, University of Malaya, Malaysia. The participants answered the questionnaire using a five-point scale (from ‘strongly disagree’ to ‘strongly agree’). The survey results were cross-tabulated using the SPSS (Statistical Package for the Social Sciences) software. The results showed that all the participants responded positively (agreed) that the upload background picture feature works as a cue to help users in memorising their password (refer to Table 7.6). The results also showed that 66.7% of the respondents strongly agreed that the upload background picture feature aided them in memorising their password. To verify whether knowledge (literacy) of the picture-based password authentication has any statistical significance with the proposed upload background picture feature, a Chi-Square test was conducted. The survey results showed that 90% of the participants reported that they have knowledge of picture-based password authentication (refer to Figure 7.10). However, the Chi-Square test result indicated that the p-value of 0.197 is greater than 0.05 (refer to Table 7.7). Therefore, both variables, Q1 and Q2, are not statistically significant. It means that the proposed upload background picture feature can aid users in memorising their password even though the users do not have knowledge about picture-based password authentication.

Table 7.6: Results of Cross-Tabulation of the Responses to Q1 and Q2

			Q1		Total
			Agree	Strongly Agree	
Q2	1 Yes	% within Q2	29.6%	70.4%	100.0%
	2 No	% within Q2	66.7%	33.3%	100.0%
Total		% without Q2	33.3%	66.7%	100.0%

Q1: Do you agree that superimposing a background picture onto the BPG system can aid users in memorising their password?

Q2: Do you know what picture-based password authentication is?

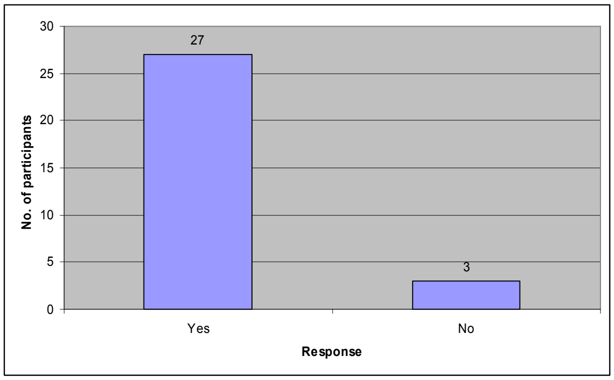


Figure 7.10: Survey on Participants’ Knowledge of Picture-based Password Authentication

Table 7.7: Chi-Square Test for Q1 and Q2

	Value	df	Asymp. Sig. (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	1.667	1	.197		
Continuity Correction(a)	.417	1	.519		
Likelihood Ratio	1.556	1	.212		
Fisher's Exact Test				.251	.251
Linear-by-Linear Association	1.611	1	.204		
N of Valid Cases	30				

7.3 Analysis and Testing of the Enhanced BPG System

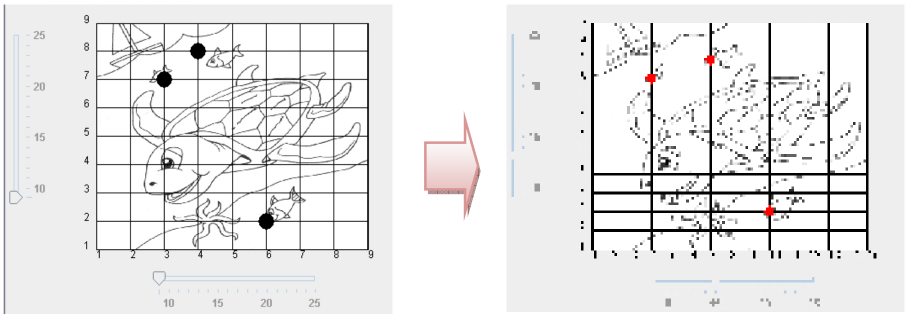
This section discusses the analysis and testing of the enhanced BPG system with respect to the method used to improve memorability. The testing was only conducted on the following additional features of the enhanced system:

i. Grid Line Scaling Feature, and

ii. Loose Authentication Feature.

7.3.1 Grid Line Scaling Feature

The grid line scaling feature was designed to increase the usability of the enhanced BPG system. The users can use the grid line scaling feature to identify more preferred points to be used as their password. A survey was conducted to determine whether the grid line scaling feature is able to improve the users’ memorability. The survey instrument is a three-page hybrid-format questionnaire, which contains seven questions (refer to Appendix C). The questionnaire consists of both fixed-format questions and free-format questions. There are two data types – nominal data and ordinal data. In this particular case, an ordinal data type was used in the questionnaire to determine the usability of the grid line scaling feature. The participants answered the questionnaire using a five-point scale (from ‘strongly disagree’ to ‘strongly agree’). The survey involved 30 participants who were randomly identified from among the students of the FCSIT, University of Malaya, Malaysia. The participants comprised 15 undergraduate students and 15 postgraduate students. The participants were given a demonstration on the use of the grid line scaling function before answering the questionnaire. Figure 7.11 shows an example of a password drawn during the demonstration.



Chosen points (eyes of the fishes) cannot be identified using the grid line scaling function

Figure 7.11: Example of an Enhanced BPG Password

The survey result showed that a majority of the participants (93.3%) agreed that the grid line scaling function is able to aid users in memorising their password. Two postgraduate students were non-committal in their responses. i.e., they neither agreed nor disagreed. They stated that the grid line scaling function is user-friendly, but are uncertain whether this feature is able to aid the users in memorising their password.

They believed that the users still need to memorise the correct grid line scales for both vertical and horizontal sites when creating their passwords.

A Chi-Square test was conducted to determine whether there is any association between the upload background picture feature and the grid line scaling feature. The test result, as shown in Table 7.8, shows that the p-value of 0.115 is greater than 0.05. Therefore, variable Q3 and variable Q4 are independent of each other, and they are not statistically significant. It means that the upload background picture feature and the grid line scaling function do not have any influence on each other when they are used to help users in memorising their password.

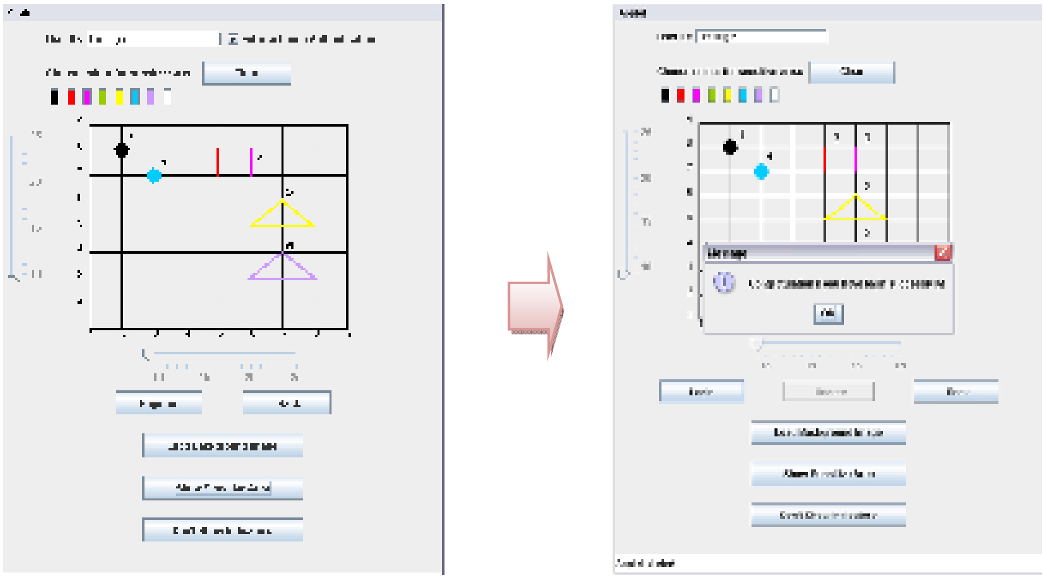
Table 7.8: Chi-Square Test for Q3 and Q4

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	4.320	2	.115
Likelihood Ratio	4.724	2	.094
Linear-by-Linear Association	3.302	1	.069
N of Valid Cases	30		

Q3: Do you agree that the "grid line scaling" function used in the enhanced BPG system is able to aid users in memorising their password?
Q4: Do you agree that superimposing a background image onto the enhanced BPG system can aid users in memorising their password?

7.3.2 Loose Authentication Feature

The purpose of implementing the loose authentication feature is to aid the users in memorising their password. A survey was conducted to evaluate the effectiveness of this feature. The survey instrument is a three-page hybrid-format questionnaire, which contains seven questions (refer to Appendix C). The questionnaire consists of both fixed-format questions and free-format questions. There are two data types – nominal data and ordinal data. In this particular case, an ordinal data type was used in the questionnaire to determine the usability of the loose authentication feature. The survey involved 30 participants comprising 15 undergraduate students and 15 postgraduate students, who were randomly identified from among the students of the FCSIT, University of Malaya, Malaysia. The participants were given a demonstration on the use of the loose authentication function. The participants answered the questionnaire using a five-point scale (from ‘strongly disagree’ to ‘strongly agree’) to evaluate the usability of the loose authentication feature. Figure 7.12 shows an example of a password drawn during the demonstration.



