Jebriel, Salem Meftah (2014) *Empirical approach towards investigating usability, guessability and social factors affecting graphical based passwords security*. PhD thesis.

http://theses.gla.ac.uk/5399/

Empirical Approach Towards Investigating Usability, Guessability and Social Factors Affecting Graphical Based Passwords Security

By

Salem Meftah Jebriel
alsewi@dcs.gla.ac.uk

Submitted in fulfilment of the requirements for

the degree of Doctor of Philosophy

School of Computing Science

College of Science and Engineering

University of Glasgow

September 2013

Declaration

I declare that this thesis was composed by myself and that the work contained therein is my own, except where explicitly stated otherwise in the text.

(Salem Meftah Jebriel)

Abstract

This thesis investigates the usability and security of recognition-based graphical authentication schemes in which users provide simple images. These images can either be drawn on paper and scanned into the computer, or alternatively, they can be created with a computer paint program.

In our first study, looked at how culture and gender might affect the types of images drawn. A large number of simple drawings were provided by Libyan, Scottish and Nigerian participants and then divided into categories. Our research found that many doodles (perhaps as many as 20%) contained clues about the participants' own culture or gender. This figure could be reduced by providing simple guidelines on the types of drawings which should be avoided.

Our second study continued this theme and asked the participants to try to guess the culture of the person who provided the image. This provided examples of easily guessable and harder to guess images.

Our third study we built a system to automatically register simple images provided by users. This involved creating a website where the users could register their images and which they could later login to. Image analysis software was also written which corrected any mistakes the user might make when scanning in their images or using the Paint program. This research showed that it was possible to build an automatic registration system, and that users preferred using a paint tool rather than drawing on paper and then scanning in the drawing. This study also exposed poor security in some user habits, since many users kept their drawings or image files. This research represents one of the first studies of interference effects where users have to choose two different graphical passwords. Around half of the users provided very similar set of drawings.

The last study conducted an experiment to find the best way of avoiding 'shoulder surfing' attacks to security when selecting simple images during the login stage. Pairs of participants played the parts of the observer and the user logging in. The most secure approaches were selecting using a single keystroke and selecting rows and columns with two key strokes.

Table of Contents

Table of Figures

List of Tables

Acknowledgements

First and foremost, all praise is for Allah, Who enlightened us with faith and knowledge, and who is sufficient for us and has sheltered us.

I express my gratitude to the greatest and the wisest man in this world, my father. You have always been my model. You are the first teacher who guided me through my life. I learned so much from you. Thank you so much for everything you have done for me and I hope my prayers and good deeds will return a little from the many you gave to me. Of course, this work would never even have started without the blessings and prayers of my mother; I express special thanks for always being everything to me. Thanks for every moment you spent watching over me. Thanks for the everlasting prayers, tenderness, support, and care. To both of you, I submit this work. May Allah bless you and give you health and long lives.

I would like to thank my wife, Khulud, who stood beside me all through this trip. To my wife and my children, thank you very much for being incredibly understanding and supportive. Without you all, this degree would have been so hard.

I am also indebted to my wonderful supervisor, Ron Poet, for providing me with assistance and direction whenever I needed it. I am grateful for his support and unlimited cooperation in my research and for the leadership he provided on numerous occasions. I am also thankful for his friendship and have been really glad to work with him. To Ron, then, thank you for your unlimited support.

To my second supervisor, Dr. Karen Renaud, I also say thank you so much for your support. The credit goes, after God Almighty, to Dr. Ron and Dr. Karen in the completion of this work, as without them, this research would never have appeared and I would never have had the skills I have now.

Great thanks are also sent to my father and mother in law. They pushed towards finishing my work with their prayers. Special thanks are deserved by my brothers and my sister for their support, and I also thank my brothers in law and sister in law. I also express thanks to all of my relatives. All of them were very supportive.

To my close friends and all the Libyan community in Glasgow, thanks to you all for the support and help you have given me. May Allah grant you bright futures and everlasting success.

I also thank all the staff and all my colleagues in the School of Computer Science at Glasgow University, and all my colleagues and friends in Misurata who helped me to complete some of the experiments in this thesis. Thanks to the several hundred participants who took part in our user studies. Their cooperation and feedback were key to the success of this research.

Last but not least, special thanks to the Libyan embassy in London and to Libyan Higher Education for their unlimited support.

Chapter One
Introduction

This chapter contains the following subsections: Introduction to User Authentication, Motivation, Thesis Statement, Thesis Contributions and Publications followed by an Overview of the Thesis.

1.1 Introduction to User Authentication

"Who are you, Master?" he asked.
"Eh, what?" said Tom sitting up, and his eyes glinting in the gloom. "Don't you know my name yet? That's the only answer. Tell me, who are you, alone, yourself and nameless."

Lord of the Rings
—J.R.R. TOLKIEN

Authentication is a process that proves someone's identity. This should be distinguished from the assertion of identity and from deciding what constitutional rights accumulate to that identity [1].The term identification normally means a User ID which is used to identify the user, whereas the authentication stage verifies that the user is the legitimate owner of the ID [2]. Therefore, authentication protocols are the basis of security in many distributed systems, and it is essential to ensure that these protocols function correctly [3].One common way of doing this is that the user supplies a user name for an account, and a password. If the password is entered correctly, the user can log in to that account, thereby acquiring the access rights and privileges of the account. Human factors play a major role in authentication, and in many cases authentication failure can be attributed to poor user behaviour [4], [5], [6].

Many studies [7-9] divide authentication into three possible approaches. These three approaches depend on the human factors of authentication and will include one of the following:

- *Something you know* (e.g. a password). This is the most common kind of authentication.
- *Something you have* (e.g. a smart card). This kind of equipment must be with you whenever you wish to be authenticated.

- *Something you are* (e.g. a fingerprint). This is based on something intrinsic to the principal being authenticated and it is widely known as a biometric. Some of these biometric approaches require expensive devices.

Additionally, there can be other authentication factors:

- *Somebody you know* (social network of the user)[10]. This is also called 4th factor authentication.
- *A web of trust-forming relationships between authentication credentials.*
- *Location-based authentication, such as used by credit card companies to ensure that a card is not being used in two places at the same time.*
- *Time-based authentication, allowing access during normal working hours.*

The most common means of authentication is a password. A password is a string of characters that you needed when you log onto a computer system to verify that you are the right account holder.

Since the password's introduction in the late 1960s [11], most computer applications have adopted this method to authenticate users. Many studies [12, 13] have investigated alphanumeric passwords and pointed out the well-known limitations of textual passwords, such as memorability and guessability. A strong alphanumeric password should be at least 8 characters long (ideally longer) for good security. Long passwords are difficult for humans to remember and may also depend on the number of accounts held by a person. In addition, passwords should not contain a word or series of words that can be found in a standard dictionary (this prevents 'dictionary' attacks), and neither should they contain personal information such as a user id, family name, pet, or a birthday which may easily be disclosed to a brute force attacker. This means making a password stronger but also making it harder for the user to remember.

As an alternative, researchers have tried many techniques to replace text passwords, for example, using sounds, such as polyphonics, and hand signatures for authentication [14]. Graphical passwords are another alternative to text passwords. These were introduced in 1996 by Blonder [15]. The idea of using graphical passwords instead of textual passwords was based on some psychological studies [16] which indicated that people can remember pictures better than words. Additionally, user studies have shown that graphical passwords are easier to remember than textual passwords [17, 18].

A graphical password can be defined as follows: "*A graphical password system is an authentication system that works by having the user select from images, in a specific order, presented in a graphical user interface (GUI). The graphical-password approach is also called graphical user authentication (GUA*)" [19]. Many techniques have been designed in the field of graphical passwords since 1996, and most existing graphical password systems can be classified as being based either on recognition or on recall mechanisms. More details of these will be addressed in the next chapter.

Different graphical password systems use different kinds of images and the best way to use these images varies according to the mechanism of the graphical system, i.e. whether it is recognition or recall. Most recognition-based graphical passwords use pictures, images and photos, see Chapter Two for examples. In this thesis, hand-drawn images are suggested for use as a recognition-based graphical technique, particularly at the registration stage, through two different methods, Scan and Paint. The concept of using hand-drawn images (doodles) as recognition-based graphical passwords was introduced by Renaud [20]. Renaud's system focused on the memorability of using doodles as graphical passwords, whereas this research concentrates on the usability of hand-drawn images.

Firstly a study was undertaken of the cultural aspects of user-drawn images for authentication, comparing the types of minimal images chosen by Scottish and Libyan participants. The work on the cultural aspects of using graphical passwords was continued by conducting an experiment to see if knowledge of a person's culture made it easier to guess their graphical passwords.

Another major theme in this work was an investigation to see if the process of submitting hand-drawn images could be automated, making it easier to scale up this type of authentication system. Two systems were compared where users either drew their simple images on paper and scanned it in or used a paint program to create their images. This study also allowed the researcher to investigate how users coped when they had to register two different graphical passwords.

Furthermore, the present thesis also examines another security issue faced by graphical passwords, known as shoulder surfing. Guessability and 'shoulder surfing' are effective ways to obtain information and many of the studies reviewed in the next chapter are concerned with developing techniques to protect graphical passwords from these threats. Moreover, the present study investigates the proper and secure ways of selecting pass-images in challenges set up to prevent shoulder-surfing.

A few prior studies have used hand-drawn doodles as authentication techniques. The first was designed by Goldberg, et al.[21], and the second study was designed by Govindarajulu and Madhvanath [22]. Both systems are classified as recall-based techniques whereas the third study by Renaud [20] was classified as a recognition-based technique. The first study was not applied in a real system whereas the second study was applied as an authentication mechanism in a web browser. Chapter Two describes these techniques in depth.

1.1.1 Hand-drawn images and culture familiarity

Many scholars, for example, Sidis and Goodhart [23] and Russell [24], have comprehensively discussed the term "feeling of familiarity" and it seems that is distinct and well understood. Sidis and Goodhart [23], gave a brief description, almost humorously, of the experience of feeling of familiarity in the following quote:

> "*What again happens when we meet with a person who is strangely familiar to us? The 'strange' familiarity consists in the arousal of a number of specific representations, many of which are recognized as incongruous and are rejected. Representations rise and revolve round that percept. The mind tingles with cognitive anxiety, with mental throes on the eve of giving birth to the specific associations, resulting in final recognition. This peculiar condition of subexcitement of representative elements started by the perception of an object constitutes the state which is termed the sense of familiarity. Familiarity is vague recognition, recognition not as yet made specific*".

This description of the experience of familiarity well explains the feeling of seeing something like a picture, person or an event that is familiar to us, and as the quote suggests, experiencing something familiar can at times seem like a cruel trick of the mind. This can be helpful to give us some degree of confidence that the event or the pictures we saw occurred in the past. This degree of confidence could be either low or high which is affected by the strength of the familiarity feeling [25] and [26](for example, if the degree of confidence is low then more recollection processing is needed but if the degree of confidence is very high, the recognition decision will be easier). The level of the familiarity feeling and the strength of the memory are intimately related [25], [27], [6], [28]. If there is a strong familiarity feeling with an event such as drawing images by hand, this will give at least a recognition sign for a prior occurrence [26]. In terms of a recognition based graphical password, it would be useful to develop a scheme that uses hand-drawn images as pictures which would ensure a high level of familiarity with users while studying the "*cultural familiarity*" of those hand-drawn images could improve the recognition memory of graphical passwords.

1.1.2 Why use hand-drawn images rather than other images?

The characteristics of hand-drawn images, as stated by Renaud [29], which make them suitable for use in authentication, are as follows:

1. Hand-drawn images are very simple and quickly produced.
2. Hand-drawn images are fairly hard to precisely describe.
3. Hand-drawn images cannot be duplicated. Each image drawn is different in some small way, even if it is in the same category: for example a car drawn by one author will never match one by another author. This reflects the uniqueness of the author as a human being.
4. Berger [30], points out that there is a relation between the drawer and his drawings. He argues that *"The drawer and the drawing engage in a kind of unarticulated dialogue, making drawing a two-way process. This process is bound to lay down stronger memories than the mere passive viewing of other pictures*".

The most important feature of hand-drawn images is that most people can use them, whether they are young or old, educated or uneducated; however, they also have particular requirements when used in authentication. In the authentication stages, it is necessary to distinguish the hand-drawn pass doodle for each user from the distractor doodles that are displayed in the challenge sets, to avoid a wrong selection.

1.2 Motivation

The motivation behind this research is based on several observations drawn from other studies. One motivation for examining the application of graphical schemes is that humans have a remarkable capability to remember pictures [17]. Psychological studies maintain that people remember pictures more easily than words, including concrete nouns [16], [31].

Another motivation of this research is that most of the recognition-based graphical passwords systems have been developed in Western countries, involving users from those countries. However, cross-cultural studies in computer science have revealed that people from different cultures differ in their way of using technologies: see Ford and Kotzé [32], and Anandarejen et al. [33].

One other motivation behind this research which can be added is that using doodles as a graphical password have been shown to be more memorable than other types of images, such as personal capture pictures, photos, and global images [29].

In addition, another motivation for this research is “what we do is what we remember more”. Much evidence has been gathered to support the notion that what we do (our actions), can be remembered very well, as found by Casasanto and Dijkstra [34] , Loula et al. [19], Englecamp et, al. [35], and Koriat et al. [36]. Thus, creating graphical passwords by drawing hand images could offer good memorability.

The design of any technique should make it easy for users to use as well as requiring minimal time, effort and basic equipment. The system of Govindarajulu and Madhvanath [22], who used doodles as recall based systems, requires that expensive items of equipment, such as a touchpad and digitizing tablet, are attached to a computer and users also need time to learn how to use the system. The methods used in this research require only basic technologies to create a password: a printer and scanner, and easily available software such as a paint system.

1.3 Thesis Statement

A major goal of this research is to how to create and use hand-drawn images as a knowledge-based authentication scheme that is usable, and secure. The cultural aspects of user-drawn images for authentication are also investigated.

This research focused on hand-drawn graphical passwords because of their potential for increased usability and security. The main research statement is:

The choice of hand-drawn images is affected by a user's culture, and this can have an impact on their usability and security. In addition, it is possible to build a system that allows a user to submit their own hand-drawn images without the need for an administrator, making the system more scalable.

The main work began with a cultural investigation, with new ideas being formed and tested as the research progressed. Three main research objectives of this thesis are described below.

Objective 1: To investigate the cultural aspects of chosen hand-drawn images between three cultures; to empirically investigate of the relative impact of cross-cultural influences in drawing doodles between Scottish, Libyan and Nigerian participants.
With regard to this objective, the research aims try to answer these questions:

Q1. Does culture play an important role in the selection of pictures by Scottish, Libyan and Nigerian users? Can we quantity this effect?
Q2 .Is it possible to guess other people's hand-drawn image passwords depending on his/her personality characteristics, such as cultural features or nationality?

Objective 2: To create and empirically test new designs that address the usability of using hand-drawn images by demonstration, via automatic registration of hand-drawn images as graphical passwords on two systems: the use of a hand-drawn images technique vs. the use of a program-based drawing technique.
To meet this requirement the present research aims to answer the following questions:

Q3. Is it possible to automate the registration of hand-drawn images?

Q4. How does the usability compare between registering hand-drawn images by scan and hand-drawn images created with paint?

Objective 3: With respect to security of using general hand-drawn images as graphical password, to empirically evaluate the effects of shoulder surfing.
This leads to the final question:

Q5. What is the safest way of selecting hand-drawn image passwords?

1.4 Thesis Contributions and Publications

The main constituent parts of this research can be summarised as follows:

1. A user study offering a cross-cultural comparison was conducted. The study compared three different user groups: Libyans, Nigerians and Scots to investigate the cultural aspects of user-drawn images for authentication and how culture might affect the choices and usage of drawn images as password. The study showed that culture can play a partial role in the selection of hand-drawn images. It was also found that gender could sometimes influence the type of image drawn.
2. A related user study was conducted to find out whether or not an attacker could guess a user’s cultural background based on his hand-drawn images. This study showed that an attacker could sometimes guess the culture and also gender of a user, and that some types of image helped an attacker more than others.
3. A system was built to see if it was possible to automate the registration process when user drawn images are used as a graphical password. Two approaches were implemented. In the first, the scan system, users drew their pass images on paper and scanned them in, while in the second they used a computer paint program to create them. The results of a user study showed that the automation worked and that users preferred the paint rather than the scan system. The users had to create two different graphical passwords, each of four images. The user study showed that many users drew very similar images for both passwords.
4. Another user study on the security against a shoulder-surfing attach was conducted. It found that the use of two keystrokes was the most secure.

Finally, significant portions of the research presented in this thesis have been peer-reviewed and published:

- S. M. Jebriel and R. Poet, "Preventing shoulder-surfing when selecting pass-images in a challenge set," presented at Innovations in Information Technology (IIT), an International Conference in Abu Dhabi in 2011.
- S. M. Jebriel and R. Poet, “Automatic Registration of User Drawn Graphical Passwords”, Workshop on Human Factors in the Safety and Security of Critical Systems, 18 March 2013, Glasgow. (which is not peer reviewed)
- S. Jebriel and R. Poet, "Exploring the guessability of hand-drawn images based on cultural characteristics," in *Computer Science and Information Technology (CSIT), 2014 6th International Conference on*, 2014, pp. 5-13.
- S. Jebriel and R. Poet, "Automatic registration of user drawn graphical passwords," in *Computer Science and Information Technology (CSIT), 2014 6th International Conference on*, 2014, pp. 172-177.

1.5 Overview of the Thesis

The remaining part of this thesis is divided into six further chapters.

Chapter Two consists of a literature review of two main areas of prior study. The first part is a review of well-known graphical password authentication schemes and several existing authentication mechanisms and will identify some of the problems that have occurred when using some of these techniques. The second area is concerned with some of the factors of security and usability that have been studied.

Chapter Three presents a user study on the cultural aspects of user-drawn images for authentication and how culture might affect the choice and usage of drawn images as passwords. It describes a comparison of selecting and drawing everyday pictures or doodles, details of their analysis, and explains how culture may play a role when drawing and selecting doodles and compares the different results obtained from Scots, Libyans and Nigerians.

Chapter Four focuses on one of the most important security issues related to graphical passwords: guessability. This chapter presents an experiment conducted on guessability of hand-drawn images. It describes how the design of the website used the analysis of the data gathered from users. Hand-drawn images used with the website in this experiment were selected from hand-drawn images gathered from the previous studies described in Chapters Three and Five.

Chapter Five discusses and presents the analysis and the design of the automatic registration study, in three main sections. The first section describes the software used in extracting hand-drawn images. The second presents the design of an online website using two main systems, scan and paint. The third section presents an empirical study to test these systems and an analysis of all the data, and presents and discusses the results.

Chapter Six takes a broader view of security and discusses how to prevent shoulder-surfing when selecting pass-images in a challenge set. In this chapter, an empirical study conducted at Glasgow University is described and the results are discussed.

Chapter Seven discusses the overall design strategies that can be extracted and generalised from this research. It also suggests further research directions that fall beyond the scope of this thesis, and makes other concluding remarks.

Chapter Two
Literature Review

This chapter reviews the prior literature related to graphical passwords in general. It also explores some security and strategic usability issues involved with graphical passwords in detail, such as threats and vulnerabilities and the usability layers of such systems. This is chapter divided into nine sections and is organized as follows. The first section gives an overview of the enormous classification of graphical passwords. Section 2.2 discusses the security of graphical passwords including the threats encountered by recognition based systems and also defines usability and describes the usability elements of graphical passwords. Section 2.3 reviews the definition and background of Recognition Based Graphical Passwords. Section 2.4 reviews the definition and background of Recall Based Graphical Passwords. Section 2.5 reviews the definition and background of Cued Recall Based Graphical Passwords. Section 2.6 displays some graphical password based on hand-drawn images. Section 2.7 highlighted some graphical password reviews. Section 2.8 considers and describes cross culture studies in graphical password in term of drawings. Finally, Section 2.9 presents the summary of this chapter.

2.1 Classification of Graphical Password Systems

Many studies have classified graphical passwords into different categories; for example, De Angeli, et al. [17] classified graphical passwords into the following three categories:

- Cognometrics
- Locimetrices
- Drawmetrics

The term Cognometric refers to using the innate cognitive abilities of the human brain such as face recognition, whereas the term Locimetrics refers to mechanisms that require clicking on selected points in an individual image through the authentication stage. The Drawmetric system requires the user to reproduce a pre-drawn outline drawing.

Tao [37] divided graphical passwords into two main categories:

- Image-based schemes
- Grid based schemes

In Image-based schemes, the system uses images and pictures as a background and according to number of images displayed these are divided into two subclasses, single-image schemes and multiple-image schemes. The grid based schemes are based on a grid mechanism to create passwords.

In addition, other graphical password studies such as the survey by Suo et al.[38] have divided graphical password schemes into two main categories:

- Recognition based systems
- Recall based systems

The next sections will follow the graphical password categorisation of Dirik, et al. [39], which classified graphical schemes into three systems:

- Recognition based systems
- Pure recall based systems
- Cued recall based systems

In a recognition based system, the users have to recognise their pass image on images when they see them again. When they register, the user either provides their own images or chooses from a collection provided by the system. When they log in, they are shown their pass image, together with a number of distractor images, in a challenge set. There may be several challenge sets, each with pass images, or one challenge set which may contain several pass images, to provide the desired level of security. These systems rely on the psychological evidence that it is easier to recognise an image when it is seen again, rather than to recreate it again.

In a recall based system, the user has to recreate their pass image every time they log in. This is similar to a written signature used to sign documents. A cued recall based system provides cues to users to help them repeat their initial actions, such as selecting points in an image each time they log in. The present research focuses on recognition based systems, but the literature on recall and cued recall is also mentioned to provide a complete picture of this subject area.

2.2 The Security and Usability of graphical passwords

2.2.1 Security of Graphical Passwords

Many studies in this chapter will show that the security and usability are related to each other. Many secure systems in general and authentication solutions in particular can benefit from improvements in usability. According to Abdullah [11], most previous studies of graphical passwords were concerned either with security or usability, but not both. This section will discuss the security factors, while the usability factors will be discussed in more detail in the next section.

There are a number of ways in which graphical password systems are vulnerable to attack, as outlined by Poet and Renaud [40]:

- **Brute Force**: A brute force attack is a trial-and-error method used to obtain a password. In recognition based systems the user is helped to remember their pass image by showing it to them, along with distractors. This will also help the attacker, since they know that one of the images shown will be the correct pass image. This is vulnerable to a brute force attack if the attacker is allowed to try a number of variations of image choices without hindrance.

- **Denial of Service**: one possible solution preventing the attacker from getting the password by using a brute force technique is a denial of service after a small number of incorrect trails. However, an attacker can deliberately try to log in as someone else, failing enough times to force the victim to re-enrol. Thus, requiring re-enrolment to avoid a brute force attack should be used with caution.

- **Intersection Attack**: This attack is specific to recognition based systems and occurs when a graphical system uses different distractors each time in the challenge set. The intruder can simply keep refreshing the display to see which image does not change. This can be avoided by fixing the distractors at registration.

- **Shoulder-Surfing**: Standing behind someone and looking over their shoulder in order to memorise the graphical password, is known as shoulder surfing. This is one of the most common ways to attack people who use graphical passwords and since the images are displayed and the user needs to identify the image, most often by clicking on it, there is a high risk of disclosure. To avoid this, some recognition-based systems use the keyboard rather than the mouse to allow users to choose their password, which makes it much harder for an observer to identify the target image.

- **Social Engineering**: Some graphical password systems allow users to use their own pass images, which might be guessed by an attacker if they can relate the images to a particular person. This is a problem with images such as photographs but less so for minimal image types such as sketches (doodles) and Mikons, which are icons created by a computer program. These are provided by the user but are much less likely to be easily attributed to the artist. A standard social engineering attack [41] on text passwords follows the pattern: "There is a problem with your account. I am a system administrator. I need your password to fix the problem. Tell me your password". This is harder to achieve with a graphical password, but if the image was easy to describe, a user might fall victim to this form of social engineering attack. For this reason, images that are harder to describe are safer.

- **Dictionary Attacks:** Dictionary attacks represent another possible threat to graphical authentication systems [42]. A dictionary attack is a type of brute force attack where the attacker uses a dictionary of graphical passwords or images for some techniques which use normal images, and this can be applied to recognition type. In cued recall, the attacker creates a program that can spot the popular click points on an image.

The above threats could be grouped in different ways. De Angeli et al [43]. have proposed that the security of recognition-based systems can be judged in terms of three aspects; their guessability, observability, and recordability. These aspects can be summarised as follows:

- Guessability: the probability that an attacker can guess the user's password;
- Observability: the probability of an attacker being able to observe the authentication process or the password;
- Recordability: the ease with which an attacker can record a user's password by using certain techniques.

Additionally, Renaud extends previous areas to include analysability and resistability [44]. Analysability is the probability of an attacker successfully gaining the implementation details of the software used, e.g. bugs in the code which could be exploited. Resistability is the probability of the auxiliary attempts to secure the system, an example provided is a three strikes policy where the user is locked out after three unsuccessful authentication attempts.

Biddle et al.[45], classified possible attacks into two general categories based on knowledge authentication: guessability, which means the ability of a fraudster to guess the code, and capture attacks (observability), i.e. the ability of a fraudster to observe the code as the user enters it.

2.2.2 Usability of Graphical passwords

ISO 9241-11[46] defines usability as *the extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use.* In addition, Sasse [47] defined a usable system (based on Shackel 1975) as one which ensures that :

- *the intended users can meet a desired level of performance operating it (task performance);*
- *the amount of learning/practice required to reach that desired level of performance is appropriate (learnability);*
- *the system does not place any undue physical or mental strain on the user (user cost);*
- *Users are satisfied with the experience of interacting with the system.*

2.2.2.1 Layered Model of Usability

The usability of any products, including software and hardware, is the main goal of an interface designer, and its level is usually determined after applying a usability test to the product with participants or by going through checklists. Van Welie et al. [48] broke down the concepts of usability into a layered model which provides a very clear view, as shown in **Error! Not a valid bookmark self-reference.**.

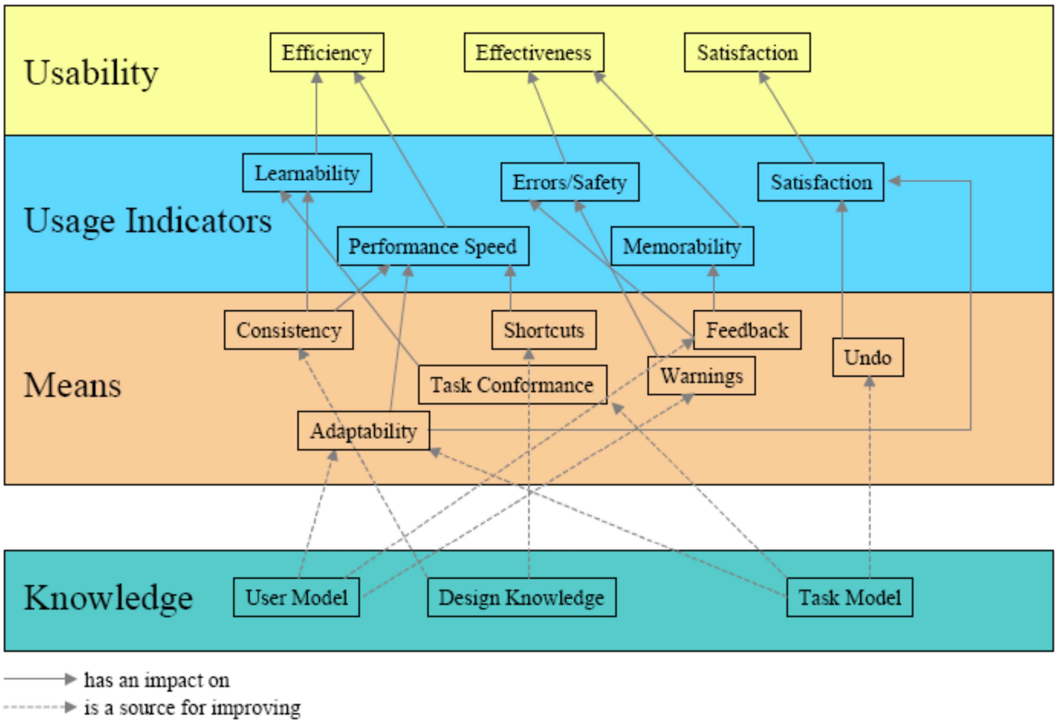


Figure 2-1 Layered Model of Usability

Many prior studies, such as Schultz et al. [49] have pointed out some of the usability factors that affect schemes especially with regard to authentication techniques including some of those mentioned above. The main usability factor investigated in extensive detail by most studies of graphical passwords and other authentication techniques is memorability, as examined by Renaud and De Angeli [50] and Christina and Jean-Marc [51]. The next subsection will discuss some factors of usability including memorability, time to learn, speed of performance, rate of error by both users and systems and subjective satisfaction, as discussed by Sollie [52].

2.2.2.2 Memorability

Memorability is the main issue of usability when considering passwords and the various studies mentioned above and others have focused on how users can remember the graphical passwords and what factors affect doing so, such as human factors (*primary memory and long term memory*). Some studies have pointed out that remembering a pictorial password is not a problem (according to the features in pictures, such as faces) as much as remembering the order of it. Davis et al. [53]'s study demonstrated that approximately 75% of participants entered their pictorial password in an incorrect order:

"I had no problem remembering the four pictures, but I could not remember the original order."

Every scheme has some parameters that may affect their memorability, as stated by Harsh and Newman [54]; these might include the number of images displayed per panel, the number of images a user must select per panel and the number of panels displayed per authentication attempt.

2.2.2.3 Time to learn

The learning phase or the level of learnability affects both the cost of system implementation and users' acceptance. This phase analyses and studies how easy it is for users to use the graphical authentication technique. Moreover, it examines the time and effort needed to learn this technique; for example, if the user needed a long time then they might not use the technique as effectively because of the effort involved. Less complex systems are preferred by users and they feel more comfortable using them.

2.2.2.4 Speed of performance

One of the most important factors is the users' opinions of the usability of the system and its speed of performance. This is known as efficiency. Speed performance measures acceptable time expenditure during the authentication phase. The use of the system affects its users and may become a critical issue if it takes too much effort and time.

2.2.2.5 Rate of errors

The main goal of this factor is to measure the rate of errors performed by both the users and the systems of the authentication system. As users forget a password four times a year on average [52], the designer of any authentication technique should take account of this fact. Furthermore, the authentication system or the implementation of it will not work perfectly if the system has too many user errors. On the side of the system, the number of errors in terms of both failures to enrol and failures to acquire should be small or zero.

2.2.2.6 Subjective satisfaction

The feedback from users who have accessed the system is a very important phase of measuring its usability. This information will indicate if the mechanism is regarded as satisfactory by the user or not. On the other hand, it determines whether or not the system affects the users' satisfaction and if the system carries any privacy issues which are important to the user.

However, many of the graphical password techniques described in the previous sections were concerned with memorability on one hand and also tried to be secure enough. Usability plays an important role between tools and their users. Effective tools allow users to achieve their tasks in the best possible way. This should be applied to graphical password systems. In order for graphical passwords systems to work, their users must be able to utilise them accurately and effectively, as Hafiz et al. [55], have argued.

2.2.3 Memorability

2.2.3.1 The memorability of images

Strong text passwords are difficult to remember and the basic reason for investigating graphical passwords is that it is easier to remember images than text. Putting this another way, there are more easily memorable images than text passwords. Humans have a remarkable capability to remember pictures as has been shown by De Angeli et al. [17], and Goldstein and Chance [56]. Psychological studies maintain that people remember pictures more easily than words, even if the words are concrete nouns, as cited by Thorpe and Oorschot [31] and Shepard [57].

2.2.3.2 The Memorability of user performed tasks

The images used in graphical authentication are not all remembered equally. Two studies, which will be described in more detail later in this chapter, have studied this. In Déjà Vu [58], abstract art images were proved to be less memorable than photographic images. In an experiment where home photos and hand-drawn images were compared, it was found that the most memorable were hand-drawn images [29].

Some compelling reasons were provided for these findings by Andrada [59]. Much evidence has been gathered to support that what we do (our actions), can be remembered very well. As Casasanto and Dijkstra [34] stated, “Motor action is memory”. Loula et al. [19] have also investigated the memory of motor actions, while Englecamp et, al. [35] and Koriat et al. [36] also reported on the additional memorability of self-performed tasks. Nyberg et al.[60] argued that self-performed tasks are remembered better than verbal materials

However, it is not necessary for a person to repeat the same actions for the initial memory to “fire”. For example, people could recognise their own drawings without getting visual feedback when they initially drew the pictures [61]. A number of senses including vision and touch are involving in the drawing process, and the feedback from motor activities is also used as the drawing progresses, with various sensory inputs giving continuous feedback to guide the drawing process. Sensory processes turn out to be essential in laying down memories during actions. Leynes et al. [62] showed that sensory characteristics provided unique information for action memories, and that this sensory information was often activated when the action was remembered. This finding appears to have been confirmed by the findings of other researchers, and this can be summarised as follows:

- Longcamp et al.[63] found that when people read the letters of the alphabet they had previously written, the same regions of their brains that were activated by the writing process were re-activated.
- Pianists can recognise recordings of their own performances, even when the sound is removed during the initial recording of the performance [64].
- Flach et al. reported that people can identify their own clapping [65].
- Loula et al. [66] proved that people were best at identifying their own movement, even in poor lighting conditions, when they saw videos of their own, their friends’ and strangers’ movements.

These examples all refer to memory of motor skills. In the context of creating hand-drawn images, the motor skills used involve mouse movement and hand action.

When a person remembers activities they have previously carried out, memories of the action planning process will come to mind. A related finding is that doodling while listening to someone speaking actually helps the listener to retain what was said more effectively than if they had not doodled [59]; more details about this study will be provided below. This finding seems to confirm that the memorial advantages of engaging in actions are not confined to memories of the actions themselves.

There is a strong case for concluding that it is better to actively engage than merely to look, if a strong memory trace is desired. There is also evidence that, having carried out the action, one can expect enhanced recognition performance of any artefact related to the original action [67]. However, only a few graphical password systems can be classified as based on self-performed tasks where the users have to create their passwords from scratch, such as graphical passwords based on Mikons [68] and those based on standard shapes [69]. Both of these are discussed in more detail later in this thesis.

2.3 Recognition Based Graphical Passwords

The main differences between these systems lie in the types of image used and whether the user chooses options provided by the system, or provides their own images. The three archetypal examples for this category are described in the next sub sections.

2.3.1 Déjà Vu

Dhamija and Perrig [58] proposed and designed a graphical authentication technique called Déjà Vu. The main idea of their technique was that the system generates a collection random images from Andrej Bauer’s Random Art collection. The users are asked to create their password (an image portfolio) by selecting a fixed number of images (five images were applied) from this collection. Afterwards, the user is asked to identify the images correctly in order to be authenticated. Déjà Vu has three phases:

- Portfolio creation
- Training
- Authentication

In the portfolio creation phase, the server presents a large set of images and the users have to select a specific number from it. The next step is the training phase which requires users to identify their selection images from a challenge set to aid memorability. The users who identify all the portfolio images correctly on logging in are authenticated and this is the final Déjà Vu phase. The majority of users have reported that image portfolios were easier to remember than PINs and passwords. In addition, the results showed that 90% of all participants succeeded in using Déjà Vu, while only 70% succeeded in using text-based passwords and PINs. This technique has several advantages: for example, the using of hard to describe (abstract) images offers a system which is strongly resistant to a social engineering attack and these images are more memorable according to the participants of the study. Furthermore, the technique prevents users both from choosing a weak password and from writing it down or sharing it with others. The main drawback of Déjà Vu is the time required for the authentication phase.

2.3.2 Pass Face

One of the most important types of recognition-based schemes which have been investigated by many other researches is a technique that uses faces. The principles of this kind of system are based on psychology studies such as that by Feingold [70]. One of the earliest applications involving the use of faces for authentication was Real User Corporation's PassFaces^{TM} system [71]. The idea for this application was created by Real User Corporation and evaluated by Brostoff and Sasse [72]. This technique has improved since they launched it in 2000 [73]. The system displays a random set of faces (typically 3 to 7) to a user to serve as their secret authentication code, thus the system itself chooses the pass images. In the next phase, the system takes the user through a 'familiarization process' which helps them to imprint the faces in their mind. At the stage of authentication, the user has to pick out their assigned faces from consecutive groups of nine faces.

Two psychology studies, by Levin [74] and Langlois et al. [75] have shown that people find it difficult to recognize members of a race different from their own. Additionally, people prefer choosing attractive faces (e.g., facial symmetry, youthfulness, averageness). Moreover, the studies have found that attractive children and adults are judged more positively than unattractive children and adults, even by those who know them. Theoretically, the major drawback of using faces as an authentication mechanism is the ability to disclose a password by tracing the attributes of the faces, such as their races, the colour of the skin and their gender. This is why the Real User System assigns faces to the user rather than letting them choose. However this also makes the faces harder to remember.

2.3.3 Story scheme, everyday objects

Davis et al. [53] invented a new system, in the form of a story password scheme, and compared it with a version of PassFace. In the story scheme, users asked to create their password by picking up and remembering sequences of one or more pictures from lifestyle categories. This involved pictures of subjects such as food, animals, scenic locations, and male and female models and making a story from them. Then, the users are asked to click their pictures choosing at the first stage (*in the same order*) which will be displayed in a 3×3 grid to be authenticated.

In the Face scheme users were asked by the researchers to choose four faces from two categories namely black or white, male or female normal people and models. At the authentication phase the system will continuously display a random grid of nine faces. Then, users have to choose one face from one grid each time. Their findings indicated that the Story scheme is harder to remember than the Faces scheme.

2.3.4 Summary and A Comparison of other GUA Algorithms Based on Recognition Schemes

In this section, fourteen graphical password based recognition schemes were studied and compared. Table 2-1 shows a comparative on two main factors of graphical password which is usability and security. The four usability factors were compared are memorability, efficiency, effectiveness and user satisfaction whereas the common security attacks are: brute force, dictionary, spyware, shoulder surfing, social engineering and guessing. Additionally, the table demonstrates the advantages and disadvantages of each scheme if it is found.

Table 2-1 Usability Features and Possible Attacks on Recognition-Based Graphical Password

No	System	Created By	Proposed Date	Image	Login Interference	Usability					Security							Advantages	Disadvantages
						Tested	Memorability	Efficiency	Effectiveness	Satisfaction	Tested	Brute Force	Dictionary	Spyware	Shoulder Surfing	Social Engineering	Guessing		
1	Déjà Vu Figure 2-2	Dhamija and Perrig [58]	2000	abstract	Identify correct pass images.	**PT**	**Y**	**N**	**Y**	**-**	**T**	**N**	**Y**	**Y**	**N**	**Y**	**N**	Prevents users both from choosing a weak password and from writing it down or sharing it with others.	The main drawback of Déjà Vu is the time required for the authentication phase.
2	PassFaces Figure 2-3	Brostoff and Sasse [72]	2000	Faces	Select face from of grid of faces.	**PT**	**Y**	**N**	**Y**	**-**	**T**	**N**	**N**	**Y**	**N**	**N**	**N**	Passfaces have been shown to be very memorable over long intervals.	Predictable.
3	Convex Hull Clicks Figure 2-4	Sobrado and Birget [76]	2002	objects	Select object from number of display.	**PT**	**Y**	**N**	**Y**	**-**	**PT**	**N**	**Y**	**-**	**Y**	**Y**	**N**	Is intended to prevent shoulder surfing and guessability.	Difficulty in identifying objects from crowded display of objects.
4	Jansen Figure 2-5	Jansen et al. [77]	2003	thumbnails	Select images based on a theme.	**PT**	**Y**	**N**	**Y**	**-**	**T**	**Y**	**N**	**N**	**Y**	**N**	**Y**		The main drawback of this system is the limitation in the number of thumbnails which creates risk of a brute force attack and also it has a small password space.
5	Story Figure 2-6	Davis et al. [53]	2004	pictures	Identify portfolio images from among decoys.	**N**	**-**	**-**	**-**	**-**	**PT**	**N**	**-**	**-**	**N**	**-**	**N**		Story scheme is hard to remember (sequence order).
6	Handwing Figure 2-7	Renaud [20]	2006	Hand writing	Users had to select their handwriting PIN, postcode and doodles.	**PT**	**Y**	**-**	**-**	**Y**	**N**	**-**	**-**	**-**	**-**	**-**	**-**	High memorability.	• Probability of recognition of the users' hand writing digits by people who knew them. • The PINs and the post codes could easily be recorded. • The observability of the system is very high.