Original Password Sequence:
black dot indicator, blue dot indicator, red line indicator, pink line indicator, yellow triangle line indicator, purple triangle line indicator

Loose Authentication Password Sequence:
black dot indicator, red line indicator, pink line indicator, yellow triangle line indicator, purple triangle line indicator, blue dot indicator

Generated Password Encoding:
(2,8,[0,0,0])(3,7,[0,204,255]){(5,8,[255,0,0])(5,7,[255,0,0])}{(6,8,[255,0,255])(6,7,[255,0,255])}{(6,6,[255,255,0])(5,5,[255,255,0])(6,5,[255,255,0])(7,5,[255,255,0])(6,6,[255,255,0])}{(6,4,[204,153,255])(5,3,[204,153,255])(6,3,[204,153,255])(7,3,[204,153,255])(6,4,[204,153,255])}

Password Before Hashing:
(2,8,[0,0,0]),{(5,8,[255,0,0])(5,7,[255,0,0])},{(6,8,[255,0,255])(6,7,[255,0,255])},{(6,6,[255,255,0])(5,5,[255,255,0])(6,5,[255,255,0])(7,5,[255,255,0])(6,6,[255,255,0])},{(6,4,[204,153,255])(5,3,[204,153,255])(6,3,[204,153,255])(7,3,[204,153,255])(6,4,[204,153,255])},(3,7,[0,204,255])

Figure 7.12: Loose Authentication Demonstration

The survey result showed that a majority of the participants (86.7%) agreed that the loose authentication function is able to aid users in memorising their password. Four participants (two undergraduate students and two postgraduate students) were non-committal in their responses, i.e., they neither agreed nor disagreed. They stated that the loose authentication function provides an alternative way to memorise their password, but they were uncertain whether it is able to aid the users in memorising their password. They believed that the users still need to memorise their passwords before they can make use of the loose authentication function.

A Chi-Square test was conducted to determine whether there is any association between the upload background picture feature and the loose authentication function. The test result, shown in Table 7.9, shows that the p-value of 0.134 is greater than 0.05. Therefore, variable Q5 and variable Q6 are independent of each other, and they are not statistically significant. This means that the upload background picture feature and the loose authentication function do not have any influence on each other when they are used to help users in memorising their password.

Table 7.9: Chi-Square Test for Q5 and Q6

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	4.018	2	.134
Likelihood Ratio	3.868	2	.145
Linear-by-Linear Association	3.295	1	.069
N of Valid Cases	30		

Q5: Do you agree that the loose authentication function used in the enhanced BPG system is able to aid users in memorising their password?
Q6: Do you agree that superimposing a background image onto the enhanced BPG system can aid users in memorising their password?

Another Chi-Square test was conducted to determine whether there is any association between the grid line scaling function and the loose authentication function. The test result, shown in Table 7.10, indicates that the variables, mentioned above, are not statistically significant of each other because the p-value of 0.807 is greater than 0.05.

This means that the grid line scaling function and the loose authentication function do not have any influence on each other when they are used to help users in memorising their password.

Table 7.10: Chi-Square Test for Q7 and Q8

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	1.612	4	.807
Likelihood Ratio	2.193	4	.700
Linear-by-Linear Association	.094	1	.759
N of Valid Cases	30		

Q7: Do you agree that the loose authentication function used in the enhanced BPG system is able to aid users in memorising their password?
Q8: Do you agree that the "Grid Line Scaling" function used in the enhanced BPG system is able to aid users in memorising their password?

7.4 Analysis and Testing of the VIP Pro System

This section discusses the analysis and testing of the VIP Pro system in terms of the methods used: to improve memorability; to prevent FOA attack; and to mitigate shoulder-surfing attack. The following aspects of VIP Pro were tested:

i. $|X|$ Password Interval

ii. $|J|$ Partial Password Interval

iii. Metaheuristic Randomisation Algorithm (MRA) Distribution Range

iv. Mitigate Shoulder-Surfing

v. Chronological Story-Based Cued Recall Technique.

7.4.1 $|X|$ Password Interval

The $|X|$ significant interval of the proposed algorithm is tested to determine the number of selection of the secret password pictures used in the VIP Pro system. Permutation is used to calculate the total number of secret password pictures selection using the following formula: $\left[({}^{N}P_{x}) \sum_{j=4}^{x} ({}^{x}P_{j}) \frac{16!}{(16-j)!} \right]^{-1}$ (4)

Figure 7.13 shows a graph of the |*X*| password interval analysis. The graph shows that the proposed method requires a user to register eight pictures as his/her password in order to achieve a higher number of selection result when compared with the VIP3 system (benchmark system). Thus, to obtain a better outcome from a password guessing attack, the significant interval of |*X*| within 8 to 16 was identified.

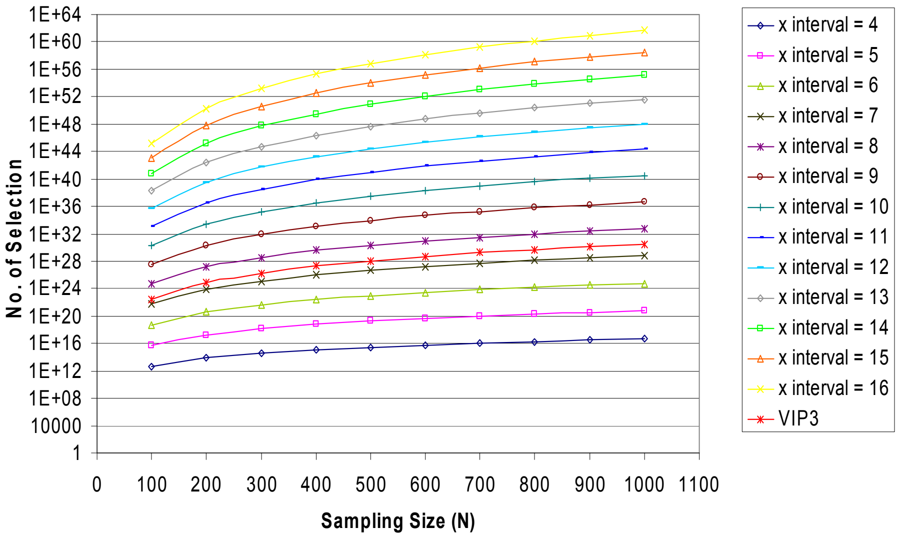


Figure 7.13: Empirical Analysis of the |*X*| Password Interval

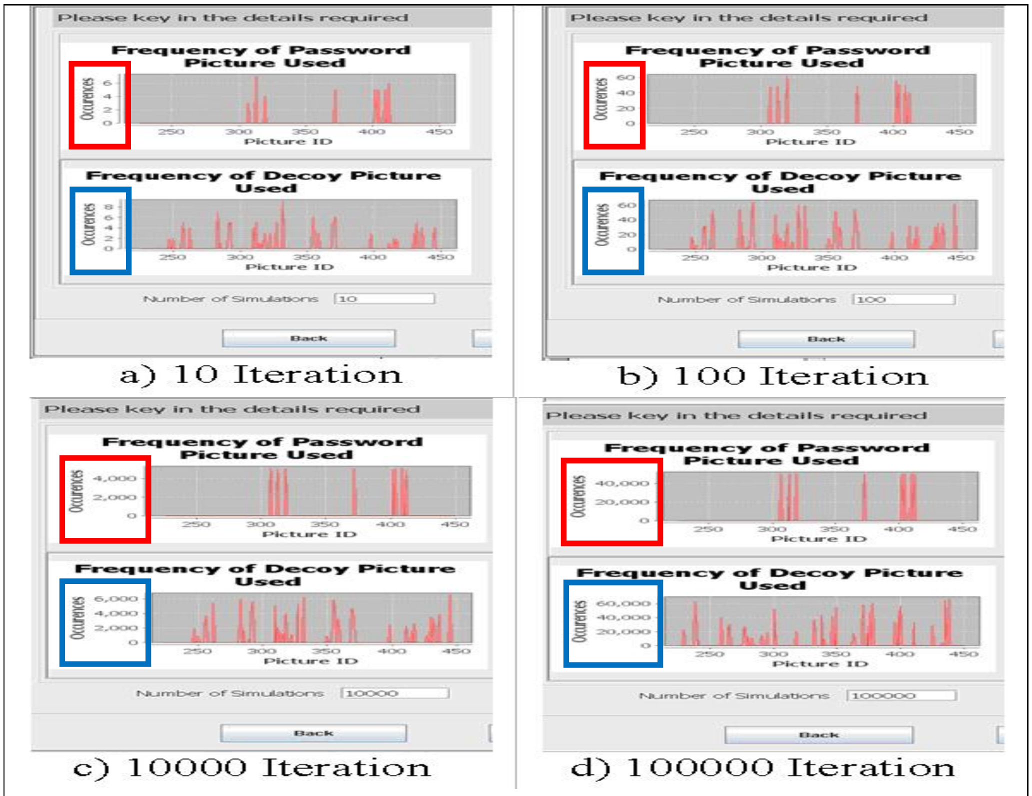
7.4.2 |*J*| Partial Password Interval

To determine the metaheuristic interval used in the proposed method, the relationship between the |*J*| secret password pictures and the MRA interval was listed and analysed (refer to Table 7.11). Let $R_i^{j_{n..m}}$ denotes the generic MRA interval for the proposed system, where *n* and *m* is the minimum and maximum number of partial passwords used during authentication, respectively. R_i is the reused decoy pictures interval with $i \in \boldsymbol{N_0}$. Table 7.11 shows that the first and the last distributions are not suitable to be used because they are highly vulnerable to shoulder-surfing and guessing attacks, and the decoy pictures generated from the previous attempt will either all be selected or none of them will be selected.