No	System	Created By	Proposed Date	Image	Login Interference	Usability					Security							Advantages	Disadvantages
						Tested	Memorability	Efficiency	Effectiveness	Satisfaction	Tested	Brute Force	Dictionary	Spyware	Shoulder Surfing	Social Engineering	Guessing		
7	3-D Figure 2-8	Alsulaiman and Saddik [78]	2006	objects inside the 3-D virtual environment	Select the interacts with objects inside the 3-D virtual environment as stored at the registration stage.	N	-	-	-	-	N	-	-	-	-	-	-	A large password space.	No user testing or security results are reported, making usability or security evaluations difficult.
8	Tricerion Figure 2-9	Fraser [79]	2006	symbols	Insert correct symbols password from the symbols keypad.	NT	-	-	-	-	NT	-	-	-	-	-	-	Helping user to remember symbols instead of characters	Lack of usability and security test
9	VIDOOP Figure 2-10	Osborn et al. [80]	2008	pictures	Entering a series of one or more password elements corresponding to the graphical images that stored.	N	-	-	-	-	PT	-	-	-	-	-	-	This device shows a high level of security.	Lack of usability test.
10	RGGPW Figure 2-11	Lin et al. [81]	2008	geometric shapes	User needs to click the objects in the same order as that which has been saved on the server's image database.	T	-	-	-	-	PT	y	-	y	y	y	-	it does not require a large image database and it is not necessary to repeat mouse clicking at the same position	Future usability evaluations should be concerned with improvements to two main factors: firstly, the shapes are similar and convergent which may confuse the users. Secondly, overlapping colours may cause a lack of focus.
11	Use Your Illusion Figure 2-12	Hayashi et al. [82]	2008	distorted images	Selecting portfolio images from among panels of decoys.	T	Y	Y	Y	Y	PT	-	-	-	Y	Y	-		NA

No	System	Created By	Proposed Date	Image	Login Interference	Usability					Security							Advantages	Disadvantages
						Tested	Memorability	Efficiency	Effectiveness	Satisfaction	Tested	Brute Force	Dictionary	Spyware	Shoulder Surfing	Social Engineering	Guessing		
12	JETAFIDA Figure 2-13	Eljetlawi and Ithnin [83]	2008	pictures	Entering correct username and select the three saved passwords.	**T**	**Y**	**Y**	**N**	**Y**	**PT**	-	-	-	**N**	-	**N**	Exhibit high usability and user acceptance.	Security evaluation needed.
13	TwoStep a hybrid Figure 2-14	Van Oorschot and Wan [84]	2009	Picture + alphanumeric password	Entering a correct: 1- Username and text password. 2- Select the images from image portfolio.	**N**	-	-	-	-	**PT**	**Y**	-	**Y**	-	-	-	The system is offering a high resistance of security from keylogging and phishing.	The usability of the system requires more attention.
14	Mikons Figure 2-15	Renaud [68]	2009	Digital images	Insert 4 correct mikons from the distractor mikons.	**PT**	**Y**	**Y**	-	-	**N**	-	-	-	-	-	-		• One of the limitations of this study it that it was carried out on a very small sample size and with a young age group of users. • The Mikon drawing tools did not contain a pen or eraser, and were not as flexible as drawing by hand.

NA= Not Available NT= Not Tested T= Tested PT= Partly Tested Y= Yes N= No - = Not Researched

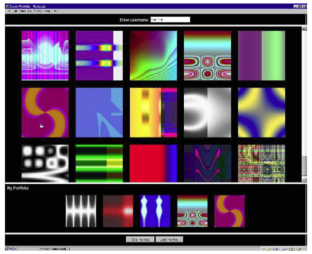


Figure 2-2 Déjà Vu

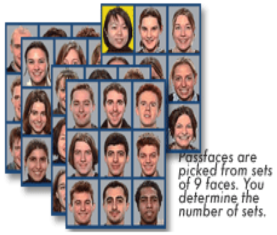

Passfaces are picked from sets of 9 faces. You determine the number of sets.

Figure 2-3 PassFaces Scheme

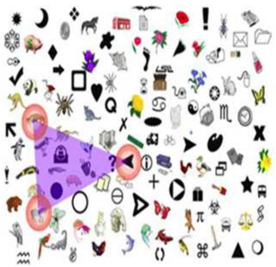


Figure 2-4 Convex Hull Clicks Scheme

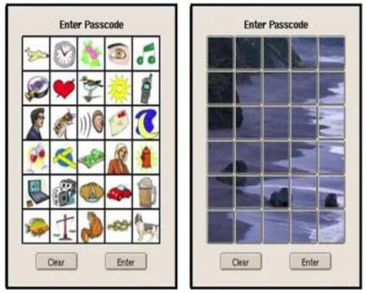


Figure 2-5 Jansen Scheme

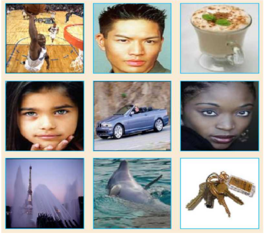


Figure 2-6 Story Scheme

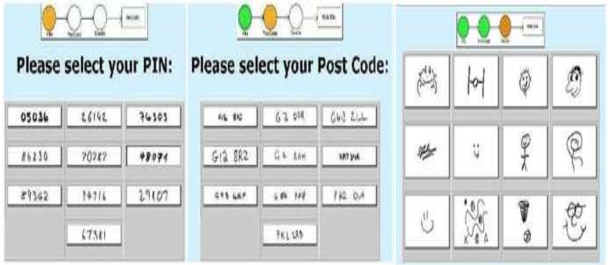


Figure 2-7 Handwing Scheme

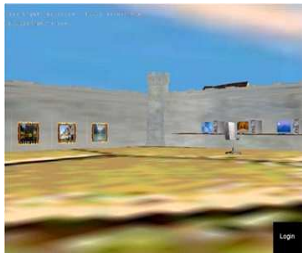


Figure 2-8 3-D Scheme

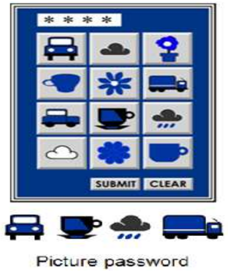


Figure 2-9 Tricerion SMA Scheme

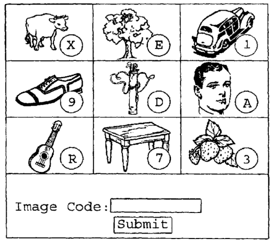


Figure 2-10 VIDOOP Scheme

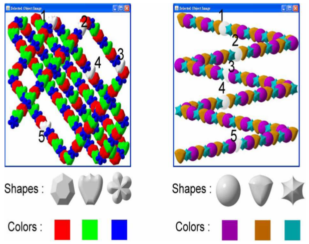


Figure 2-11 RGGPW Scheme

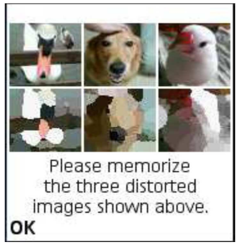
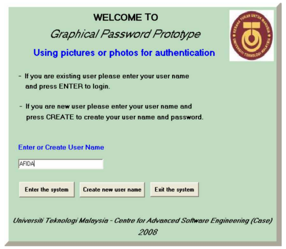


Figure 2-12 Use Your Illusion Scheme



WELCOME TO

Graphical Password Prototype

Using pictures or photos for authentication

- If you are existing user please enter your user name and press ENTER to login.
- If you are new user please enter your user name and press CREATE to create your user name and password.

Enter or Create User Name

AFIDA

Universiti Teknologi Malaysia - Centre for Advanced Software Engineering (Case) 2008

Figure 2-13 JETAFIDA Scheme

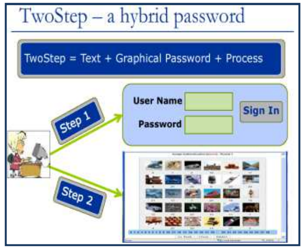

TwoStep – a hybrid password
TwoStep = Text + Graphical Password + Process
Step 1
Step 2
User Name
Password
Sign In

Figure 2-14 TwoStep a hybrid Scheme

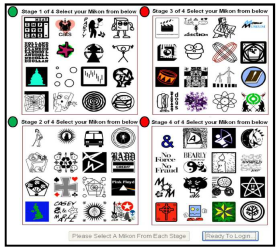

Stage 1 of 4 Select your Mikon from below
Stage 3 of 4 Select your Mikon from below
Stage 2 of 4 Select your Mikon from below
Stage 4 of 4 Select your Mikon from below
Please Select A Mikon From Each Stage
Ready To Login

Figure 2-15 Mikons Scheme

2.4 Recall-Based Graphical Passwords

As the name indicates, under this type of system, users have to produce or recall their password to access the system. These techniques do not provide any framework of hints, context or cues to help users to produce their passwords, such as cued recall systems. The most two archetypal examples for this category are described in the next sub sections.

2.4.1 Draw A Secret

One of the most famous studies of recall based techniques was introduced by Jermyn et al. [85]. Their technique is called Draw a Secret (DAS). The concept of this technique is that users draw their unique password on a 2D grid by using primarily devices such as personal digital assistants (PDAs) which offer graphical input capabilities via a stylus. The users are asked to draw their password on 4×4 grid and to remember the places they drew. The drawing of the password will be encoded into a sequence of coordinate pairs (i.e. the location of the cells). The distinguished coordinate pair will be inserted in the sequence for each “penup” events, for example the drawing in Figure 2-16. Here, the coordinate sequence generated by this drawing is:

(2,2); (3,2); (3,3); (2,3); (2,2); (2,1); (5,5)

Where (5; 5) is the special coordinate pair used to signify a “penup” event which is the place where a pen is lifted from the display surface.

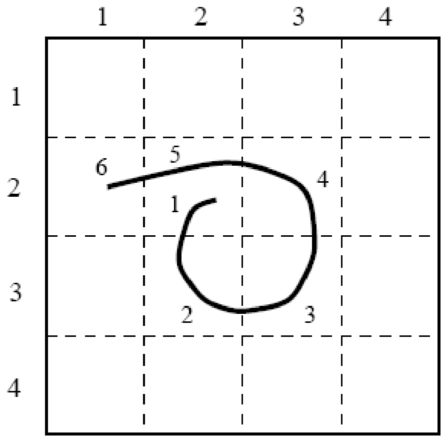


Figure 2-16 Draw a Secret DAS

The authentication stage will be successful if the users redraw their choices correctly in the same order. This technique offers a large password space and a good chance of memorability. The major drawback of DAS is that repeating drawings that are significantly similar is difficult, as stated in the paper: “difficulties might arise however, when the user chooses a drawing that contains strokes that pass too close to a grid-line”. If the drawing of the password is close to the grid lines or intersections, then the scheme may not distinguish which cell the user is choosing. This condition seems to be too strict. Users might get disturbed if consecutive logins fail due to the difficulty of inputting a password. As a result, the cells of the grid must be sufficiently large.

2.4.2 Yet Another Graphical Password (YAGP)

Gao et al. [86] designed a graphical password depending on a recall based technique called Draw-A-Secret (DAS). Yet Another Graphical Password (YAGP) is the name of Gao’s system. YAGP has several features that overcome some of the problems faced by DAS; for example, YAGP offers (1) Free drawing positions where the exact stroke positions are no longer required by encouraging greater user concentration on the image (each drawing will be coded with regard to the stroke’s elements which are pen-down, pen-moving and pen-up on the grid screen, not the position). (2) Strong shoulder surfing resistance in two ways: first, the technique is a position-free scheme, so the user can draw his or her graphical password anywhere on the canvas; for example, on the corner, which makes shoulder surfing a difficult task. Second, the stroke sequence cannot be reflected by the graph in YAGP, and the authentication process notices it as a critical checking factor which leads to the impossibility of repeating the sequences of the strokes. (3) A large password space is obtained by using a more precise grid granularity (see Figure 2-17).

Three experiments were carried out by a sample of thirty users. The first experiment asked users to draw graphical passwords three times in a different grid canvas, and then to redraw them to authenticate them as well as asking their neighbours to examine shoulder surfing possibilities. The second phase of the experiment was designed to find the rational threshold value of similarity (accepted between 55%-80%). Eighteen users were asked to draw their password six times with a different threshold and the results showed the 60% threshold value of similarity to be the most suitable. The third stage of the experiment investigated the memorability of YAGP. The users were asked to perform authentication after two days. The finding was that 27 out of 28 graphical passwords were recalled successfully. Moreover, 15 participants successfully recalled their password after 15 days. Overall, the experiments demonstrated the effectiveness of YAGP.

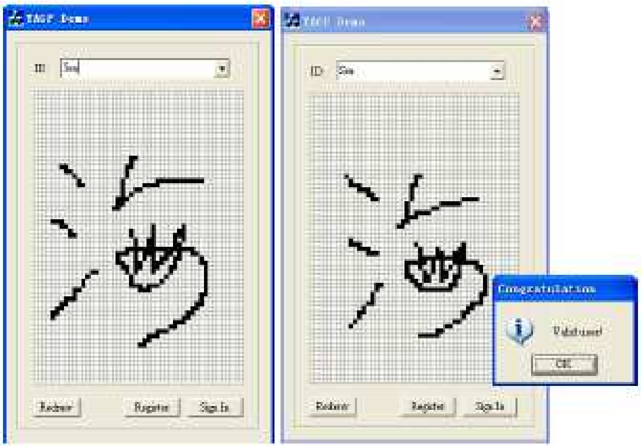


Figure 2-17 YAGP Scheme

2.4.3 Summary and A Comparison of other GUA Algorithms Based on Recall Schemes

Similar to Table 2-1 in the previous section of recognition based techniques, eight graphical passwords based on recall schemes were studied and compared. Table 2-2 shows a comparative on two main factors of graphical password (usability and security).

Table 2-2 Usability Features and Possible Attacks on Recall-Based Graphical Password

No	System	Created By	Proposed Date	Image	Login Interference	Usability					Security							Advantages	Disadvantages
						Tested	Memorability	Efficiency	Effectiveness	Satisfaction	Tested	Brute Force	Dictionary	Spyware	Shoulder Surfing	Social Engineering	Guessing		
1	DAS Figure 2-16	Jermyn et al. [85]	1999	Redraw on grid cells	Redraw such that the drawing touches the registered sequence of coordinates.	T	N	Y	Y	N	T	N	Y	N	Y	N	Y		• Difficulty in redrawing precisely. • This technique offers a large password space.
2	Passdoodle Figure 2-18	Varenhorst [87]	2004	doodles	Is similar to DAS, allowing users to create a free hand-drawn as a password, but without a visible Grid + pen colour, number of pen strokes, and drawing speed.	NT	-	-	-	-	PT	-	-	-	Y	-	-		It has been confirmed that doodles are more difficult to crack as there is a theoretically larger number of possible doodle passwords than text passwords.
3	Grid Selection Figure 2-19	Thorpe and van Oorschot [31]	2004	Drawing on grid cells	Is similar to DAS with Grid selection.	T	N	N	Y	Y	PT	-	-	-	N	-	-	This definitely increases the DAS password space	
4	Doodle as a master password Figure 2-20	Govindarajulu and Madhvanath [88]	2007	doodles	Redraw their doodle using a touchpad or a digitizing tablet.	NT	-	-	-	-	NT	-	-	-	-	-	-		Required expensive equipment.
5	Eye Pass Figure 2-21	De Luca et al. [89]	2008	eye-gestures	Inputs the stroke shape correctly as well as performing the correct eye gestures.	NT	-	-	-	-	PT	N	N	N	Y	N	N		• Technique is the difficulty for the user to perform two strokes in the same direction. • It also requires special eye tracking equipment.
6	YAGP Figure 2-17	Gao et al. [86]	2008	redraw	A user is authenticated if he/she inputs their stroke shape correctly as well as performing the correct eye gestures.	PT	Y	-	Y	-	PT	-	-	-	Y	-	-	• Free drawing positions. • A large password space.	

No	System	Created By	Proposed Date	Image	Login Interference	Usability					Security							Advantages	Disadvantages
						Tested	Memorability	Efficiency	Effectiveness	Satisfaction	Tested	Brute Force	Dictionary	Spyware	Shoulder Surfing	Social Engineering	Guessing		
7	Recall A Story Figure 2-22	Maetz et al. [90]	2009	Picture + background image	The user is required to select the background + (images, positions).	**NT**	-	-	-	-	**NT**	-	-	-	-	-	-	• Offers a large password space, • ease of recall and that, • The password can be printable. • The printed image does not completely reveal the password since the order is unknown and the power of the password depends on the password space.	
8	Recall Based Shape Figure 2-23	Alia et al. [69]	2012	slanted shapes	Users have to know the correct: shape abbreviation, order of drawing shapes and the size of the drawing shapes.	**NT**	-	-	-	-	**NT**	-	-	-	-	-	-	• Shapes and password as strokes on the grid, since the designed shape (shape of stroke) can be easier to remember than text by authorized users. • Large password space. • Resistant to shoulder-surfing	

NA= Not Available NT= Not Tested T= Tested PT= Partly Tested Y= Yes N= No - = Not Researched

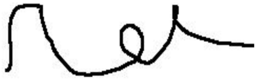


Figure 2-18 Passdoodle Scheme

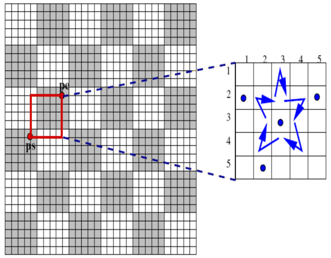


Figure 2-19 Grid Selection Scheme

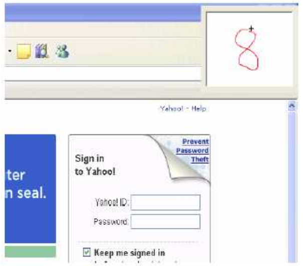
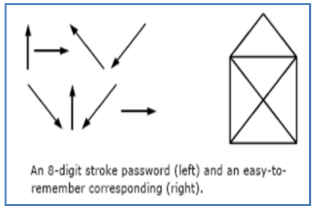


Figure 2-20 Master Doodle Scheme



An 8-digit stroke password (left) and an easy-to-remember corresponding (right).

Figure 2-21 Eye Pass Scheme

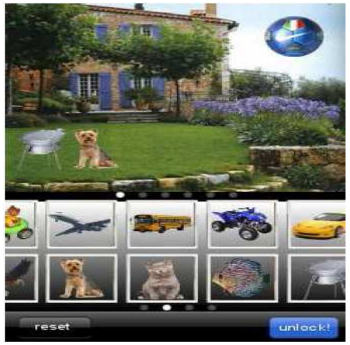
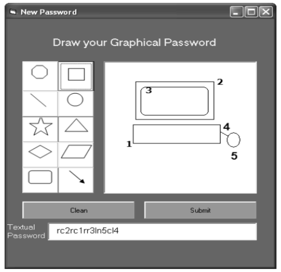


Figure 2-22 Recall A Story Scheme



Textual Password rc2rc1rr3ln5cl4

Figure 2-23 Recall Based Shape Scheme

2.5 Cued Recall Based Graphical Passwords

In pure recall based graphical password schemes, the system will not give any hints or cues to help the users to reproduce their password, whereas the users will be offered a framework of hints, context, and cues to reproduce their password or to help them make their reproduction more accurate in a Cued recall-based system. The most two archetypal examples for this category are described in the next sub sections.

2.5.1 Blonder System

The first recall image based system, was created by Blonder [15] as cited in [91]. They created a scheme that displays a predetermined image such as a horse's face, as shown in Figure 2-24, below. Users need to create their passwords by clicking or touching the various *Tap Regions* in the image displayed. Moreover, they have to remember the location and the sequences of their clicking as this information is needed at the authentication stage. This technique has a similar drawback to most other techniques, which is the limited space of the selection area. Also, users can only select their password from the object of the image, not the background. Furthermore, click-points that fall within some acceptable tolerance of the original points which are part of the design of the image should be accepted by the system since it is unrealistic to expect users to accurately target exactly the same location each time.

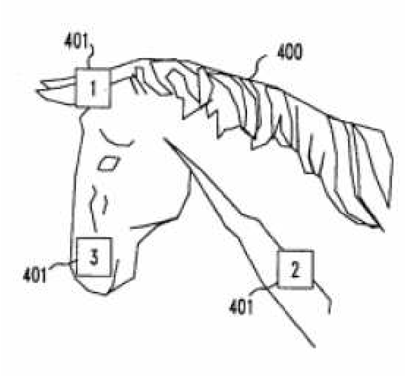


Figure 2-24 Blonder's scheme

2.5.2 PassPoints scheme

In order to cover the image limitations of the Blonder scheme, Wiedenbeck, et al.[92] created a new system called PassPoints. In the PassPoints system any natural picture or painting could be used but at the same time had to be rich enough in order for it to have many possible click points. Acutely, the main purpose of the used images is only to help the user to remember the click point, therefore the existence of the image has no role. User has to select some points on the picture in a certain sequence as password during the registration phase. When logging in, the user only needs to click close to the chosen click points as on the registration stage, and inside some adjustable tolerable distance, say within 0.25 cm from the actual click point. One of the main advantages of the PassPoints scheme is that a user can click on any place on the image which offers a good password space, but the main drawbacks for such schemes are the shoulder-surfing risk and usability problems. (A simple image of PassPoints scheme are shown in Figure 2-25)

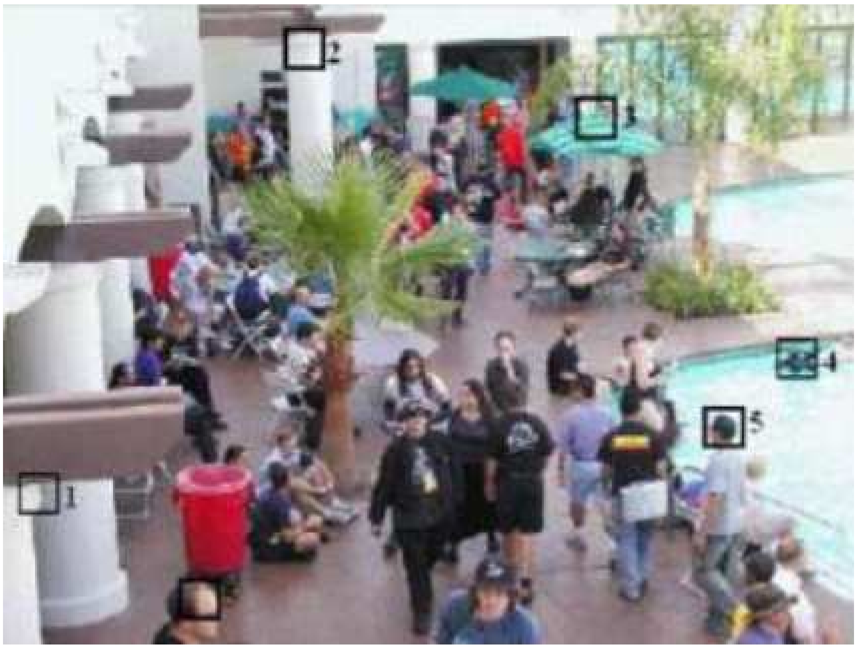


Figure 2-25 PassPoints Scheme

2.5.3 Summary and A Comparison of other GUA Algorithms Based on Cued Recall Schemes

Twelve graphical password based on cued recall schemes were studied and compared. Table 2-3 shows a comparison among these schemes.

Table 2-3 Usability Features and Possible Attacks on Cued Recall-Based Graphical Password

No	System	Created By	Proposed Date	Image	Login Interference	Usability					Security							Advantages	Disadvantages
						Tested	Memorability	Efficiency	Effectiveness	Satisfaction	Tested	Brute Force	Dictionary	Spyware	Shoulder Surfing	Social Engineering	Guessing		
1	Blonder Figure 2-24	Blonder [15]	1996	Face	Click within those tap regions and in a sequence.	T	Y	N	Y	Y	T	Y	N	N	Y	N	Y		If input precision is large password will be easy to crack, if small it will be difficult for the user to tap at exact points.
2	V-GO Figure 2-26	Paulson [93]	2002	Image with objects	Repeating a sequence of actions	NT	-	-	-	-	NT	-	-	-	-	-	-		Weak passwords, password space is small.
3	PassPoints Figure 2-25	Wiedenbeck, et al.[92]	2005	image	Make sequence of click points on image	PT	Y	Y	Y		T	Y	N	N	Y	N	Y	has an advantage in password space over Blonder-style graphical passwords and recognition-based graphical password, such as Passfaces.	Passpoints are difficult to learn.
4	VisKey SFR Figure 2-27	SFR IT Engineering[94]	2005	Background image	Click within those tap regions and in a sequence. images stored in the device	PT	Y	N	Y	-	T	Y	N	N	Y	N	Y	Large password space.	User cannot click where he wants because of predetermined tap regions.
5	Pass Go Figure 2-28	HaiTao[37], Passlogic Inc. Co.	2006	Grid intersection points.	Draw the password using grid intersection points instead of grid cells.	PT	Y	Y	-	N	PT	Y	-	-	-	N	N	Users selected longer passwords and used colour, both resulting in greater password complexity than in DAS	User cannot click where he wants because of predetermined tap regions.
6	BDAS(Background Draw-a-Secret) Figure 2-29	Dunphy and Yan [95]	2007	Back ground image	Redraw the secret on the background image.	PT	Y	N	Y	-	PT	-	-	-	Y	-	-	Using background image helped people to make their drawing passwords more complicated and less predictable, and aid people to re-create them in the correct locations on the drawing grid.	Of course BDAS does not eliminate weak drawings; however it gives users a better environment with which to create a good one.

No	System	Created By	Proposed Date	Image	Login Interference	Usability					Security							Advantages	Disadvantages
						Tested	Memorability	Efficiency	Effectiveness	Satisfaction	Tested	Brute Force	Dictionary	Spyware	Shoulder Surfing	Social Engineering	Guessing		
7	Cued Click Points (CCP) Figure 2-30	Chiasson et al. [96]	2007	Multiple images	5 Single clicks on 5 multiple images.	**PT**	**Y**	**Y**	**Y**	**-**	**PT**	**N**	**-**	**-**	**-**	**-**	**-**	Being cued as each image is shown and having to remember only one click-point per image appears to be easier than having to remember an ordered series of clicks on a single image.	Hotspots still remain an issue.
8	Multifactor click points Figure 2-31	Sabzevar and Stavrou [97]	2008	Two similar Pictures (object + reference)	Click in the locations that match the locations received by the server.	**NT**	**-**	**-**	**-**	**-**	**T**	**-**	**Y**	**Y**	**Y**	**Y**	**Y**	The advantages of this system are that it can be ideal whenever there is a necessity to enter sensitive or private data.	In this system, users are provided with a personal handheld device such as a cell phone to receive the location of the password on the images. Therefore, users have to carry their personal handheld device all the time.
9	Come from DAS and Story (CDS) Figure 2-32	Haichang et al. [98]	2010	A collection of images + curve	Selecting pass image one by one with the same sequence by drawing the curve starting from the given image(red rectangle) ending the image marked with a green rectangle.	**PT**	**Y**	**Y**	**Y**	**-**	**PT**	**-**	**-**	**-**	**Y**	**-**	**-**	CDS has inherited the advantages of the story algorithm and achieved a strong level of security. The difference from the story algorithm is that the user does not need to input a direct password, only to remember the sequence of the password.	
10	Cued recall grid Figure 2-33	Lashkari et al[99]	2010	Grid of shapes	Selecting grid of shapes in different size grids	**T**	**Y**	**Y**	**Y**	**Y**	**PT**	**Y**	**Y**	**Y**	**Y**	**Y**	**-**		The main drawback of this technique was its vulnerability to a brute force attack.

No	System	Created By	Proposed Date	Image	Login Interference	Usability					Security							Advantages	Disadvantages
						Tested	Memorability	Efficiency	Effectiveness	Satisfaction	Tested	Brute Force	Dictionary	Spyware	Shoulder Surfing	Social Engineering	Guessing		
11	CD-GPS Figure 2-34	Deval et al. [100]	2013	Multiple images	Clicking on the images were used in sequence and also to draw a secret on the single image.	**NT**	-	-	-	-	**NT**	-	-	-	-	-	-	• It will be hard for attackers to guess the password. • Users will only be able to confirm that they were authenticated after all clicks have been completed, so it also difficult for any attackers to find out at which image their guesses had been incorrect.	
12	GeoPass Figure 2-35	Thorpe et al. [101]	2013	Google Maps	Placing the selected location “X" marker near his or her previously chosen location.	**PT**	**Y**	-	**Y**	-	**PT**	-	-	**Y**	**Y**	**Y**	-	Large password space.	

NA= Not Available NT= Not Tested T= Tested PT= Partly Tested Y= Yes N= No - = Not Researched

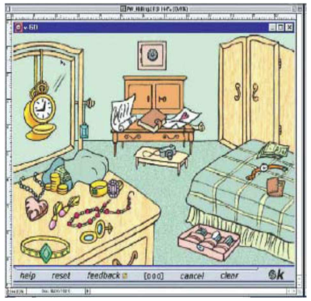


Figure 2-26 V-Go Scheme

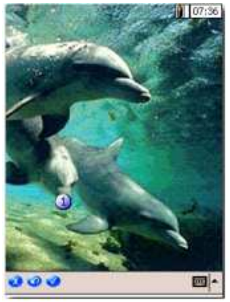


Figure 2-27 VisKey Scheme

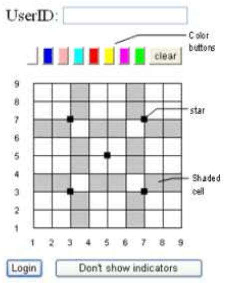


Figure 2-28 Pass Go Scheme

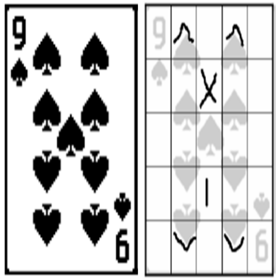


Figure 2-29 BDAS Scheme

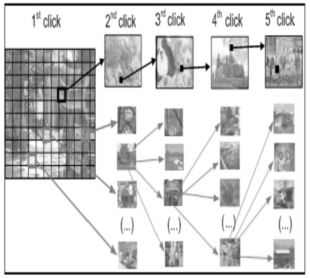


Figure 2-30 CCP Scheme

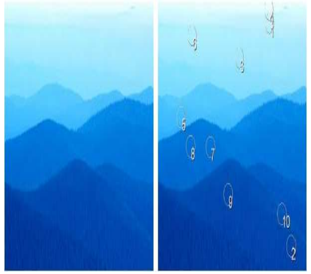


Figure 2-31 Multifactor Click Points Scheme

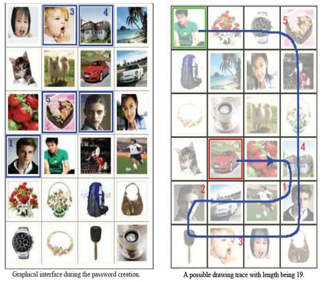

Graphical interface during the password creation.
A possible drawing trace with length being 19.

Figure 2-32 CDS Scheme

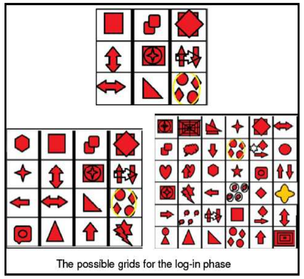


Figure 2-33 Cued Recall Grid Scheme

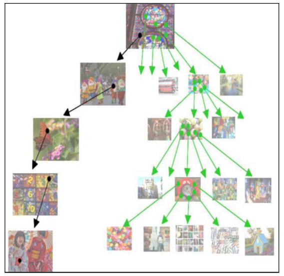


Figure 2-34 CD-GPS Scheme

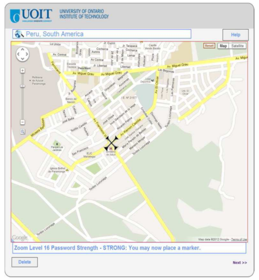


Figure 2-35 GeoPass Scheme

2.6 Hand-Drawn Doodles in Graphical User Authentication GUA

2.6.1 Doodling As a Secondary Task

Andread [59] answered the question: *do doodles improve or hinder attention to the primary task when people are listening to lectures or telephones?* In the study, researchers asked 40 participants to listen to a voice message for a period of two and a half minutes. This message contained some information, such as the names of places and people.

The participants were divided into two groups, with one of the groups assigned to draw some doodles while they listened to the message while the other group listened to the message only. It was found that those who drew doodles during the listening could remember the names better than the other group on an average of 7.5 versus 5.8 for those who did not. Andrade claimed that "*if a person is given a tedious task, such as listening to a telephone conversation which is not important, their mind can wander. This leads to the dispersal of attention and the low level of performance*".

Additionally, the results showed that volunteers who drew doodles remembered the details by 29% more than the volunteers who did not draw, without affecting the main task. Andrade stressed that "*the study indicates that a scribble can be in our daily lives, what we are doing is to help us function better rather than it being a futile entertainment we should refrain from*".

In fact, the first mentioned of using a doodle as a graphical password was by Jermyn et al. [85] as cited in Goldberg et al. [21]. The first published paper designed for using doodles as a recall based authentication mechanism was by Goldberg et al. [21], in which 13 participants took part, each of them being asked to draw their password using a pen and paper as well as selecting a textual password and user name, rather than a real system. This scheme was called "Passdoodles" and was similar to the DAS system. The principle of the scheme is that it consists of at least two strokes, which can be in different colours. The exact order of strokes and the number and direction of the strokes in redrawing the doodle as it was initially drawn is the main part of the authentication stage of this mechanism. The results of this study indicated that the users could recall both their alphanumerical passwords and their doodles (i.e. the components of the visual parts of the doodles). Nevertheless, most of them could not redraw their doodles perfectly. However, the participants observed that the Passdoodle is easy to remember compared to an alphanumerical password and they expected that it would be a more secure technique.

2.6.2 Doodles as generalised signatures

After two years of previous study, Varenhorst [87] investigated the use of doodles as a means of authentication in a pervasive environment by choosing three different recognition methods which were as follows:

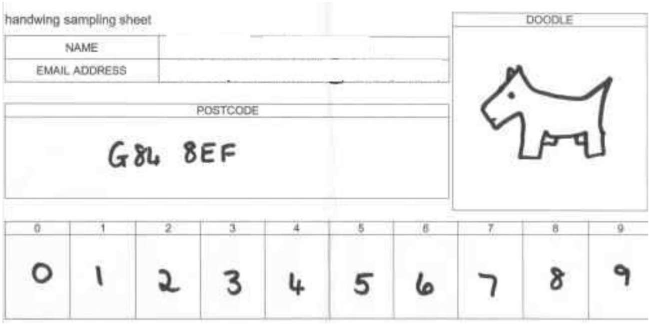
- Distribution grid
- Speed comparison
- Variance in grid

The method distribution grid was applied to boxing the doodle based on its high and low points, stretching it to a grid and combining the doodles for various training purposes, as shown in Figure 2-36, below. The speed comparison examined the speed of drawing the doodles by focusing on the points of the stroke and the distance between the two strokes which is different between different users. The variance in grid measured the variance between the specific doodle’s points over its values on the blurred distribution map. These three methods affected the flexibility of using hand-written doodles. In the study, a sample of ten users was asked to create and then repeat a unique finger trace on a touch screen device. Once it was complete they could see their traces. The conclusion of the Passdoodle study illustrated the possibility of applying recognition technology to new fields such as hand writing and drawing recognition.

Figure 2-36 Example of a Passdoodle

2.6.3 Handwing

Renaud [20, 102], proposed a web authentication mechanism that uses doodles as one of its authentication stages. This technique is called Handwing and was proposed as a safeguard on low-risk sites. This technique was implemented on a low security website for elderly users. All twenty users who were members of a church were asked to create their password by hand-writing some details including individual numerals, doodles and post codes on a provided form such as that shown in Figure 2-37.



handwing sampling sheet

NAME

EMAIL ADDRESS

POSTCODE

G84 8EF

DOODLE

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

Figure 2-37 Biometric Collection form

Users then collected their password generated from the information on the form above by means of their email address. Once they received their passwords three stages of authentication were needed before they could login successfully. Firstly, users had to select the correct PIN number from ten displayed handwriting PIN numbers by recognizing their handwritten digits. Secondly, again as at the same first stage, users had to recognize their handwritten postcode from the ten postcodes displayed on the next screen. Finally, users had to select their hand written doodle from the final screen that displayed twelve doodles. Figure 2-7 shows the three authentication stages. Once users had chosen all three components correctly, they were allowed to enter the website.

The study of twenty elder users (11 females and 9 males) pointed out that during the nine months (the duration of the experiment) only one authentication failure happened as a result of choosing the wrong doodles. This technique demonstrated some security drawbacks such as the probability of recognition of the users' hand writing digits by people who knew them. Moreover, the observability of the system is very high. Additionally, the PINs and the post codes could easily be recorded, whereas doodles are very difficult to guess because the system used over 200 doodles and many of them were similar to the user's drawings.

2.6.4 Choosing Distractors

Poet and Renaud [103],[40] produced an automatic algorithm that prevents the selection of distractors that are too similar to the pass image or to each other, which could confuse users. The basic idea of the algorithm is that it prevents the emergence of similar distractors in the same screen by calculating each doodle's weighted sum, and then comparing it with the threshold rate set by the system. The similar doodles have a weight below the threshold. To achieved the automated classification algorithm three different measurements were taken into account to calculate the sum of doodles' weights, which are the number of separate white regions, the number of separate black regions and the number of joins between lines (see Figure 2-38). The number of white regions, black regions and joins is therefore calculated for each doodle. Moreover, the differences in the number of white regions, black regions and joins are calculated for a pair of doodles. These three differences are combined to form one numbers using a weighted sum. Consequently, the doodles will be considered as similar only if the calculated numbers are below a threshold. The three measurements are processed through a series of operations to be calculated including their connectivity (*thinning, shaving, combining joins and fattening operation*) and joins. The results of this algorithm worked well as long as the threshold was determined correctly.

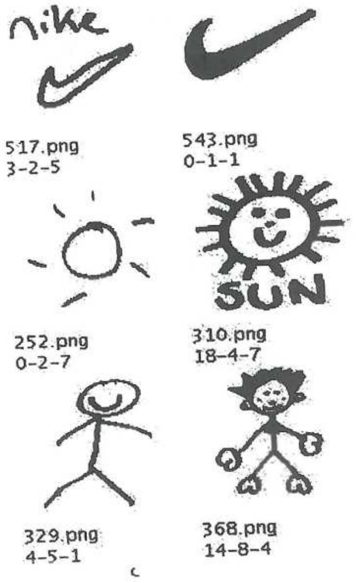


Figure 2-38 Three similar pairs of doodles

2.7 Reviews of Graphical Passwords

A framework called Magic Triangle for Graphical User Authentication GUA was proposed by Lashkari et al.[104] to evaluate the security of graphical passwords, as shown in Figure 2-39.

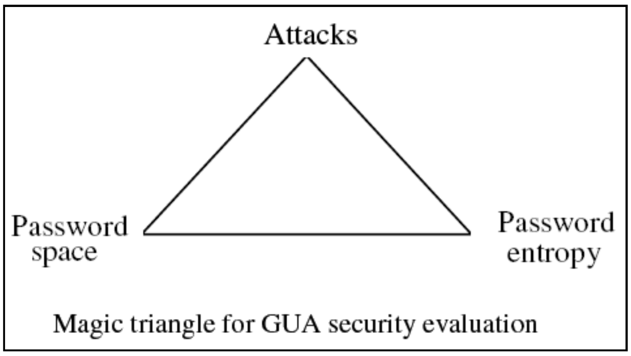


Figure 2-39 Security Evaluation Triangle

This framework was applied and used to evaluate most of the graphical password algorithms and research studies published between 1996 and 2010 that have been mentioned in this chapter. As has been illustrated in the present study, some of the researchers focused on attacks and related their findings on attacks to the GUA algorithm; other researchers focused on password spaces and tried to define a formula for calculating the number of possible passwords in each algorithm. But in surveying these researches up until this point, there had not yet been a complete evaluation framework or criteria that would cover all aspects of security for the GUA algorithm. The triangular evolution framework covered all aspects of security for the GUA algorithm.

2.7.1 Entropy of picture and text passwords

Komanduri and Hutchings [105] drew comparisons between text-based passwords and picture-based passwords in terms of entropy. Many studies have compared text-based passwords and picture-based passwords but none of them have focused on maintaining a measurably high level of entropy. The aim of the Komanduri and Hutchings study was a comparison of character and picture password systems with equal entropy. The study involved 23 participants who were divided into two groups which used picture-based and character-based passwords where both types of passwords had the same strength. The length of the password chosen by the participants both of the pictures and the characters was eight items selected from a set of 80 characters or pictures.

The study allowed nine days for the participants to perform their tasks individually including training and testing on Day 1 and Day 2, up to Shoulder-Surfing Resistant Input on Day 9. According to the memorability assessment in this study, the results found that both character-based passwords and picture- based passwords of very high entropy were easily forgotten because of the use of serial ordering of the input passwords. Additionally, a shoulder-surfing-resistant input method was evaluated too, although the finding was not very successful. Six of the 15 users revealed their password through insecure behaviour (meaning that they were using the on-screen mouse cursor to keep track of password items which is similar to the experiment described in Chapter Six).

2.7.2 Shoulder-Surfing using graphical passwords

The first work on user recognition using two method to select passimages was studied by Hayashi et al.[82] .The authors set out two possible measures to counter against the risk of shoulder surfing. Firstly, they suggest the selection of passimages using entry by keyboard, while in doing so, ensuring that the location of the authentication images are changed each time so that no observer will be able to memorise the key which is pressed to select the location of the image. The second suggested measure to counter shoulder surfing is to guard against having any indication on the screen highlighting which of the images was chosen (this would reduce the chances of successful shoulder surfing).

Hasegawa et al. [106], presented a format combining the low-frequency components of a distractor image with the high-frequency components of the chosen passimage. The method involved the application of a discrete wavelet transform to the passimage and the distractor image. Another suggestion, by Gao et al. [98],was the use of the lowest frequency band of the distractor image (involving an indirect selection of images) was proposed as a safety measure against shoulder surfing in a scheme whereby users would select their passimages in a specific order. To perform authentication, a user has to plot a path through the passimages which they are presented with in grid form, in the right order. However, with this proposal, no study was carried out by the authors which examined whether in fact the approach was effective or not against the threat of shoulder surfing. It does seem that it is an approach which might result in a possible reduction in security because path could be drawn which would cover every image which had been presented, in which case all that would be required would be to establish the right order.