Table 7.11: MRA Interval with Minimum and Maximum *j*=4

Range	**Probability Distribution**	**Reused Frequency**
$R_0^{j_{4..4}}$	0.00	0
$R_1^{j_{4..4}}$	0.01-0.16	1
$R_2^{j_{4..4}}$	0.17-0.24	2
$R_3^{j_{4..4}}$	0.25-0.33	3
$R_4^{j_{4..4}}$	0.34-0.41	4
$R_5^{j_{4..4}}$	0.42-0.49	5
$R_6^{j_{4..4}}$	0.50-0.58	6
$R_7^{j_{4..4}}$	0.59-0.66	7
$R_8^{j_{4..4}}$	0.67-0.74	8
$R_9^{j_{4..4}}$	0.75-0.83	9
$R_{10}^{j_{4..4}}$	0.84-0.91	10
$R_{11}^{j_{4..4}}$	0.92-0.99	11
$R_{12}^{j_{4..4}}$	1.00	12

Figure 7.14 shows an example of the offline FOA simulation attack for $R_1^{j_{4..4}}$. The figure shows that, the password pictures used cannot be obtained based on highest frequency of occurrence after implementing the proposed method. This proves that the reused decoy picture concept is more effective, when compared with the VIP3 system, in preventing offline FOA attack.



a) 10 Iteration

b) 100 Iteration

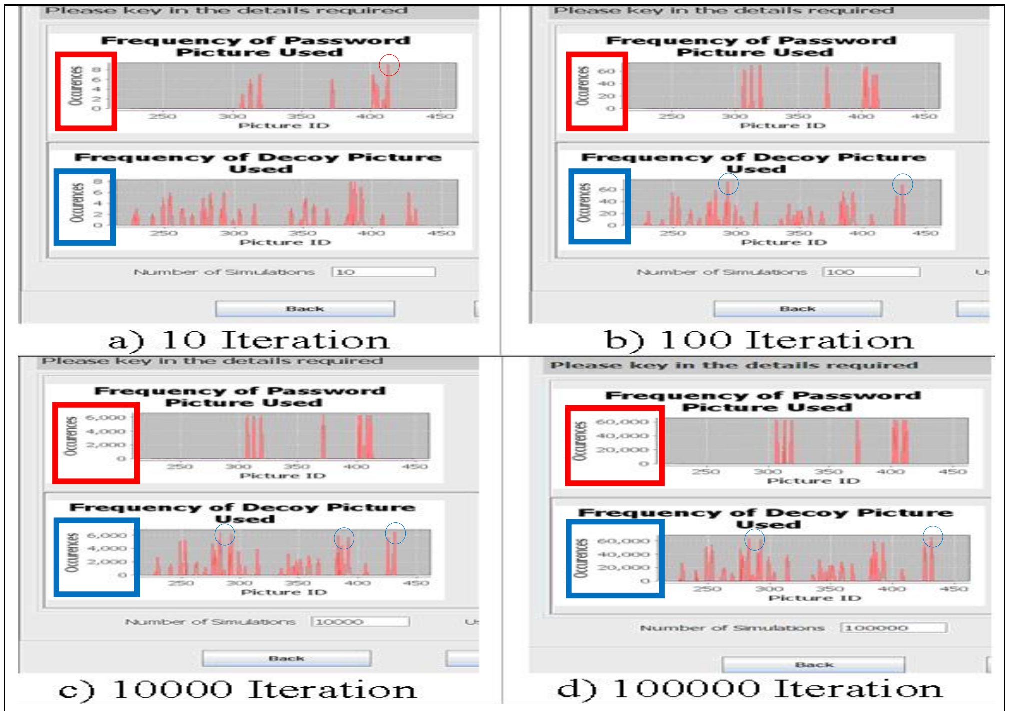
c) 10000 Iteration

d) 100000 Iteration

The password pictures used cannot be obtained based on highest frequency of occurrence although the number of iteration has increased from 10 until 100000.

Figure 7.14: Analysis and Observation Result for $R_1^{j_{4..4}}$

Testing was then carried out for the other i values for $R_i^{j_{4..4}}$. The test results showed that the value of i which is within the interval of 1 to 11 is significantly more robust against FOA attack (refer to Appendix D for the offline FOA simulation results). To improve the fixed number of secret password selection, the upper value for j was increased. The simulation result showed that, although the maximum number of secret password pictures used for an authentication has been increased to 5, the proposed method was still able to produce positive results for the following intervals: $R_i^{j_{4..5}}$, $i = \{1, 2, 3, 4, 5, 6, 7, 8, 9 \text{ and } 10\}$. However, when the maximum value of j was increased to 6, the simulation results were no longer significant to prevent FOA attack (refer to Figure 7.15). Thus, the significant interval of J which is within the domain of $4 \leq |J| \leq 5$ was identified (other offline FOA simulation results are available in Appendix D).



One of the password pictures has higher frequency of occurrence compared with the decoy pictures in 10 iteration simulations (circled in red). Only a few decoy pictures have higher frequency of occurrence compared with the password pictures in 100, 10,000, and 100,000 iteration simulations (circled in blue). Therefore, it is predictable that the password used can be obtained based on the highest frequency of occurrence when the number of iterations increases beyond 100,000 iterations.

Figure 7.15: Analysis and Observation Result for $R_1^{j_{4.6}}$

7.4.3 MRA Distribution Range

After determining the significant interval of *J*, a heuristic approach is used to fine-tune the MRA interval to strengthen the proposed method. In the heuristic approach testing, all the significant R_i intervals were grouped. The lower bound MRA range was tested to determine if the testing result shows that the FOA attack was prevented. The upper bound value was then tested and determined using the same method (refer to Table 7.12).

Table 7.12: MRA Interval Classification

Classification 1	**Classification 2**	**Classification 3**	**Classification 4**
$\overset{j4..5}{R_1}$, $\overset{j4..5}{R_2}$, $\overset{j4..5}{R_3}$, $\overset{j4..5}{R_4}$, $\overset{j4..5}{R_5}$, $\overset{j4..5}{R_6}$, $\overset{j4..5}{R_7}$, $\overset{j4..5}{R_8}$, $\overset{j4..5}{R_9}$, $\overset{j4..5}{R_{10}}$	$\overset{j4..5}{R_2}$, $\overset{j4..5}{R_3}$, $\overset{j4..5}{R_4}$, $\overset{j4..5}{R_5}$, $\overset{j4..5}{R_6}$, $\overset{j4..5}{R_7}$, $\overset{j4..5}{R_8}$, $\overset{j4..5}{R_9}$, $\overset{j4..5}{R_{10}}$	$\overset{j4..5}{R_3}$, $\overset{j4..5}{R_4}$, $\overset{j4..5}{R_5}$, $\overset{j4..5}{R_6}$, $\overset{j4..5}{R_7}$, $\overset{j4..5}{R_8}$, $\overset{j4..5}{R_9}$, $\overset{j4..5}{R_{10}}$	$\overset{j4..5}{R_4}$, $\overset{j4..5}{R_5}$, $\overset{j4..5}{R_6}$, $\overset{j4..5}{R_7}$, $\overset{j4..5}{R_8}$, $\overset{j4..5}{R_9}$, $\overset{j4..5}{R_{10}}$
Classification 5	**Classification 6**	**Classification 7**	**Classification 8**
$\overset{j4..5}{R_4}$, $\overset{j4..5}{R_5}$, $\overset{j4..5}{R_6}$, $\overset{j4..5}{R_7}$, $\overset{j4..5}{R_8}$, $\overset{j4..5}{R_9}$	$\overset{j4..5}{R_4}$, $\overset{j4..5}{R_5}$, $\overset{j4..5}{R_6}$, $\overset{j4..5}{R_7}$, $\overset{j4..5}{R_8}$	$\overset{j4..5}{R_4}$, $\overset{j4..5}{R_5}$, $\overset{j4..5}{R_6}$, $\overset{j4..5}{R_7}$	$\overset{j4..5}{R_4}$, $\overset{j4..5}{R_5}$, $\overset{j4..5}{R_6}$

Analysis of the FOA simulation showed that the distribution ranges that have been assigned to the classification number 1, 2, 3 and 8 were not suitable to be used because the secret password pictures used can be obtained based on the highest frequency of occurrence in the lower iteration simulation. On the other hand, the classification numbers 4, 5, 6, and 7 can produce significant results with the respective distribution range. However, to prevent the proposed method from generating a large number of reused decoy pictures, the significant upper bound MRA distribution range, which is equal to $\overset{j_{4..5}}{R_7}$ was identified. (The more decoy pictures produced, the easier it will be for a password-guessing attacker to eliminate the unused decoy pictures at each authentication attempt.) Thus, the lower bound and upper bound of the MRA distribution range for the proposed system was identified as $\overset{j_{4..5}}{R_4}$ and $\overset{j_{4..5}}{R_7}$, respectively (refer to Table 7.13). The offline FOA simulation results are available in Appendix E.

Table 7.13: MRA Interval with Minimum *j*=4 and Maximum *j*=5

Range	Probability Distribution	Min Reused Frequency	Max Reused Frequency
$R_0^{j_{4..5}}$	0.00	0	0
$R_1^{j_{4..5}}$	0.01-0.18	1	2
$R_2^{j_{4..5}}$	0.19-0.27	2	3
$R_3^{j_{4..5}}$	0.28-0.36	3	4
$R_4^{j_{4..5}}$	0.37-0.45	4	5
$R_5^{j_{4..5}}$	0.46-0.55	5	6
$R_6^{j_{4..5}}$	0.56-0.63	6	7
$R_7^{j_{4..5}}$	0.64-0.72	7	8
$R_8^{j_{4..5}}$	0.73-0.81	8	9
$R_9^{j_{4..5}}$	0.82-0.90	9	10
$R_{10}^{j_{4..5}}$	0.91-0.99	10	11
$R_{11}^{j_{4..5}}$	1.00	11	12

7.4.4 Mitigate Shoulder-Surfing Testing

Figure 7.16 shows the population pyramid graph generated from the testing results. In order to test and verify whether the proposed method is able to mitigate shoulder-surfing attack, 73 participants were randomly identified to perform shoulder-surfing attacks. The participants were categorised into expert, normal, and control groups. To ensure that the participants have knowledge of the shoulder-surfing attack, and the skill to perform a shoulder-surfing attack, 30 of the participants who had taken the computer security subject or are conducting computer security research in the FCSIT, University of Malaya, Malaysia, were randomly identified and categorised under the expert group. Another 38 participants who were categorised under the normal group were members of the public who were randomly identified from among the visitors of the Seoul International Invention Fair, held in Korea. The control group comprised five undergraduate students who were randomly identified from among the undergraduate students in the FCSIT, University of Malaya, Malaysia. It was assumed they have the knowledge, and the skill level between those in the expert group and those in the normal group.

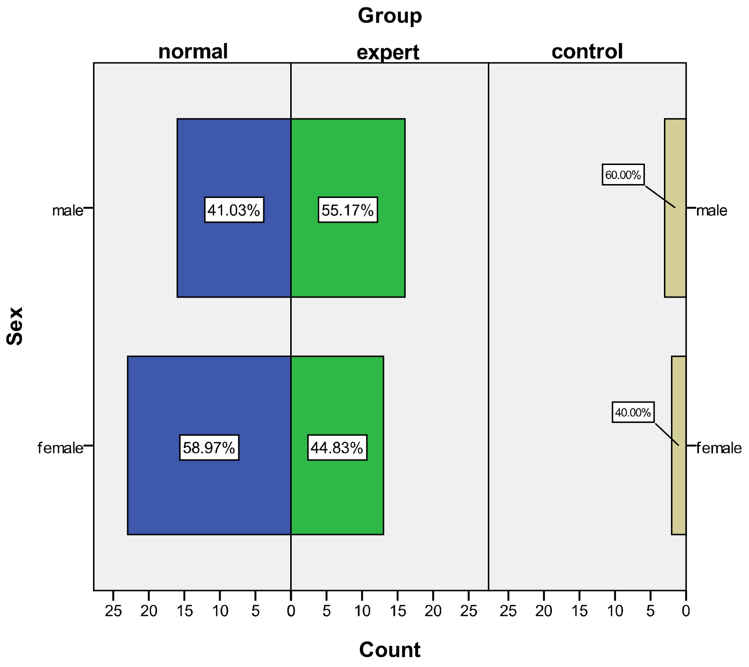


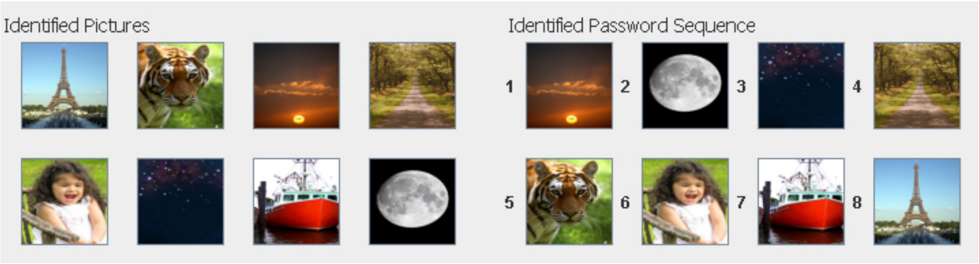
Figure 7.16: Population Pyramid Graph

The role of the attacker was explained to all participants, assigned as attackers, before they began the attack. They also witnessed a demonstration of the login process. Each shoulder-surfing attacker was allowed three consecutive attempts to guess the authorised user's password. The attackers' accounts were blocked if they failed to be authenticated after the third attempt.

The test result showed that all the shoulder-surfing attackers failed to guess the authorised user's password correctly. An interview was conducted with each shoulder-surfing attacker regarding their choice of the password picture when guessing the authorised password. The interview results showed that most of the shoulder-surfing attackers were confused when they could only identify several selected password pictures in the challenge set. As a result, most of the pictures they selected were based on what they remembered, for example: the positions of the secret password pictures used in the demonstration set (using key logging attack concept); redundant pictures that were generated in the previous attempt (FOA attack); new pictures that were generated in the current challenge set; and similarity concept of the password pictures used such as colour, shape and category. Thus, the outcome of the shoulder-surfing simulated attacks provides evidence that the proposed falsifying authentication method (partial password selection and metaheuristic randomisation algorithm) used in the VIP Pro system is able to mitigate shoulder-surfing attack, regardless of the competency level and gender of the attackers.

7.4.5 Chronological Story-Based Cued Recall Technique

A survey was conducted to verify the effectiveness of the chronological story-based cued recall technique used in the VIP Pro system to aid users in memorising their password. The survey instrument is a two-page hybrid-format questionnaire, which contains five questions (refer to Appendix C). The questionnaire consists of both fixed-format questions and free-format questions. There are two data types – nominal data and ordinal data. The survey involved 32 participants, who were randomly identified from among the student population of the FCSIT, University of Malaya, Malaysia. The participants were briefed on how to login to the VIP Pro system. They were also taught to create a chronological story-based password by using another set of password. An example of a password with its accompanying story is shown in Figure 7.17. Following the briefing, the participants were required to login using the method taught to them.



Story: One day sunset before moon and stars arise in the sky, besides the rain forest there is a tiger! A baby girl shouted loudly and she wanted to take the red boat back to Paris.

Figure 7.17: A Sample Story

An ordinal data type was used in the questionnaire to determine the usability of the chronological story-based cued recall technique. The participants answered the questionnaire using a five-point scale (from ‘strongly disagree’ to ‘strongly agree’). The result of the cross-tabulation of Q9 and Q10 is shown in Table 7.14. The result shows that: 31.3% of the participants who had not previously used the chronological story-based cued recall technique had difficulty in memorising the password; 93.8% of the respondents strongly agreed that the chronological story-based cued recall technique aided them in memorising their password. However, only two respondents agreed on the benefits of the technique, but they believed there are other methods which are more effective. Unfortunately, they did not provide information on the other methods.

Table 7.14: Cross-Tabulation of Q9 and Q10

			Q10		Total
			Agree	Strongly Agree	
Q9	No	% with Q10	6.3%	25.0%	31.3%
	Yes	% with Q10	.0%	68.8%	68.8%
Total		% with Q10	6.3%	93.8%	100.0%

Q9: Did you have any difficulty in memorising the password that you have chosen prior to using the Chronological Story-Based Cued Recall Technique in the VIP Pro system?
Q10: Do you agree that the Chronological Story-Based Cued Recall Technique used in the VIP Pro system can help users in memorising their password?

The result of the Chi-Square test (see Table 7.15) indicates that the p-value of 0.030 is less than 0.05. Therefore, both variables Q9 and Q10 are dependent on each other and they are statistically significant to each other. In other words, the participants are able to memorise their password better if they have prior experience in using the chronological story-based cued recall technique.

Table 7.15: Chi-Square Test for Q9 and Q10

	Value	Df	Asymp. Sig. (2-sided)
Pearson Chi-Square	4.693(b)	1	.030
Continuity Correction(a)	1.901	1	.168
Likelihood Ratio	4.955	1	.026
N of Valid Cases	32		

7.5 Summary

This chapter discusses the analysis and testing of the proposed features in the BPG system, enhanced BPG system, and the VIP Pro system, respectively. Four aspects of the BPG system, which include shoulder-surfing testing, sensitive area testing, colour scheme testing, and upload background picture feature testing, were tested and analysed. For the enhanced BPG system, the grid line scaling function and the loose authentication function were tested and analysed. The $|X|$ password interval testing, $|J|$ partial password interval testing, MRA distribution range testing, shoulder-surfing testing, and chronological story-based cued recall technique testing were carried out and analysed for the VIP Pro system. In general, both proposed falsifying authentication methods (i.e., penup event and neighbouring connectivity, and partial password selection and metaheuristic randomisation algorithm) are capable of mitigating shoulder-surfing attack regardless of the competency levels and gender of the shoulder-surfing attackers. The proposed MRA that uses the concept of re-using the previous distracter pictures is able to prevent FOA attack. From the aspect of user memorability, a majority of the survey participants agreed and believed that proposed cued recall methods – the upload background picture feature; grid line scaling function; loose authentication function; and chronological story-based cued recall technique – can aid users in memorising their password. The next chapter presents the results and conclusion of this study.