Sreelatha et al.[107], proposed another indirect selection method, whereby a user selects pairs of images and their "key positions" on something known as a challenge screen. A challenge screen is made up of a grid of images as usual, but it requires that a user must locate their passimages in key positions and (rather than selecting the correct image) must select the corresponding pair of images. If only one passimage pair is displayed on the screen, however, this may not reduce the risk of shoulder surfing, as an attacker might view the image selected and repeat this, so the position and identity of the key passimage would not be required. Alternatively though, if multiple pairs of passimages are displayed on the challenge screen, shoulder surfing might be reduced.

Tari et al.[108] presented a study which evaluated the success of shoulder surfing attacks and set out the findings of an exercise which asked users to try to steal the password and passimages of a "victim" by shoulder surfing. Participants were given a notepad and pen and instructed to sit or stand wherever they thought might be most effective. The study employed four different configurations of knowledge-based authentication schemes: PassFaces using mouse selection, PassFaces using keyboard selection, a dictionary alphanumeric password and a strong alphanumeric password. In the exercise, the PassFaces configuration presented five challenge screens, each with nine images displayed. The passwords were five characters in length, in order to provide a comparable length. Characters and passimages had to be selected in the right order; this may have meant that the PassFaces configurations were more difficult to reproduce, and could therefore lead to an overestimation of the resistance to shoulder-surfing in cases where the order of selection is unimportant. If the same set of passimages was used in both of the alternative PassFaces configurations, one possible limitation might be in the form of a learning effect, which may potentially overestimate the success rate of the configuration which happened to be performed second.

The findings showed PassFaces to be the least vulnerable to the shoulder surfing threat, while using keyboard selection (on average, 0.55 images out of five were remembered and reproduced in the right order) while at the other end of the scale, a non-dictionary alphanumeric password was the most vulnerable (on average, 3.65 characters were remembered and reproduced in the right order) [108]. Duncan's multiple range test statistic was employed in order to find out whether a significant difference in performance existed between each different configuration. None was found between a non-dictionary 5 character password and an ordered 5-passface set, but interestingly, it was found that each of the other configurations differed significantly from the others. The study concluded that significant differences in performance could be explained by the variations in setup (e.g. dictionary and non-dictionary passwords, passimages selected using a mouse, and passimages selected with a keyboard). It could be noted that if the same passimages were selected both by keyboard and by mouse then there a learning effect may have been possible.

Two of the latest systems, Pair Pass Char (PPC) and Tricolor Pair Pass Char (TPPC), were designed to resist shoulder-surfing and spyware attacks and were presented by Rao and Yalamanchili [109]. The proposed systems were designed to support keyboard as well as graphical mouse-based input that maps password characters to other regions of the password space. Both schemes support two modes of input, namely, keyboard entry and mouse clicks. In the first scheme, Pair Pass Char (PPC), the image consists of a basic 10x10 character set, whereas the second scheme, Tricolor Pair Pass Char (TPPC), uses the tricolour version of the basic character set where each character appears in three colors: red, green and blue, and is randomly spaced in a 17x17 grid. However, to login to the system, the user has to mix their textual password to produce several pass-pairs, and then follow four predefined rules to get his session password on the login screen. This protocol is also applied in the second scheme, TPPC with more colors and letters.

Twenty computer science graduate students were used in an experiment to test the memorability, usability and login time of both systems. The students were asked to test both systems by using a 4 character password, a 5 character password and a 6 character password for both systems. The study noted that the average time spent in the second system was higher than that spent in the first one with different lengths of the passwords. It was also found that 64% of the participants in the study found the rules for the TPPC scheme to be more difficult to apply than the PPC scheme. Last but not the least, the memorability of the first scheme was found to be much better than the second scheme where users had to remember colored password combinations.

Many proposed graphical techniques that have been designed to be resistant to shoulder surfing are complicated, such as those proposed in the study outlined here and that of Chen et al.[110], where the main concern was security rather than usability. Unfortunately, none of the existing text-based shoulder surfing resistant graphical password schemes is both secure and efficient enough[110].

2.8 Culture effects on computing and drawings

This section briefly describes and examines what culture means and therefore defines the meaning of cross-culture. In addition, it reviews some research on cultural differences in human-computer interaction and examines the potential effects of cultural differences on the usability and the security of recognition based graphical passwords.

2.8.1 Culture

The meaning the word culture is cultivation of soil, as Hofstede [111] points out. However, it also can be defined as "that complex whole which includes knowledge, belief, art, morals, law, custom and any other capabilities and habits acquired by man as a member of society" Tylor [112]. There are many definitions of culture, some very limited and focused such as that of Shweder and LeVine's [113], who view culture as a set of shared meaning systems whereas Kluckhohn believes that:

> *Culture consists in patterned ways of thinking, feeling and reacting, acquired and transmitted mainly by symbols, constituting the distinctive achievements of human groups, including their embodiments in artefacts; the essential core of culture consists of traditional (i.e. historically derived and selected) ideas and especially their attached values"* (quoted in Hofstede [111]).

Hofstede [114] refined the definition of culture based on Kluckhohn's definition: the people carried the component of "mental programs" from their childhood and it was developed during their studying and working lives. Hofstede [111] divides people's mental programs into the three levels of cultural layers: individual, collective, and universal levels.

The individual level of mental programs is a unique level containing individual traits, and is of course not shared between any two people, although part of people's individual level is inherited from their parents. At the collective level of mental programs, people from certain groups or societies share behaviours such as manners of eating, treating parents, and the languages that they speak to express themselves. These behaviours differ from group to group, and can formulate different national cultures. Hofstede [111], [114] states that the collective level or national culture is entirely learned from childhood and not genetically inherited from parents.

Finally, the universal level of mental programs is shared between people around the world and contains normal behaviours such as crying to express sorrow and laughing to express happiness. People inherit most of this level of their mental programs from their parents. These are learned behaviour patterns that are shared by all of humanity, collectively. No matter where people live in the world, they share these universal traits. Examples of such "human cultural" traits O'Neil [115], include:

1. *Communicating with a verbal language consisting of a limited set of sounds and grammatical rules for constructing sentences*
2. *Using age and gender to classify people (e.g., teenager, senior citizen, woman, man)*
3. *Classifying people based on marriage and descent relationships and having kinship terms to refer to them (e.g., wife, mother, uncle, cousin)*
4. *Raising children in some sort of family setting*
5. *Having a sexual division of labour (e.g., men's work versus women's work)*
6. *Having a concept of privacy*
7. *Having rules to regulate sexual behavior*
8. *Distinguishing between good and bad behaviour*
9. *Having some sort of body ornamentation*
10. *Making jokes and playing games*
11. *Having art*
12. *Having some sort of leadership roles for the implementation of community decisions.*

While all cultures have these and possibly many other universal traits, different cultures have developed their own specific ways of carrying out or expressing them.

Working from O'Neil's [115] third cultural layer, no. 11, of having art, the next subsection is divided into two parts: 1- Cultural effects on usability and security of recognition-based graphical password authentication. 2- Cultural effects on drawings.

2.8.2 Cultural effects on recognition-based graphical password authentication

Studying the usability and security of many graphical passwords remains incomplete although they are good in technical terms [38]. One of the very important subjects to be studied in this field is the cultural effects of using images as a recognition based password. Actually, most graphical password systems were developed in western countries, and this could be argued that applying such graphical password schemes in other countries and cultures will involve more attention to cultural impacts, especially, on usability and security. Sometimes the use of these systems is not suitable for users from different countries and cultures (i.e. it is unclear whether the developers considered cultural differences when they designed their schemes, especially the image types which came from a particular culture).

Actually, only very few studies focus on this, for example, Monrose and Reiter [116] carried out a study on a recognition based graphical password scheme. Their study focused on faces, and they examined if the ‘race effect’ of the faces would affect the user’s choice of graphical password. Twelve face type categories were involved in their study: 1- typical Asian male, 2- typical Asian female, 3- typical black male, 4- typical black female, 5- typical white male, 6- typical white female, 7- Asian male model, 8- Asian female model, 9- black male model, 10- black female model, 11-white male model, and 12- white female model. The finding of the study clearly showed that the participants were biased to choose faces that belonging to the same race as the graphical password.

However, user acceptance and user performance are the two main concepts of usability on computerize systems [117], in which culture would have an influence on them. This can be applied on graphical passwords systems as well and the analysis of many graphical schemes shows that there is a relationship between culture and the usability aspects of human computer interaction.

User acceptance is very important for any successful information technology system Davis [118] and Venkatesh et al.[119]. To develop and design any system, developers should be aware of the differences of individuals’ intentions. Studying the differences in the use of these technology systems will help to build a successful system that reflects the cultural differences. However, several cross-cultural studies have shown that user acceptance models (The technology acceptance model (TAM) and innovation diffusion theory (IDT) are two acceptance models developed by researchers Venkatesh et al.,[119]) were highly affected by people’s cultures. Therefore, the culture plays very important factor in using technologies and it has been shown that people from different cultures are vary in their ways of adopting or using technologies [33], [120], [121], [122] and [123]. Finally, social pressure also has a direct impact affecting technology acceptance, which is another important factor [33].

User performance is another goal of developing any computer system. However, the capabilities and limitations of the information processing by the human mind has a great effect on the user’s performance, Ford [124]. Human information processing including retaining, acquiring, and using information, Vockell [125], are divided into two objects Mayer and Moreno[126]. The verbal objects such as words are stored and represented distinctly in verbal form in memory whereas the visual objects such as pictures are stored and represented distinctly in image form in memory and in some cases the objects are processed in the human brain with both image and verbal forms (Paivio [127]).

However, the human information processing works through cognitive processes which include activities such as attention, perception and recognition, learning, reading, and remembering [126], [127]. All these processes are affected by different cultures[128], which lead Boduroglu et al.[129] to conducts a study between East Asian culture and western culture. The finding of Boduroglu et al.[129]'s study showed that people from East Asian cultures handle information processing differently from people from western cultures and this was refereed to different cultural values.

However, not only were the activities mentioned above demonstrated to differ between East Asian and Western people: the researchers also demonstrated cultural effects and differences in the preceding brain images and in drawing. The next section will review several studies concerning cultural effects on visual information processing and drawings.

2.8.3 Cultural effects on Drawings

In contrast to the lack of cross-cultural studies into graphical passwords, cross-cultural behavioral differences in the visual processing of objects and backgrounds as a function of cultural groups have been widely researched. Many studies such as those of Chua, et al.[130], Gutchess et al.[131], Huntsinger et al. [132] , Masuda and Nisbett [133], Nisbett et al. [128] and Goto et al. [134] have demonstrated behavioural differences in the visual processing of objects and backgrounds and ways of drawing objects, between different group of people s and within different age groups.

2.8.3.1 Cultural effects on human image processing

Culture can affect perception and recognition processes, as demonstrated by Abbott [135], with work done in 1970 (cited in Hwang [136]), which showed that Scots are more likely to focus on the various parts of a whole, whereas Chinese are more likely to look at wholes. Abbott showed a picture containing a boat under a tree to two groups of teenagers, Scottish and Chinese, and then asked them to write a story about what they saw in the picture. The finding of his study showed that the majority of the Scottish mainly focused on the boat rather than the whole picture in their narratives, whereas the Chinese did not include the boat in their stories or only mentioned it lightly without going into great detail. The Chinese narratives focused on whole picture and discussing the general view without going into details whereas the Scottish narratives focused on subjects on the picture and discussed them with more details.

Another study showed that people from different cultures focus their attention differently on the same case Masuda and Nisbett [133]. The study conducted between two cultural groups: 63 American and 41 Japanese students and it divided into three phases. The first phase, the participants were asked to look at ten short animated underwater scenes consisting of fish and other marine animals such as bubbles, snails , coral reefs, and smaller fish in the a background and then to write an essay about what they had seen. American participants were less focused and concentrated on the background objects in their essays than the Japanese participants. The relationships between the different objects in the scenes were considered more Japanese participants than the American participants.

In the second phase, the participants were shown 90 pictures: half of the pictures contained objects that were included in the ten scenes and the other half contained objects that were not included in the ten scenes. Three types of backgrounds with the 90 pictures were presented to the participants: the original background of the object as previously seen in the first phase, a novel background, and no background. Thus, six different types of pictures were presented:

1. original objects with original background
2. original objects with no background,
3. original objects with different background,
4. novel objects with original background,
5. novel objects with no background, and
6. Novel objects with new background.

The participants were then asked to determine if they had or had not seen each object during the first phase. According to the results of this phase, American participants were less affected by changing the original backgrounds of objects and they are still recognised them. In contrast, the Japanese were not easily able to recognise the original objects if their original backgrounds had changed.

It has been noted that the environment could have effaced the Masuda and Nisbett [133] result and it could be argued that Japanese are more familiar with underwater life than Americans, because of their island geography. Therefore, Masuda and Nisbett [133] conducted another object study with different objects, using animals living in America with American landscapes to respond to that argument. A sample of 44 Japanese and 41 American participants were selected and asked to view 48 pictures of American animals. Half of the pictures containing animals from the previous study of Masuda and Nisbett were shown to the participants and the other half contained different animals and all the pictures were embedded either with their original background or a new background.

Thus, four different types of pictures were presented to the participants:

1. original object with original background,
2. original object with new background,
3. new object with original background, or
4. new object with new background.

Again, the participants were asked to answer if they had seen the pictures in the first part of the study or not, and participants were not advised that there would be a recognition test during the process, so as not to elevate their memory functions artificially.

The finding of this study clearly showed the there was no difference from the result gathered from the previous study and the American participants focused on the central objects of the pictures, the objects (American animals), whereas Japanese participants were more likely to look at the complete pictures and link their elements together. The Japanese participants were also more highly affected by changing the background of the original objects than the American participants.

From the Masuda and Nisbett [133] study, it is noted that the recognition response times by the Japanese participants were faster for recognising an object on its original background than for recognising it with a novel background. Therefore the recognition response time was tested and then the result analysed for both Japanese and American participants. The Japanese were more likely to link the object with its background instinctively, whereas the American participants had no significant difference in response time recognising objects against the original background or against a novel one. Overall, the recognition response time of Japanese participants was faster than the American participants.

However, most studies mentioned in this section made a comparison between East Asians and Westerners in their visual processing as well as being object focused, and in summary, they showed that the East Asians are focusing more on the background of the images whereas the Westerners are focusing on the objects. Thus, overall, it can be concluded that people from different cultures look at pictures in measurably different ways (Goh, et al [137]).

2.8.3.2 Cultural effects on ways of drawings objects

For the past two decades, cultural and cross-cultural perspectives on human behavior have found their way increasingly into mainstream psychology [138]. Many psychological association journals have highlighted more and better studies on culture in the world, explaining our understanding of human behaviour in cultural contexts. Even though our understanding of the role of culture as human psychology is rapidly growing, one area still largely ignored is the cross-cultural study of creativity. However, creativity is involved in a wide range of activities which have been studied by researchers [139], including creating significant art works and architectural structures, and writing novels and poems, as well as minor forms of creativity that occur in daily life. In fact, the 1960s and 1970s had the highest number of cross-cultural or cross-ethnic studies reviews and research conducted on creativity [140] and, creativity and culture [141].

One of the creative activities of the cross-cultural research described in this section is drawing. Particularly, many previous studies highlighted this activity in term of cross-culture among cultural groups with different ages and gender and also drawing tasks were investigated in many areas. For example, drawings created in response to verbal stimuli such as “earth from an insect’s point of view” or “the beginning of time” [142], drawings created after viewing visual images [143], the Draw-a-Person test [144], and drawings of fantastic animals [145] were investigated in drawing tasks.

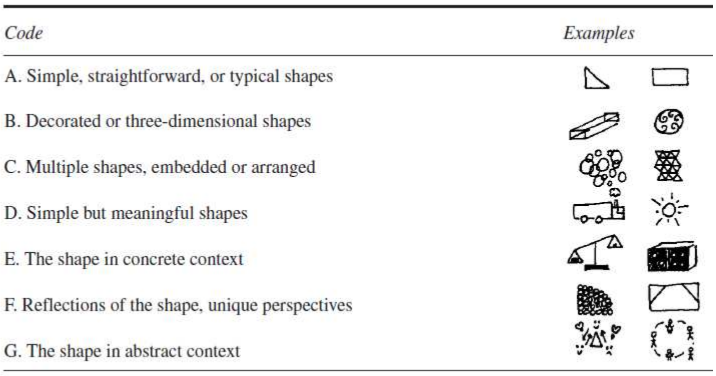
Only a little research has been done on culture and creativity since the 1970s [138], and most of these studies on drawing compared two main cultures, Western and Asian, especially, American and Chinese [138], [132] and[146].

However, one of important studies done in this field of cross-cultural drawing is by Chen et al.[138] .The study addressed three research questions: Q1.Are there cultural differences in the judgment of drawing creativity? , Q2. Are there cultural differences in the average levels of creativity in drawings? , and Q3. Which features define creative drawings within and across cultures?

A sample of 50 European Americans and 48 Chinese were selected from a larger sample in the United States and China and asked to draw representations of geometric shapes. Participants were instructed to draw three geometric shapes pictures with the titles of Triangle, Rectangle and Circle. The group of participants was divided into two halves to ensure that cross-cultural comparisons were not confounded by testing conditions, which influenced by explicit instructions to "be creative" or not. The first half were randomly assigned to a "be creative" condition, whereas the other half were assigned to a "standard condition" (i.e., no explicit request for being creative).The be-creative condition was "Drawing Creatively this task involved drawing creatively and participants were asked to create a drawing that was highly creative and imaginative and to create drawings that are both original (novel, uncommon) and also appropriate (artistically effective). The standard condition was, "Visual Imagery" this task involved drawing visual images in response to verbal stimuli and participants were asked to make drawings that the participant personally found intuitively or subjectively appealing. Approximately 10 minutes were given to the participants to complete the tasks and draw a set of eight drawings (only the three geometric shapes are examined in the study).

A 4-inch by 5-inch index card was used to present each drawing after it was removed from its original packet. Eight Chinese judges (four male and four female) in China and six European American judges (two male and four female) in the United States evaluated each of these 294 original drawings. All the judges were undergraduate students. They rated all drawings along four dimensions: uniqueness (was defined as the degree to which the drawing showed a novel representation), technical quality (was defined as the degree to which the drawing demonstrated technical artistic ability), creativity, and liking (using judges' own subjective definition of creativity on their subjective reaction to the drawing, respectively) using a 5-point scale.

Finally, two independent coders (who did not participate in the previously described judging task) coded each drawing according to seven thematic categories (see Figure 2-40).



Code	Examples
A. Simple, straightforward, or typical shapes	
B. Decorated or three-dimensional shapes	
C. Multiple shapes, embedded or arranged	
D. Simple but meaningful shapes	
E. The shape in concrete context	
F. Reflections of the shape, unique perspectives	
G. The shape in abstract context	

Figure 2-40 Drawing Codes

The results of Chen et al.[138], showed a high consensus between Chinese and European American judges, and the two groups were similar in rating the creativity of drawings. Furthermore, Judges liked best those drawings they judged more creative. Representations of geometric shapes in contexts (either concrete or abstract) involved in this experiment were considered the most creative drawings. These results run counter to the belief that there are wide cultural variations in the evaluation of and attitudes toward creativity, and demonstrate the feasibility of cross-cultural comparisons.

Another earlier study compared a drawing task among culture groups: Huntsinger et al. [132] conducted a cross-cultural study on drawings between second-generation Chinese-American and Caucasian-American young children. The study had two purposes: firstly to determine whether differences in drawing performance, creativity, and the related skills of visual discrimination, fine muscle coordination, and spatial ability exist between the two groups. The second purpose was to determine which parental beliefs and practices are associated with the performance difference, if one exists.

A total of 80 volunteers were recruited in this study, divided into 40 Chinese-Americans (10 preschool girls, 10 preschool boys, 10 kindergarten girls, and 10 kindergarten boys) and 40 Caucasian-Americans (10 preschool boys, 10 preschool girls, 10 kindergarten boys, and 10 kindergarten girls). All volunteers were tested individually in a comfortable setting in their day care centre or in their home. They were tested on many parts, including: 1-Test of Early Mathematics Ability, 2- Children were asked to draw a picture of a person by making the very best picture that they can. 3- Visual discrimination. 4- Spatial relations. 5- Name writing tasks. For the second purpose, parents were interviewed and asked to answer a questionnaire on demographic information and educational attitudes. For the drawing task, the Harris-Goodenough scoring test[1] was used to score the all drawings, carried out by a graduate art student who was blind to the ethnicity of the children and rated the drawings for creativity on a 5-point Likert scale, with 1 representing "least creative" and 5 representing "most creative." Creativity was defined as the addition of unusual or unique elements to the drawing.

The results indicated that Chinese-American young children were more advanced in their drawing and handwriting than were Caucasian-American children and the drawings of Chinese-American children were rated as more creative. It was also found that Chinese-American parents set aside more time each day for the child to focus on fine muscle activities than did Caucasian-American parents.

2.9 Summary

As the purpose of this research which is investigating the usability and security of recognition based graphical password based on hand drawn images. This chapter has mainly focusing on five literature areas: Firstly, the usability and the security of recognition-based graphical passwords. Secondly, graphical passwords based authentication. Thirdly, the memorability of self-performance tasks. Fourthly, the use of hand-drawn images as graphical password. Finally, cross culture on human-computer interaction and drawings.

However, this chapter has summarised the prior literature related to graphical passwords, focusing upon recognition-based graphical passwords as self-performance tasks. In most cases, the user chooses their pass images from a system supplied collection. This speeds up the registration phase, but the pass images may be less personal and thus less memorable. A number of studies have used faces which have revealed a number of problems. Some faces are chosen more often than others, making it easier for an attacker to guess them. There is some literature on systems when the user supplies the pass image, either as a photograph or by drawing or creating a simple image. Research in this area has focussed on memorability. This has revealed a gap in the literature relating to cultural effects when creating simple images and issues of scale when registering user created simple images. This thesis helps to fill this gap in knowledge.

[1] Goodenough scoring test is a psychological projective personality or cognitive test used to evaluate children and adolescents for a variety of purposes.

Also, this chapter has shown that recognition based systems are easier to use than other systems because it is easier to recognise an image when seeing it again than recall it all over again. Recall based systems might seem to be more secure, but in practice, a user will only be able to approximate his earlier actions, for example, when drawing a secret or selecting click points. The login system will need to make allowances for this, leading to a reduction in security.

Within recognition based systems, user performed tasks are easier to remember than system provided images. However, there is an additional administrative load involved in processing the user supplied images at registration time. Chapter Five looks at how this task can be automated.

Moreover, the use of hand-drawn images as a graphical password is a subject to one of a very important field which is cultural characteristics. To see if there is a relationship between the users' hand- drawn passwords and their culture, a study of investigated which aspects of user-drawn images for authentication among cultures was most important, and also exploring the guessability of these hand-drawn images. Actually, the literature reviews showed very few cross-cultural studies achieved in graphical password based on recognition authentication. Chapter Three and Chapter Four address the effects of culture on the use of hand-drawn images as recognition based graphical passwords.

Chapter Three
Cultural Aspects of User Drawn Images for Authentication

3.1 Introduction

Graphical passwords, like any password, can be attacked. The types of attack on Recognition, Recall and Cued Recall based techniques are different. The main attack types on recognition based techniques are categorised into the three areas of concern [147]; *guessability, observability* and *recordability*. Guessability refers to the probability that an attacker can guess the user's graphical password, observability refers to the probability of an attacker being able to observe the authentication process of the graphical password and recordability refers to the probability of an attacker being able to obtain a user's graphical password from a description of it. In this chapter, the guessability attack will be investigated in terms of 'how cultural reasons affect the choice and use of hand-drawn images as graphical passwords'. In other word, a social engineering attack where the attacker tries to guess the correct image based on either the previously acquired information or cultural knowledge about the user.

This study investigates these cultural aspects as they apply to the use of simple images, such as doodles, in the context of a graphical authentication system. Additionally, an investigation of how the cultural factors affect the choice and use of doodles as graphical passwords will be taken into account in this study. In fact, the present study is a combination of computer science and psychology. The computer science part is concerned with the use of hand drawn images in the information security field. An example of how the psychology biases effect the selection of images as graphical passwords was introduced by Monrose and Reiter [116]. Recognizing faces from the same race as the subject is easier than recognizing other races, a phenomenon known as the "race effect" [148, 149]. Monrose and Reiter found that there was significant correlation between participants' selected pass faces and their race and gender and they found the theoretical "race effect" to exist in a recognition-based graphical password system.

Similarly, behavioral differences in image processing between different cultural groups have been well documented by many studies such as [130], [131], [132], [133]. One of the most important recent studies was that by Goh et al.[137], which compared Asian and Westerners' focus on image features. The most important finding was that East Asians spend more time focusing on the background of images, such as groups of people, while those from a Western culture tend to be more focused on foreground objects, such as an individual person. And also it supports the findings of the studies that mentioned in Chapter Two

A recent investigation of how cultures play a role in selecting pictures as graphical passwords was presented by Aljahdali and Poet [150]. This study is one of the latest studies in this field and its central idea was similar to that of the present study which is published in this thesis approximately three years after this work was completed. The results showed significant cultural impact on the pictures chosen by participants in two different countries (Saudi Arabia and the UK). The differences between the Aljahdali and Poet study and the present research are highlighted in the Table 3-1, below:

Table 3-1 Comparison of Aljahdali and Poet and presented study

	Aljahdali and Poet (Pictures)	Present research (Hand drawn images)
Similarity	Studying the cultural impact of chosen images as graphical passwords.	
Groups Comparison	Comparison between Arabs (Saudis) and Westerners(British)	Comparison between Arabs (Libyans), Westerners(Scots) and Africans (Nigerians)
Main Differences	Using Pictures	Hand drawing own images
Task	System provided the images	Self-performed task, users drew the images
Resource	Limited Choice	Unlimited (Own Creation)
Method	On System	On Paper (questionnaire)

In our study, users from different cultures were asked to provide doodles that could be used as graphical passwords. They then filled in a questionnaire giving their views on the usability and security of the system. Finally, the submitted doodles were analysed to detect any cultural bias in the doodles provided by the users.

3.2 The aim of this study

There are three approaches to a guessing attack [147]:

1. Random guessing;

2. Guessing based on predictable user choices for a population of users (group bias);
3. Guessing based on an individual user's preferences (individual bias).

In this chapter, the 2nd approach is discussed. The aim is to investigate the cultural aspects of chosen doodles between three cultures and to examine if there is a relationship between the doodles drawn among the three cultures which may affect the problem of attacks against a user's pass image set in recognition based authentication scheme. The chapter will also address the following question:

Q. Does culture play an important role in the selection of hand-drawn images as graphical passwords by Libyan, Africans (Nigerians) and Westerners (Scots)?

As consequently, the hypothesis can be defined as:

H1: Many hand-drawn image passwords can be recognised by the cultural features that the image contains.

3.3 Experimental procedure

3.3.1 Participants

The population of this study came from three different regions: the Arab world (Libyans), Africa (Nigerians) and the Western world (Scots). A total number of 237 participants took part in the study, the majority from Libya and the next subsection illustrates this information in detail.

3.3.1.1 Libyans

A total of 152participants from Libya took part in this study.More than 95%were undergraduate students from Misurata University, from the Faculty of Education and the Faculty of Information Technology, while the others were from the Higher Institute of Comprehensive Occupation, Misurata, and the Higher Institute for Training of Trainers in Misurata. There were 34 males and 118 females in the age range of 18 – 60, with a mean age in the range of 21-30.

3.3.1.2 Nigerians

Twenty Nigerian students studying in Glasgow also took part in this study. Nearly two-thirds of the participants were postgraduate students at Glasgow University, the same environment as the Scottish participants who are detailed in the next subsection. There were 14 males and 6 females all aged from 21 to 30.

3.3.1.3 Scots

A total of 65 Scottishparticipants from Glasgow also took part in this study, and they represented Western culture. They were from the Engineering and Biomedical schools in Glasgow University and also from the Business School and School of Life Sciences of Glasgow Caledonian University. They numbered 29 males and 36 females with average ages in the range 21-30. More than 50% were postgraduate students.

3.3.2 Method

The participants were given a questionnaire which was divided into two main parts. Most of the questions were multiple choices. The questions with a limited range of answers utilized a tick box method to select the appropriate answer(s). The first part included general questions on computer usage, while the second part introduced the participants to using simple drawings as passwords. They were asked to draw 4 doodles that they might use as passwords and then, finally, to report their feelings about the drawings. The questions asked were:

General and everyday life questions:

1. Gender
2. Age with answered of age group (10-20,21-30,31-40,41-50 and >60)
3. How would you classify yourself? With 7 answers categories (African, Arab, Asian, Australian, European, Hispanic and other).
4. How long have you been living in the UK?
5. Level of education (Primary school, High school, Undergraduate, Postgraduate or uneducated).
6. Number of different computer accounts with scale answer group (0, 1-5, 6-10, 11-20 and >20)
7. Number of different passwords with scale answer group (0, 1-3, 4-8, 9-15 and >15).
8. How often do you use the computer? In hours.

9. How often do you use the the internet?In hours.
10. How often do you have to use a password? In times.
11. Do you like a drawing?
12. Have you constructed drawings using a computer?

Another five questions were asked relating to the graphical password:

13. Would you be happy to provide doodles as passwords?
14. Please draw four doodles in the boxes below, assuming that these doodles will represent your passwords?
15. How long did that take you? In minutes.
16. How much did you enjoy making the drawings?
17. Do you think a friend could guess your doodle when shown a collection of doodles?

3.3.3 Data collection

3.3.3.1 Libya

The data was collected during lectures with permission of the lecturers. All the data was collected between the 23th and 27th of May 2010. Approximately 180 questionnaires were distributed and 152 were returned. The participants had approximately one hour to complete and return the questionnaire (see Appendix A).

3.3.3.2 Glasgow (Scots and Nigerians)

In this case the data was not collected during lectures, and not all the participants were students. The data was collected between 15th of May and 8th of June 2010. Approximately 90 questionnaires were distributed and 85 were returned. They took an average of one hour to complete them too.

3.4 Results and Explanations

This section is divided into two main sub sections regarding the types of information collected: the differences between cultural groups in computer usage and the differences between cultural groups with regard to the collected drawings.

3.4.1 Computer Usage

The results presented in this section are drawn from the data collected from the three different groups on how they deal with their computer accounts and passwords daily uses of computer. This is important to give a clear picture of their security behavior and experience of using a computer [151], and therefore their ways of dealing with passwords, and also whether or not they are familiar with using visual images such as doodles as passwords.

3.4.1.1 Number of Computer Accounts

Figure 3-1shows the number of computer accounts held by the three cultural groups. The most striking result is that a large number of Libyans did not have any computer account, while only a small number had more than five. On the other hand, almost all of the Scots and Nigerians participants had at least one computer account. About 70% of the Nigerians had between 1-5 computer accounts while more than half of the Scots had more than five.

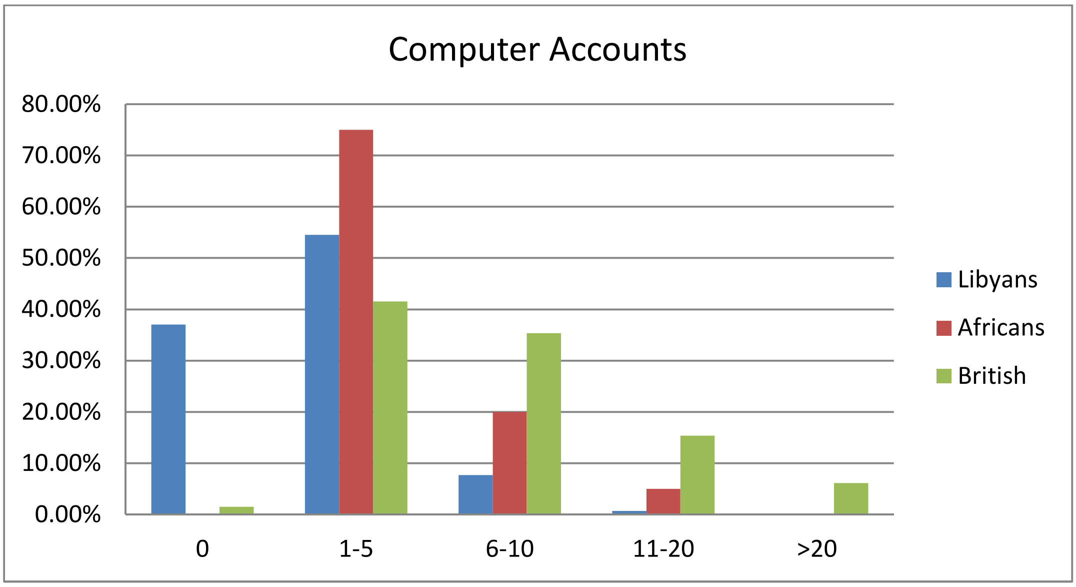


Figure 3-1 Computer accounts held by the three groups

3.4.1.2 Number of passwords

Figure 3-2 illustrates the number of passwords held by the different groups. Not surprisingly, the Libyans without computer accounts did not have any passwords. As expected, the shape of the data for all groups in Figure 3-1 and Figure 3-2 is very similar. It should be noted, however, that the horizontal scale is different. It is also evident that the Nigerians and the Scots are similar to one another with regard to the number of passwords held. 42% of Scottish subjects had between 1-5 computer accounts, while 48% had between 1-3 passwords. This indicates that some of the participants were using the same password for more than one account. Also, the more accounts a user had, the more they reused their passwords. It is also notable that several users had many passwords, with 8% of Scottish having at least nine.

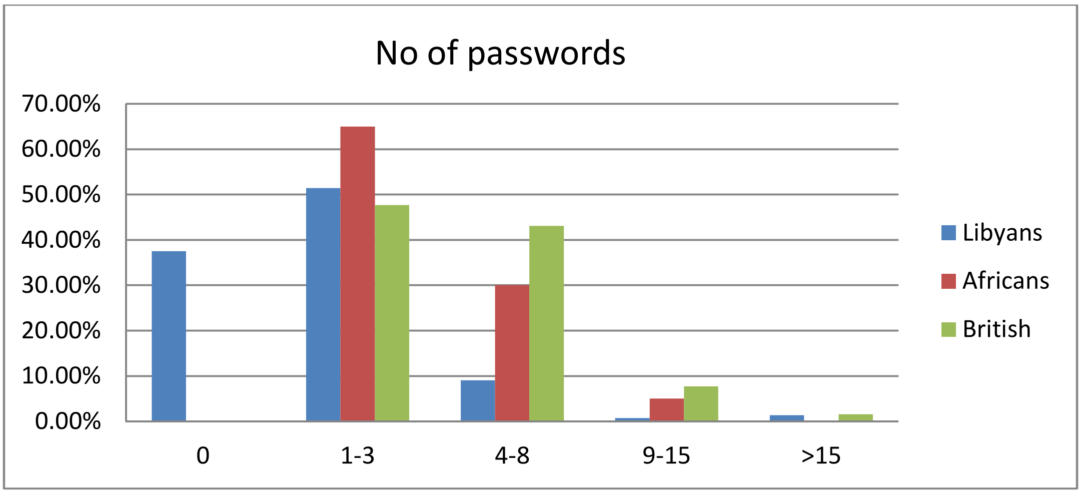


Figure 3-2 Number of passwords held by the three groups

3.4.1.3 Average usage of passwords

Figure 3-3 shows the average number of times passwords were reported as being used on a daily, weekly and monthly basis by the three groups (Libyans, Nigerians and Scots). The average use of passwords by Westerners and Nigerians is larger than for Libyans. The daily average use of passwords is five times higher for Nigerians in comparison to Libyans. This is almost certainly due to the number of computer accounts and passwords that the Libyans held.

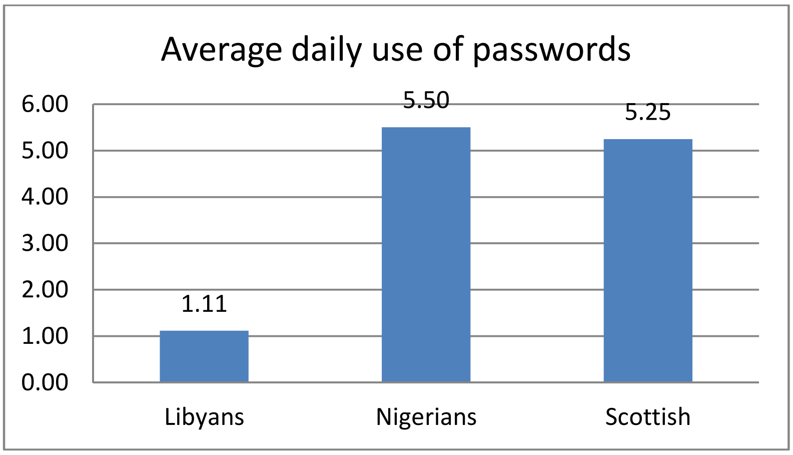


Figure 3-3 Average usage of passwords in times

3.4.1.4 Average computer usage in hours

The use of computers differs from user to user in all areas, for example, access to the internet, use to play games, and learning. However, as can be seen in Figure 3-4, approximately 6.5 hours were spent daily by Nigerians and Scots on computers, and just over 3 hours on average were spent daily by Libyan participants.

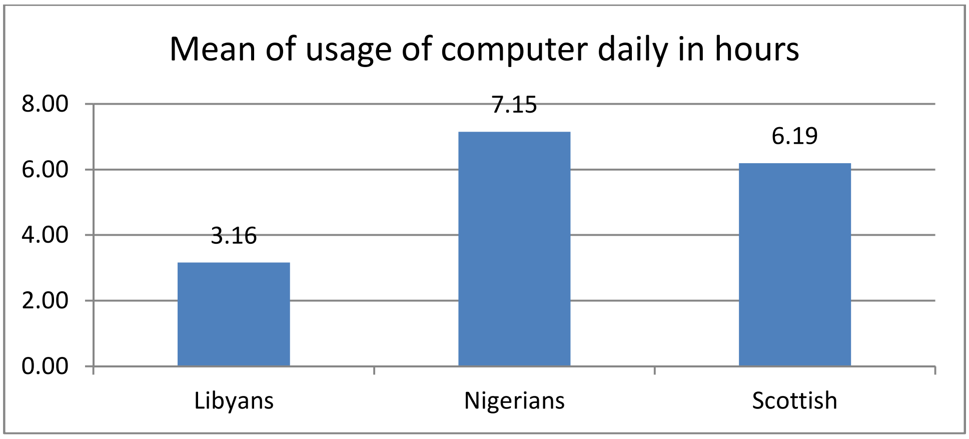


Figure 3-4 Average computer usage daily, in hours

3.4.1.5 Average usage of the internet in hours

The internet is the greatest communication network used by people around the world and many of them spend a great deal of their time on the internet. Nowadays, many network providers offer increased opportunities to use the internet via smart phones and tablets. Although the internet is a very important resource of information for students, some countries and universities do not have widely accessible facilities. Figure 3-5 displays the average time that the participants spend on the internet. Overall, the average time spent on the internet by Scots and Nigerians was much higher than the average time spent by Libyans.

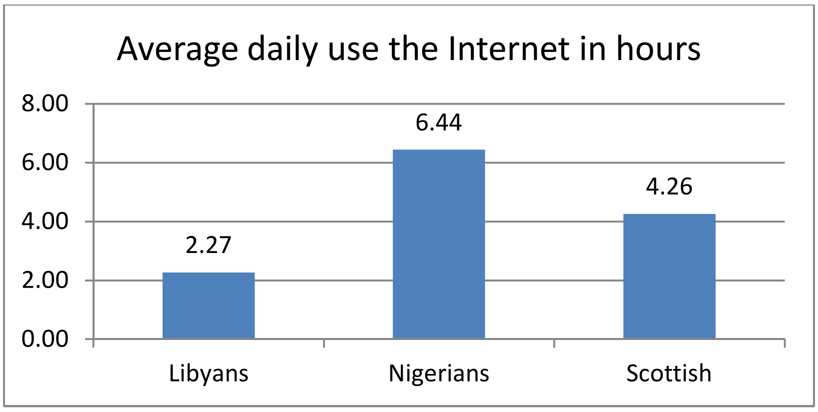


Figure 3-5 Average usage of the internet, in hours

As can be seen from the result in this section of 3.4.1, the Libyans are less using computer than either Scottish or Nigerian. This could affect the idea of using hand-drawn images as a graphical password. However, the next section is exploring the results of using computers on drawing on one hand and if the participants would like to use their hand-drawn as graphical password on the other hand.

3.4.2 Hand-drawn task

In this subsection three issues are associated with creating drawings by hand. These comparisons are directly related to drawing and using hand-drawn images as graphical passwords.

- **Enjoying Drawing:** At this point of the research, the results showed that the percentage of Scots who enjoyed drawing was less than the percentage of Libyans and Nigerians and with the comparison shown in Figure 3-6, it can be observed that the figure is as follows: just under 60% for Scottish and nearly 70% for Libyans and Nigerians. Participants answered the question of whether they liked to draw or not and they were asked to provide the reason why they do not like it, if this is the case.

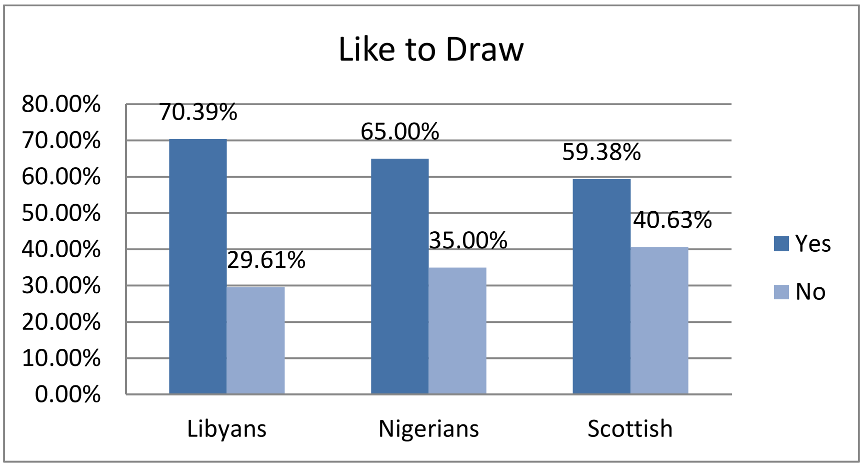


Figure 3-6 Participants' drawings preferences

- **Using the computer for constructed drawing:** Interestingly, despite the results illustrated in Figure 3-7, although many Libyans liked drawing, about 90% of them had not used a computer to construct a drawing. Furthermore, approximately 8% of the Scots who said they enjoyed drawing had not used a computer to construct drawings whereas most Nigerians who liked drawing had an experience with drawing on a computer. Again, participants were asked a question as to whether they had used the computer for drawing or not.