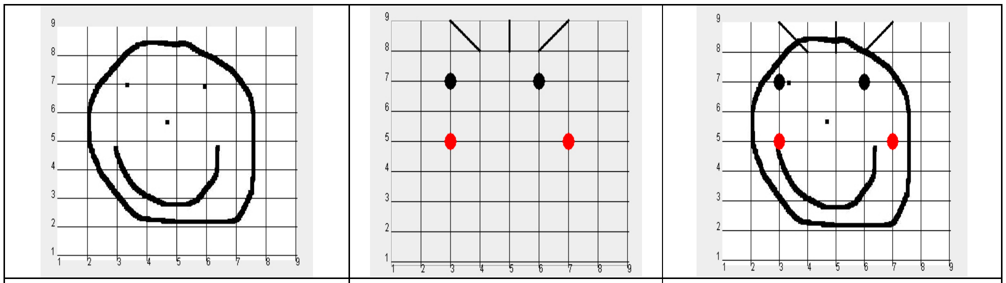
Chapter 8 Result and Discussion

8.1 Introduction

The previous chapter discussed the analysis and testing phases of the proposed systems. The results of the analysis and testing of the proposed systems – BPG, enhanced BPG and VIP Pro systems – are discussed in this chapter.

8.2 Results of the BPG System

Table 8.1 shows the synthesis of the results of the BPG system. From the analysis of the results and testing conducted on the system, it had been proven that the proposed method, which uses the penup events and the neighbouring connectivity manipulation, is capable in mitigating shoulder-surfing attack. In terms of users' memorability, the survey results show that the proposed upload background picture feature and cued colour scheme can help to improve the ability of the users in memorising their password. In addition, the personalised background picture feature reduces the users' tendency to create a centred and symmetrical password. Figure 8.1 illustrates the non-centred and asymmetrical passwords created using the upload background picture feature.



Sample Background Picture | Sample Password | Password + Background Picture

Figure 8.1: A Non-Centred and Asymmetrical Password

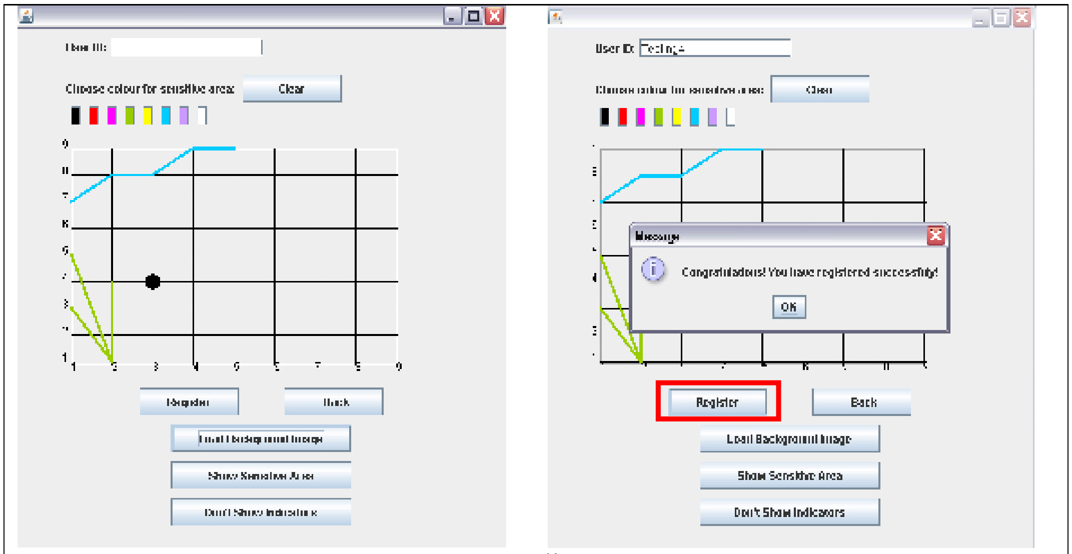
Table 8.1: Synthesis of the Results of the BPG System

Locimetrics and Drawmetrics Hybrid Authentication System		**Password Space**	**Memorability**	**SS**	**HD**	**FOA**
Cued Recall	BPG	▪ Larger password space compared with the Pass-Go system. ▪ Unlimited password space. However, the password space is dependent on the number of keystrokes made by a user.	▪ Depends on the number of keystrokes made by a user. ▪ Easy to remember if fewer strokes are made. However, the BPG system can reduce the tendency to draw centred and symmetrical pictures, because of the use of the upload background picture function. ▪ Difficult to memorise if more and complex strokes are made. ▪ Different colour scheme, and upload background picture function have been used as a cue in BPG system to increase usability, and to improve the memorability of a user.	√	√	N/A

Key:
SS: Shoulder-Surfing Attack
HD: Hotspots Dictionary Attack
FOA: Frequency of Occurrence Analysis
× : vulnerable to
√ : invulnerable to
N/A : Not Applicable

There are specific preferred areas in any picture used by a user. Therefore, other authentication systems such as Background Draw A Secret, and PassPoint are vulnerable to hotspots attack if the background picture has been identified by the attackers. This is because the chosen positions might be more predictable using a hotspot analysis attack launched by the attackers.

However, the verification process of the BPG system relies on the proposed encoding mechanism rather than the background picture used by any user. The background upload picture feature only works as a cued method to aid users in memorising their password, for example, creating a password with the GUI and encoding shown in Figure 8.2:



User ID: Testing4

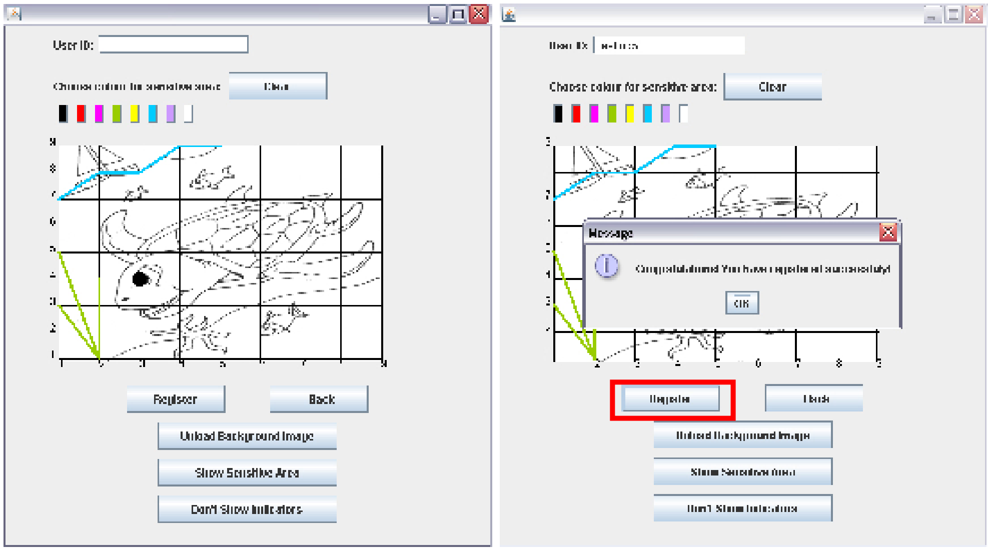
Congratulations! You have registered successfully!

Encoding:
(3,4,[0,0,0]){(1,3,[153,204,0])(2,1,[153,204,0])}{(1,5,[153,204,0])(2,1,[153,204,0])}{(2,4,[153,204,0])(2,3,[153,204,0])(2,2,[153,204,0])(2,1,[153,204,0])}{(1,7,[0,204,255])(2,8,[0,204,255])(3,8,[0,204,255])(4,9,[0,204,255])(5,9,[0,204,255])}

Hash value:
49ac665bc9ed98377135b256a14c37d2

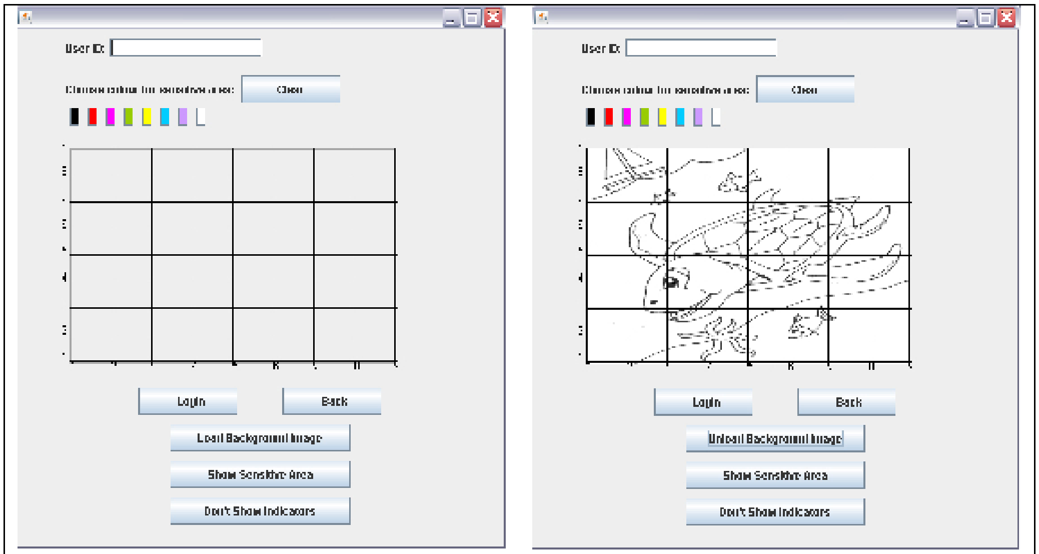
Figure 8.2: Example of a Password

Figure 8.3 shows the same password created using the cued upload background picture function. The hotspots may seem to be a problem in the BPG system, but during the verification process, attackers will be presented with a blank G×G grid to draw the password, as shown in Figure 8.4(a). Therefore, the attackers will not have a clue as to the background image used by an authorised user. However, if the attackers are able to obtain the background picture used by the user (refer to Figure 8.4(b)), they would still be required to produce the correct penup event and neighbouring connectivity with their hash values.



Congratulations! You have registered successfully!

Figure 8.3: Example of a Password Created Using the Upload Background Picture Function

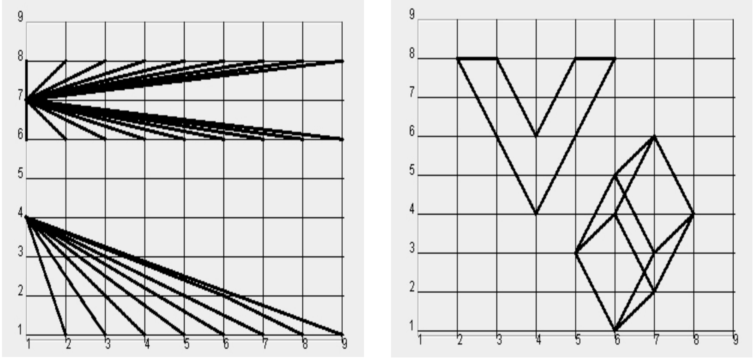


(a) BPG default login GUI

(b) An identical background used by the intruder during login

Figure 8.4: Attackers' Attempt

With regard to the connectivity of a line indicator, the proposed system can be used to connect from one intersection point (x, y) to another point within the set of $(x \pm i, y \pm i)$ neighbours, where i = {0, 1, 2, …, 8}. An analysis of the line indicator connectivity shows that the BPG system is able to fully utilise the G×G grid instead of restricting the users to connect an intersection (x, y) point to its eight-nearest-neighbour cells. Thus, users who are familiar with the BPG system, should be able to draw more lines and shapes, as compared with the use of Pass-Go. Figure 8.5 shows the lines and shapes samples that cannot be produced by the Pass-Go system.



(a) Line indicators with no nearest neighbour connection restriction

(b) Shapes that cannot be drawn using the Pass-Go system

Figure 8.5: Lines and Shapes Samples That Cannot be Drawn Using Pass-Go System

With regard to the password spaces, the password length of the BPG system can be denoted as $\sum_{i=1}^{L_{\max}} NumberOfColours \times G^2 \times (NumberOfColours \times G^2 + (G^2 - 1))^{i-1}$, where L_{max} is the number of strokes used in creating a password, G is the size of the grid used in the BPG system, and *NumberOfColours* refers to the number of colours used in the BPG system. A stroke in the BPG system 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 8.2 shows a comparison of the password space between the BPG system and the benchmark system (Pass-Go). It is obvious that the proposed system has larger password spaces when compared with the Pass-Go system (except for Coloured Pass-Go-9, the BPG system has slightly larger password spaces at $L_{\max}$ = 4, 6, 7, 8, 9, and

10). Moreover, it shows that the password space for the proposed system increases linearly as the number of strokes increases (see Figure 8.6).

Table 8.2: Password Space Comparison

L_{max}	1	2	3	4	5	6	7	8	9	10
Pass-Go-9 (adopted from Tao, 2006)	6	13	19	26	32	39	45	52	58	64
Coloured Pass-Go-9 (adopted from Tao, 2006)	9	19	28	37	47	56	65	75	84	94
BPG	9	19	28	38	47	57	66	76	85	95

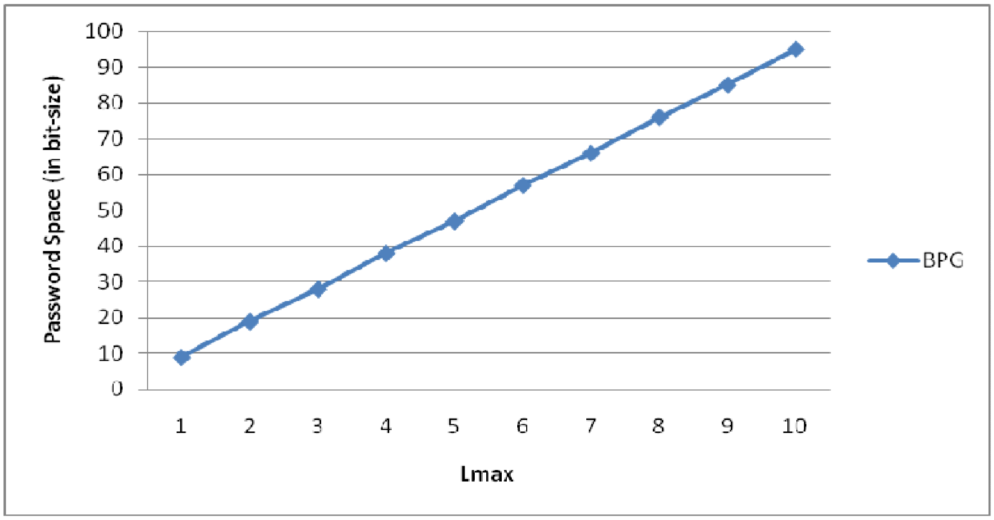


Figure 8.6: BPG Password Length

8.3 Results of the Enhanced BPG System

Table 8.3 shows the synthesis of the results of the enhanced BPG system. The enhanced BPG system inherits most of the good features of the BPG system, therefore, it is able to mitigate shoulder-surfing attack and hotspots dictionary attack by using the proposed falsifying authentication method, and the cued upload background picture feature.

With regard to users' memorability, the enhanced BPG system implements the grid line scaling feature and loose authentication method to improve the users' memorability, besides the use of the upload background picture feature and the cued colour scheme.

The survey results showed that a majority of the participants agreed that the grid line scaling feature was able to improve the users' ability in memorising their password. Besides, the use of the upload background picture feature, and the "grid line scaling" feature has reduced the users' tendency to create a centred and symmetrical password.

Table 8.3: Synthesis of the Results of the Enhanced BPG System

Locimetrics and Drawmetrics Hybrid Authentication System		**Password Space**	**Memorability**	**SS**	**HD**	**FOA**
Cued Recall	Enhanced BPG	▪ Larger password space compared with the BPG system. ▪ Unlimited password space. However, the password space is dependent on the number of keystrokes made by a user.	▪ Depends on the number of keystrokes made by a user. ▪ Easy to remember if fewer strokes are made. However, it can reduce the tendency to draw centred and symmetrical pictures, because of the use of the upload background picture function as in the BPG system. ▪ Difficult to memorise if more and complex strokes are made. ▪ Uses the same cued techniques as in the BPG system (colour scheme and upload background picture function) to increase usability and memorability. Besides, the enhanced BPG system implements two more cued techniques (grid line scaling feature and loose authentication method) to improve users' memorability.	√	√	N/A

Key:
SS: Shoulder-Surfing Attack
HD: Hotspots Dictionary Attack
FOA: Frequency of Occurrence Analysis
× : vulnerable to
√ : invulnerable to
N/A : Not Applicable

Furthermore, the enhanced BPG system uses the loose authentication method to help users in memorising their password. In this method, a user can identify his/her password using the sequence of the dot indicators followed by the sequence of the line indicators or, vice versa, instead of using the actual keystroke sequence. Although the loose authentication method is an alternative way for the users to login, it indirectly increases the risk of guessing attacks because of the more exceptional passwords that can be used during the authentication process. Nevertheless, the guessing attack can be overcome by using the penup event and neighbouring connectivity manipulation feature of the falsifying authentication method, mentioned in the previous chapter.

With regard to the connectivity of a line indicator, the enhanced BPG system enables the users to connect from one intersection point (x, y) to another point within the maximum scaling limit, $(x \pm i, y \pm i)$, where i = {0, 1, 2, …, 24}. In this way, more password spaces can be produced when compared with the BPG system.

With regard to the password spaces, the password length in the enhanced BPG system is denoted as $\sum_{i=1}^{L_{\max}} NumberOfColours \times G^2 \times (NumberOfColours \times G^2 + (G^2 - 1))^{i-1}$. Table 8.4 clearly shows that the enhanced BPG system can provide larger password space when compared with the BPG system (except that both systems have the same password space when the enhanced BPG system uses minimum scaling). In addition, the password space produced by the enhanced BPG system increases more linearly when compared with the BPG system, when the number of strokes increases (refer to Figure 8.7).