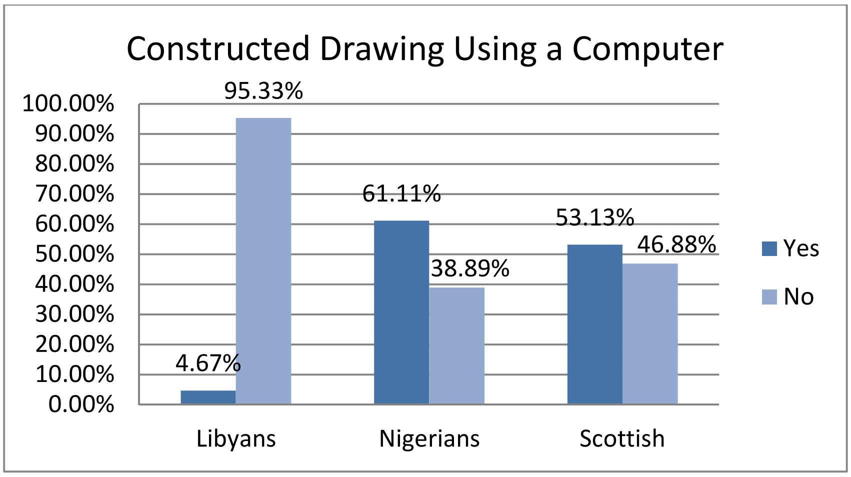


Figure 3-7 Constructed drawings using a computer

- **Would they enjoy using doodles as password**: Three scales were used to answer the question of the enjoyment of providing hand-drawn images as graphical passwords: Yes, No and I do not know. Regardless of the manner in which they use hand-drawn images as graphical passwords, most of the search results in this experiment shown in Figure 3-8indicate that approximately 45% of Scots did not know if they wanted to use hand-drawn images as passwords or not. In addition, about 32% of them did not agree to use doodles as graphical passwords and fewer than 20% would accept the use of hand-drawn images as password, similar to the level expressed by the Nigerians. In comparison with the Libyans, it can be seen that just over 55% of them agreed to use doodles as passwords and the percentage of the Libyans who did not agree and did not know if they would provide doodles as passwords are the same at 20%.

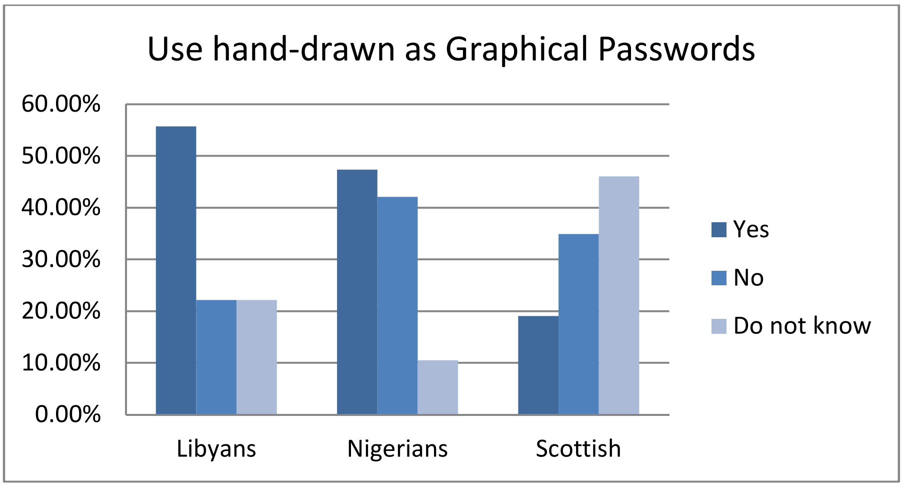


Figure 3-8 Like to use hand-drawn as graphical passwords

3.4.2.1 Complete drawing task

Most of the participants of this study completed their hand drawings of four images. A scan be seen, about 90% of the Scots completed the task successfully (61 out of 66), while 3% of them did not draw and 6% did not complete the drawing task, and this can be related to their enjoyment of drawing as stated in their answers. Additionally, approximately 95% of the Nigerians (18 out of 19) completed the task and only 5% of them did not draw, while about 82%of the Libyans (134 out of 152) provided drawings.

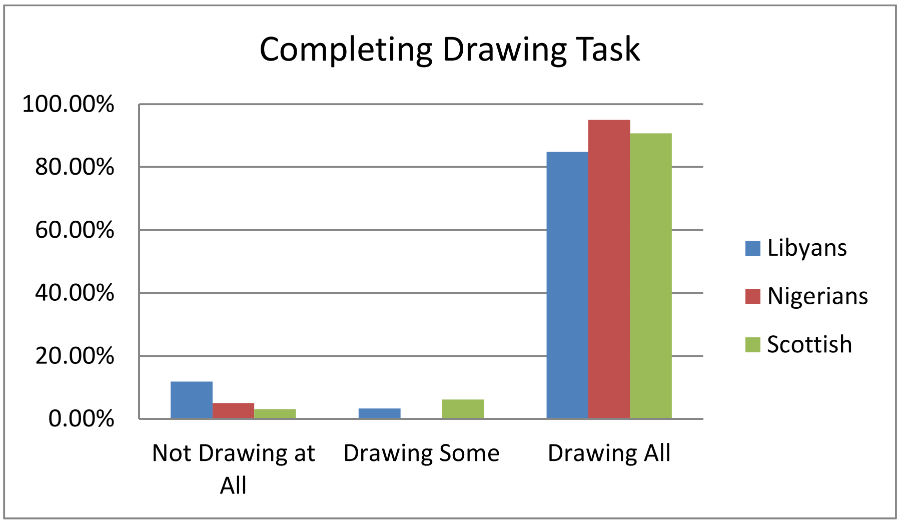


Figure 3-9 Completing drawing task

3.4.2.2 Average time spent on drawing

Drawing skills differ from person to person and cannot be measured exactly because of many factors. Some people do not like drawing at all, and others do like drawing; this is a result of human preferences and capabilities, e.g.:

"I do not like drawing because I do not know how to draw"

"I hate drawing with no reason"

However, Figure 3-10, below, shows the calculation of the average time in minutes that were spent drawing the four doodles by the participants who made a drawing. The difference between the average times in all categories is not large; it is just under 2 minutes.

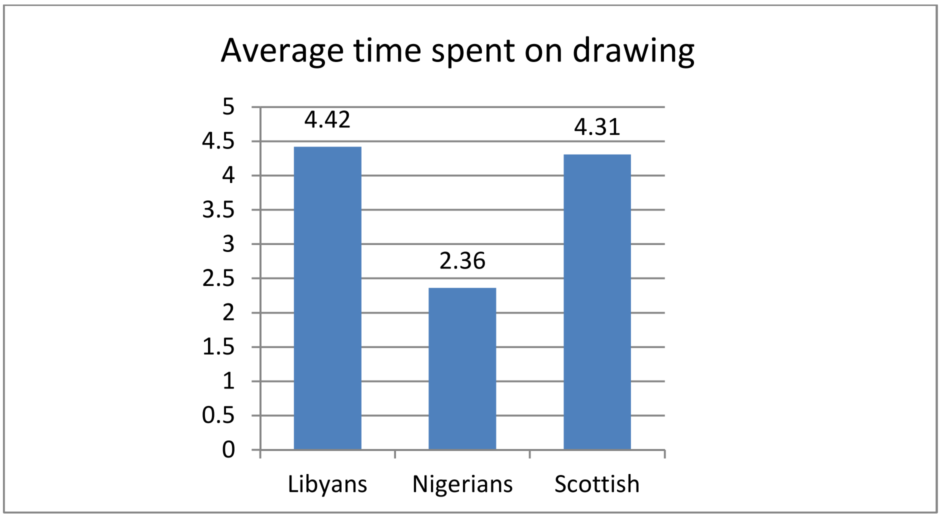
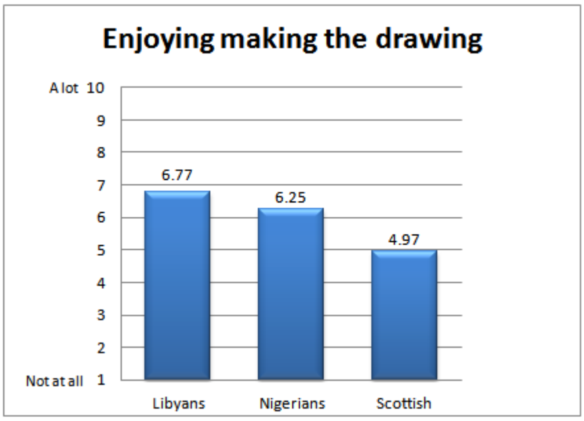


Figure 3-10 Average time spent on drawing

3.4.2.3 Enjoyed drawing

Opinions differed on the extent the participants had enjoyed drawing in this study. A question was asked as to whether they enjoyed providing hand-drawn images as graphical passwords, with a scale ranging from 1-10 used ("1" being the weakest to "10" for the strongest).



Variable	Libyans			Nigerians			Scottish		
	AVG	Medin	Mode	AVG	Medin	Mode	AVG	Medin	Mode
Enjoying making the drawing	**6.77**	7	10	**6.25**	6.5	5	**4.97**	5.00	5.00

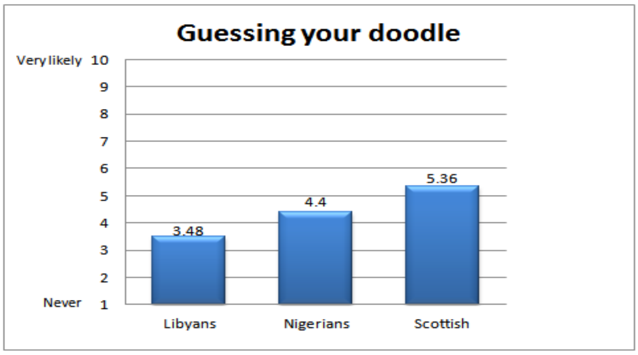
Figure 3-11 Enjoyment when completing the drawing task for the three groups

Figure 3-11shows the level of enjoyment which was gained from drawing for the three groups. It is clear that the Libyans generally enjoyed drawing, with a median response of 7 and the most popular answer 10. Scottish people on average slightly disliked drawing. Another way of presenting the information is the percentage of people with a positive response (6-10). The results are:

- 65% Libyans.
- 65% Nigerians.
- 45% Scots.

3.4.2.4 The probability of guessing drawing doodles

Theoretically, predicting or guessing someone's drawing could be subject to several factors, and the most important of these is the surrounding around the person - for example, the family members, friends and relatives who can recognize the person's hand-drawn. This can be also applied to Libyans, Nigerians and Westerners alike. In practical terms, it would still be difficult to guess another person's drawing. In this research, most contributors agreed that it would be hard for others to guess their drawings. A scale ranging from 1-10 was used ("1" being the strongest to "10" for the weakest) to answer the question as to whether the participants' drawn images could be guessed by other people.Figure 3-12 displays the average scales of the prediction for all groups, again on a scale of (1-10). Nearly 56% of the Scots participants were satisfied with the complexity of their drawings, while around 80% of Nigerians and 60% of Libyans were satisfied with the perceived difficulty of guessing their doodles.



Variable	Libyans			Nigerians			Scottish		
	AVG	Medin	Mode	AVG	Medin	Mode	AVG	Medin	Mode
Guessing your doodle	**3.48**	3	1	**4.4**	4.5	1	**5.36**	5.00	5.00

Figure 3-12 Estimates of probability of guessing drawing doodles

3.5 Cultural Aspects of User Drawn Images

This study was designed to examine the probability effects of culture on people's drawings. Previous studies have indicated cultural differences in various drawing and general cognitive tasks between cultural groups, especially between Asians and Americans, but no studies have been conducted on a comparison of Western (Scots), African (Nigerians), and Arab (Libyan) cultural groups. However, over the past two decades, cultural and cross-cultural perspectives on human behaviour have found their way increasingly into mainstream psychology, as observed by Chen et al. [138]. Chen et al. studied the ways in which drawings are created, but the study involved in this research will focus only on the subject of the drawings.

There are many ways of categorising drawings; for example, suggestions have been made by Snodgrass and Vanderwart [152], Cycowicz, et Al. [153], Alario and Ferrand [154] and Janssen et al. [155]. Cycowicz et Al. [153] set out 13 categories: four-footed-animals, basic level, birds, clothing, fruit, furniture, human body parts, insects, kitchen utensils, musical instruments, tools, toys, vegetables and vehicles. Janssen et al. [155] categorised150 drawings into 149 modal names.

The present study has found the categorisation suggested by Ruth Rostron, a professional handwriting analyst and vice-chair of the British Institute of Graphologists, to be useful. A popular description of her work is provided by the journalist Mandy Francis[2]. Rostron argues that some drawings have moral connotations or cultural connotations or even reflect the personality of the person; for example, using rounded shapes and curved lines often represents emotional people who want harmony and crave affection. Also, practical people tend to use straight lines and squares. Determined people often use corners, zigzags and triangles. Finally, hesitant people normally use light, sketchy strokes.

‘*A large doodle shows a person is confident and outgoing, while a small one suggests the person prefers to observe rather than participate*.’

Here are her categories, together with their meaning:

Faces

Happy faces, sad faces and funny faces are often a good indication of the mood or character of the person. A nicely drawn, good-looking face suggests you see the good in others.

Game Boards and Mazes

Patient and persistent people can be determined by drawings of game grids such as noughts-and-crosses and Nine Men's Morris, or by a black and white chess board. It also sometimes refers to the people who are prone to mood swings or perhaps could be weighing up various options regarding a tricky situation.

[2] A journalist at the Daily Mail, who wrote the article “*What your doodles really say about you Arrows for ambition, flowers for family a graphologist translates your idle scribbles*”, 10:12, 12 September 2011. Read more: http://www.dailymail.co.uk/femail/article-2036328/What-doodles-really-say-Arrows-ambition-flowers-family.html last accessed on 03/06/2013.

Flowers

A friendly, family-centric person could be known by their drawing of flowers which might contain rounded petals around a circular flower centre. Moreover, if the drawing of the centre of the flower was a circle and the petals were pointy, this could indicate that the person is probably hiding a warm heart behind a prickly defensiveness. Also, a bunch flowers might mean the person is sociable. Drooping flower heads indicate that they might be burdened by worry.

Butterflies

Butterflies, birds and bees indicate the person is flighty and romantic and does not want to be tied down or landed with difficult tasks or problems.

Squares or boxes

Drawing a square indicates controlling a situation or thinking through a problem. Square shapes often indicate progress; for example, a cube or box square reflects that the person is likely to be efficient and analytical and to be able to deal with difficult situations with little fuss.

Zigzags

Zigzags are common doodle drawings and show energetic thinking. Patterns made up of soft, flowing, curvy lines indicate a romantic, female approach to things, whereas patterns made up of lots of straight lines indicate more aggressive, masculine characteristics.

Stick figures

Controlling the emotions of a person and being incredibly focused on the goals in life is recognized by drawing a simple stick figure. It is commonly drawn by highly successful people.

These categories represent a useful starting point, but it was necessary to add a number of extra categories when analysing our doodle collection. The extra categories are as follows:

- an eye
- figures (not stick figures)
- trees
- scenery
- animals
- machines
- the sun and moon

- pencils, books and envelopes
- sports related
- food
- flags
- maps
- musical notes
- candles
- general objects
- simple abstract shapes
- spirals

*Table 3-2 The numbers are all frequencies per 1000**

Description	Libyans		Nigerians		Scots		All			Gender		Total
	M	F	M	F	M	F	L	N	S	M	F	
Faces	86	83	38	0	86	91	83	28	89	77	82	80
Eye	9	10	0	50	22	14	9	14	17	11	12	12
Hearts	0	2	19	100	0	49	2	42	30	4	17	13
Figure	0	2	0	0	11	0	2	0	4	4	2	2
Stick Figures	0	2	58	0	0	14	2	42	8	11	5	7
Butterflies / Birds	0	15	19	0	0	7	11	14	4	4	12	10
Animals	26	7	19	0	65	84	11	14	76	38	26	30
Flowers	69	163	58	0	22	140	142	42	93	50	152	120
Trees	60	90	58	0	43	56	83	42	51	54	78	71
Houses	17	49	58	0	11	56	42	42	38	23	49	41
Scenery	9	2	19	0	54	14	4	14	30	27	5	12
Cars / Boats / Planes	17	36	58	0	75	35	32	42	51	46	35	38
Machinery	78	41	77	0	65	7	49	56	30	73	31	44
Candle	0	10	0	0	0	0	8	0	0	0	7	5
Object	17	10	19	250	97	7	11	83	42	46	17	26
Game Boards / Mazes	17	0	0	0	0	0	4	0	0	8	0	2
Pencil / Book	17	46	0	0	11	0	40	0	4	11	33	26
Words / Letters	155	124	38	50	32	21	131	42	25	88	96	93
Musical note	0	7	0	0	0	21	6	0	13	0	10	7
Sports related	52	22	96	0	43	0	28	69	17	57	16	29
Food	0	44	19	0	22	35	34	14	30	11	40	31
Arrows	17	0	96	50	0	0	4	83	0	27	2	10
Flag	9	2	0	0	11	7	4	0	8	8	3	5
Map	17	2	19	0	0	0	6	14	0	11	2	5
Stars	17	51	77	100	43	49	44	83	47	38	52	48
Sun	9	27	0	0	0	7	23	0	4	4	21	16
Squares / Boxes	43	32	58	0	54	105	34	42	85	50	49	49
Spiral	0	0	0	50	43	21	0	14	30	15	7	10
Simple shape	172	66	38	350	151	84	89	125	110	138	80	98
Flowing zigzags	26	2	0	0	11	14	8	0	13	15	5	8
Sharp zigzags	17	5	19	0	22	21	8	14	21	19	9	12
Intricate patterns	43	46	38	0	11	42	46	28	30	31	44	40

The results are shown in Table 3-2, above, where the numbers are all frequencies per 1000, and so the numbers in each column add up to 1000. The first six columns give the totals for Libyan males and females, Nigerian males and females and Scottish males and females, respectively. The next three columns give the totals by nationality and the following two do so by gender. The final column is the total frequency. These numbers have not been adjusted to account for the different numbers from each country or the different gender totals.

The number of drawings, and participants, in each category were as follows. Most of the participants provided four drawings, but a small number of them provided only two or three.

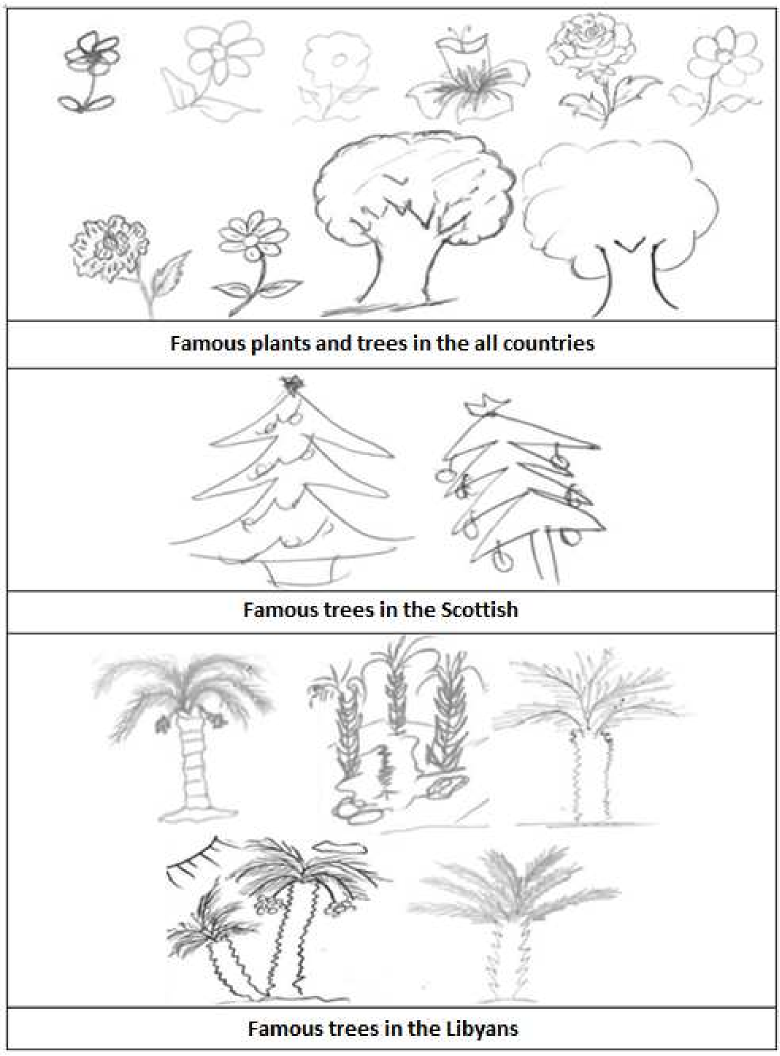
- Libyan males: 116 drawings by 29 participants
- Libyan females: 411 drawings by 105 participants
- Nigerian males: 52 drawings by 13 participants
- Nigerian females: 20 drawings by 5 participants
- Scottish males: 93 drawings by 24 participants
- Scottish females: 143 drawings by 37 participants

3.6 Analysis of the Results

The various categories will now be examined, starting with the most popular, in decreasing frequency. The small number of Nigerian females (five), and the relatively small total number of Nigerians (13) led to the Nigerian results often being different from the Libyan and Scottish ones.

Flowers and Trees

12% of the drawings were of flowers, and these were popular with Libyan and Scottish females. A doodle of a flower is a strong indication that the author is female. Trees were also popular, making up 7.1% of the sample. In this case there was a slightly weaker bias towards females. Libyans were also slightly more likely than Scottish participants to draw flowers. The Nigerian totals are anomalous, and are based on 3 drawings of flowers and trees respectively by Nigerian males. The types of flowers drawn by all the groups were very similar. However, the trees that actually grow in Libya and Scotland are very different and so we might have expected this to be reflected in the doodles. This is not very strongly supported by the data, since 58% of the Libyan tree drawings were of a generic kind and just 36% were of trees that can be found in the desert. A sample of the trees and flowers which were drawn is shown in Figure 3-13, below.



Famous plants and trees in the all countries

Famous trees in the Scottish

Famous trees in the Libyans

Figure 3-13 Trees and plants among Scots and among Libyans

Simple Abstract Shapes

These were popular with all groups, making up nearly 10% of the total. There was a slight weighting towards the male participants, but again, the Nigerian results were anomalous, with simple abstract shapes being more popular with Nigerian females. A collection of simple abstract shapes is shown in Figure 3-14, below.

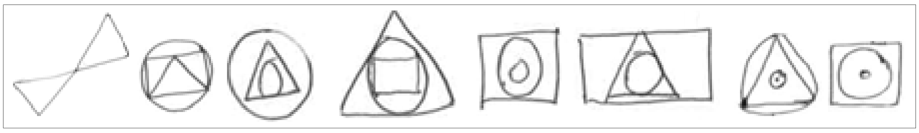


Figure 3-14 Undefined shapes

Words and Letters

This was a popular type of doodle with the Libyan participants (13.1%), but less so with other groups. The alphabet used would obviously distinguish Libyan and Scottish participants very quickly. There was no noticeable difference in gender in this category.

Faces

Faces were another popular category with Libyans and Scots, but slightly less so with Nigerians (8% of all drawings). There was no obvious gender bias, and this category could not be used to distinguish between Libyans and Scots.

Ruth Rostron indicated that the facial expression drawn indicates the mood of the drawer. The expressions on the faces in the present study's responses were: 52% happy, 40% normal and 8% sad.

The five categories described above accounted for nearly half (46.2%) of all the drawings. We will now consider the next few categories, each contributing between 4% and 5%.

Squares and Boxes

4.9% of the doodles were in this category, and they were fairly evenly distributed between males and females. Scottish females were significantly more likely to choose this type of drawing than any other group.

Stars

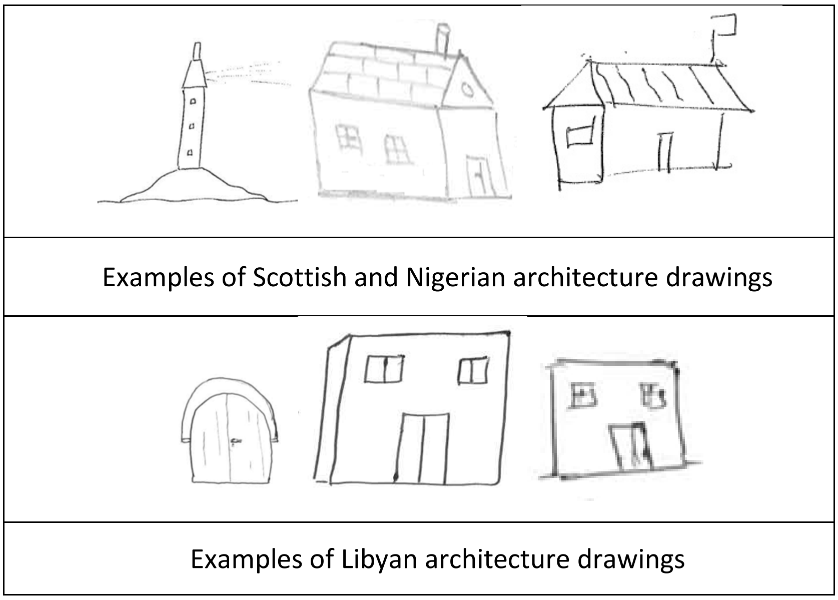
4.8% of drawings were of stars, which were quite popular with Nigerians. If the participant who had drawn a star was known to be Libyan, then they were highly likely to be female.

Machinery, Cars Boats and Planes

4.4% of the drawings were of machinery, and almost all drawings of this category were computers. Males were significantly more likely to draw machinery than females. In contrast, the 3.8% of drawings of forms of transport were evenly distributed between males and females. There was no great national difference between these types of drawings.

Houses

4.1% of drawings were houses, and these were mostly drawn by females, apart from the three houses drawn by Nigerian males. The types of houses were different, based on nationality, with Libyans living in houses with flat roofs and Scots houses being portrayed with angled roofs. This is illustrated in Figure 4-14, below. However, the majority (80%) of houses drawn by Libyans had angled roofs, and so the type of house drawn is not a discriminator. Again, this category was mainly chosen by females, excluding the three pictures of houses by Nigerian males.



Examples of Scottish and Nigerian architecture drawings

Examples of Libyan architecture drawings

Figure 3-15 Architecture drawings

Intricate Patterns

4% of the drawings fell into this category. There was a gender difference among Scots.

The rest of the categories accounted for a further 26% of drawings. The remaining 28% of doodles covered a number of different categories. The most interesting ones will now briefly be discussed.

Hearts

These make up a small number of the total images, mainly because they were not popular with Libyans. They were quite popular with Nigerian and Scottish females, and are thus a good indication of a non-Libyan female. Only one male drawing, from a Nigerian, was of a heart.

Animals

These were quite popular with Scots of both genders, totaling 7.8% of Scottish drawings.

Objects

Generic objects were very popular with Scottish males (9.7%) but not with Scottish females. They were also popular with Nigerian females (25%).

Pencils and Books

These were quite popular (4.6%) with Libyan females and also with some Libyan males. Overall, they are a good indication first that the participant is Libyan, and then that they are female.

Sports Related

Sports related images were quite popular with males everywhere (5.7%) but not very popular with females.

Food

Conversely, drawings about food were quite popular with Libyan and Scottish females (4% overall for females).

Arrows

This is one of Rostron's key categories, but drawings of arrows were only popular with Nigerians, especially males.

Flags and Maps

This was a fairly rare category, but the flags and maps gave a strong hint as to nationality.

Zigzags

This is another of Rostron’s categories which was not chosen very much. Both flowing and sharp patterns were drawn more by males than females.

3.7 Discussion

There have been some prior studies of cross-cultural responses [156],[138]. One of their major concerns has been whether there is "*universal agreement on the value or merit of particular responses to particular questions*" (Greenfield, 1997, p. 1116). Few studies have been carried out specifically to address such concerns. In this study of creativity in drawing, a comparison between Scots and Libyans was made on the basis of examining what they drew. The concerns focused on their selection of the type of drawing to create, and examining whether culture had effectively played a role in this selection. Prior studies [133, 134, 137, 138, 157, 158]have focused on how objects were drawn, and found relations between the objects and the backgrounds of the pictures on one hand and on the other hand, the relations between the objects contained in pictures with physical brain connectivity. However, differing from the rationale of those psychology studies, this study is concerned with using hand drawn images as a part of authentication systems and exploring previous studies of psychology. The results of the present study are divided into two parts: the first is related to computer use and the second examines the hand-drawn images themselves and how these are related to culture and gender.

3.7.1 Computer and Internet usage

As mentioned in section 3.4.1, the infrastructure of countries in terms of their communications and telecommunications plays a major role in developing that country. Most computer activities are dependent on good access to the internet. Nowadays, many applications, especially interactive ones, are connected directly to the internet; for example, some popular games are played through the internet and many users can simultaneously play against or with one another. However, some cultural habits also exert an influence and can affect the usage of computer activities, especially with regard to the internet. The results of this part of the present study clearly demonstrate the validity of these facts; for example, most Libyans do not have the internet in their homes, therefore the effectiveness of a computing process is less important to them. Some reasons for this include infrastructure limitations, such as the price of the internet which is very high compared to Western countries, and the absence of telephone lines in some parts of the country.

Also, as mentioned before, the culture or environment may play a role in how computers are used, especially with regard to the internet. Most Arab countries have conservative families, and most of these families do not allow girls to use computers outside the home, e.g. at Internet Cafes. Libya is one of those countries. According to

Internet World Stats [159], only 5.4% of Libyans use the internet, whereas about 82.5% of Scots do so.

3.7.2 Creativity in drawing

This study cannot provide any insight into Nigerian drawing habits because the sample size was too small and there were too many different categories. The four most popular categories were:

- 7 females: simple shapes.
- 5 females: abstract objects.
- 5 males: sport related.
- 5 males: arrows.

The strongest indications of cultural influence were doodles featuring writing (9.3% of all doodles). The alphabet used will, of course, clearly distinguish between Arabic and Latin letters. Words can also reveal more information about the drawer, for example their favourite football club. Flags and maps can also give away this type of information, but they were quite rare (1% of doodles).

Drawings of animals were, an indication that the participant was Scottish rather than Libyan, by a ratio of 7 to 1. This was a popular category (7.6%) with Scots. Simple objects were also more popular with Scots by 4 to 1, making up 4.2% of Scottish doodles. Squares and boxes were also more popular with Scots than Libyans by 2 to 1 and made up 8.5% of Scottish doodles.

Some categories which might have been expected to give insight into culture failed to do so. Most drawings of houses portrayed sloped roofs, irrespective of culture. Similarly, most trees were generic. Also, more Scots than Libyans drew pictures of scenery, although this category was quite rare. It would be interesting to see whether or not more Asians would draw pictures of scenery, as was predicted by Goh et al. [137].

If the doodles in the five categories that give hints about culture are added up, then 20% of Libyan doodles and 24% of Scottish doodles give same hints about culture.

Flowers, making up 12% of all images, were a major indication that the drawer was female, with a ratio of 3 to 1. Houses (4.1%) were also chosen more by females than males, with a ratio of 2 to 1. Minor categories such as Hearts (1.3%) and Butterflies / Birds (1.0%) were also more popular with females, with a ratio of 4 to 1. On the other hand, machinery

(4.4%) is preferred by males rather than females, by a ratio of 2 to 1. Sports (2.9%) are also more popular with males, with a ratio of 3 to 1.

Adding up these categories as before indicates that 21% of male doodles and 28% of female doodles throw some light on the gender of the drawer.

If we now consider that each participant had to provide four doodles as their passimages, we can conclude that in a large number of cases it will be possible to guess the gender and nationalities of some of the participants in the study correctly.

3.7.3 Acceptability of using drawings for authentication in a Muslim country

Going back to the results shown in Figure 3-6 in section 3.4.2of enjoying drawing, it can be noted that many participants in the three groups said that they do not love drawing. In fact, there were different opinions about the lack of love for drawing. Most of these opinions related to a lack of ability in drawing (human skills). Interestingly, two participants from Libya referred their lack of love for drawing to religion and said:

"It is prohibited to draw beings with souls"

However, only two of the 152 Libyan participants (1.3%) referred to their opinion of drawing as a religious issue, which obviously does not significantly impact upon the task of hand-drawing images and using them as graphical password in such country. But, this issue should be mentioned here as it is one of the cultural factors which might be relevant, and religious drawings could easily be recognised by other people, especially when they are not from the same country and religion.

However, most authentication systems have been developed in Western countries [150] and most of them are Christian, so it would be difficult to see different aspects between users in those countries. Similarly, the 22 Arab countries are Muslim. For strong security, hand-drawn images from within the same culture should be taken into account when implementing the authentication system and using the same cultural images as distractors in order to remove any security implications of the use of such systems.

3.8 Conclusion

Three main conclusions can be drawn from the research presented in this chapter. Firstly, Libyan students are much more receptive to the idea of using doodles as passwords than Scottish students. Libyans enjoyed drawing more and are also more confident about the security of a doodle based authentication system. Therefore using doodles could be accepted as a password in Libya.

Secondly, some doodles may be influenced by the users' culture, which makes them easier to guess. This can be a problem if distractors are chosen from a general pool of doodles provided by the users. Thus, it may be better if the distractors are chosen from doodle passwords provided by users of a similar cultural background.

The third conclusion is that the Nigerians in this study were culturally more similar to the Scots in their choice of doodles. This is a weaker result because these subjects are from a special group, i.e. of Nigerians studying in Scotland, and from a smaller sample. Thus, further study by a large sample of Nigerian in both countries Scotland and Nigeria would be beneficent.

Differences between cultures in many subjects have been well documented by many scientists and researchers except on drawings. Research over the past two decades has demonstrated that culture has an important influence in the ways people experience, express and label emotions. However, very little research has made cross-culture comparisons, especially in drawings. The aim of this research has therefore been to ascertain the level to which differences in culture might affect our choice and use of drawn doodles as passwords. More specifically it has investigated the usage of computers and made a comparison between Libyan people (Arabs) and Scots (Westerners) as a part of cross-cultural study.

3.8.1 Limitations

Finally, several limitations of this study should be noted. First, because the data gathering took place only in Misurata city in Libya and Glasgow in Scotland, however different they are from each other, it remains to be established whether they can be taken to be generally representative and that the findings on cross-cultural agreement in decisions on what to draw can be generalized to other cultures. Second, because this study used decisions concerning several categories, it is unknown whether our finding can be generalized to decisions on other types of drawings. Each of these limitations should be addressed in future research.

Chapter Four
Exploring the Guessability of Hand Drawn Images Based on Cultural Characteristics

As a complement to the study described in the previous chapter, which investigated how culture plays a role in selecting pictures as graphical passwords, we carried out an experiment to explore the guessability of hand-drawn images based on cultural characteristics. In this experiment, we used images which were collected and analysed as described in the previous chapters, and the participants were asked to guess which culture the images came from.

4.1 Introduction

Selecting easily remembered passwords is a well-known security issue since these can also often be guessed easily[160],[161].This also applies to graphical passwords. Again, the level of guessability refers to the ease with which an attacker can guess the user's authentication secret (passimages in recognition-based graphical passwords and the series of action and clicks points in recall based graphical passwords).As mentioned in the previous chapter, the three most frequent guessing attack approaches related to recognition graphical password are: random guessing, guessing based on predictable user choices for a population of users, and guessing based on an individual user's preferences.

Random guessing usually refers to the number of attempts needed to guess the right passimage. This depends on the number of images displayed on each authentication screen and the number of screens; for example, assuming that *x* is the number of the images per screen and *y* is the number of screens, the maximum number of attempts needed to guess the password can be calculated as $1/(x^y)$ and therefore the random guessability value is x^y.

This had been taken into account in the design of the website used in the experiment in Chapter 3, where *x* was 16 and *y* was 4, thus the random guessability value was 65536.

Guessing based on predictable user choices for a population of users is the second most frequent guessability approaches and is based on users’ choices of password, whether text or graphical. In fact, the security of passwords could be influenced by the user’s choice and this makes the passwords susceptible to dictionary attacks. Thus, this can also be impacted by graphical passwords, as noted by De Angeli et al. [162],who highlighted that an evaluation of the predictability of user-selected passimages is required. Another research study which tested the effect of the user choice of images on security used two schemes, i.e. the Story and Face schemes. This was done by Davis et al. [53].

The last guessability approach is based on an individual user's preferences in their choice of images. This depends on how much knowledge the attackers have about the users and what the user's preferences are. The attacker could guess the user's passimages more successfully than the level expected by chance. Renaud claimed that an attacker could guess others’ writing or hand drawn images if they knew their style and that this could be applied to relatives who are near and close to people[20]. Hayashi et al. also carried out an experiment to test the hypothesis that “*an attacker can make more accurate guesses about authentication images if the attacker possesses information about the user who chose them*". They evaluated “individualized educated guess attacks" [163] and the results showed that eight out of 15 attackers correctly identified a target set of three images within 10 guesses.

The research reported in this chapter is based on the second guessability approach, of guessing based on predictable user choices for a population of users. The aim of this research is to examine whether or not an attacker could guess hand drawn images chosen as graphical password by others, based on knowledge of some cultural information like where they come from or their religion or even their hopes and aims. This would introduce for a bias in the user choice of images and has an impact on guessability. The work also considers the probability, based on generalised rules and instructions, of drawing a very strong password resistant to guessability, depending on the results from this experiment. Finally, an answer is sought to the question:

Q. Is it possible to guess other people’s hand image passwords depending on their personal characteristics, such as cultural features or nationality?

Consequently, the hypothesis can be defined as:

H1: Many hand image passwords can be recognised by the cultural features that are contained in the image.

H2: Are drawn images guessed by males different from drawn images guessed by females.

H3: Are drawn images guessed by participants from different countries similar.

4.2 Experimental Details

4.2.1 Participant information and time required

A total of 62 participants took part in this experiment: 51 males and 11 females, with average ages in the range of 25-29 and mode in the range of 18-24. Figure 4-1 depicts the demographic profile of all the participants. Most of the participants for this study were from different schools at the University of Glasgow and the majority of them were from the School of Computing Science. All the participants were well educated and about 44% of them had an MSc degree. The biggest three groups were Scottish, Libyans and Nigerians. The experiment took about six weeks to collect data from the participants and it took approximately 10-15 minutes for each participant to complete all the tasks.

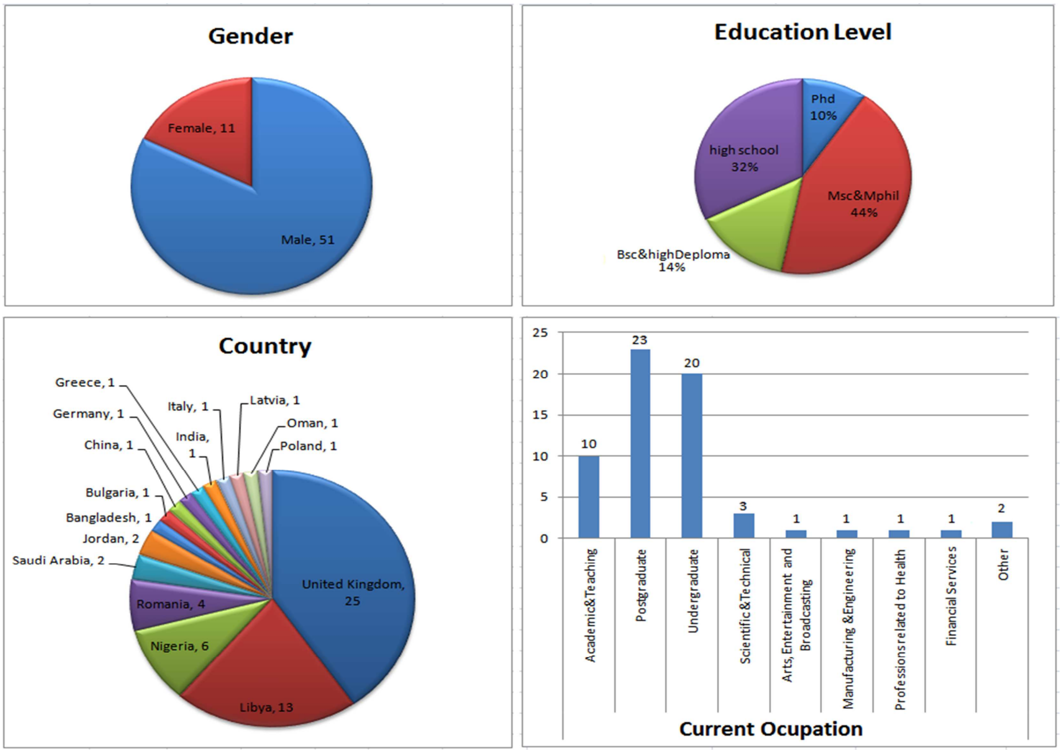


Figure 4-1 Demographic information about users

4.2.2 Experimental design

The experiment was designed such that each participant had to guess the cultural origins of hand drawn images displayed on four screens, each with 16 images, using a drag and drop method. A website was created to meet the requirements behind this experiment. The experimental website was built using three main components: PHP, JavaScript and MySQL as the database. The feature of drag and drop was supported by HTML5[3].The screens and the stages of the experimental website are described in details in Appendix B.