Table 8.4: Enhanced BPG Password Space

L_{max}	1	2	3	4	5	6	7	8	9	10
Enhanced BPG (Minimum Scaling)	9	19	28	38	47	57	66	76	85	95
Enhanced BPG (Maximum Scaling)	12	25	37	50	62	75	87	99	112	124

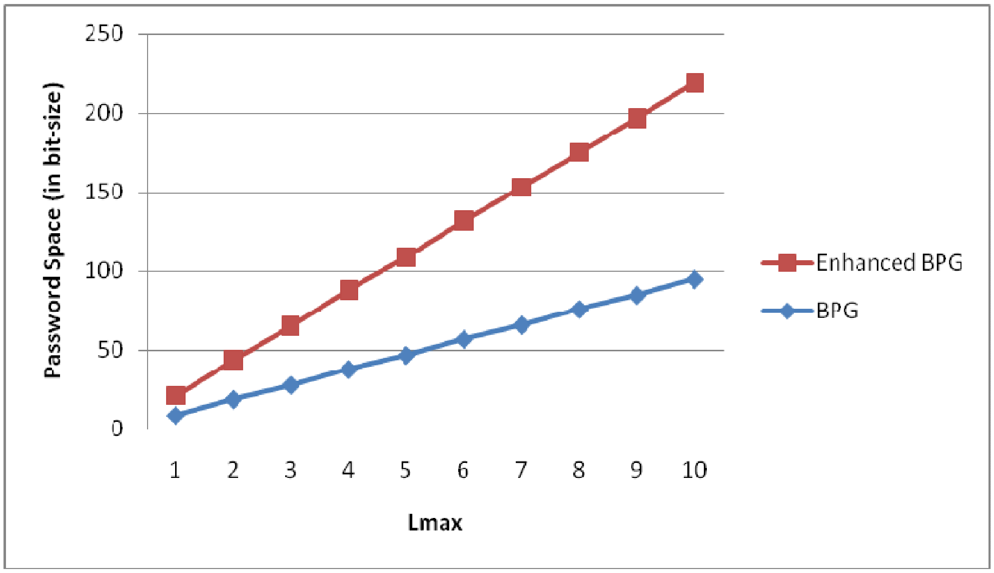


Figure 8.7: Password Length Comparison

Although the enhanced BPG system produces larger password space when compared with the BPG system, it has a higher probability of a guessing attack against it, compared with the BPG system. This is because more exceptional passwords can be used during the password authentication process if the loose authentication method is enabled. However, this problem can be overcome by using a more complex password or by using a combination of more neighbouring connectivity, penup event, and the “show/hide indicator” functions during the password creation and verification processes.

8.4 Results of the VIP Pro System

Table 8.5 shows the synthesis of the results of the VIP Pro system. The simulation results provide evidence that it can prevent FOA attack by using the metaheuristic randomisation algorithm (MRA) to re-select the old distracter pictures in the previous challenge set. The results also indicate that it is able to mitigate shoulder-surfing attack by using the hybrid method of partial password selection and MRA.

Table 8.5 Synthesis of the Results of the VIP Pro System

Searchmetric Authentication System			Password Space	Memorability	SS	FOA
Recognition	Cued Recall	VIP Pro	▪ Generic Password Space: $\frac{N!}{(N-K)!}$ N is the total number of pictures generated at each round, K is the number of selected password pictures. ▪ Larger password space compared with VIP3	▪ Easy to memorise. ▪ More difficult to memorise when compared with the VIP1 system and the VIP2 system. ▪ Uses chronological story-based cued recall technique to help users to memorise their password.	√	√

Key:
SS: Shoulder-Surfing Attack
FOA: Frequency of Occurrence Analysis
× : vulnerable to
√ : invulnerable to
N/A : Not Applicable

With regard to users' memorability, a majority of the survey participants agreed that the use of the chronological story-based cued recall technique improves the users' ability in memorising their password.

With regard to password space, the VIP Pro system has been proven to provide larger password space when compared with the benchmark system (VIP3). Table 8.6 shows a comparison of the password space provided by the VIP3 system and that provided by the VIP Pro system. In the VIP3 system, the users are always allowed three attempts to authenticate themselves by identifying four secret password pictures in the 4×4 grid, based on the searchmetric authentication system. As a result, the probability of the attackers guessing the password correctly in the VIP3 system is denoted as $\left[({}^{N}P_{8})({}^{8}P_{4})\frac{16!}{(16-4)!}\right]^{-1}$, which is approximately equivalent to [73382400(${}^{N}P_{8}$)]$^{-1}$ for each attempt. On the other hand, for the VIP Pro system, the generic probability for the attackers to guess the password correctly is denoted by equation (4), stated in Section 7.4.1.

However, there are no predetermined value for x and j compared with the VIP3 system. The value of x is set based on each user's preference, while the value of j will be determined by the VIP Pro system using uniform randomisation algorithm. Thus, if the number of secret password pictures chosen by a user is set to $x = 8$, the probability of an attacker guessing the secret password pictures correctly in the VIP Pro system for each attempt is equivalent to $\left[({}^{N}P_{8})\sum_{j=4}^{5}({}^{8}P_{j})\frac{16!}{(16-j)!}\right]^{-1}$ (based on equation (4)), which is approximately equivalent to $[3595737600\ ({}^{N}P_{8})]^{-1}$. Therefore, the proposed system is able to improve by approximately 49 times the security of the password against guessing attacks, when compared with the VIP3 system (assuming the total sampling size (N) used by both systems are the same). In addition, the VIP3 system is approximately 3770 times more vulnerable to the password guessing attack when compared with the VIP Pro system, if the password pictures selection used in the VIP Pro system is increased to the maximum limit.

Table 8.6: Password Space Comparison

System	**Password Space**	**Password Guessing Probability**
VIP3	$\left[({}^{N}P_{8})({}^{8}P_{4})\frac{16!}{(16-4)!}\right]$	$[73382400\ ({}^{N}P_{8})]^{-1}$
Proposed System	$\left[({}^{N}P_{8})\sum_{j=4}^{5}({}^{8}P_{j})\frac{16!}{(16-j)!}\right]$	$[3595737600\ ({}^{N}P_{8})]^{-1}$
Proposed System (Using Maximum Password Pictures)	$\left[({}^{N}P_{8})\sum_{j=4}^{5}({}^{16}P_{j})\frac{16!}{(16-j)!}\right]$	$[276651648000\ ({}^{N}P_{8})]^{-1}$

8.5 Summary

This chapter discussed the results of the analysis of the proposed systems. The results of the tests have shown that both proposed falsifying authentication methods (i.e., penup event and neighbouring connectivity manipulation, and partial password selection and MRA) can mitigate shoulder-surfing attack. Besides, the reused decoy picture concept has also been proven to be able to prevent FOA attack. The proposed systems can improve the password spaces. In order to assist users in memorising their password, various cued techniques have been integrated and implemented in the proposed systems. The survey results showed that the proposed cued techniques (i.e., upload background picture function, cued colour scheme, grid line scaling function, loose authentication method, and chronological story-based cued recall technique) are able to assist the users in memorising their password. The next chapter presents the conclusion of the study.

Chapter 9 Conclusion

9.1 Introduction

This chapter presents the achievement of the objectives, contributions, and future directions of this research.

9.2 Achievement of the Objectives

The following are the objectives of the research:

1. To propose falsifying authentication methods to mitigate shoulder-surfing attack. The methods include the use of: (a) penup event and neighbouring connectivity; (b) partial password selection and metaheuristic randomisation algorithm.
2. To design and implement the proposed falsifying authentication methods, specifically related to the picture-based password authentication clusters.
3. To evaluate the capability of the proposed methods in mitigating shoulder-surfing attack.
4. To evaluate the capability of the metaheuristic randomisation algorithm in preventing FOA attack (only for the searchmetric cluster).

Two falsifying authentication methods – penup event and neighbouring connectivity manipulation, and partial password selection and metaheuristic randomisation algorithm methods – were proposed to meet the first objective. The approaches used and the outcomes are as follows:

i. The concept of bypassing nearest neighbour from one intersection point to another point to trick the attackers when drawing a password in a G×G grid cells environment was proposed.

ii. The concept of holding the mouse click long enough before manoeuvring the mouse to another intersection point to create a ‘flawed’ keystroke or penup event was proposed.

iii. The concept of selecting partial password pictures rather than a fixed number of pictures or all the password pictures identified by a user during the enrollment process was proposed.

iv. The concept of re-using the previous distracter pictures to increase the frequency of occurrence of the distracter pictures to prevent FOA attack was proposed.

To achieve the second objective, the proposed methods were transformed into workable systems. They were used as a tool to gather data or feedback from survey participants to evaluate the capability of the proposed methods in mitigating shoulder-surfing attack, and in preventing FOA attack, respectively. The approaches used to achieve the third objective and the outcomes are as follows:

i. The BPG system – a standalone system, which incorporates the penup event and neighbouring connectivity manipulation method, was designed and implemented.

ii. A new colour scheme, and the upload background picture function in the BPG system to help users in memorising their password, were designed and implemented.

iii. An enhanced BPG system, which uses grid line scaling function and loose authentication method to aid users in memorising their password, was designed and implemented.

iv. The VIP Pro system – a standalone system, which incorporates the partial password selection and metaheuristic randomisation algorithm (MRA), was designed and implemented.