4.2.2.1 Hand drawn image codes

All of the hand drawn images used in this experiment were collected from the previous studies mentioned before in this thesis, some in Chapter 5 and the majority from Chapter 3. Each image was coded using three digits. The first digit represented the country where the person who originally drew the image came from. The second digit represented the image categories, which were 1: Sport, 2: Religious, 3: Nation, 4: Plants and Trees, 5: Landscape and Views, 6: Buildings 7: General. The last digit was the number of the image in its category. An example is shown in Figure 4-2.

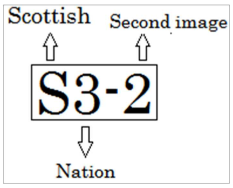


Figure 4-2 Image Code

All 64 hand drawn images used in this experiment were divided into 4 screens. All images are displayed in Figure 4-3.

[3] HTML5 Drag & Drop is supported in Firefox 3.5+, Chrome 3.0+, and Safari 3.0+. Support in Internet Explorer is not as simple, http://www.htmlgoodies.com/html5/tutorials/html-5-drag-drop-basics.html#fbid=oqH-PGflj1gLast accessed on 07-09-2013. Therefore, the participants were asked to use Firefox, Chrome and the latest version of IE (Internet Explorer).

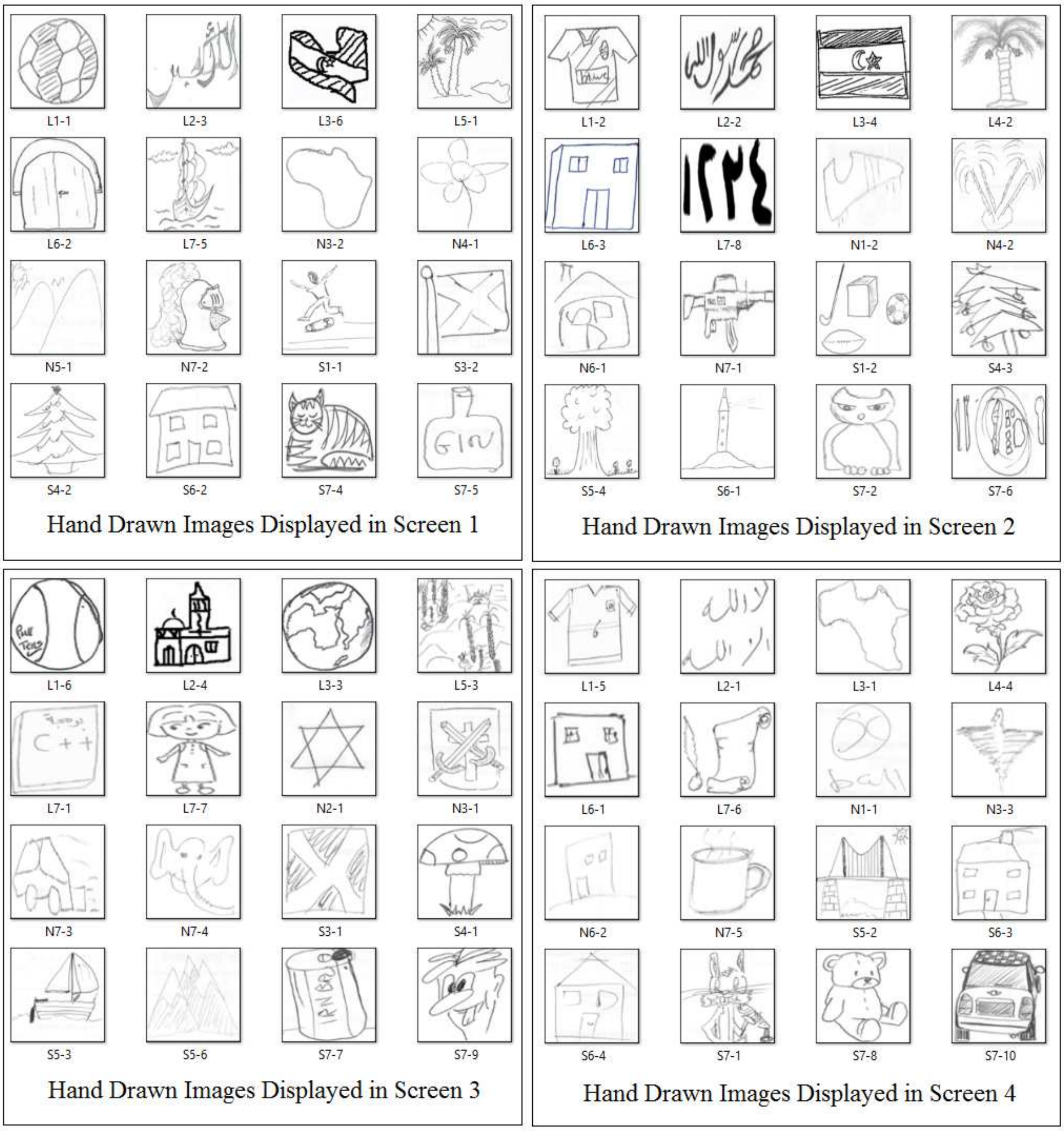


Figure 4-3 Four screens displayed the doodles used in this experiment

All 64 hand drawn images used in the experiment were selected randomly from the seven categories mentioned in section 4.2.2.1 and were divided into:

1- 24 Scottish hand-drawn images.
2- 24 Libyan hand-drawn images.
3- 16 Nigerian hand-drawn images (which were based on the limited images provided in Chapter 3).

<u>Note:</u> *The images on each screen were displayed randomly to the participants, not as listed in the figure above.*

4.2.3 Experimental procedure

4.2.3.1 Instructions to the participants

The instructions were given to the participants in two ways: on an information sheet and in an email sent to each of them. Also, more information was hosted on the main page of the experimental website. The instructions were as follows:

1. Participants were asked to enter the experimental website on www.guessdoodle.com.
2. Before starting the experiment, they were asked to read the information displayed and understand the idea behind this study and how they should perform.
3. The users were asked to provide some basic information about themselves in the next screen.
4. They were then asked to try to put hand drawn images displayed in the four screens into one of the national categories: Scottish, Libyan and Nigerian. If they did not know which was likely to be correct, they could use the I Do Not Know category.
5. After they finished all screens they were entered into a prize draw to win one of 3x £20 Amazon gift vouchers.

Notes:

I. The website screens allowed the participants to change the category of the selected image (i.e. if the one of the selected images was put into a category by mistake, the participants could change this and put it into the right one).

II. Once the user dragged the selected image it was zoomed automatically to give clear details of the image, to help them put it into the right category, as shown in Appendix B.

4.3 Results and Discussion

The number of correct, incorrect and ‘do not know’ choices per image are given for all users, males and females and users from different nationalities. We also looked at individual users, to judge who were most and least successful.

4.3.1 The most guessed and un-guessed image by all users

The results of this subsection were calculated for all the participants, ignoring any variables such as gender, and also for all the hand drawn images used in the experiment. This led the research to divide the findings into three categories:

1- The ten most guessed images;
2- The ten most incorrectly guessed images, and
3- The ten most unknown guessed images.

Firstly, Table 4-1, displays the order of the doodles guessed correctly most frequently by the participants, starting with doodle S3-2 which had the highest score of 61 correct guesses out of 62 and ending with doodle L1-2 which had the lowest score, of 0 correct guesses. Figure 4-4 displays 15 hand drawn images, representing the most easily guessed images. It can be noted that the most easily guessed images contained either religious or national symbols. The first two images represented the flag of Scotland and were drawn by Scots and those received the highest score while the third and fourth images contained Islamic words and were drawn by Libyans. The fifth image contained the flag of Libya and the sixth and seventh images also contained Islamic words and marks. The eighth image contained a very famous soft drink in Scotland whereas the tenth and eleventh images were drawn by Nigerians, one was the face of an elephant, which may be well known in Nigeria and the other was a map of Africa. Together, these indicated that high scoring images may contain some features of the country, religion and environment that the person drawing the image came from.

Secondly, Table 4-2displays the order of the doodles that were most frequently guessed incorrectly by the participants, starting with doodle N7-2 which got the highest score of 53 incorrect guesses, ending with doodle S7-8 which had the lowest score of 1 wrong guess. Figure 4-5also displays 13 hand drawn images representing the most incorrectly guessed doodles by the participants. Also, it can clearly be seen from the figure that there are two types of images:

- General images which do not contain any hints of where the image came from, such as L1-1, L4-4 and N5-1.

- The second type of images was interesting as they contained some environmental hints such as L3-1, N3-1 and N7-2. This will be discussed in more detail in section 4.4.1, below.

Thirdly, Table 4-3 displays the order of the most difficult to guess doodles, starting with doodle id N3-3 which received the highest score of 35 ‘unknown’ classifications and ending with doodle id S3-2 which did not receive this classification at all. Figure 4-6 displays 15 hand drawn images representing the doodles most frequently scored as unknown. Most of the images did not contain any hints referring to either the country or the culture the image came from.

Table 4-1summarises the frequency of all the hand-drawn images used in this work including those correctly guessed, incorrectly guessed and marked as unknown.

Table 4-1 Order of highest guessed images

The Highest Guessed	
Doodle	Correct
S3-2	61
S3-1	60
L2-1	57
L2-2	57
L3-4	56
L2-3	54
L2-4	54
S7-7	54
L3-6	52
N7-4	50
N3-2	48
S7-6	48
S1-2	44
S4-3	44
S4-2	42
L7-8	38
S7-10	38
L7-1	36
L4-2	35
L5-3	35
S5-6	35
S7-8	35
S5-4	34
S6-3	34
L5-1	33
S1-1	31
N4-2	30
S5-2	29
S6-2	29
S6-1	28
S6-4	28
S7-9	26
S5-3	25
L6-1	23
L6-2	23
L6-3	23
S4-1	23
L7-6	22
N1-1	21
N1-2	21
S7-1	18
S7-4	18
S7-2	17
N6-1	16
N6-2	16
N7-1	15
L3-1	14
N3-3	10
L4-4	9
L7-5	9
S7-5	9
N7-3	8
N4-1	7
L7-7	6
N5-1	6
L3-3	4
N3-1	4
N2-1	3
L1-1	2
N7-2	2
L1-5	1
L1-6	1
N7-5	1
L1-2	0

10 Most guessed images

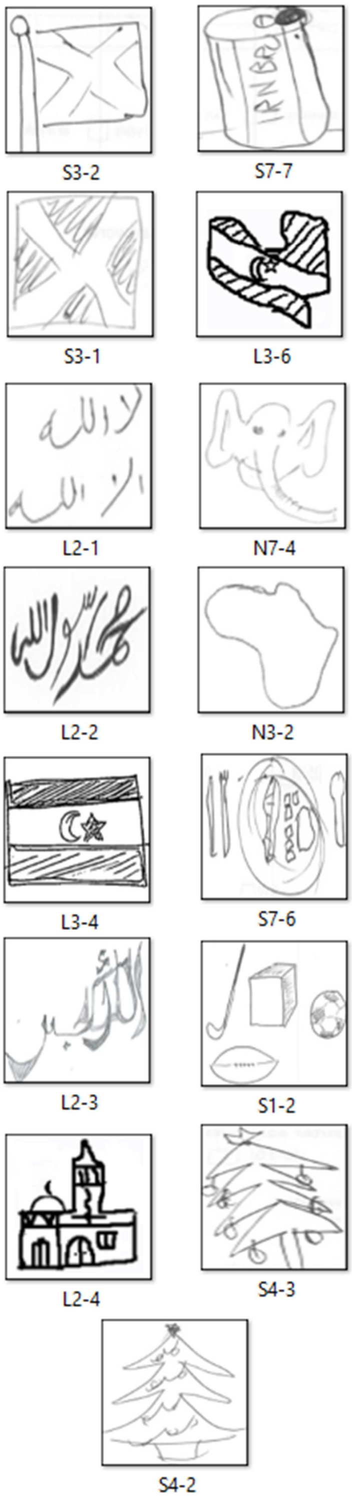


Figure 4-4 Most guessed images

Table 4-2 Order of most frequent incorrectly guessed images

Wrong guessed	
Doodle	Wrong
N7-2	53
L1-2	52
L1-5	51
N3-1	50
L1-1	50
N5-1	45
N7-5	43
L3-1	42
L1-6	41
N7-1	39
L4-4	36
L7-5	36
S7-5	36
N6-1	30
N4-1	28
L7-7	28
L3-3	28
N2-1	27
N1-1	25
N7-3	24
L5-1	23
S5-3	23
L7-6	23
L6-3	22
L4-2	20
L5-3	20
N4-2	20
N1-2	20
N6-2	20
S5-6	16
S6-4	16
S6-1	15
L6-1	15
S5-4	14
S5-2	14
L6-2	14
S7-4	13
S7-2	13
N3-3	13
S7-10	12
S6-2	12
L7-1	10
S4-1	10
N3-2	9
S1-2	9
L2-4	8
L7-8	8
S6-3	8
L3-6	7
S7-9	7
L3-4	6
S1-1	6
S7-1	6
S7-6	5
S4-2	5
L2-3	4
L2-2	3
S4-3	3
S3-1	2
L2-1	2
S7-7	2
N7-4	2
S3-2	1
S7-8	1

10 Most incorrectly guessed images

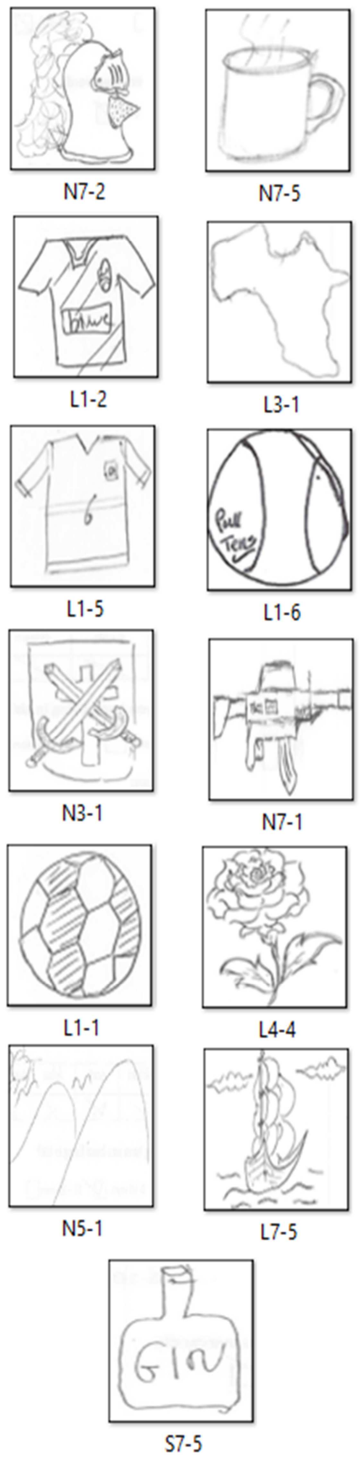


Figure 4-5 Most incorrectly guessed images

Table 4-3 Order of most difficult to guess images

Difficult to guess	
Doodle	Do Not Know
N3-3	39
S7-1	38
N2-1	32
S7-2	32
S7-4	31
L3-3	30
N7-3	30
S4-1	29
S7-9	29
L7-7	28
N4-1	27
N6-2	26
S7-8	26
L6-2	25
S1-1	25
L6-1	24
N1-2	21
S6-2	21
L1-6	20
S6-3	20
S6-1	19
S5-2	19
N7-5	18
S6-4	18
L4-4	17
L7-5	17
S7-5	17
L7-6	17
L6-3	17
N6-1	16
N1-1	16
L7-1	16
L7-8	16
S4-2	15
S4-3	15
S5-3	14
S5-4	14
N4-2	12
S7-10	12
N5-1	11
S5-6	11
L1-2	10
L1-5	10
L1-1	10
N7-4	10
S1-2	9
S7-6	9
N3-1	8
N7-1	8
N7-2	7
L4-2	7
L5-3	7
L3-1	6
L5-1	6
S7-7	6
N3-2	5
L2-3	4
L3-6	3
L2-1	3
L2-2	2
L2-4	0
L3-4	0
S3-1	0
S3-2	0

10 Most difficult to guess images

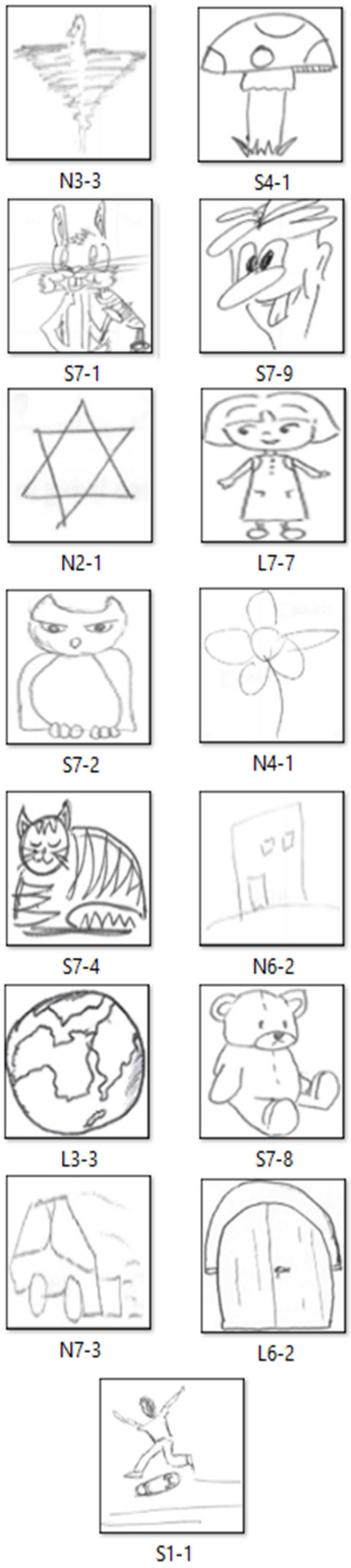


Figure 4-6 Most difficult to guess images

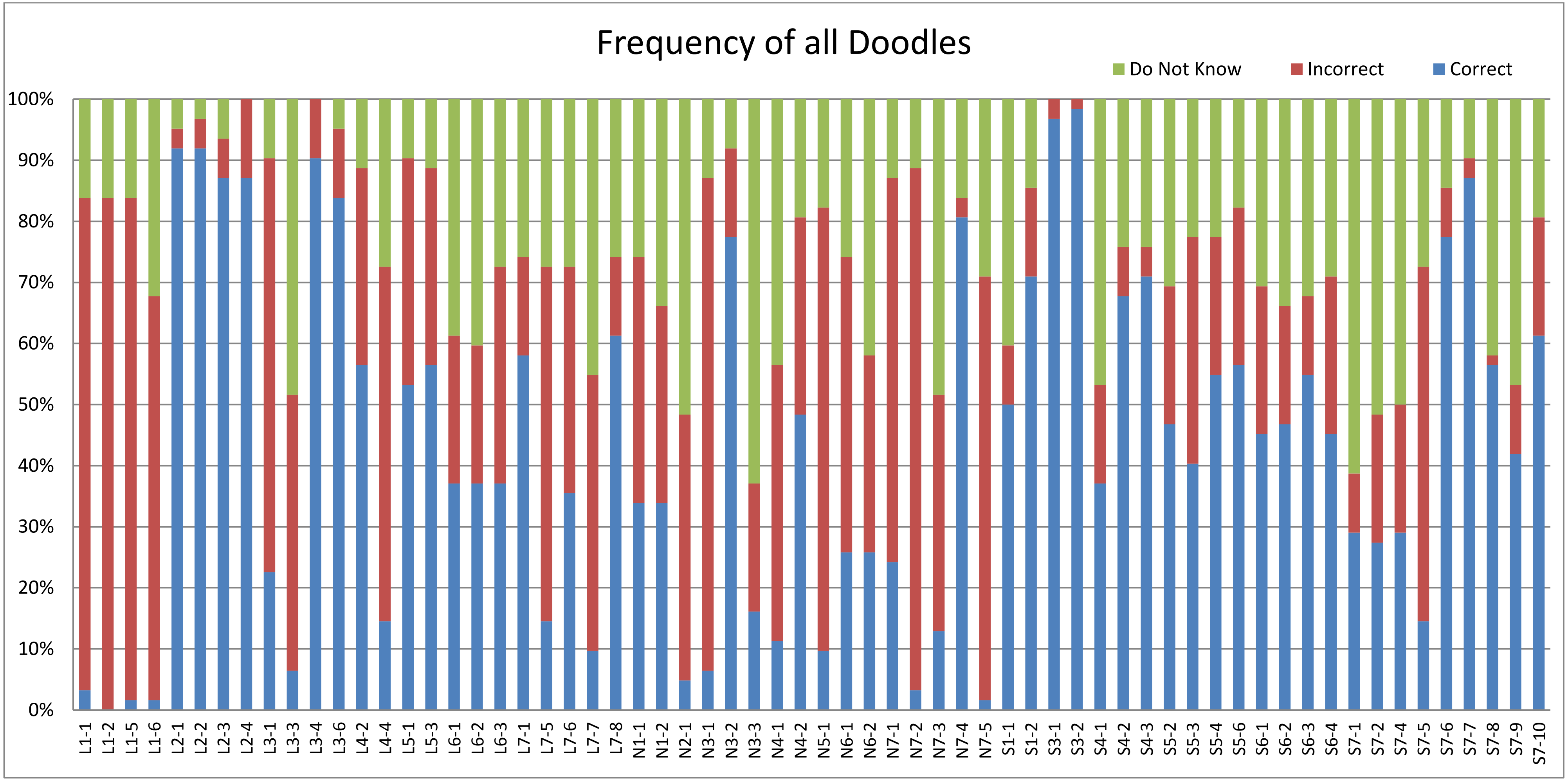


Figure 4-7 Summary of the frequency of all hand drawn images (Doodles)

4.3.2 Guessability by gender

The participants were divided into two main categories depending on their gender. The purpose of dividing participants into males and females was to examine whether or not the guessability of drawn images was influenced by gender.

Table 4-4 displays the order of the most frequently guessed, incorrectly guessed and classified as ‘don’t know’ doodles among males and females. The results from the 51 male and 11 female participants show that there was not much difference between their image predictions. Also, it can clearly be seen that from the most frequent five images there is only one difference between males and females, which was image S7-6, displayed in Figure 4-8, and this is consistent with the findings of the previous section.

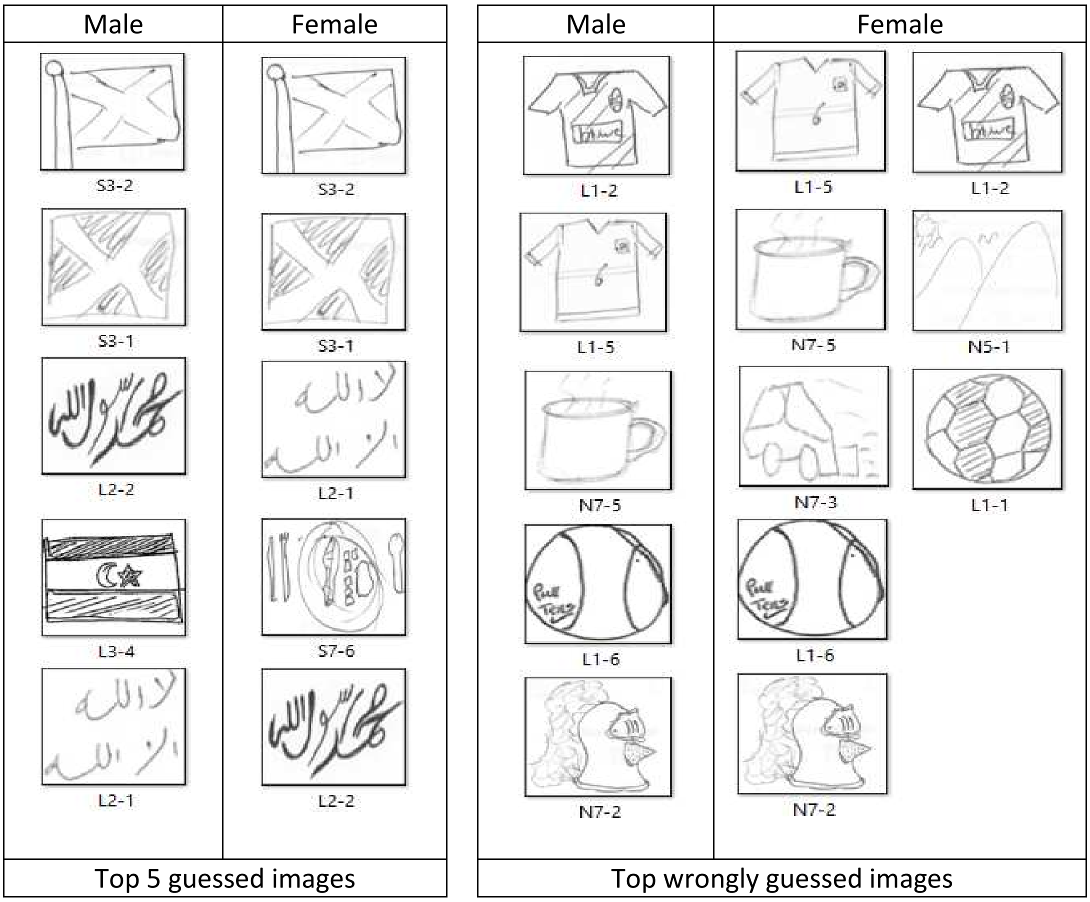


Figure 4-8 the most frequently guessed and wrongly guessed images, by Gender

Table 4-4 Order of correctly guessed and incorrectly guessed images, by Gender

Male 51		Female 11		Male 51		Female 11		Male 51		Female 11	
Doodle	Correct	Doodle	Correct	Doodle	Wrong	Doodle	Wrong	Doodle	Do Not Know	Doodle	Do Not Know
S3-2	50	L2-1	11	N7-2	45	N5-1	11	N3-3	34	L3-3	6
S3-1	49	S3-1	11	L1-2	43	N7-5	10	S7-1	32	N2-1	6
L2-2	47	S3-2	11	L1-5	42	L1-1	9	S7-2	29	S7-1	6
L2-1	46	L2-2	10	L1-1	41	L1-2	9	S7-4	28	N3-3	5
L3-4	46	L2-4	10	N3-1	41	L1-5	9	L7-7	26	S4-1	5
L2-3	45	L3-4	10	L3-1	36	N3-1	9	N2-1	26	N1-1	4
S7-7	45	S7-6	10	N5-1	34	L1-6	8	N7-3	26	N7-3	4
L2-4	44	L2-3	9	L1-6	33	L7-5	8	S7-9	26	S6-2	4
L3-6	43	L3-6	9	N7-5	33	N7-2	8	L3-3	24	L1-6	3
N7-4	42	S4-2	9	N7-1	32	S7-5	8	N4-1	24	L6-2	3
N3-2	41	S4-3	9	L4-4	31	L5-1	7	S4-1	24	L6-3	3
S7-6	38	S7-7	9	L7-5	28	L7-7	7	N6-2	23	L7-8	3
S1-2	37	L7-1	8	S7-5	28	N7-1	7	S1-1	23	N1-2	3
S4-3	35	N7-4	8	L3-3	25	N7-3	7	S7-8	23	N4-1	3
S4-2	33	S5-4	8	N6-1	25	L3-1	6	L6-1	22	N6-1	3
L7-8	32	S5-6	8	N1-1	22	L5-3	6	L6-2	22	N6-2	3
S7-10	32	S6-3	8	N2-1	22	L7-6	6	N1-2	18	N7-4	3
L5-3	31	S7-8	8	N4-1	22	N4-1	6	S6-3	18	S5-2	3
L4-2	30	N3-2	7	L7-7	21	S5-3	6	L1-6	17	S6-1	3
L5-1	30	N4-2	7	L6-3	18	L4-2	5	N7-5	17	S7-2	3
L7-1	28	S1-1	7	L7-6	17	L4-4	5	S6-2	17	S7-4	3
S5-6	27	S1-2	7	N4-2	17	N1-2	5	L7-6	16	S7-8	3
S7-8	27	S7-9	7	N7-3	17	N2-1	5	S5-2	16	S7-9	3
S5-4	26	L6-1	6	S5-3	17	N6-1	5	S6-1	16	S7-10	3
S6-3	26	L6-2	6	L5-1	16	S6-4	5	S6-4	16	L1-1	2
S5-2	25	L7-8	6	N6-2	16	S7-2	5	L4-4	15	L1-2	2
S6-2	25	S6-1	6	L4-2	15	L6-3	4	L7-1	15	L1-5	2
S1-1	24	S7-4	6	N1-2	15	N6-2	4	L7-5	15	L4-4	2
S6-4	24	S7-10	6	L5-3	14	S5-2	4	S7-5	15	L6-1	2
N4-2	23	L4-2	5	S5-6	14	L3-3	3	L6-3	14	L7-5	2
S5-3	22	S4-1	5	S6-1	13	L6-1	3	S4-2	14	L7-7	2
S6-1	22	L3-1	4	L6-1	12	N1-1	3	S4-3	14	N7-1	2
L6-3	19	L4-4	4	L6-2	12	N3-2	3	L7-8	13	N7-2	2
S7-9	19	L5-3	4	S5-4	12	N3-3	3	N6-1	13	S1-1	2
L7-6	18	L6-3	4	S6-4	11	N4-2	3	S5-4	13	S5-3	2
N1-2	18	L7-6	4	S7-4	11	S1-2	3	N1-1	12	S6-3	2
S4-1	18	N1-1	4	N3-3	10	S6-2	3	S5-3	12	S6-4	2
L6-1	17	N6-2	4	S5-2	10	L2-3	2	N4-2	11	S7-5	2
L6-2	17	S5-2	4	S7-10	10	L3-6	2	N5-1	11	S7-7	2
N1-1	17	S6-2	4	S4-1	9	L6-2	2	S5-6	10	L3-1	1
S7-1	14	S6-4	4	S6-2	9	L7-1	2	S7-6	9	L4-2	1
S7-2	14	S7-1	4	L7-1	8	L7-8	2	S7-10	9	L5-1	1
N6-1	13	L5-1	3	S7-2	8	S1-1	2	L1-1	8	L5-3	1
N7-1	13	N1-2	3	L2-4	7	S5-4	2	L1-2	8	L7-1	1
N6-2	12	N3-3	3	S6-3	7	S5-6	2	L1-5	8	L7-6	1
S7-4	12	N6-1	3	L7-8	6	S6-1	2	S1-2	8	N3-1	1
L3-1	10	S5-3	3	N3-2	6	S7-4	2	N3-1	7	N3-2	1
L7-5	8	S7-2	3	S1-2	6	S7-10	2	N7-4	7	N4-2	1
N7-3	8	L3-3	2	S7-9	6	L2-2	1	L4-2	6	N7-5	1
S7-5	8	L7-7	2	L3-4	5	L2-4	1	L5-3	6	S1-2	1
N3-3	7	N4-1	2	L3-6	5	L3-4	1	N7-1	6	S4-2	1
N5-1	6	N7-1	2	S7-1	5	S4-1	1	L3-1	5	S4-3	1
L4-4	5	L7-5	1	S1-1	4	S4-2	1	L5-1	5	S5-4	1
N4-1	5	N3-1	1	S4-2	4	S4-3	1	N7-2	5	S5-6	1
L7-7	4	N7-2	1	S7-6	4	S6-3	1	L2-3	4	L2-1	0
N2-1	3	S7-5	1	L2-1	2	S7-1	1	N3-2	4	L2-2	0
N3-1	3	L1-1	0	L2-2	2	S7-6	1	S7-7	4	L2-3	0
L1-1	2	L1-2	0	L2-3	2	S7-9	1	L2-1	3	L2-4	0
L3-3	2	L1-5	0	N7-4	2	L2-1	0	L3-6	3	L3-4	0
L1-5	1	L1-6	0	S3-1	2	N7-4	0	L2-2	2	L3-6	0
L1-6	1	N2-1	0	S4-3	2	S3-1	0	L2-4	0	N5-1	0
N7-2	1	N5-1	0	S7-7	2	S3-2	0	L3-4	0	S3-1	0
N7-5	1	N7-3	0	S3-2	1	S7-7	0	S3-1	0	S3-2	0
L1-2	0	N7-5	0	S7-8	1	S7-8	0	S3-2	0	S7-6	0

However, Figure 4-9, Figure 4-10 and Figure 4-11illustrate slight differences in the mean scores affected by gender, for example images L5-1, L5-3, L6-1 and L6-2 in Figure 4-9, and L5-1 and L5-3 in Figure 4-10with a differentiation rate of 50%. Finally, S7-2 and S7-4 also have a differentiation rate of just under 50% in Figure 4-11.

Guessed Images Based on Gender

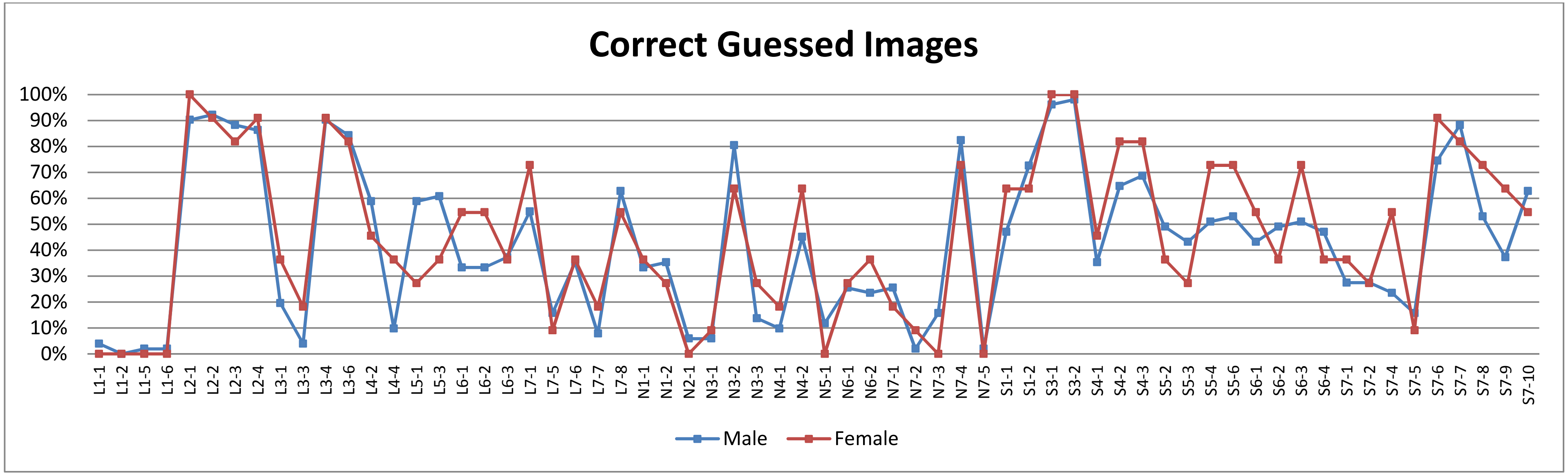


Figure 4-9 a comparison on gender for guessed images

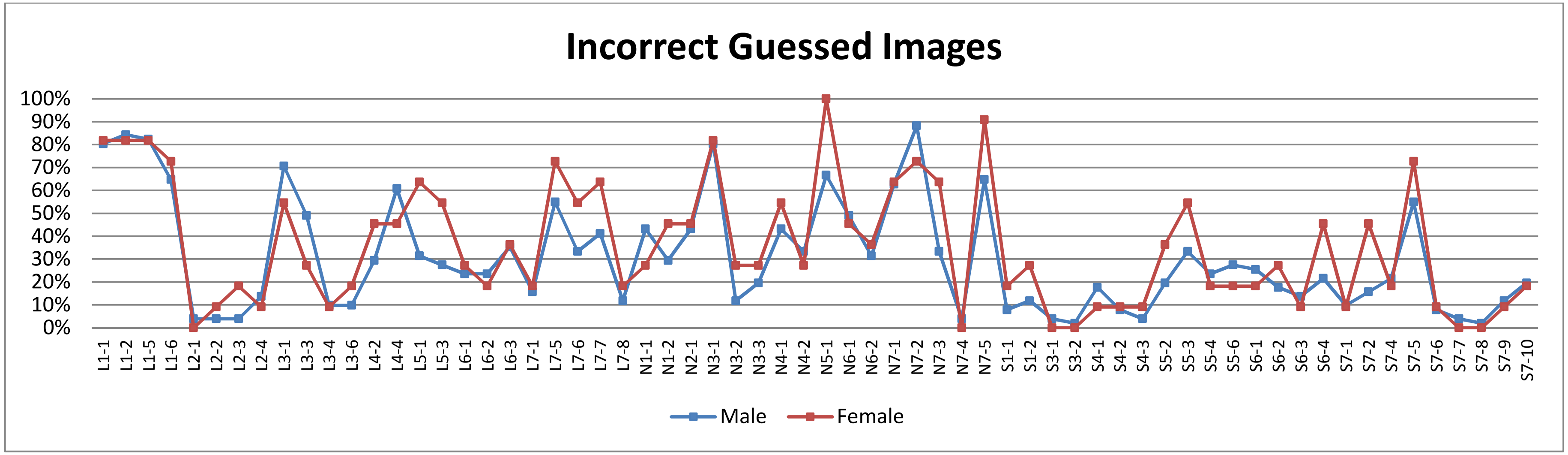


Figure 4-10 a comparison on gender for incorrect guessed images

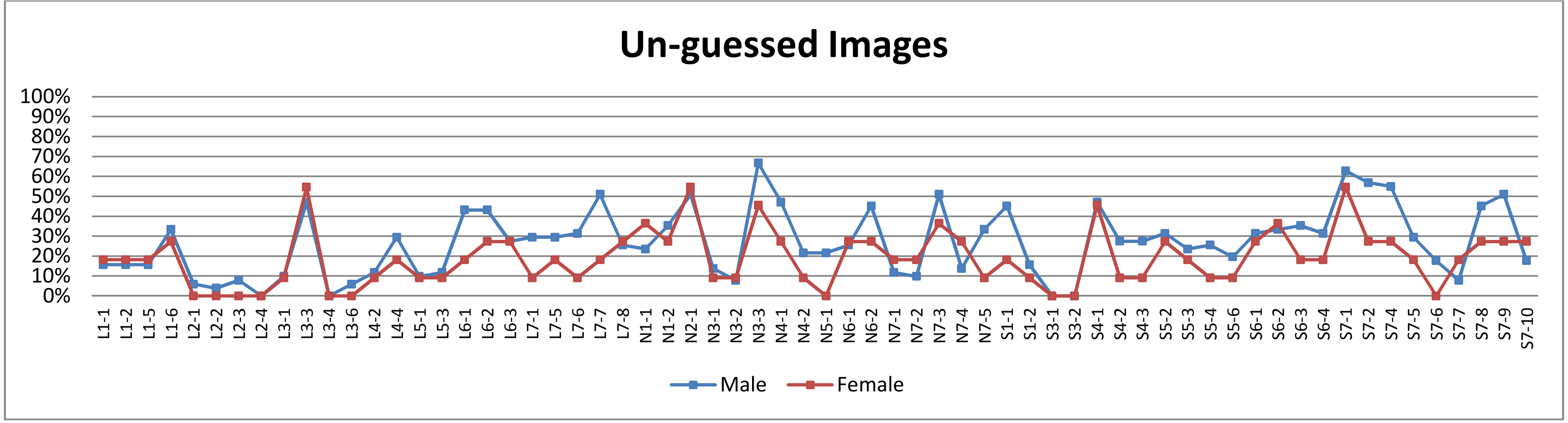


Figure 4-11 a comparison on gender for unknown guessed images

4.3.3 The most guessed and un-guessed image by Nationality

In this section, the participants were divided into four main categories depending on their nationality: Scots, Libyans, Nigerian and Other countries. The purpose of dividing participants into these four categories was to examine whether the guessability of drawn images was influenced by participants from these countries or not. It can be seen from Table 4-5 that the Libyan and Scottish participants were more able to guess images drawn from their own cultures, which indicates that they may have recognised these images.

However, Figure 4-12, Figure 4-13 and Figure 4-14, illustrated that several images were significantly different in their mean scores as affected by nationality; for example images L5-1, L5-3, L6-1, L6-2, L6-3, S5-6 and S6-4 in Figure 4-12 which sometimes recorded a differentiation rate of up to 70%. L5-1, L5-3, S5-2, S5-4, S6-2 and S6-4 in Figure 4-13 were affected by Nigerians rather than by other nationalities and sometimes had a differentiation rate of up to 80%. Finally, L6-1, L6-2, N1-2, N2-1, S6-4, S7-4 and S7-8 had differentiation rates of up to 40%, as the Figures show. Thus the ability to guess some images strongly depends on the culture of the attacker.

Table 4-5 Order of correctly and incorrectly guessed images, by nationality

Scottish (25)				Libyan (13)				Nigerian (6)				Other Nationality (18)			
Doodle	C	W	DN	Doodle	C	W	DN	Doodle	C	W	DN	Doodle	C	W	DN
S3-2	25	0	0	L2-3	13	0	0	N3-2	6	0	0	S3-2	17	1	0
S3-1	25	0	0	S3-2	13	0	0	S3-2	6	0	0	L2-2	17	0	1
S7-7	24	0	1	L3-6	13	0	0	L3-6	6	0	0	S3-1	17	1	0
S1-2	22	2	1	L2-2	13	0	0	L3-4	6	0	0	L2-1	17	0	1
L2-2	22	2	1	L3-4	13	0	0	S7-7	6	0	0	L2-3	16	2	0
L3-4	21	4	0	S3-1	13	0	0	S7-8	6	0	0	L3-4	16	2	0
L2-4	21	4	0	L2-4	13	0	0	L2-1	6	0	0	L2-4	16	2	0
L2-1	21	2	2	N7-4	13	0	0	L2-3	5	0	1	L3-6	15	2	1
N3-2	20	3	2	L2-1	13	0	0	S7-6	5	1	0	S7-6	15	1	2
L2-3	20	2	3	L5-1	12	0	1	L2-2	5	1	0	S7-7	15	1	2
S4-2	20	1	4	L4-2	12	0	1	S3-1	5	1	0	N7-4	14	0	4
S4-3	19	1	5	N3-2	11	2	0	N7-4	5	0	1	S7-8	14	0	4
L3-6	18	5	2	S4-2	11	0	2	L7-1	5	1	0	S1-1	13	2	3
S5-4	18	1	6	L6-2	11	0	2	L7-6	5	1	0	L7-8	13	2	3
N7-4	18	2	5	S7-6	11	1	1	N1-1	5	1	0	S5-6	13	3	2
S7-6	17	2	6	S4-3	11	0	2	S1-1	4	0	2	S1-2	12	4	2
S7-10	16	2	7	L5-3	11	1	1	S4-3	4	1	1	L7-1	12	1	5
S6-2	15	2	8	S6-3	11	1	1	N6-1	4	1	1	S7-10	12	5	1
S5-6	15	5	5	S6-4	11	2	0	S6-1	4	1	1	N3-2	11	4	3
S6-1	14	3	8	L6-3	10	1	2	L7-8	4	1	1	L5-1	11	7	0
L7-1	12	6	7	L7-8	10	0	3	L2-4	4	2	0	N4-2	11	6	1
S7-9	12	1	12	S7-7	9	1	3	S5-3	4	2	0	L4-2	11	7	0
S5-2	12	4	9	L7-6	9	2	2	S7-9	4	1	1	L5-3	11	6	1
S6-3	12	2	11	L6-1	9	2	2	S7-10	4	1	1	S4-3	10	1	7
N4-2	11	7	7	S1-2	8	0	5	L6-1	4	1	1	S4-2	9	2	7
L4-2	11	9	5	S5-2	8	3	2	S6-3	4	1	1	S5-4	9	6	3
L7-8	11	5	9	S1-1	7	1	5	L6-2	3	2	1	S6-1	8	6	4
L5-3	11	9	5	N1-2	7	2	4	S7-4	3	2	1	S7-9	8	2	8
S7-8	11	1	13	S5-6	7	2	4	N1-2	3	1	2	S5-2	8	2	8
S4-1	10	3	12	L7-1	7	2	4	N4-2	3	1	2	S6-2	7	3	8
N6-2	10	4	11	S6-2	6	2	5	L6-3	3	1	2	S4-1	7	2	9
S6-4	10	4	11	S7-10	6	4	3	S4-1	3	1	2	S5-3	7	9	2
L5-1	9	11	5	N1-1	6	4	3	S4-2	2	2	2	S6-3	7	4	7
S7-4	9	4	12	N4-2	5	6	2	S1-2	2	3	1	S6-4	7	5	6
S5-3	9	7	9	S5-4	5	3	5	S5-4	2	4	0	S7-4	6	5	7
S7-2	8	3	14	N6-1	5	7	1	L5-3	2	4	0	N7-1	6	11	1
S1-1	7	3	15	S5-3	5	5	3	N6-2	2	2	2	L6-1	6	5	7
N1-2	7	9	9	S7-8	4	0	9	S7-1	2	2	2	N1-1	6	10	2
N7-1	7	15	3	S7-1	4	1	8	N4-1	1	2	3	L6-2	5	4	9
L3-1	7	14	4	L7-5	3	7	3	N5-1	1	4	1	S7-2	5	4	9
S7-1	7	2	16	S7-5	3	7	3	L5-1	1	5	0	L6-3	5	9	4
L6-3	5	11	9	S7-2	3	3	7	S6-2	1	5	0	L7-6	5	9	4
L6-2	4	8	13	S4-1	3	4	6	S7-2	1	3	2	L4-4	5	6	7
L7-5	4	12	9	S6-1	2	5	6	N7-1	1	5	0	L3-1	5	11	2
S7-5	4	12	9	N7-3	2	2	9	L4-2	1	4	1	N3-3	5	4	9
N6-1	4	12	9	S7-9	2	3	8	N7-3	1	3	2	S7-1	5	1	12
L6-1	4	7	14	L7-7	2	6	5	L7-7	1	4	1	N1-2	4	8	6
N3-3	4	5	16	L4-4	2	9	2	S5-2	1	5	0	N4-1	3	7	8
N1-1	4	10	11	L3-1	2	11	0	L1-1	0	6	0	N6-1	3	10	5
N2-1	3	13	9	N4-1	1	7	5	N7-2	0	5	1	N6-2	3	7	8
N3-1	3	17	5	N5-1	1	8	4	L7-5	0	5	1	N5-1	2	14	2
N7-3	3	10	12	N7-1	1	8	4	S7-5	0	5	1	L7-5	2	12	4
L7-6	3	11	11	L3-3	1	6	6	L1-2	0	5	1	S7-5	2	12	4
N4-1	2	12	11	N6-2	1	7	5	N2-1	0	3	3	N7-3	2	9	7
N5-1	2	19	4	N3-3	1	2	10	L1-6	0	5	1	L1-1	1	14	3
L3-3	2	8	15	L1-5	1	9	3	N3-1	0	4	2	N7-2	1	16	1
L7-7	2	11	12	L1-1	0	12	1	L3-3	0	4	2	N3-1	1	16	1
L4-4	2	15	8	N7-2	0	11	2	S5-6	0	6	0	L3-3	1	10	7
L1-1	1	18	6	S7-4	0	2	11	N7-5	0	6	0	L7-7	1	7	10
N7-2	1	21	3	L1-2	0	10	3	L4-4	0	6	0	N7-5	1	13	4
L1-6	1	15	9	N2-1	0	1	12	L3-1	0	6	0	L1-2	0	14	4
L1-2	0	23	2	L1-6	0	8	5	N3-3	0	2	4	N2-1	0	10	8
N7-5	0	16	9	N3-1	0	13	0	S6-4	0	5	1	L1-6	0	13	5
L1-5	0	20	5	N7-5	0	8	5	L1-5	0	6	0	L1-5	0	16	2

Guessed Images Based on Nationality

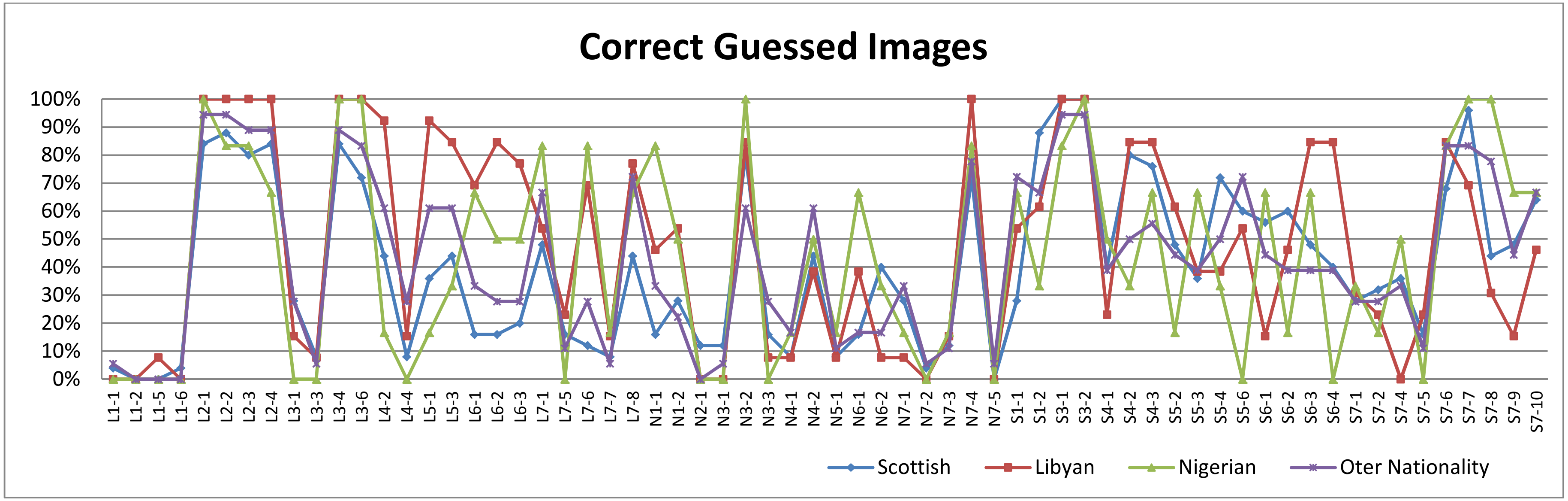


Figure 4-12 a comparison on nationality for correct guessed images

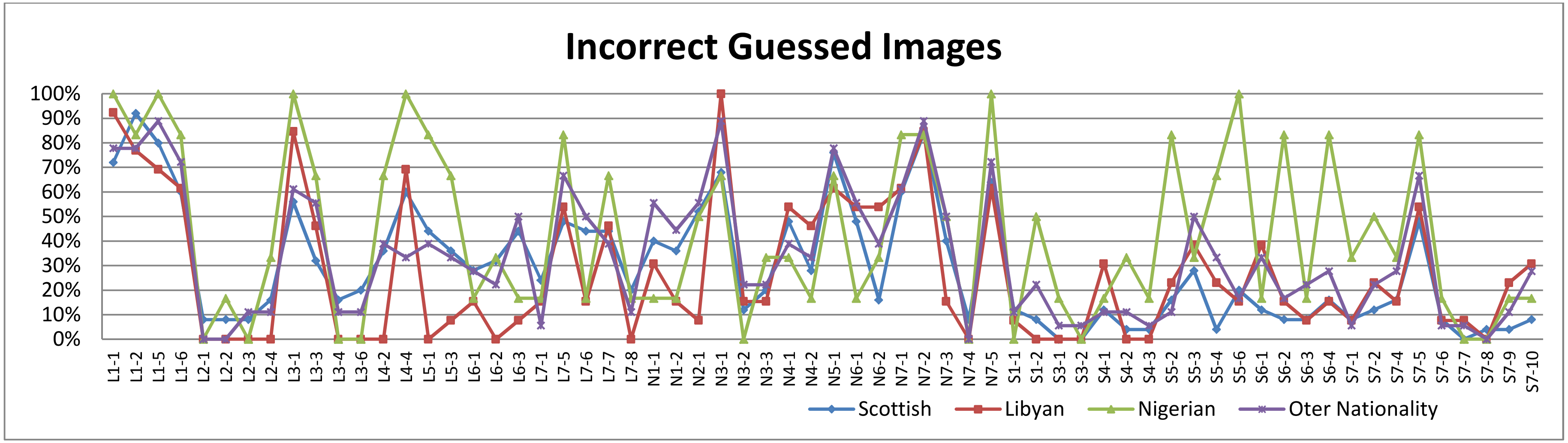


Figure 4-13 a comparison on nationality for incorrect guessed images

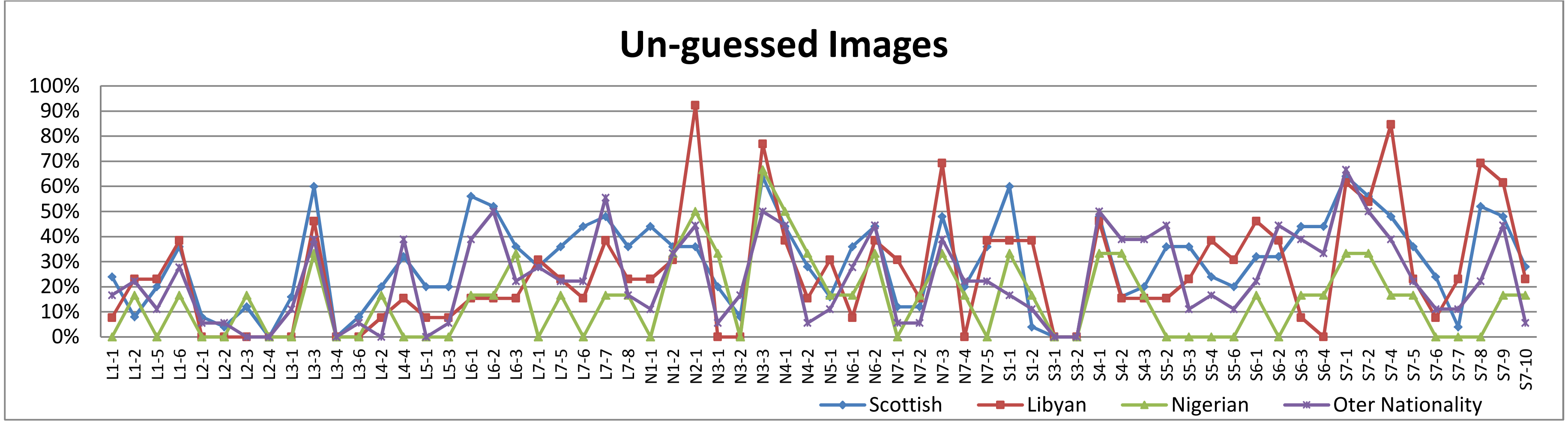


Figure 4-14 a comparison on nationality for unknown guessed images

4.3.4 The users who guessed the most images

The ability of guessing images differed from user to user. Table 4-7, displays the rank of the participants who guessed more hand-drawn images, ordered from the highest to the lowest, and also displays the gender and the country of origin of those participants. Before that, Table 4-6, below, shows that the most successful participant was able to guess 42 out of 64 hand drawn images whereas the lowest recorded was 14 images out of 64. The most frequently guessed scores by all participants was 32 images and the mean was 28.

Table 4-6 Guesses by participants

Average	Mode	Max	Min
28	32	42	14

This might leads to the ability of predicted the image’s categories where many images used in this experiment contained some cultural hints. Obviously, abstract images were less observed than other images, almost 50% of the images were not discovered and hard to recognize by the participants.

Table 4-7 User guessing rankings

Rank	User	Gender	Country	Guessed Rate
1	U04	Male	Jordan	42
2	U41	Male	Greece	41
3	U21	Male	United Kingdom	40
4	U46	Male	Libya	39
5	U58	Male	Nigeria	37
6	U48	Male	Libya	36
7	U25	Male	Libya	36
8	U36	Female	United Kingdom	35
9	U23	Male	United Kingdom	35
10	U39	Male	United Kingdom	34
11	U49	Male	Libya	33
12	U55	Male	Saudi Arabia	33
13	U44	Male	Libya	33
14	U34	Female	United Kingdom	32
15	U30	Male	United Kingdom	32
16	U60	Male	Nigeria	32
17	U18	Female	Romania	32
18	U05	Female	United Kingdom	32
19	U56	Female	Nigeria	32
20	U61	Female	Oman	32
21	U11	Female	Latvia	32
22	U26	Male	Libya	31
23	U28	Male	Libya	30
24	U08	Male	United Kingdom	30
25	U31	Male	Germany	30
26	U35	Male	Romania	30
27	U42	Male	United Kingdom	30
28	U01	Male	Saudi Arabia	29
29	U52	Male	Libya	29
30	U29	Female	Poland	29
31	U27	Male	United Kingdom	29
32	U19	Male	Libya	29
33	U47	Female	Libya	29
34	U50	Male	United Kingdom	28
35	U14	Male	United Kingdom	27
36	U12	Male	United Kingdom	27
37	U33	Male	Bulgaria	27
38	U57	Male	Nigeria	27
39	U59	Male	United Kingdom	27
40	U13	Male	United Kingdom	25
41	U32	Male	Italy	25
42	U62	Male	Libya	25
43	U45	Male	Libya	24
44	U43	Male	Libya	24
45	U02	Male	Bangladesh	24
46	U22	Male	United Kingdom	23
47	U54	Male	Jordan	23
48	U20	Male	United Kingdom	23
49	U06	Female	United Kingdom	23
50	U24	Male	Romania	22
51	U09	Male	United Kingdom	22
52	U51	Male	Nigeria	22
53	U53	Male	Nigeria	21
54	U38	Male	United Kingdom	21
55	U40	Male	Romania	20
56	U16	Male	United Kingdom	19
57	U07	Male	United Kingdom	19
58	U10	Male	India	19
59	U17	Male	China	17
60	U15	Female	United Kingdom	17
61	U03	Male	United Kingdom	14
62	U37	Male	United Kingdom	14

4.3.5 Overall guessed images drawn by cultural groups and by categories

It has been shown by the work reported in this section that it is possible to construct a guessing attack based on the bias in the user's choice of images. The bias in user selection towards particular image categories has been shown for the drawn images and was summarised in Figure 4-15. It can be seen that the highest category, with a mean score of 45%, was religious imagery, and then came nations with a mean of 34%, while the last category was sport, with a mean of 15%.

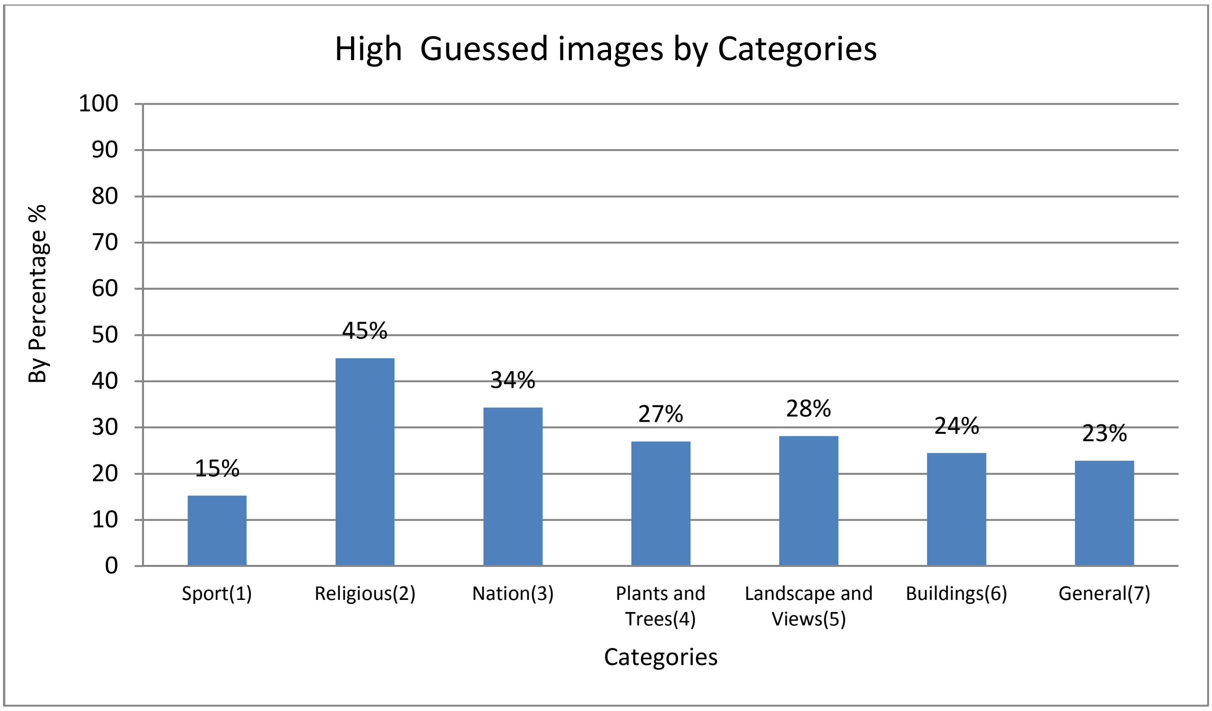


Figure 4-15 Most frequently guessed images, by category

Additionally, the bias in user selection towards an image of a particular country was shown for the drawn images, also as displayed in Figure 4-16 and it can be observed that the most guessed images drawn by country were the Scottish ones, with a mean score of just under 35% followed by the Libyan doodles, with a mean of about 25% and last in terms of guessability came the Nigerian drawings, with a mean of 14%.

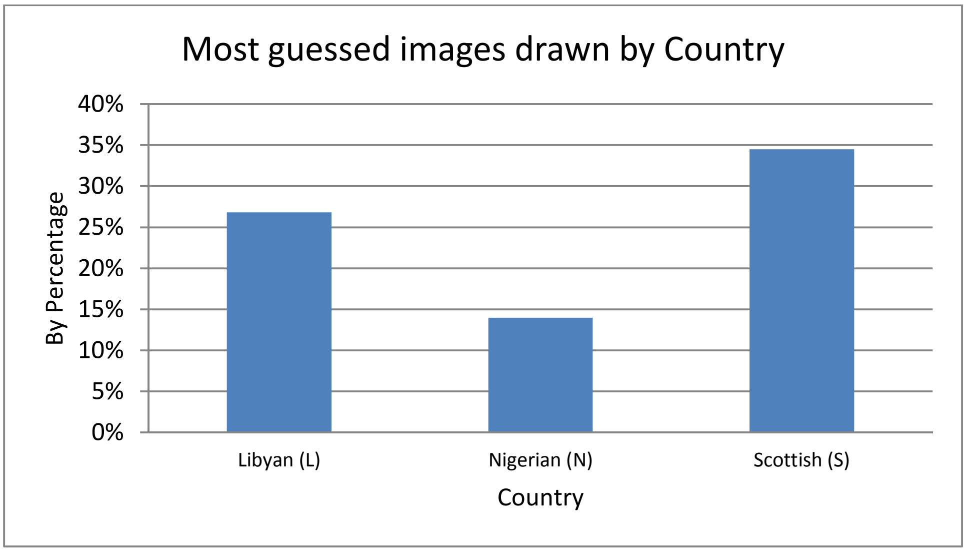


Figure 4-16 Most guessed images drawn, by country

4.4 Discussion

The findings of the previous study by Hayashi et al.[40] differed from the study reported in this chapter. Hayashi et al considered educated guess attacks against the Use Your Illusion scheme (a type of image) where the passimages were provided by users. Two educated guessing attacks were used: collective educated guess attacks and individualized educated guess attacks. Collective educated guess attacks refer to the guessing of the images that are most popular with a collection of users, whereas the individualized educated guess attacks refer to the guessing of the images that were selected by an individual user. Two user studies were required to examine both attacks, and these evaluated the use of the distortion of images approach taken in [39] to mitigate these attacks. However, the differences between the present study and that reported by Hayashi et al. are that the images and types of attacks were not the same. First, the kinds of images used have not been the same, as here we have used hand- drawn images which are more abstract images. Second, the type of attack examined in this work is based on collective information about user biases. In contrast, in the study by Hayashi et al. [40], the attack was based on knowledge about the users who were going to be attacked (or their potential biases). The protocol used with the participants was also different in the prior study, as three authentication images were set out to be guessed from a set of 27, where here the participants were asked to guess all 64 images and tried to put them into right categories. However, in Hayashi et al.'s study, three of the 15 attackers correctly identified all three passimages from the set of 27 images shown within 10 guesses, in the context of strangers' guesses (educated guess attacks). Images with similar properties were selected by these attackers by exploiting the connection between the images taken by the victim, which is different from the attack modelled in this chapter which places the images in common categories and prioritises them for guessing.

English and Poet [164] also investigated the guessability of images, calling this attack SOGA, meaning a Semantic Ordered Guessing Attack. The study focuses into exploring the feasibility of prioritised guessing attacks. The challenge screen presented images in which the attacker selects the most probable. 64 users were provided sets of 4 images, which belonged to one of twelve distinct categories. the categories ordering from most to least probable. Additionally, constructing a challenge screen for each passimage and choosing the image from most likely category given the ordering noted is the next step that an attack launched by. However, varying degrees dependent on how distractors are selected for a given challenge screen became apparent that bias in user choice could decrease the estimated guessability. Two schemes were applied in this study, one with doodles and the other with photographic images. They reported that guessability was increased by a factor of 18 with photographic images and by 3.3 times with doodles.

The present study has therefore been different in that it has focused on one main criteria, culture, rather than the more general characteristics in the other studies.

4.4.1 Security of drawings

The results shown in Table 4-1, Table 4-2, Table 4-3, Table 4-4 and Table 4-5 show that there was a varying level of security in the drawings. However, the drawings displayed in Figure 4-18 give a clear view of the most secure doodles which could be used as graphical passwords and which could not. The drawings were focused on the categories rather than the image itself. The images shown in this section were organised according to the score of how many times they had been guessed. The images used here were scored “0” only in the previous tables and meanwhile were coloured Red, Yellow or Green reflecting their security, as shown in Figure 4-17. As mentioned earlier in the results of this experiment, some images contain clear environmental hints but were guessed incorrectly, for example images L3-1, N3-1 and N7-2 displayed in Figure 4-5. This led to a further investigation, and from this, four images were picked from the images with higher scores for incorrect guesses. These were L3-1, N3-1, N7-1 and N7-2.

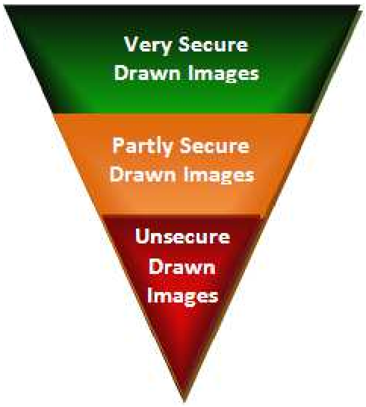


Figure 4-17 Triangle of security against guessing

The statistical test shown in Table 4-8, below, demonstrates that some doodles were classified into the wrong category based on the information on that image, for example doodle number L3-1 was drawn by a Libyan participant and contained the continent of Africa, and it is evident that 68% of participants chose the wrong category and thought it was drawn by a Nigerian. In fact this conflict happened because Libya is also located in Africa. Other examples are N3-1 and N7-2 which were drawn by Nigerians, the first contained an armour shield with two swords and a cross, and the second contained a warrior’s helmet. The doodles were expected to be drawn by Scots and this can be noted from the table where 71% and 82% of the participants classified them into the Scottish category. Another image, N7-1, was also drawn by a Nigerian and contains a Kalashnikov rifle. 61% of participants categorised the image as being drawn by a Libyan. In fact, there is no clear reason for this and it could be influenced by the civil war which had happened in the country. However, this indicates that a drawing that contains cultural hints might be suitable for security reasons if it is hard to guess.

Table 4-8 Frequency of the four most incorrect doodles

Doodle	(U) Unknown	(L) Libyan	(S) Scottish	(N) Nigerian
L3-1	10%	23%	0%	68%
N3-1	13%	10%	71%	6%
N7-1	13%	61%	2%	24%
N7-2	11%	3%	82%	3%

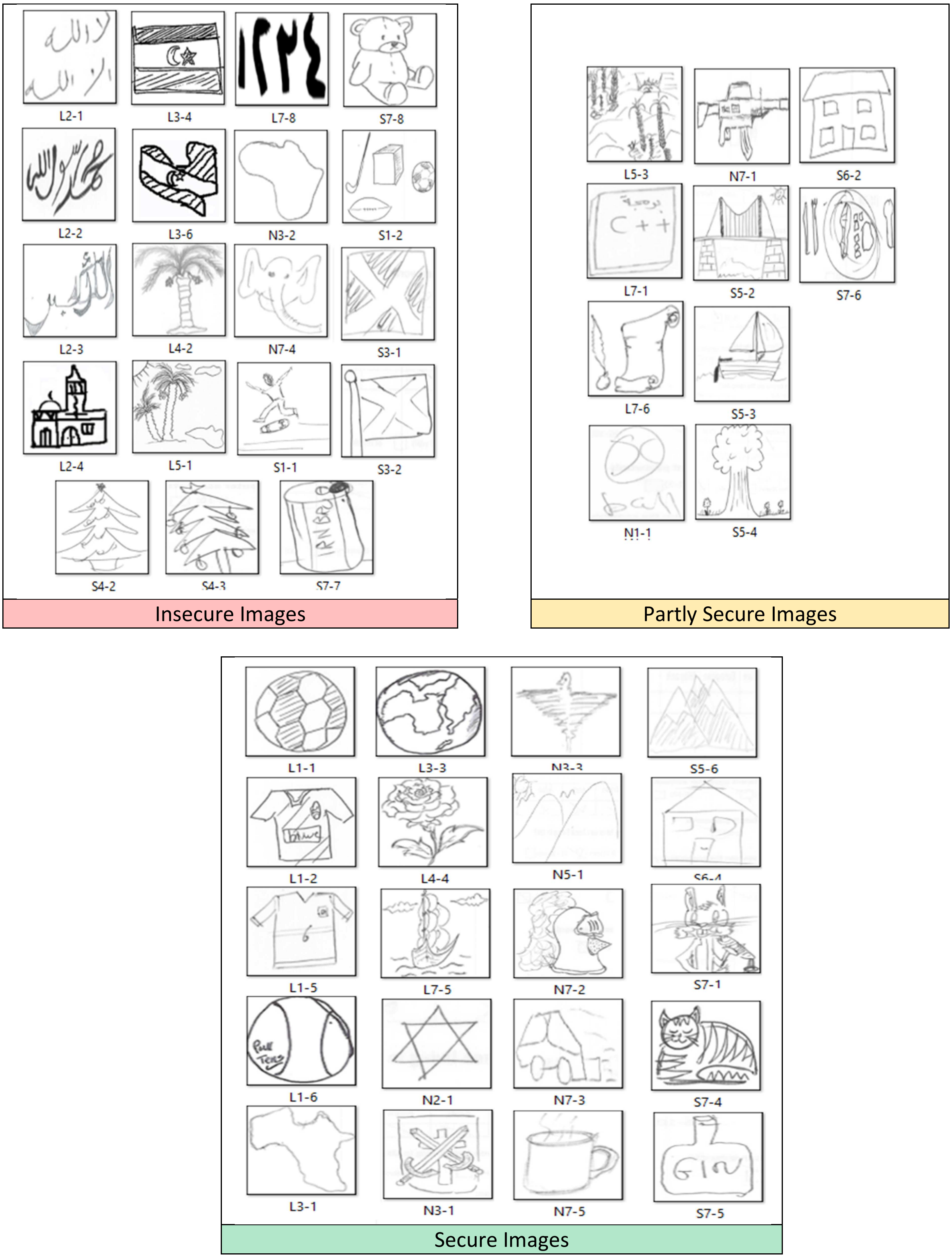


Figure 4-18 Levels of security of hand-drawn images

4.5 Conclusion

The proposal behind the work which has been presented here was to examine whether or not people could guess the hand-drawn images which were used as the graphical password of others, if they know some cultural information about the users, such as where they came from or their religion or even their hopes. The study also aims to contribute evidence of a bias in the user choice of images and considers the impact this could have on guessability. However, the results show that there is no difference between males and females and between members of different cultures in their ability to guess images. One clear result of this work is that it is apparently highly possible to guess other people’s pass images if they contain cultural characteristics, especially religious marks, otherwise it is much more difficult to guess them, and also this depends on many factors:

1. The culture where the system was used; for example if the participants are Libyans and they used such a system in Libya then the images containing Islamic marks could be not used by attackers to distinguish one user from another.
2. The place where the system was used with hand-drawn images. for example if the participants lived in Scotland then images containing national marks like flags would be hard for attackers to guess.
3. Fake attention of the users. Users can make their hand-drawn graphical passwords hard to guess by providing images that contain some cultural characteristics which are not related to them, for example the image shown in 4.4.1.

Many governments such as Hong Kong [165] and the USA [166] try to guide their people to choose a strong password. We can use the results from this chapter to provide additional guidelines for choosing a good graphical password:

1. Do not draw any image containing national landmarks that are related to your country, such as flags.
2. Do not draw any image containing religious, information such as a place of prayer.
3. Do not draw any image containing special brands of companies famous in your country such as a can of IrnBru in Scotland.
4. Do not draw any image containing text.

Chapter Five
Automatic Registration of User Drawn Graphical Passwords

5.1 Introduction

Text based passwords suffer from a major problem in that memorable passwords are not very secure and secure passwords are not very memorable [167]. Graphical passwords have been proposed as an alternative since it has been convincingly argued that images are easier to remember than text phrases [17]. In other words, many prior research studies [35], [36], [63], [168] have argued that drawings are memorable and there are a large number of different memorable graphical passwords.

There are two major types of graphical password systems: these are recognition and recall based [55] systems. In a recognition-based system, the user has to recognise their own graphical password from a collection of other images. In a recall-based system, the user has to remember their pass image and reproduce it when they log in. A text based password is a recall system since the user has to remember their password. Similarly, a paper signature is an example of a recall-based image password. The user has to reproduce their signature to sign a document.

This chapter focuses on recognition-based systems. One advantage of a recognition- based system over a recall-based system is that it is easier to recognise an image when shown it again, rather than recreate it again from scratch [36], [169]. One disadvantage is that if an attacker is shown the actual pass image then they simply needs to guess the correct one from a collection of distractor images. The security of recognition-based systems has been widely studied [40], [55] and is not the subject of this chapter, and focused only on the usability investigation of using hand drawn images.

A wide variety of types of images have been used as recognition based graphical password, including pictures, art and simple drawings [170], and user supplied simple drawings form a distinct category because they are created by the user as a form of simple art, rather than being supplied or chosen by the user. The creative effort involved makes them easier to recognise again later [61].

One feature of all graphical password systems is that the effort needed to register the pass images is greater than that which is required to register a text based password. They may be as easy to use and less error than text based passwords when the user logs in, but the initial effort needed to choose or create the graphical password may represent a significant barrier to adoption. The ease of registration is significantly affected by the types of images used and whether a recognition or recall-based system is used. These are now broken down further in the following subsections.

5.1.1 Registration when the system provides the images

Most graphical password systems provide the user with a framework [171] or a sample collection of images [58] or pictures [172] or shapes [173] to choose their password at the registration stage. Consequently, registration in these systems is straightforward but it may take same time, which may put off some users.

5.1.2 Registration when the user provides the images

If the user has to supply pass images at the registration stage, the amount of effort involved depends on whether the image already exists; it could, for example, be a photograph in their personal collection, or whether it must also be created by the user, for example in the form of a simple drawing.

In previous studies [20, 29], an administrator has provided users with a form on which to draw their pass image. The administrator then scanned this form into their system and worked on the resultant image file, splitting it into separate pass image, storing each image in a file and storing references to these files in a database associated with the users. This chapter focuses on automating this process.

5.1.3 Automatic registration of user drawn images

One way of eliminating the administrator role is to let the users scan in their own artwork and register the resulting image file. There are however many ways in which the user might get this wrong and so the system must be able to detect and correct these mistakes automatically. Software must be able to replace the human administrator. There are two parts to this software. The first part must be able to guide the user through the registration process, since a human will not be on hand to offer advice and correct errors. The second part of the software takes the submitted image file and detects and corrects any errors. It can be assumed that some, or even many, users will ignore any guidance provided when they create and submit their pass image.

Alternatively, a user may use a computer drawing tool to create their pass image. This bypasses the scanning stage, eliminating some of the possible errors. However, it is harder to create an image with a mouse than with a pen, and users may find it harder to create a pass image that they like. Once again, the system must therefore provide guidance when the user creates their pass image, and include image analysis to detect and correct any flaws in the submitted image.

The present study has built a system to explore the automatic registration of simple drawings and to seek answers to a number of questions:

1. How effectively can users be guided through the registration process?
2. How effective is our image analysis software at detecting and correcting user mistakes after scanning drawn images?
3. How effective is our image analysis software at detecting and correcting user mistakes after submitting an image created by a computer drawing program?
4. Which method of providing their image did users prefer?

5.2 Drawing on Paper, Scanning and Image Analysis

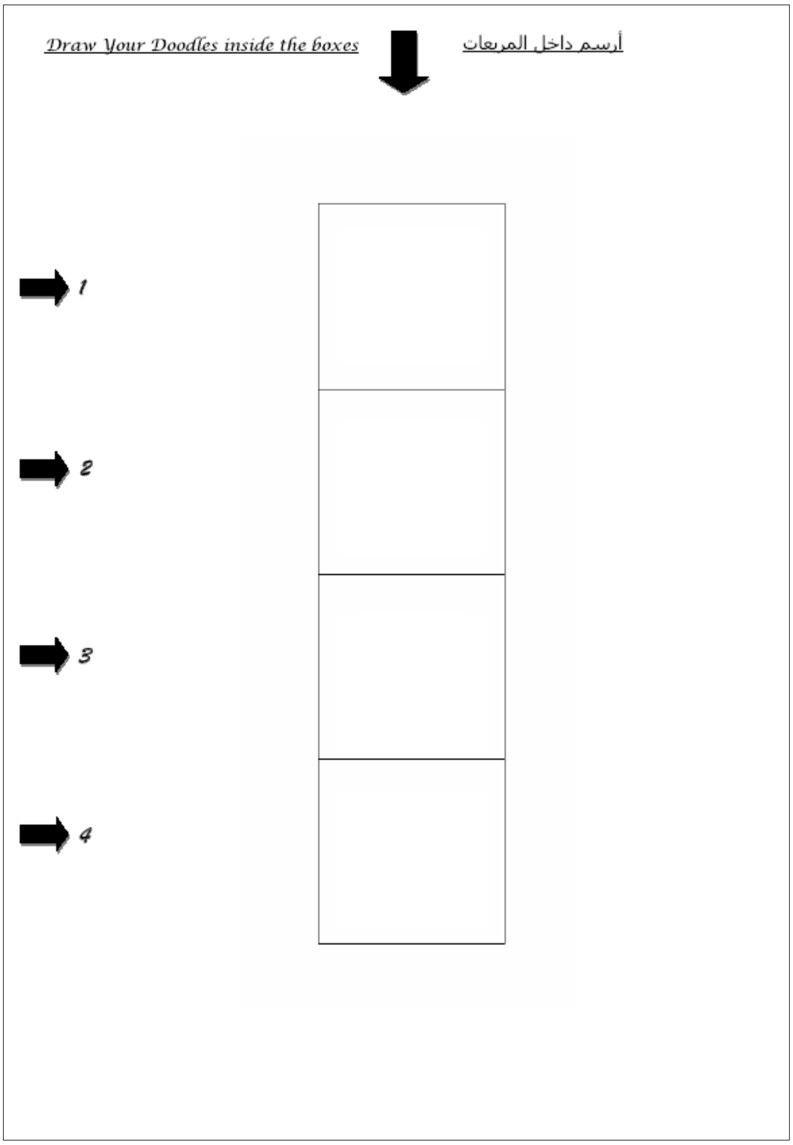
This section will describe the image analysis of drawings scanned in by users and the errors which were subsequently found. This process contains a series of steps and the algorithms can be summarized in the following points which describe the normal process if everything goes well;

1. Reading the scanned form file into a Java program as a Java image object.
2. Converting the image object into an array of black and white pixels (stored as Booleans).
3. Finding the edges of the boxes containing the 4 drawings.
4. Copying each drawing to their black and white pixel array.
5. Writing each drawing as a PNG file.
6. Associating these drawing image files in the user’s profile in a database.

The next sections describe the steps in more detail. The software was written from scratch in Java by the author.

5.2.1 Design of the Drawing Form

The system used a drawing form which was designed to meet all the conditions listed in the previous section. Users printed out the form, drew their images in the boxes, scanned the form in and submitted the file that was produced. A copy of this form is shown in Figure 5-1.



Draw Your Doodles inside the boxes أرسم داخل المربعات

1

2

3

4

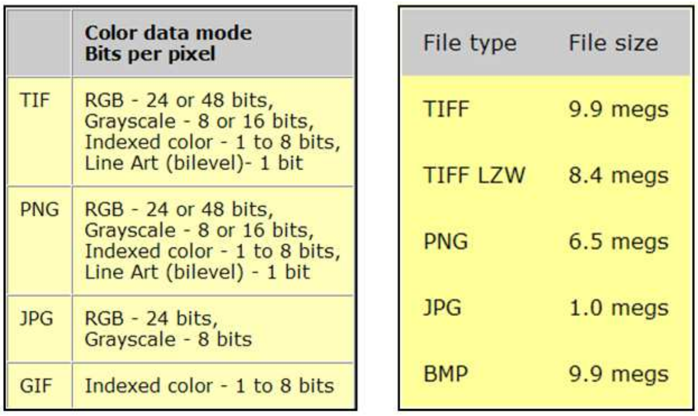
Figure 5-1 Drawing Form

The boxes were made small to discourage the production of over-elaborate drawings. Users see their drawings at about half this size when they log in. The four boxes had the same width and height and this enabled the software to determine the edges of each drawing image box. The four boxes were located exactly in the middle of the form. In addition, three different places on the form were identified to determine whether the paper had been scanned in the right direction or not and these three places were represented by three pixels: 2 blacks (inside the arrows) and one white (on the opposite side from one of the arrows located on the form). More details about this are described in section 5.2.4. An earlier prototype version of the form had larger spaces for the images, and same participant provided elaborate drawings rather than doodles which the smaller boxes prevented this.

The use of arrows in standard places made it easier to write the image recognition software.

5.2.2 Java and image file format

There are many types of image formats, such as TIF, JPG, GIF and PNG (Portable Network Graphics).The tables below describe some of the features of these formats, as described by Fulton[174]. Java has libraries to read files in all of these formats and also to write them out again. Thus, the image analysis software can cope with many different image file formats supplied by the user. PNG was used in the experiments.