To achieve the third objective, case studies were conducted to evaluate the capability of the proposed methods in mitigating shoulder-surfing attack. The approaches used to achieve the fourth objective and the outcomes are as follows:

i. The first proposed method, which uses the penup event and neighbouring connectivity method, is able to mitigate shoulder-surfing attack, regardless of the gender and competency levels of the shoulder-surfing attackers.

ii. The second proposed method, which uses the partial password selection and MRA, is able to mitigate shoulder-surfing attack regardless of the gender and the competency levels of the shoulder-surfing attackers.

To achieve the fourth objective, an offline FOA Java simulation was done to evaluate the capability of the MRA method in preventing FOA attack. The outcome of the simulation made to achieve the fifth objective is as follows:

i. The proposed MRA that uses the concept of re-using the previous distracter pictures is able to prevent FOA attack.

9.3 Contributions

The contributions of this research are as follows:

i. A new security threat known as Frequency of Occurrence Analysis (FOA) attack was identified and its counter-measure was proposed.

   FOA uses a method to identify the rate of recurrence of a set of pictures generated by a secure system. FOA occurs only in searchmetric picture-based password authentication systems where users are required to search a number of password pictures used among the other distracter pictures from a challenge set. An attacker is able to identify the password pictures used by increasing the number of iterations of the offline FOA simulation. The attacker can succeed because the uniform randomisation algorithm used by the searchmetric picture-based password authentication systems tend to select the password pictures used rather than the other distracter pictures. To retain the randomness of selecting a password, a uniform randomisation algorithm has been adapted in the proposed method. A counter-measure that utilises MRA was proposed and it works by re-selecting the old distracter pictures in the previous challenge set to increase the frequency of occurrence of the distracter pictures to overcome the FOA attack. The discovery of the FOA attack has created an avenue for researchers to gain experience and knowledge about this new security threat. Researchers will be more mindful of such threats when proposing new systems especially for the searchmetric picture-based password system.

ii. A falsifying method that uses penup event and neighbouring connectivity manipulation method to mitigate shoulder-surfing attack was proposed.

The approaches used include: (a) Techniques using the concept of bypassing the nearest neighbour from one intersection point to another point to trick the attackers when drawing a password in a G×G grid cells environment; and (b) holding the mouse click long enough before manoeuvring the mouse to another intersection point to create a 'flawed' keystroke or penup event. Our falsifying method provides alternative ways and new knowledge for researchers exploring new methods of mitigating shoulder-surfing attack.

iii. A falsifying method that uses partial password selection and MRA to mitigate shoulder-surfing attack was proposed.

New techniques such as: using the concept of selecting a significant number of password pictures instead of a fixed number of pictures or all the password pictures; and, recycling the old distracter pictures in the previous challenge set were also proposed. Because only partial password pictures that were identified by the user were used in each challenge set, the proposed method has succeeded in confusing the attackers from identifying the correct password pictures and their sequence. Any subsequent attempts to shoulder-surf the password pictures or using the FOA attack approach will not succeed. Our new falsifying method provides new knowledge to researchers to explore new ways of mitigating shoulder-surfing attack. Researchers, too, will be more mindful when proposing new systems, especially, for the searchmetric picture-based password system.

iv. A new picture-based password authentication classification tree was proposed.

An initiative to organise the reviewed systems into a new classification tree according to their respective cluster – locimetrics, drawmetrics, searchmetrics, and hybrid clusters was taken. A hierarchical evolution chart and a synthesis table of each authentication cluster were constructed according to the year of establishment and their referred systems. Researchers can make use of the information to know about the strengths and weaknesses of the reviewed systems for their researches.

v. Several cued recall methods to improve the users' memorability were proposed.

For the BPG system, the cued upload background picture, and cued colour scheme to aid users in memorising their password were proposed. Grid line scaling function and the loose authentication method were proposed for the enhanced BPG system to improve the users' memorability level. To help the users to memorise their password, the chronological story-based cued recall technique was incorporated into the VIP Pro system. The proposed cued recall methods provide an alternative way to improve the users' memorability according to the respective authentication cluster. Researchers can make use of the information to know more about the appropriateness of the cued methods, for their researches.

9.4 Limitations of the current study

Finally, a number of important limitations need to be considered and they are as follows:

i. Due to the time constraint of achieving the main objective which has been stated in section 1.4, this research only manages to focus on proposing methods to mitigate shoulder-surfing attack. Besides shoulder-surfing attack, there are other security threats such as keystroke logging, hotspots, phishing, man-in-the-middle, and spyware are also worth to be carried out further research.

ii. The study did not evaluate the minimum time for holding the mouse click to confuse or to make the attackers believe that there is an extra keystroke or penup event was created. During the mitigation of shoulder-surfing testing, the time on holding the mouse click is about 5 seconds long. Such timing was successfully confused the attackers from identifying the correct password. However, more user testing and analysis are required to be done to determine the optimum time on holding the mouse click.

iii. The usability testing in terms the time taken for users to login into the proposed systems was also omitted in this research due to time constraint.

9.5 Future Directions

There are many enhancements that can be made to the proposed systems. Some of the suggestions include:

i. Security threats

Researches should be carried out on alleviating or preventing other security threats against picture-based password authentication system besides the shoulder-surfing and FOA attacks. For example, if a picture-based password is intended to be widely used in the network or online, researches on preventing man-in-the-middle, phishing, and pharming attacks should be undertaken. Various counter-measures against such threats can be explored (see Figure 9.1).

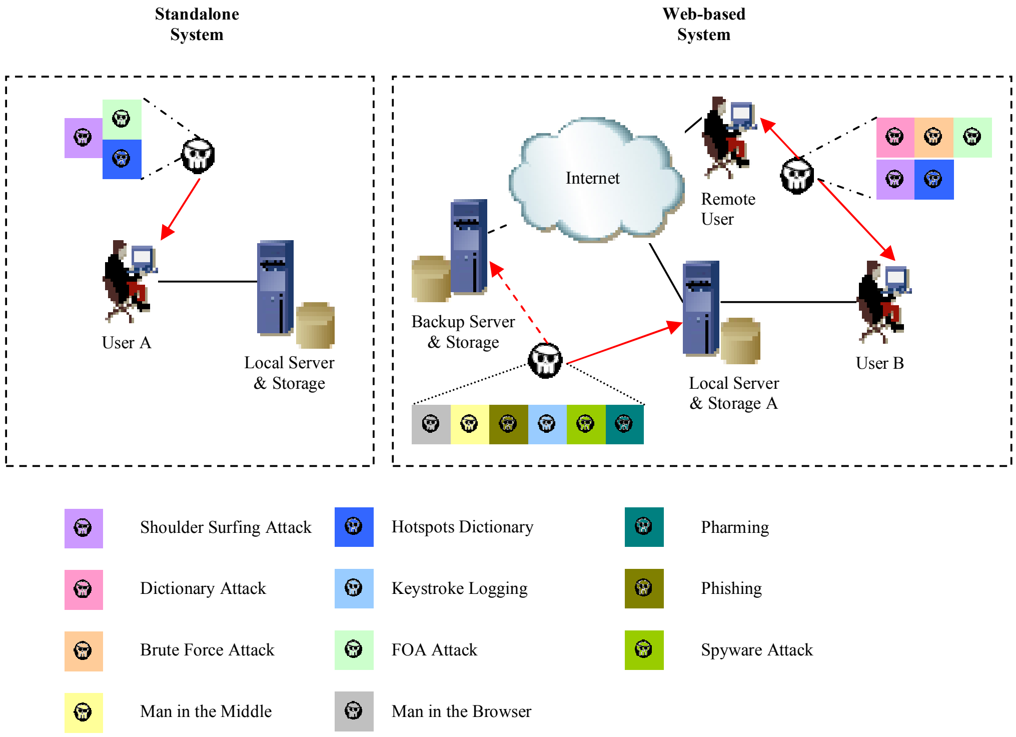


Figure 9.1: Potential Security Threats for Web-Based Picture-Based Password Authentication System

ii. Cued methods

Apart from the security issue, improving users' memorability by using various cued techniques, and educating users against creating weak passwords can also be one of the focuses in picture-based password authentication research. However, as mentioned by Wiedenbeck et al. (2005b), there are always challenges when proposing an authentication system because of the paradox that passwords are expected to comply with two fundamentally contradictory requirements, i.e., i) password should be easy for a user to memorise, and ii) password must to be secure.

iii. Other usability studies

It is a fact that most users are more familiar with alphanumeric password systems than picture-based password systems. Undoubtedly, most users will take a longer time to login into a system that uses picture-based password as compared with a system that uses alphanumeric password. Besides exploring methods for improving the users' memorability, users' study should be conducted on the time taken for users to login into a picture-based password authentication system. The maximum time limit acceptable to the majority of users must be determined for a picture-based password system to satisfy them.

9.6 Final Remarks

The proposed systems reported in this thesis have contributed towards meeting the main research objectives – to mitigate shoulder-surfing attack and preventing FOA attack. Effective new methods and algorithms have been developed in the process, and needless to say, all the experiences and knowledge gained will add on to the corpus of knowledge on picture-based password authentication systems. It is hoped that the effort made will spur further research efforts in this very interesting and challenging area of picture-based password authentication.