	Color data mode Bits per pixel
TIF	RGB - 24 or 48 bits, Grayscale - 8 or 16 bits, Indexed color - 1 to 8 bits, Line Art (bilevel)- 1 bit
PNG	RGB - 24 or 48 bits, Grayscale - 8 or 16 bits, Indexed color - 1 to 8 bits, Line Art (bilevel) - 1 bit
JPG	RGB - 24 bits, Grayscale - 8 bits
GIF	Indexed color - 1 to 8 bits

File type	File size
TIFF	9.9 megs
TIFF LZW	8.4 megs
PNG	6.5 megs
JPG	1.0 megs
BMP	9.9 megs

Figure 5-2 Image formats comparison stated by Fulton.

The first stage of image processing was to convert each coloured pixel to a single bit black or white value. If any of the red, green, or blue components were less than half strength then the pixel was black; otherwise, it was white. The actual 50% value is not critical since black pixel will have a much higher value and white pixels a much lower one.

5.2.3 Finding the edges of the boxes

The edges of the block of 4 boxes containing the drawing were found using a vertical and horizontal scanning algorithm applied to the black and white pixel array. The 4 boxes were all the same size, allowing the algorithm to identify the pixels belonging to each individual drawing. These were copied to individual black and white pixel arrays. The results applied are shown in Figure 5-3.

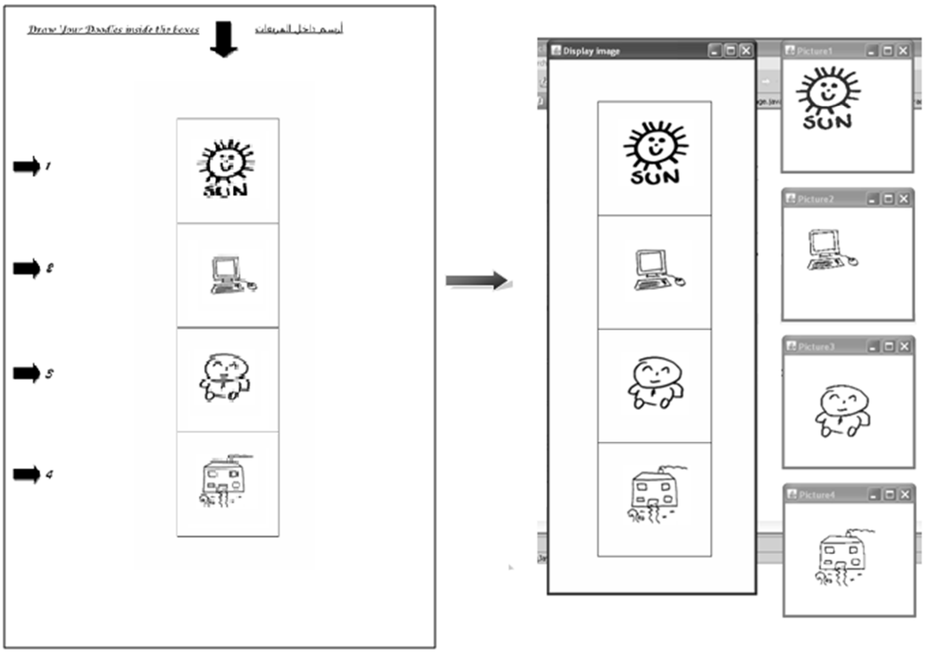


Figure 5-3 ExtractingThe Four Drawn Images

5.2.4 Correcting drawing and scanning errors

The Java code also used to correct a number of possible errors that the user could make if they did not follow the instructions. It is inevitable that some users will make mistakes and so the image analysis software must be able to detect and correct them automatically. Some of the mistakes which were anticipated were as follows:

- Drawing in the wrong colour (not black).
- Using paper that was not white; e.g. gray.
- Scanning in upside down.
- Scanning with the page tilted to one side.
- Scanning with too high a resolution.
- Poor quality scanning with some pixels missing.

5.2.4.1 Drawing in the wrong colour and using paper that was not white

The first two problems were corrected by converting to black and white pixels. This would not cope with a user who draws their picture in black on a blue sheet of paper, but that was not expected to happen often. Users were told to draw on white paper and the system can cope with gray paper because the pixel values will still be less than the 50% threshold. This is illustrated in Figure 5-4.

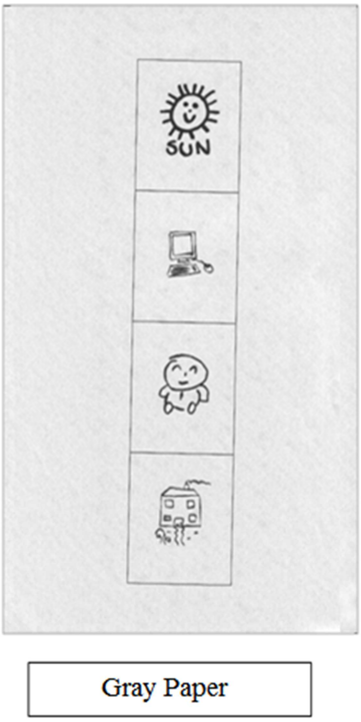


Figure 5-4 GrayPaper

5.2.4.2 Scanning in upside down

Upside down scanning is detected by locating the solid black arrow guide marks on the form using a scanline algorithm [175]. In fact, the black guide arrows on the form have two goals. The first is to guide the users to draw images on the boxes and number their drawing. The second is to determine whether or not the scanned form was scanned in the right direction. The four arrows should be on the left, and if they are on the right then the whole form is rotated by 180°. Checking whether the form is correctly aligned was performed by checking the three points on the form: The first point was located on the top arrow at the middle of the form, the second point located on the third arrow on the form and the last checking point is located on the other side of the form; an example of checking these points is shown below. If the three checking points were in the right places, this proved that the form had been scanned in the correct direction.

```
Checking Up Side Down

IF (The first point contain a black pixel) and
        (The second point contain a black pixel) and
            (The third point contain a white pixel) then

      The Form was scanned in the right direction
    Else
          The Form was scanned in the wrong direction
            Rotate form through $180^o$
End IF
```

5.2.4.3 Scanning with the page tilted to one side

A left or right tilt is detected by the algorithm to find the edges of the block of 4 boxes. An example of right and left tilted scanned image is shown in Figure 5-5.

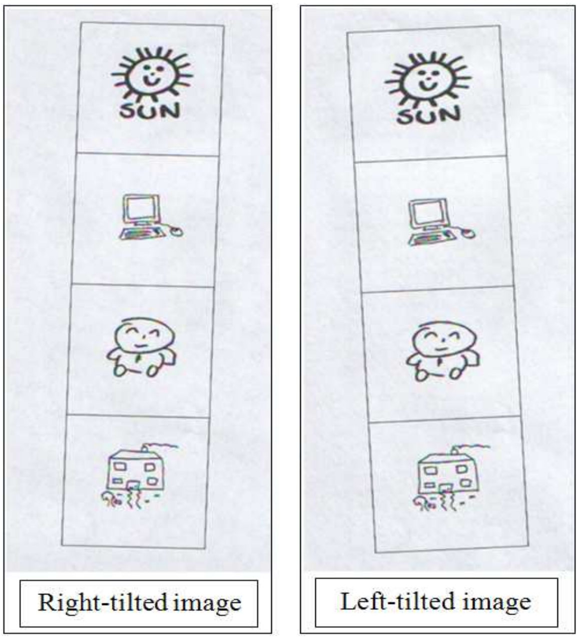


Figure 5-5 Non-accurate images

The scanline algorithm finds both the first and the last black pixel when scanning from the left, the right, the top and the bottom. This gives a measure of the degree of tilt. Each pixel is represented by two pairs of variables (x, y). Consequently, the four edges will be defined by the corner (x1, y1), (x2, y2),(x3, y3),(x4, y4). Determining whether the tilt is on the right hand side or on the left hand side, is achieved by comparing y1 and y3. If y1 > y3 then the tilt is on the right; otherwise, the tilt is on the left. If a tilt is detected then new values are calculated for the four corner points. For example, if a right tilt is detected, the following corrections are made:

```
newX1=x1;
newY1=y3;
newX2=x1;
newY2=y2;
newX3=x4;
newY3=y3;
newX4=x4;
newY4=y2;
```

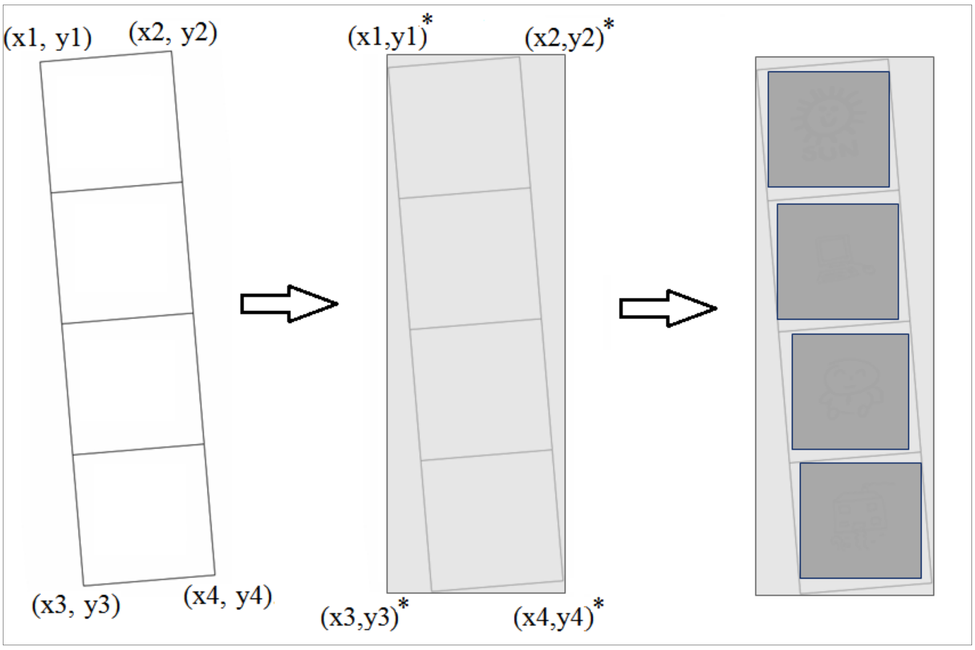


Figure 5-6 Solving a Tilt Problem.

The coordinates for each of the 4 individual boxes are then calculated from the old and new bounding box coordinates using liner interpolation. Figure 5-6, above, shows an example of how the algorithm works. Note that the edges of each individual image are cropped and the actual image are slightly rotated. This does not have a noticeable effect with simple drawings.

5.2.4.4 Scanning with too high a resolution

Detection of the use of too high a resolution is done by looking at the dimensions of the form image. A lower resolution version is constructed from the black and white pixel array, ensuring that no black pixel is lost. The dimensions of the image are determined by measuring the width and the height of each scanned form. Most of the tested forms which were examined with the software had a width of less than 900 pixels and a height of less than 1250 pixels. This resulted in individual images with dimensions of around 200*200 pixels, the desired size. In addition, during the experiments, tests were made on numerous scanned forms with different resolutions, and the results showed that only a few of the forms had a large width and height. It was noticeable that the scanned forms which had a greater width and height were classified into two types according to the size. In the first type, the size was almost two times the normal size whereas it was about three times in the second type.

In consequence, an algorithm was applied to bring the size of the scanned forms back to their normal size. A simple example is shown in Figure 5-7.

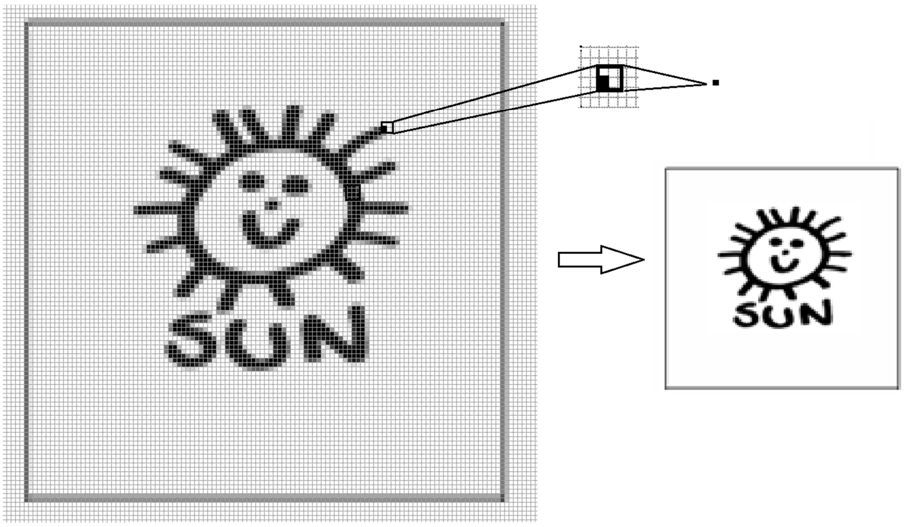


Figure 5-7 An Example of Dealing with Big Images

5.2.4.5 Poor quality scanning with some pixels missing

Finally, poor quality scanning will result in missing pixels. This will not affect step 3 of the process mentioned in section 5.2, finding the edges of the boxes, because sufficient black pixels will remain. It might however affect the quality of the final drawing, as shown in Figure 5-8. This is corrected by changing every white pixel next to a black pixel into a black pixel. This is done for all images, and will have a small visual impact for drawings that have been scanned in correctly.

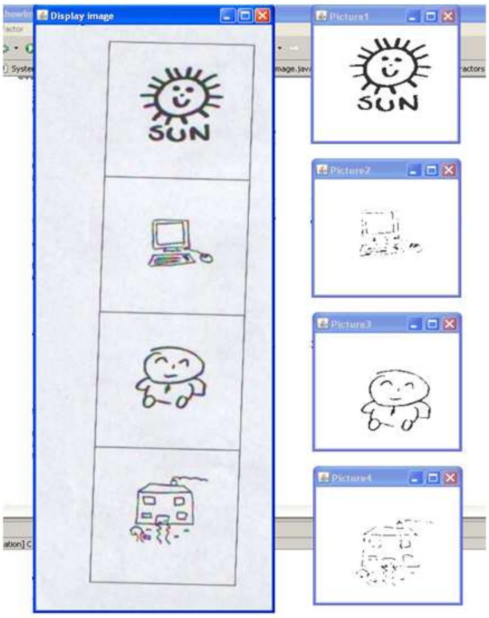
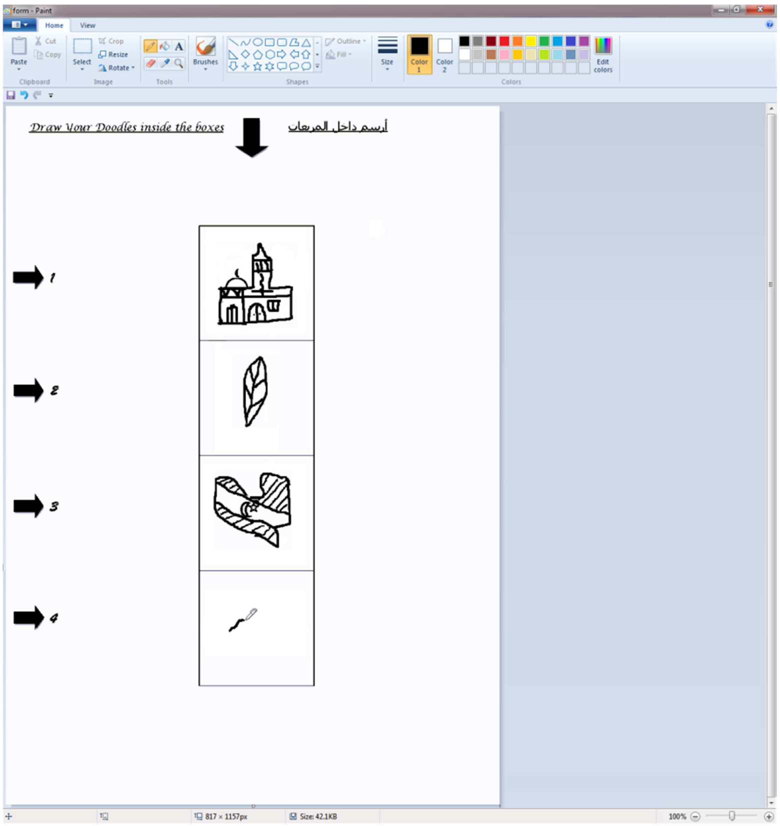


Figure 5-8 An example of missing pixels

5.3 Using Paint Software

This section illustrates the analysis of images drawn using a Paint program. Although Microsoft Paint software was adopted in the use of drawing systems in this study, any other drawing software, such as Photoshop, which is available on the user's computer, can be used. The only requirement is that the software used must produce images in a raster based format. Drawn images via the Paint software feed into the image processing pipeline but need less processing since there is less scope for user error.

The form shown in Figure 5-1 was used and the user read it into the Paint program before starting to draw their four images in the boxes provided. The users were asked to draw four images on the form using the Paint software and then to upload the saved form in PNG format. Many technical problems illustrated in the previous section were avoided with the Paint system; for example: Rotated images, Right/Left-tilted image and the quality of the scanned image. The same processes used with the scan system were applied in the Paint system to extract the four images.



Draw Your Doodles inside the boxes

أرسم داخل المربعات

Figure 5-9 Drawing Using Microsoft Paint Program

5.3.1 Correcting Paint Errors

It is inevitable that some users will make mistakes but the number of mistakes that emerged using Paint were fewer than in the scan system. The next subsections will highlight some of these possible mistakes and show how they were addressed.

5.3.1.1 Drawing in the wrong colour (not black)

One possible mistake is to draw with a different colour other than black and this problem is corrected in the same way as in the scan system, by converting the whole image into black and white pixels. If any of the red, green or blue components of a pixel were less than half strength then the pixel was black; otherwise it was white.

5.3.1.2 Using a background colour that was not white

The second possible mistake those users might make, colouring the background of the drawing form with one of many colours offered by the paint software. In fact, we do not expect that to happen. However, users were told to draw on the form only without any manipulation of the form. No one made this mistake, but the image analysis software could have corrected this problem if necessary.

5.3.1.3 Submitting the drawing form with too high resolution

The dimensions of the drawing form used in the paint system were fixed at (817x1157) pixels. Therefore, detecting too high a resolution is not applicable here unless the users manipulated the form. This is something which did not happen during the experiments.

5.3.1.4 Choosing a small sized drawing pencil

The last mistake that could happen is using a small size of drawing pencil, as shown in Figure 5-10. Choosing a small size to draw the image will affect the quality of the four generated image files. There will not be any missing pixels because there is no scanning stage, but the images could be hard to read. This was automatically corrected by the addition of extra black pixels, as described in the previous section.

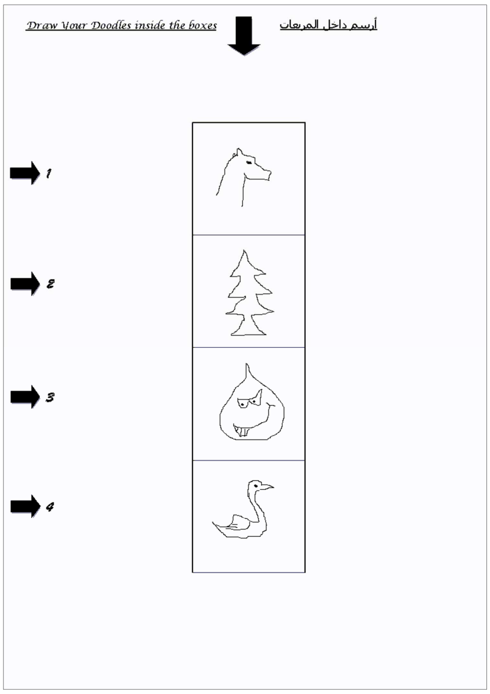


Figure 5-10 Very smallsize chosen

5.4 The Website

A website was built to run the experiments contained in the present study. It was called passdoodle and hosted on a commercial server at the following links:

www.passdoodles.net and www.passdoodles.com. These links are no longer active due to lack of funds and we could not use the university to host the website because the university would not allow connections from outside the university. This website worked with the software mentioned in the previous sections. It collected and stored basic information about the user and logged the time spent by the user on all aspects of the experiment, including successful and failed login attempts. The website contained detailed instructions, including video clips, which explained all the steps which the user had to perform.

A screenshot of the home page is shown in Figure 1 on Appendix C. The website was in both English and Arabic in order to allow experiments to be performed in Libya as well as Scotland.

The website supported three steps:

- Pre-registration;
- Full registration;
- Authentication (**login**).

Full registration could be done using either the scan-based or the Paint-based system. The links associated with each step led to pages with more detailed instructions, more description illustrated on Appendix C.

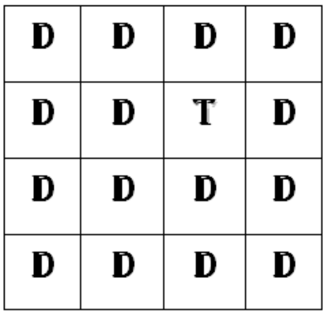
5.4.1 Offensive images

Any system that allow users to submit their own images must deal with the possibility that offensive images will be provided. Dealing with this problem is not easy, since what is offensive to one person may not be offensive to other [40]. Thus, even a human administrator may not solve the problem. This research does not address the problem of automatically dealing with offensive images, although future work in this area would be useful. We do however need to consider this problem, especially since some of the experiments were performed in a Muslim country which is sensitive to these issues. In our case, the website carried a warning and the researcher decided whether or not a submitted image was offensive; this was the reason for the 24 hour delay.

5.4.2 Authentication (Log in)

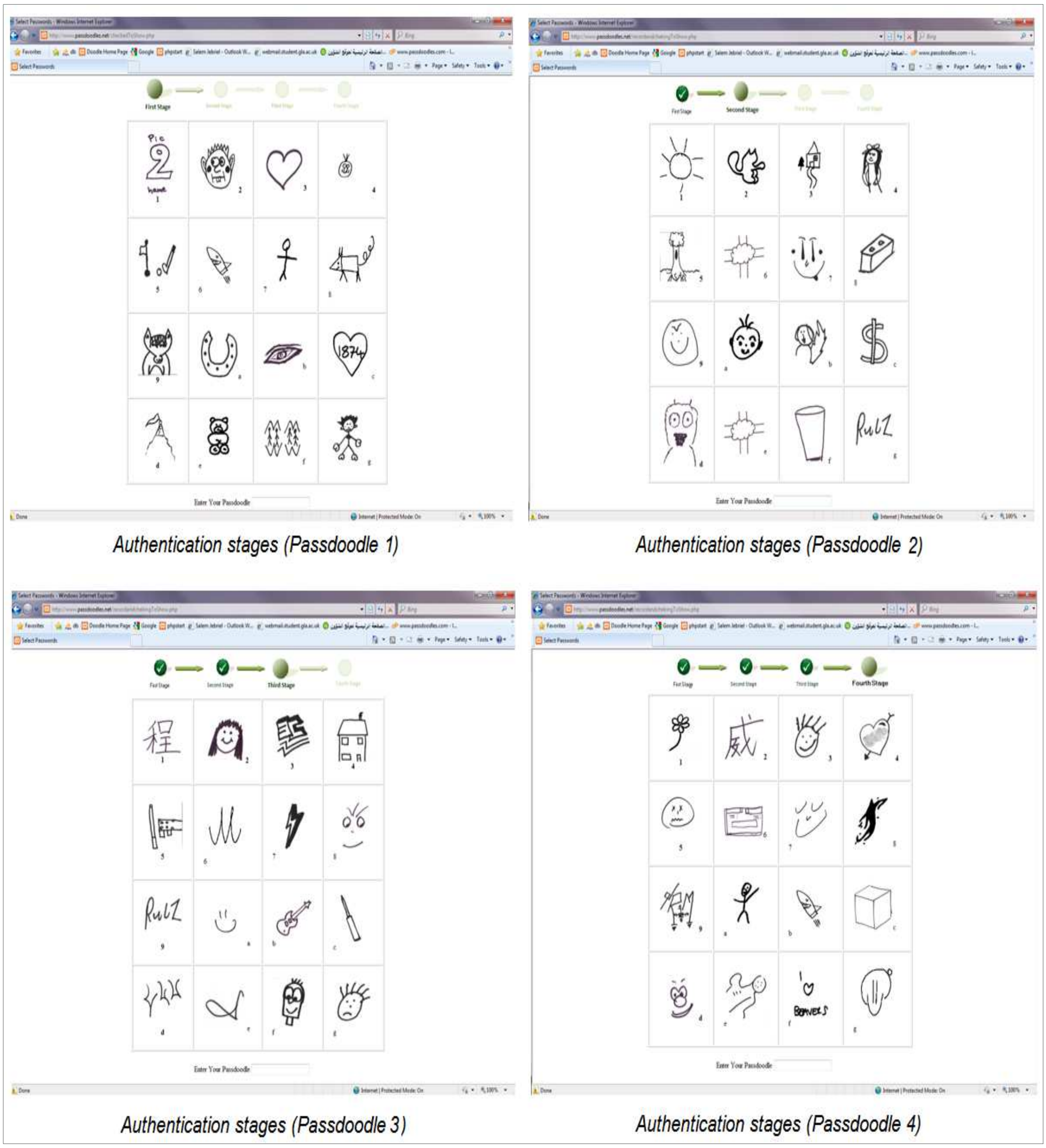
Finally, each user must login to the system for both types (scan and Paint) by using their selected username. Users were only authenticated if they passed all four authentication screens by selecting the right images. Four screens were displayed in sequence, each containing 15 distractors and one target image, as shown in Figure 5-11.

Random distractors were chosen automatically for each of the four rounds for a created account after the user completed the full registration. These distractors were then fixed, the same ones being used at every login attempt. This is to avoid an intersection attack [176]. Each image occupied a different position in the 4x4 grid each time. Samples of the four authentication screens displayed to the users are shown in Figure 5-12, below. These were presented for both types of account creation, scan and Paint and they both followed the same processes. On the other hand, the Scan type is independent from the Paint type and the user has to select the right set of 4 images in the both types.



D	D	D	D
D	D	T	D
D	D	D	D
D	D	D	D

Figure 5-11 Challenging Set
(Containing 1 target T doodle and 15 distractor doodles D)



Authentication stages (Passdoodle 1)

Authentication stages (Passdoodle 2)

Authentication stages (Passdoodle 3)

Authentication stages (Passdoodle 4)

Figure 5-12 Authentication stages

Users have to enter their correct four passdoodles to be authenticated and a small electronic ‘present’ appears if they complete the login stage without any errors; otherwise the system will ask them to try again. The electronic present contains some magic pictures and some tracking images and attractive pictures.

In this sort of system where the user supplies the images, the distractors are normally chosen from other users’ pass images. This is to make sure that they have a similar style to the actual pass images.

A library of approximately 560 hand drawn images collected from different users from previous experiments were used in this system. These images were chosen for use in the four challenge sets of each account, with each containing 15 distractors and one actual pass image. The distractors for each profile were randomly and automatically chosen after each account was created. Also, the images chosen were different for each challenge set.

At the authentication stage, each screen represents one of the user's challenge sets and each screen displays the chosen 15 distractors + the user's pass image. All these images are displayed randomly each time for each login and the security issues of using this type of system are discussed further later in the thesis.

All displayed images are numbered from 1 to 9 continuing from 'a' to 'g'. Numbering the challenge set by this method is based on a shoulder surfing study, reported in Chapter Six, which found that numbering images from 1-9 and a-g was more secure than other possible methods which were examined.

5.5 Experimental Procedure

There are a number of prior studies on how to conduct user studies, such as [177-179], which were helpful in designing this experiment. Data was collected in three ways:

- Participants answered a number of basic questions about themselves online when they created their accounts;
- User's data was logged by usage the system during the course of the experiment;
- Participants filled in a paper questionnaire to evaluate the experiment and handed it to the researcher after the experiment was completed.

A pilot study was conducted before the actual experiment in order to iron out any problems.

5.5.1 Details of the Questionnaire

The questionnaire used both open and closed forms of questions that asked participants about their experience of using the system, how usable they thought it was, and whether they preferred to use the scan or paint system. The questionnaire is included in Appendix D. The questionnaire asked participants some basic information about themselves, such as first name, sure name, gender, age, nationality, occupation, experience of computer and email address. Also, the questionnaire asked participants if they had been able to create an account, if they had been able to register scanned images and also Paint images, and whether they had been able to login to their systems. In each case, they had the opportunity, via an open question, to describe any problems that had prevented them from performing any of these activities. The participants were also asked to estimate how long they took to register their images. These self-reported times were then compared with the actual times logged by the system.

The questions on the usability of the website were based on previous studies [180] and [181]. These questions were based on the system usability scale (SUS), a usability scale that can be used for global assessments of systems usability. SUS is one of the simplest questionnaires studied (with only 10 rating scales), and yielded among the most reliable results across sample sizes. It is also interesting that SUS is the only questionnaire of those studied in [180]whose questions all addressed different aspects of the user's reaction to the website. The SUS questions (or, more precisely, statements for rating) are as follows:

1. I think that I would like to use this website frequently.
2. I found the website unnecessarily complex.
3. I thought the website was easy to use.
4. I think that I would need the support of a technical person to be able to use this website.
5. I found the various functions in this website were well integrated.
6. I thought that there was too much inconsistency in this website.
7. I would imagine that most people would learn to use this website very quickly.
8. I found the website very cumbersome to use.
9. I felt very confident using the website.
10. I needed to learn a lot of things before I could get going with this website.

The answers used a 7 point Likert scale, with 7 meaning strongly agree. There was also a N/A (not applicable) answer.

The next section of the questionnaire asked the participants what they did with their images after registration. They were given three options. The options for the images drawn on paper in the scan system were:

- Kept it.
- Threw it away.

- Disposed of it securely, for example burning or shredding it.

The options for the image files in the paint based system were similar:

- Saved it on the computer.
- Deleted it.
- Encrypted it.

This information provides insight into the participants' actual behaviour. Keeping the images is similar to writing down a text based password, and carries similar security implications.

A related question was whether the participant had used any saved images to help them to login. Again, this would help to understand how many users would actually keep their images to help them later on.

Next, the participants were asked which system they preferred, scanning or using the Paint system. They were also asked to rate how much they liked each system, using a scale of 1 to 5, with 5 meaning they liked the system a lot. They were also asked to give their opinions on the advantages and disadvantages of using the scan and Paint systems using open questions. Finally, they were given the opportunity to provide extra suggestions or comments in another open question.

5.5.2 Pilot study

A pilot study was undertaken to iron out any problems before the real test was undertaken. The participants were fellow researchers in the School of Computing Science at the University of Glasgow. They provided valuable comments on the questionnaire and the wording used throughout the system. This also ensured that the website worked and that all the correct data was logged and collected. The image analysis software also survived this test.

In fact, it should be noted that this experiment was also carried out in Libya; however problems with internet access prevented most of the participants from completing the experiment. It was therefore decided to exclude this study from the thesis.

5.5.3 The Experiment it self

Participants were recruited from various schools in the University of Glasgow and the experiment took place between 15th February and 15th May 2011. The experiment was divided into five phases:

1. The initial meeting, where the researcher met with the participants, explained what they were being asked to do, and obtained their consent.

2. The participants created their accounts privately. They also provided their basic information during this process.

3. The participants created and registered two sets of pass images, one using the scanner and the other the Paint system. Some of the participants registered using the scanner first and the others used the paint system first, in order to remove any temporal bias.

4. The participants logged into the system three times, firstly two weeks after registration, then after another two weeks and finally after a further four weeks. They were sent email reminders at the appropriate times.

5. The participants met with the researcher again and filled in the questionnaire.

5.6 Experiment Results

A total of 52 potential participants attended the initial meeting and 52 then went on to create their accounts and provide basic personal information. 41 participants then registered their images using the Paint system and using the scanner. 40 participants then logged into their systems three times, following the email prompts. Finally, 37 participants attended the final meeting and completed the questionnaire.

5.6.1 The Participants

The demographics of the participants is shown in Figure 5-13.

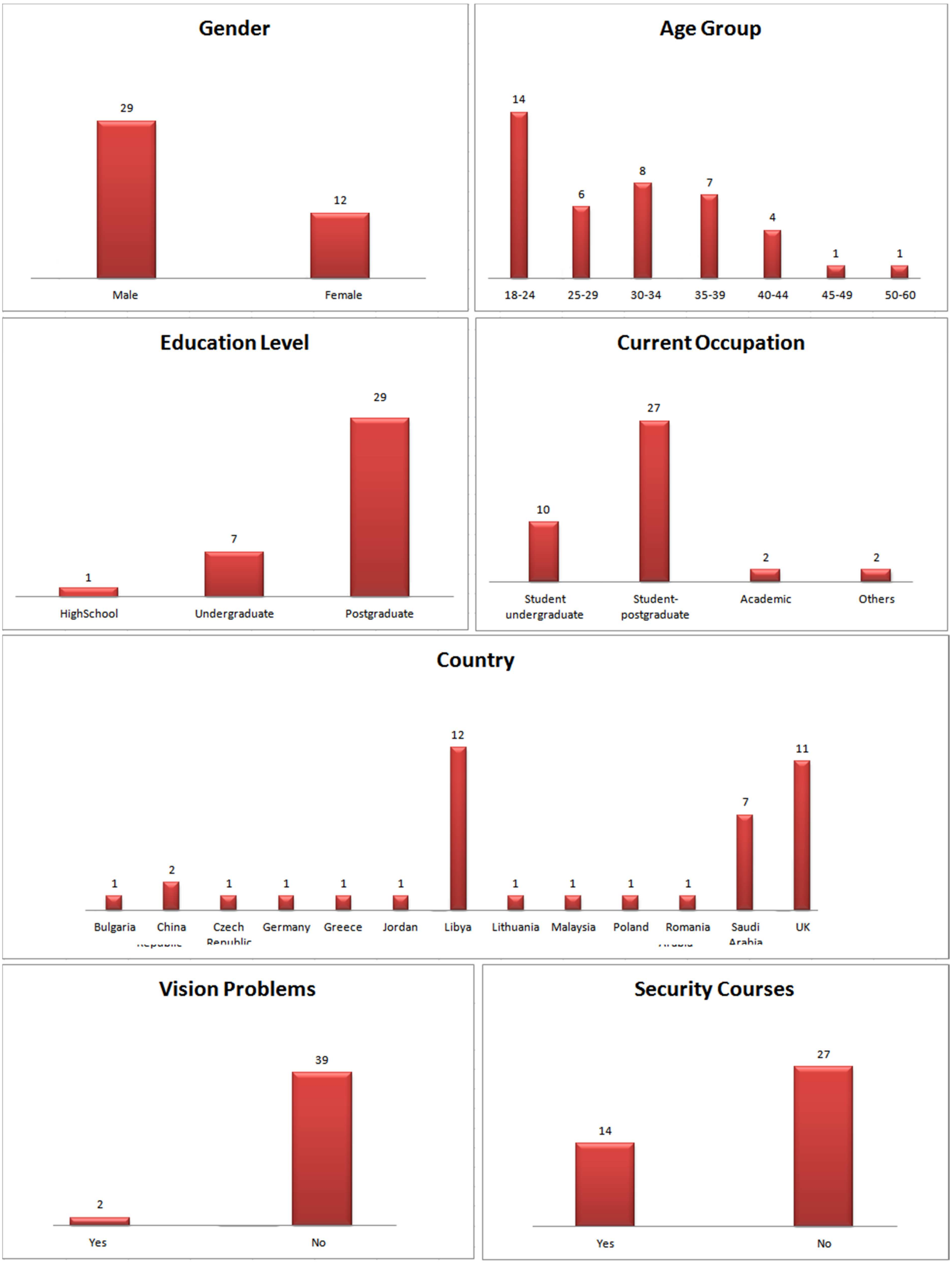


Figure 5-13 Demographic profile of participants

The total for all categories apart from the education level was 52. The total for the education level was 37 since this information was provided in the questionnaire. In retrospect, it would have been better to collect this information when the participants created their initial accounts. However, nearly 80% were postgraduate students, which were consistent with the distribution of the participants' initial accounts, and so this particular information is not very useful.

5.6.2 Dropout rates

Some participants dropped out at various stages in the experiment. Most of those who dropped out did so after creating an initial account and before registering their images. 11 participants (21%) dropped out at this stage, while 41 registered some images. One participant (2%) dropped out halfway through the authentication process, leaving 40 remaining. Finally, three participants (7%) failed to submit a questionnaire, leaving 37 who completed all stages of the experiment.

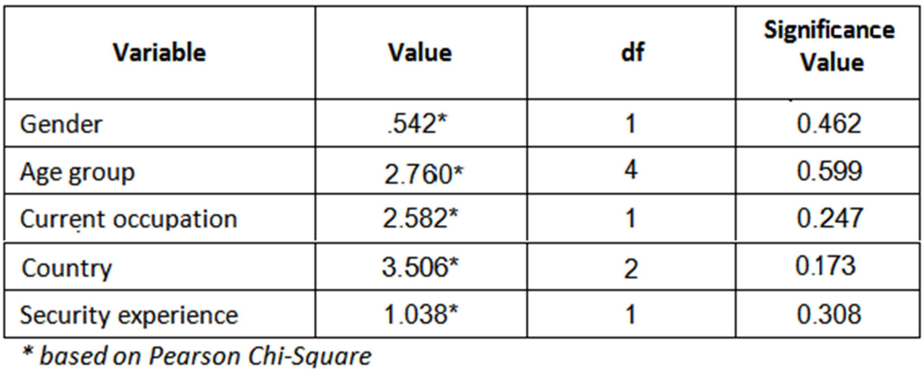
Most of the dropouts occurred when the participants came to start the work needed to register. This reflects one of the problems which affect the widespread adoption of user drawn graphical passwords: the time needed to register the images. The null hypothesis is that the participants' decisions to drop out were independent of their gender, age group, education level, current occupation, country and whether they had vision problems or had attended a security course. It is safe to assume that the decision to drop out (or to remain in the study) was an individual one, since the experiment was mainly conducted online. Thus there was no correlation between participants' decisions and a Chi-squared statistical test is appropriate. The Chi-squared test does not give reliable results if the numbers in a category is small, the threshold normally being five [182-184]. Therefore, this rules out using the test on those with vision problems, since only four participants reported that they had a vision problem. This requirement also causes problems with the country category, since many countries only had one or two participants. This test was performed with just three countries, Libya (13), Saudi Arabia (7) and the UK (15 participants). In the age category, the three older categories containing a total of six participants were integrated into one category, with an age bracket of 40-60. The test for occupation was also performed on undergraduates and postgraduates only and the test on current occupation only included undergraduates and postgraduates. The data on dropouts is shown Table 5-1.

Table 5-1 Participant dropouts

Property	Completed	Dropped Out
Gender		
Male	29	9
Female	12	2
Age Group		
18-24	14	6
25-29	6	1
30-34	8	2
35-39	7	2
40+	6	0
Occupation		
Undergraduate	10	5
Postgraduate	27	6
Country		
Libya	12	1
Saudi Arabia	7	0
UK	11	4
Security Course		
Attended	14	2
Did not attend	27	9

Table 5-2 records the results of applying the Pearson Chi-squared test to the dropout rates. It shows the Chi-squared value, the degrees of freedom (**df**) and the significance value. Significance values of greater than 0.05 indicate that the Chi-squared test supports the null hypothesis with 95% confidence.

Table 5-2 Chi-square test for independence summary results



Variable	Value	df	Significance Value
Gender	.542*	1	0.462
Age group	2.760*	4	0.599
Current occupation	2.582*	1	0.247
Country	3.506*	2	0.173
Security experience	1.038*	1	0.308

** based on Pearson Chi-Square*

The null hypothesis is supported in all cases, indicating that dropping out is not correlated with any of the variables, to a 5% confidence value. The Country variable is the closest one to demonstrating a correlation with dropping out.

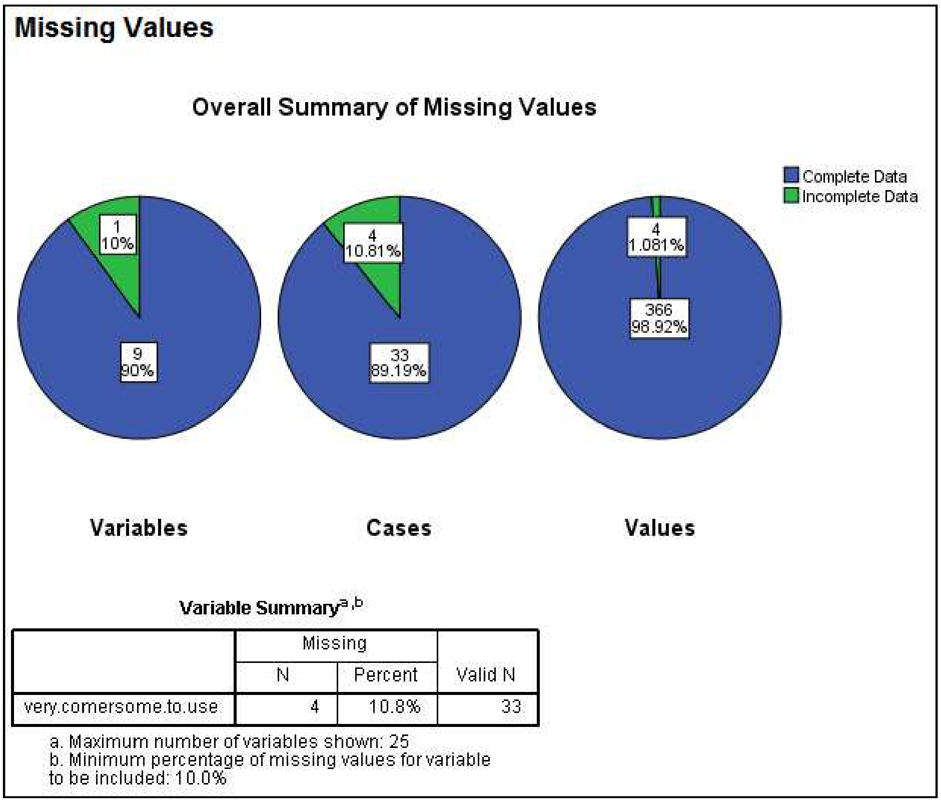
5.6.3 Satisfaction

Satisfaction is the most subjective part of usability [52], and it is necessary to try to ensure that users will continue to use the technology. In the context of this study, satisfaction was tested based on a set of Likert scales, as mentioned before.

5.6.3.1 Missing data

When researchers collect data from experiments, particularly when human beings are involved, it is rare to obtain complete data from every case. The seriousness of this issue depends on the pattern of missing data, how much is missing, and why it is missing. It is important to inspect the data for missing data[185]. Researchers [186] have categorised missing data into three categories: missing completely at random (MCAR), missing at random, called ignorable nonresponse (MAR), and missing not at random or non-ignorable (MNAR). MCAR happens when “subjects who have missing data are a random subset of the complete sample of subjects” [187]. MCAR and MAR can be ignored while MNAR cannot [185, 188, 189] because MNAR usually reflects a systematic pattern and data are not missing randomly. Tabachnick and Fidell [188] argued that if the “missingness” rate is lower than 5%, then the missing data can be ignored without any further analysis. Therefore, the SPSS statistical software package was used to identify the percentage and pattern of the missing data.

Figure 5-14shows that there were only four participants who did not answer one question in the form of rating the statement (No 8: I found the website very cumbersome to use).



Variable Summary[a,b]

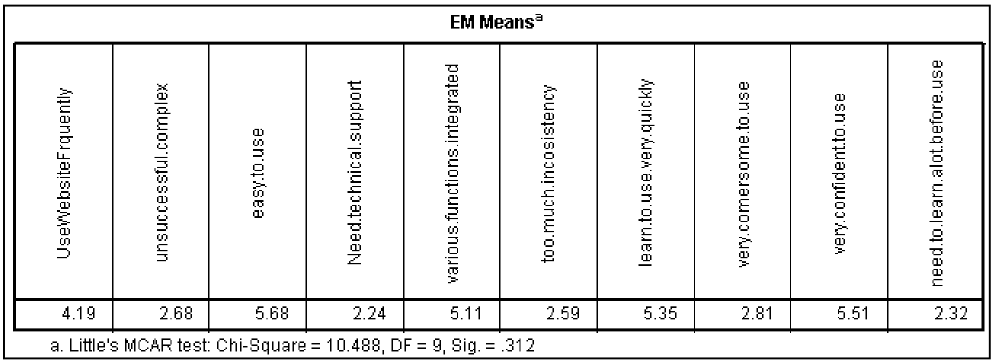
	Missing		Valid N
	N	Percent	
very.comersome.to.use	4	10.8%	33

a. Maximum number of variables shown: 25
b. Minimum percentage of missing values for variable to be included: 10.0%

Figure 5-14 Usability- Questionnaire missing data rate

The missing data rate for the all questions was found to be lower than 5% (1.08%). Only four participants out of the total of 37 incurred a 10.8% "missingness" rate which can therefore, be treated as MCAR and ignored.

Table 5-3 Little's MCAR test



EM Means[a]

UseWebsiteFrquently	unsuccessful.complex	easy.to.use	Need.technical.support	various.functions.integrated	too.much.incosistency	learn.to.use.very.quickly	very.comersome.to.use	very.confident.to.use	need.to.learn.alot.before.use
4.19	2.68	5.68	2.24	5.11	2.59	5.35	2.81	5.51	2.32

a. Little's MCAR test: Chi-Square = 10.488, DF = 9, Sig. = .312

In order to examine whether the missing data happened randomly, SPSS has an option to test this data. The test is called Little's MCAR and it was used with the data as suggested [188]. Little's MCAR is a test of whether data is missing completely at random or not. Table 5-3shows EM correlations with missing values filled in using the EM method. The results from Little's MCAR test below the table showed the data are missing completely at random. A statistically non-significant result is desired: p= 0.312 indicates that the probability that the pattern of missing diverges from randomness is greater than .05, so that MCAR may be inferred.

However, many options have been proposed to deal with missing data and can also be used with SPSS. These methods are:

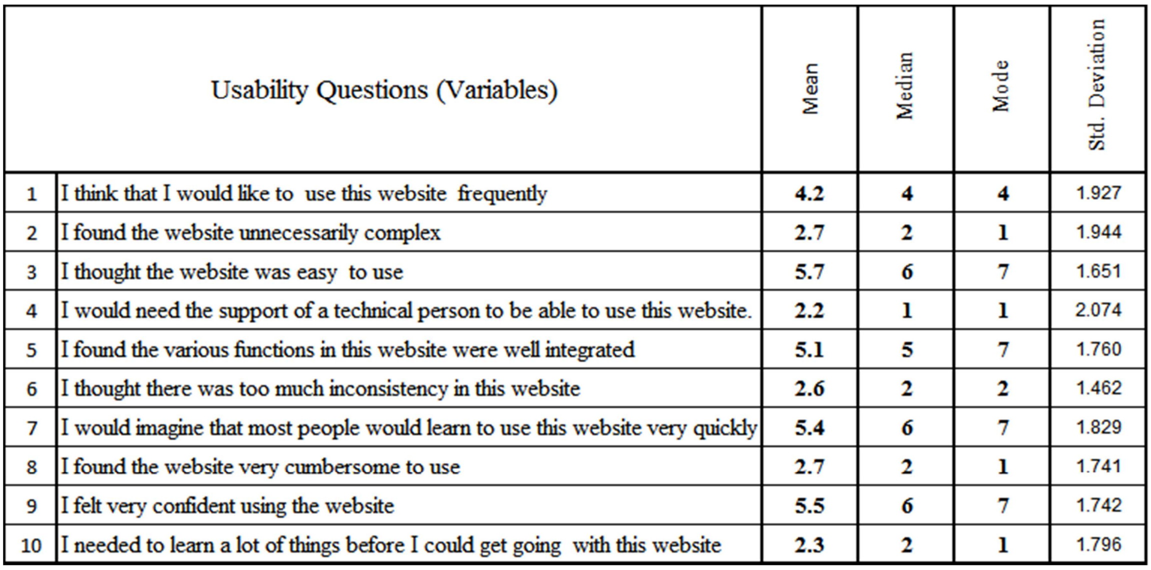
1. Deletion Methods: Listwise deletion and Pairwise deletion.
2. Single Imputation Methods: Mean/Mode substitution, Dummy variable method and Single regression.
3. Model-Based Methods: Maximum Likelihood, Multiple imputations.

Each of these methods has advantages and disadvantages which depend on many factors, such as sample size. The most suitable method suggested by prior research [190],for dealing with missing data is the Multiple Imputations approach. In our data, SPSS was used to place missing data by using Multiple Imputations.

5.6.3.2 User satisfaction

To evaluate users' satisfaction levels based on the questions asked in the questionnaire, it is first necessary to describe the mean scores for each of these questions, which are shown in Table 5-4.

Table 5-4 Descriptive statistics of usability questions for 37 participants



Usability Questions (Variables)		Mean	Median	Mode	Std. Deviation
1	I think that I would like to use this website frequently	4.2	4	4	1.927
2	I found the website unnecessarily complex	2.7	2	1	1.944
3	I thought the website was easy to use	5.7	6	7	1.651
4	I would need the support of a technical person to be able to use this website.	2.2	1	1	2.074
5	I found the various functions in this website were well integrated	5.1	5	7	1.760
6	I thought there was too much inconsistency in this website	2.6	2	2	1.462
7	I would imagine that most people would learn to use this website very quickly	5.4	6	7	1.829
8	I found the website very cumbersome to use	2.7	2	1	1.741
9	I felt very confident using the website	5.5	6	7	1.742
10	I needed to learn a lot of things before I could get going with this website	2.3	2	1	1.796

It can be noted that the lowest mean score was for the only negative-type question about the passdoodles system, i.e.: 'I would need the support of a technical person to be able to use this website,' with an average mean score of 2.2 (mode = 1, median = 1). It is also clear that the top variables scoring the highest mean of 5.7 (mode = 7, median = 6)were 'I thought the website was easy to use' and the variable scoring the second highest mean of 5.5 (mode = 7, median = 6)were 'I felt very confident using the website'. These figures indicate that online users found the passdoodles mechanism to be usable.

Overall, apart from the first question, all the positive (odd) questions scored highly and all the negative (even) questions had low scores. Thus, the participants were satisfied with the website. Question 1 was less relevant because the website did not have any interesting content.

5.6.4 User Preference

The final part of the post questionnaire asked users which method of creating the drawing they preferred- scanning a paper drawing or the Paint system. Additionally, two more Likert scale questions with a 5 point scale (1 - extremely dislike to 5 - extremely like) were asked of the participants: 1. How much do they like the scan type, 2. How much do they like the Paint type. Then, finally, an open question was asked them to give the reasons for their choice. Figure 5-15, below, shows that over four-fifths of participants preferred the Paint system whereas only 16% preferred the scan system.

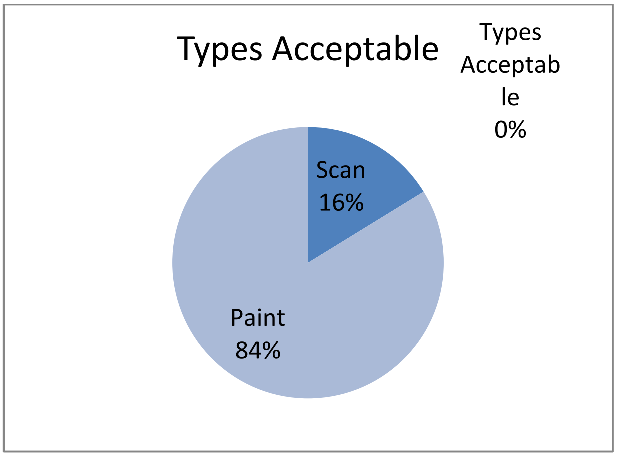
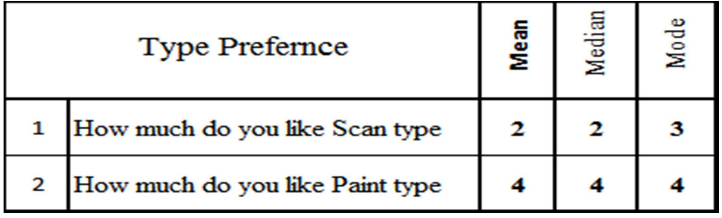


Figure 5-15 Participants' preferences between Paint system and scan system

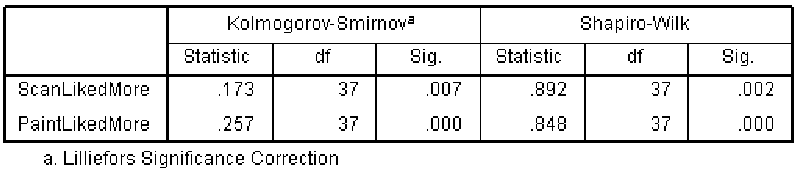
Table 5-5 Type Preferences



Type Prefernce		Mean	Median	Mode
1	How much do you like Scan type	2	2	3
2	How much do you like Paint type	4	4	4

Table 5-5, shows how much the participants liked either system. They definitely liked the Paint system, with a mean, median and mode all at 4, with the highest result possible a 5. They also disliked the scan system, with mean and median of 2 and a mode of 3. The most popular option (the mode) was average (3), but the overall feeling was below average. To see whether or not this preference for the Paint system was statically valid, we tested the null hypothesis that both systems were preferred equally. The normality of the data collected from the above two questions was checked using Kolmogorov-Smirnov and Shapiro-Wilk tests. Table 5-6 shows p<0.05 for both types which indicates that the data was not normal.

Table 5-6 Normality Test (Preference between scan and Paint systems)

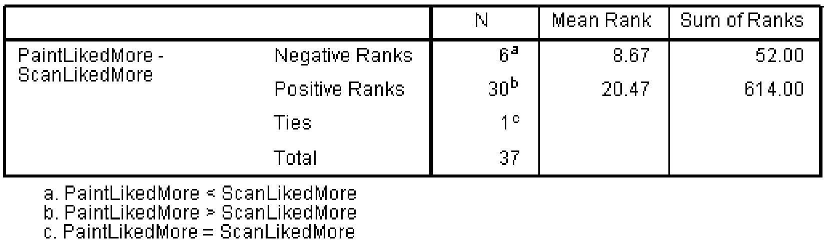


	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
ScanLikedMore	.173	37	.007	.892	37	.002
PaintLikedMore	.257	37	.000	.848	37	.000

a. Lilliefors Significance Correction

Therefore, the most suitable test for this data is the Wilcoxon signed rank test. The results of the Wilcoxon test showed that the participants significantly preferred the Paint system over the scan system. One reason for this could be that the Paint-based system requires fewer steps than the scan-based system, with consequences in terms of effort and time.

Table 5-7 Wilcoxon Test (Preference between scan and Paint systems)



		N	Mean Rank	Sum of Ranks
PaintLikedMore - ScanLikedMore	Negative Ranks	6[a]	8.67	52.00
	Positive Ranks	30[b]	20.47	614.00
	Ties	1[c]		
	Total	37		

a. PaintLikedMore < ScanLikedMore
b. PaintLikedMore > ScanLikedMore
c. PaintLikedMore = ScanLikedMore

The users also indicated their perceptions of the advantages and disadvantages of the two systems, which are listed in Table 5-8:

	Scan System	Paint System
Advantages	• Drawn doodles were accurate • Very personal (own hand writing) • Reliable • More effective • Quicker to draw on paper	• Quick and easy to draw • Does not need equipment • Hard to distinguish (good for security) • Paint software available
Disadvantages	• Hand writing may be recognised by relatives • More complicated • No privacy, since paper is produced • Takes a long time • Equipment problems	• Hard to draw • More time needed for a good drawing

Table 5-8 Advantages and disadvantages of both methods

5.6.5 Use of Images after registration

Previous studies which used hand drawn images as graphical passwords[20, 29], did not state what the users did with their images after registration. In this study the participants were asked what they did with their images on paper (scan system) or on file (Paint system). Additionally, they were also asked whether or not they had used them during the login process. These questions were addressed by the questionnaire; therefore 37 participants answered the questions.

Table 5-9 Dealing with forms (scan system)

	Scan	
Secure Disposal	8	
Thrown Away	8	
Kept	21	
Total	**37**	
Used during login process	6	

Table 5-9, shows that 21 participants kept the paper images that they had scanned in, and six of them used them to help when logging in. Of the other 16, half disposed of the images securely and the other half just threw them away. On the Paint system, Table 5-10 shows that 22 participants kept their paint program file, two of them protected it with a password, while the other 13 deleted their files. Four of them used these files to help them login.

Table 5-10 Dealing with forms (Paint system)

	Paint
Secure Saved	2
Deleted	13
Saved	22
Total	**37**
Used during login process	4

This behaviour has obvious security implications and is similar to writing down a text based password [2, 191, 192]. If an attack was made across a network then the attacker would not be able to access the saved images and this would not be a security threat. If, however, the attacker was able to access the saved images then this would be a serious problem. It is of interest to ask whether or not attending a security course led to more secure behaviours. Table 5-11 illustrates the relationship between how the images were dealt with and whether the participants had attended a security course.

Table 5-11 The relationship between security course attendance and dealing with images

	Scan		**Paint**	
	Attend Security Course		Attend Security Course	
	Yes	No	Yes	No
Secure disposal	3	5	1	1
Insecure disposal	3	5	5	8
Kept	7	14	7	15
Total	13	24	13	24

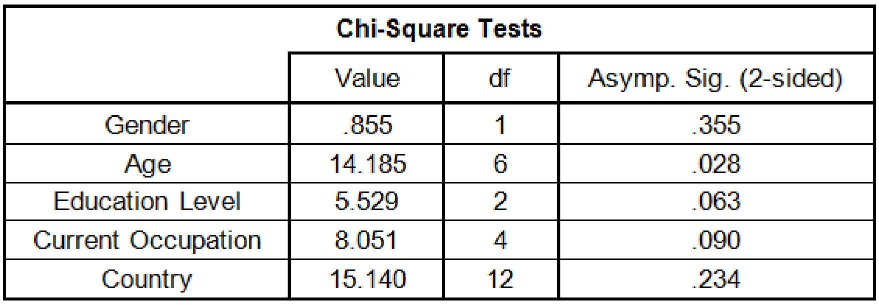
A Chi-squared test with a significance value *p >0.05* supports the null hypothesis that attending a security course is not correlated with the ways the images were dealt with, as shown in Table 5-12.

Table 5-12 Chi-square test the security course and dealing with images

Chi-Square Tests			
	Value	df	Asymp. Sig. (2-sided)
Scan	.069	2	.966
Paint	.363	2	.834

Another Chi-squared test was carried out to find out whether there were any correlations between the people who had taken a security course with the variables of gender, age, educational level, occupation and country. The results in Table 5-13 show that, apart from the age variable, the significance value *p >0.05*supports the null hypothesis that attending a security course is not correlated with the remaining variables, which means that the achievement of the experiment will not impacted upon by awareness of security issues.

Table 5-13 Chi-square test of the security course with other categories



Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Gender	.855	1	.355
Age	14.185	6	.028
Education Level	5.529	2	.063
Current Occupation	8.051	4	.090
Country	15.140	12	.234

5.6.6 Login Success Rate

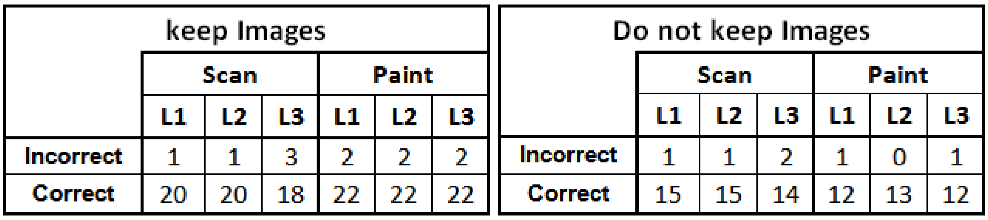
We recorded whether the participants logged in successfully or not. These statistics are recorded in Table 5-14. We assume that all those who used their saved images to help them login did so successfully, and they were ignored when calculating the success percentages. However, Table 5-14 shows the successful rates for systems, scan and Paint, for all login trails. And it is clear that there was no big difference between the systems by using these kinds of images.

Table 5-14 Success rates of authentication for both scan and Paint for all trails

Login Times		Login 1		Login 2		Login 3		Total
		Mean	Std. Deviation	Mean	Std. Deviation	Mean	Std. Deviation	**Average**
Success Rate	**Scan**	92.50%	.267	94.87%	.223	86.11%	.351	**91.16%**
	Paint	92.50%	.267	94.74%	.226	91.18%	.288	**92.80%**

Our research was focussed on the registration process, but the subsequent login stage also offered valuable information on the retention of images. 16% of participants kept their scanned images, while 11% kept their Paint files. The login success rates are consistent with other work in this area in that frequent use, i.e. a short time between Login 1 and Login 2, increases the success rate while infrequent use, i.e. a longer time between Login 2 and Login 3, decreases it. Despite the fact that some users used the drawing image forms for logging in, using these forms for both systems did not affect the success rate very much due to the small number who did so. However, Table 5-15illustrates the numbers of logins (successful and failed) for all participants (37 returned the questionnaire) who kept or did not keep their drawing forms and also who did not keep forms after registration.

Table 5-15 Successful logins among those keeping drawing forms after registration.



	keep Images					
	Scan			Paint		
	L1	L2	L3	L1	L2	L3
Incorrect	1	1	3	2	2	2
Correct	20	20	18	22	22	22

	Do not keep Images					
	Scan			Paint		
	L1	L2	L3	L1	L2	L3
Incorrect	1	1	2	1	0	1
Correct	15	15	14	12	13	12

5.6.7 A Comparison of drawing styles

Drawing with a pen on paper and drawing with a mouse using a paint program are two different activities which may lead to different styles of drawing. Also, each participant had to provide two different sets of pass-images, leading to the interesting question of how much re-use of pass-images there might be. Both of these questions will be answered in this section.

The first set of images shown in Table 5-16, below, is from a participant who clearly felt more comfortable using a pencil on paper than using the Paint program. The scanned imaged are more complex and executed with more skill. However, this participant was in the minority. More typical was the set in Table 5-17, also below, where the sets of images were of about the same level of complexity. The paint images were not executed quite as well, as can be seen by the slight wobble in the lines of the last pass-image.

Table 5-16 Styles of Drawing (I)

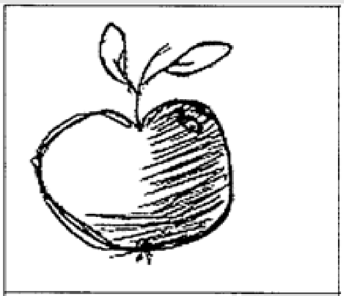
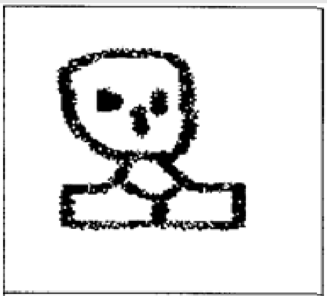
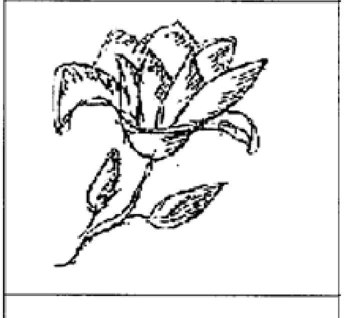
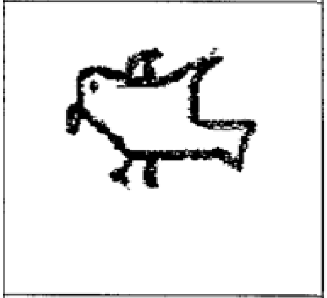
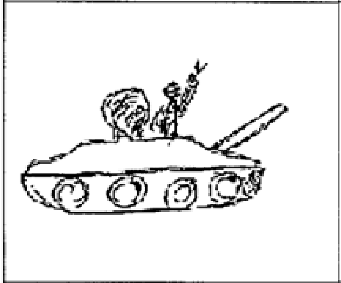
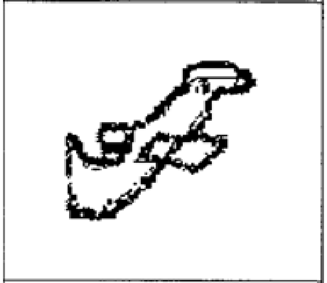
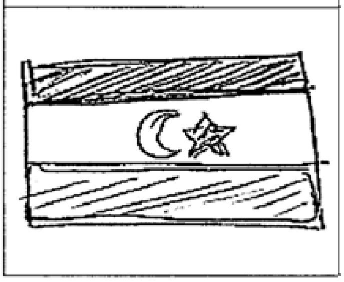
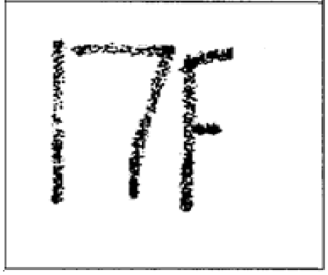
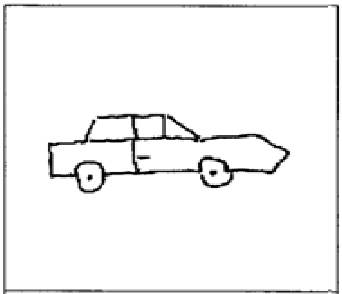
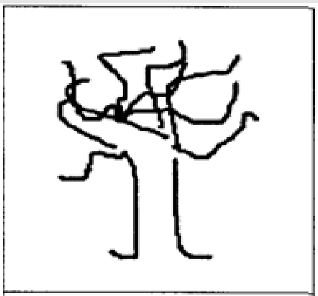
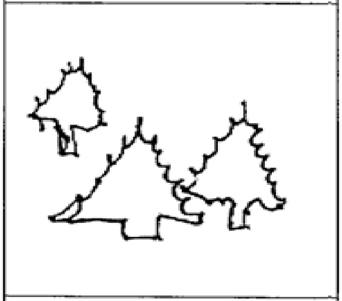
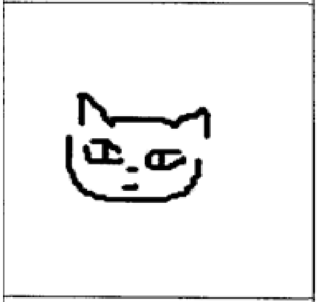
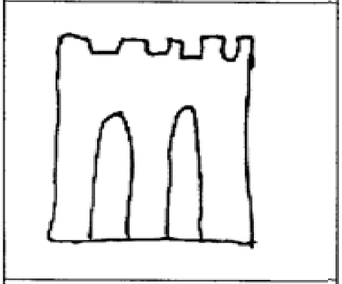
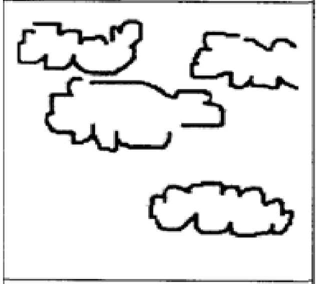
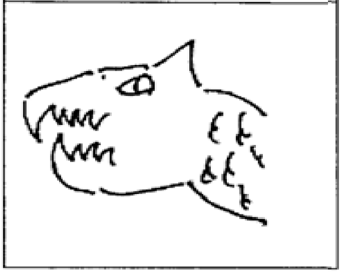
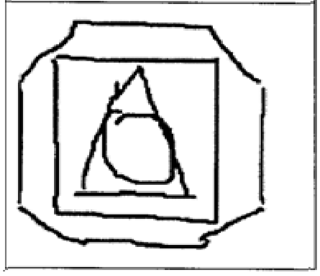
Scan= User(122)	Paint = User(123)
	
	
	
	

Table 5-17 Styles of Drawing (II)

Scan= User(146)	Paint = User(139)
	
	
	
	

Both of the participants outlined above chose a different set of images for their two tasks. This was true of 20 of the participants, or exactly half of the sample. The other half used very similar, but not identical images for both the Scan and Paint systems. This is illustrated in Table 5-18, below. This was one of the participants who drew on paper and scanned their images first and who then kept the sheet of paper. In contrast, the participant in Table 5-19, created their images using the Paint system first. Their images are all made up of lines and circles, something that works well with the Paint system. The images they produced using pen and paper were not so good.

Table 5-18 Styles of Drawing (III)

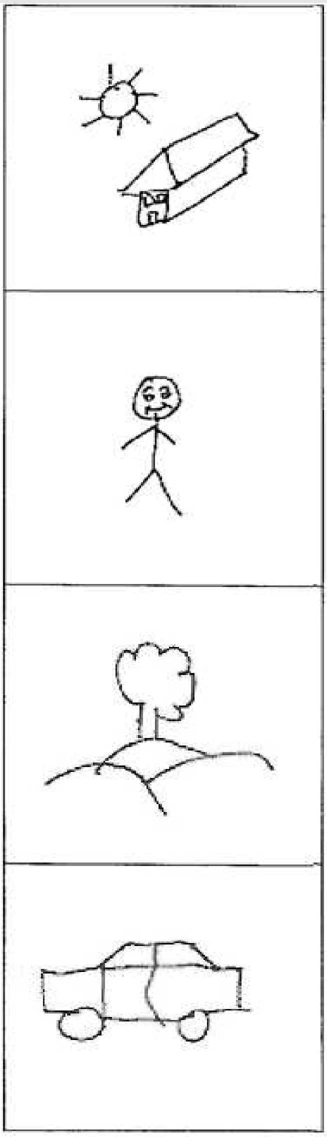
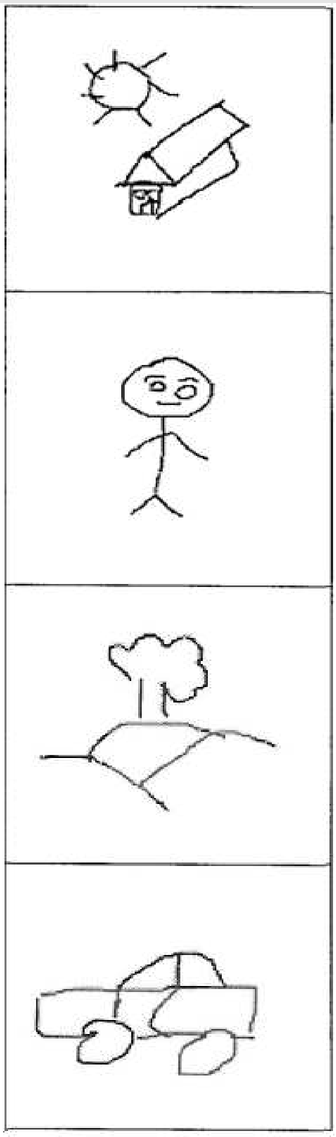
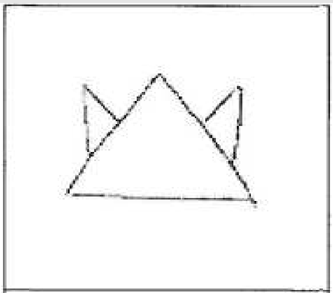
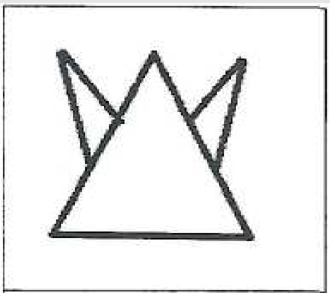
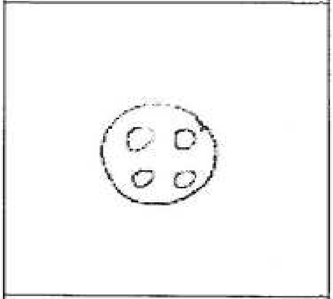
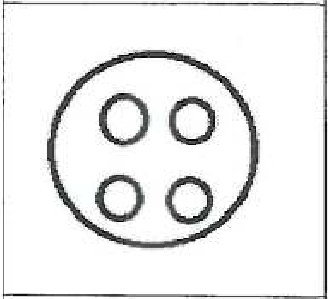
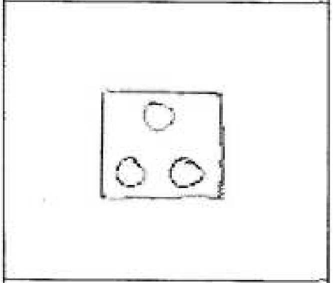
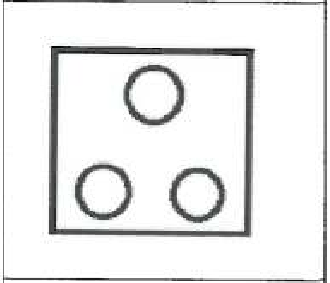
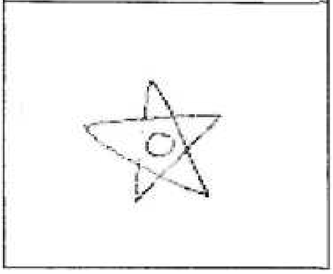
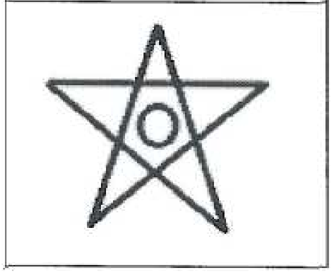
Scan= User(74)	Paint = User(75)
	

Table 5-19 Styles of Drawing (IV)

Scan= User(83)	Paint = User(82)
	
	
	
	

In summary, only one participant took advantage of the extra expressive power of pencil and paper to draw artistic images. All the others choose images that could be created equally well using a Paint program or a pencil and paper. Also, exactly half of the participants chose to reuse their ideas for images when creating the two sets. None of them were identical, but perhaps if they had been required to create two sets of pass images without knowing that a researcher would be examining their work, they may well have chosen to reuse the actual image files or sheets of paper.

5.6.8 Failure to follow instructions

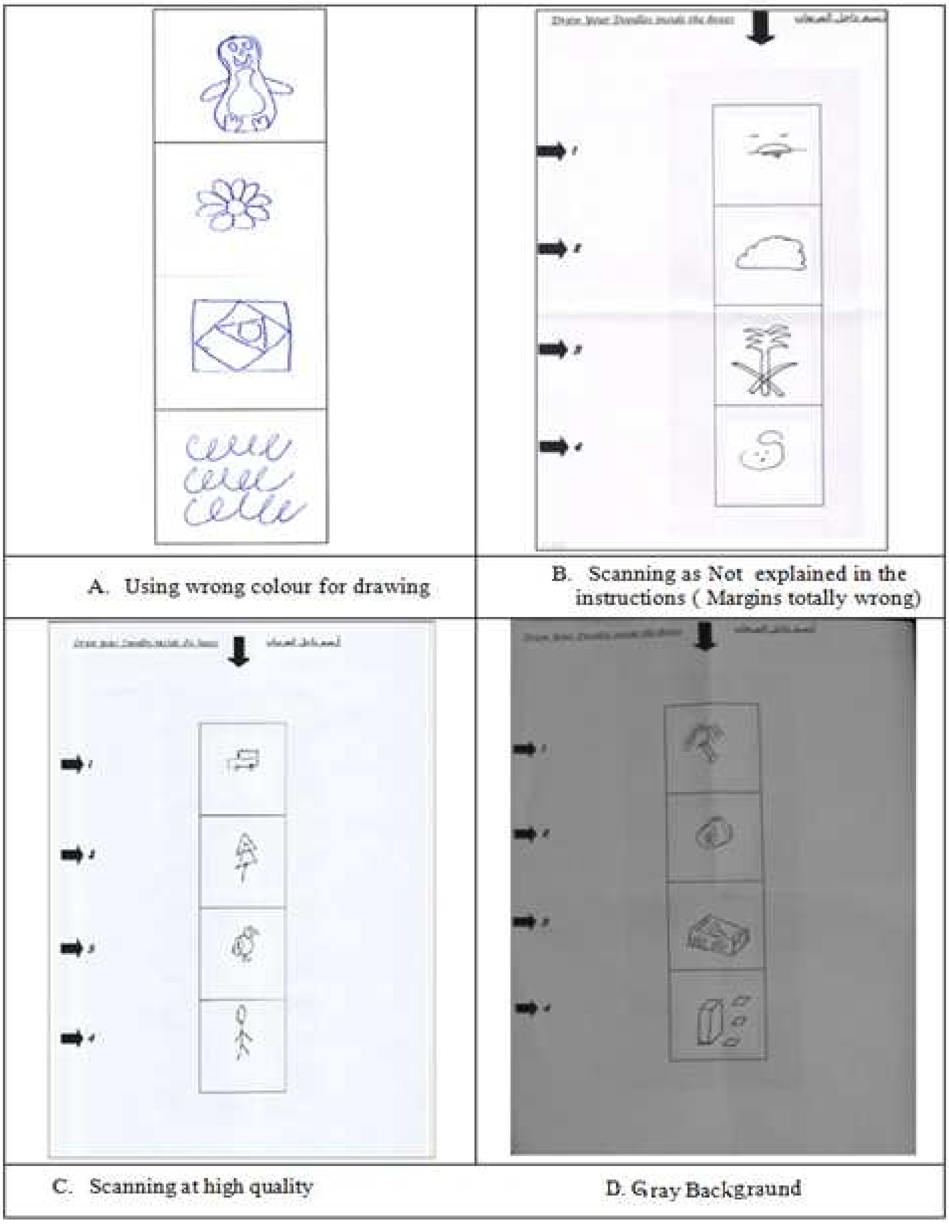
As has been discussed earlier, during the conduct of the experiment, some errors by the participants appeared. Most of these errors happened during the registration stage. Unfortunately, some of the participants did not follow the exact instructions that were provided. Despite the availability of some explanatory material for this experiment, whether these materials were available at the interview (on an information sheet or given by the experimenter) or through the passdoodles.net website, we found that some people asked for more detail.

"I would like to have the instructions more detailed"

Consequently, this indicates that some participants still found the website difficult to use. Therefore, some errors occurred which affected the usability of the system. Some of these errors can be summarised and classified into three main categories: errors that occurred during scanning, errors that occurred during Painting and errors that were common to both.

5.6.8.1 Errors during scanning

As expected, many of the participants did not follow the instructions exactly and uploaded files that contained errors. A sample is shown in Figure 5-16.



A. Using wrong colour for drawing

B. Scanning as Not explained in the instructions (Margins totally wrong)

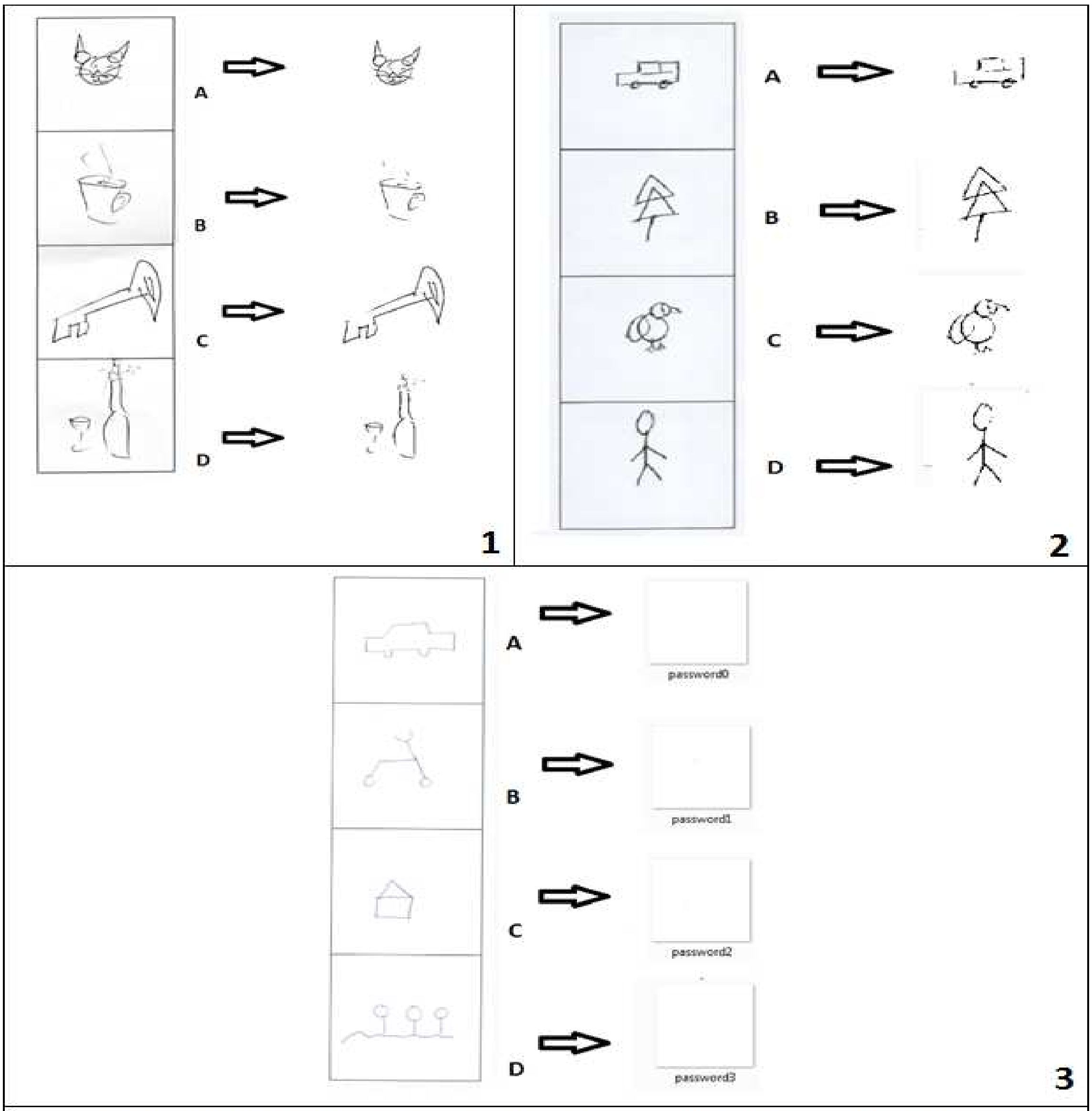
C. Scanning at high quality

D. Gray Backgraund

Figure 5-16 some errors that occurred during drawing and scanning stages

The example in Figure 5-16 (A) shows that a user has used a blue pen rather than a black one. The analysis software converts a colour image to a black and white one using a threshold scheme based on individual pixel values, and so it had no trouble in automatically converting blue to black. The margins were wrong in file (B), but the image boxes enabled the software to locate the drawings anyway. File (C) was scanned at too high a quality, which was corrected by lowering the resolution while not losing any black pixels. File (D) shows that the drawing was done on grey paper. The pixel threshold scheme corrected this error. The image processing software managed to correctly extract most of the images from the scanned drawings. Some users drew images that were too big for the boxes. Our software correctly located the bounding boxes and cropped these images.

Figure 5-17, below, illustrates more examples of errors which were caused by not following the exact drawing commands, such as the colour of the pen page. In picture (1), the participant made two mistakes: drawing using a small point size of pen and using an intermittent pen, whereas in picture (2), the participant had scanned the passdoodles form with a high quality option scan; also, in picture (3) the participant used pencil instead of black pen. As a consequence, the generated passdoodles are not clear enough, especially in cases (1) and (2) and did not appear at all in case (3), and this will affect the usability of such a technique, where the participants will not able to recognise their own passdoodles.

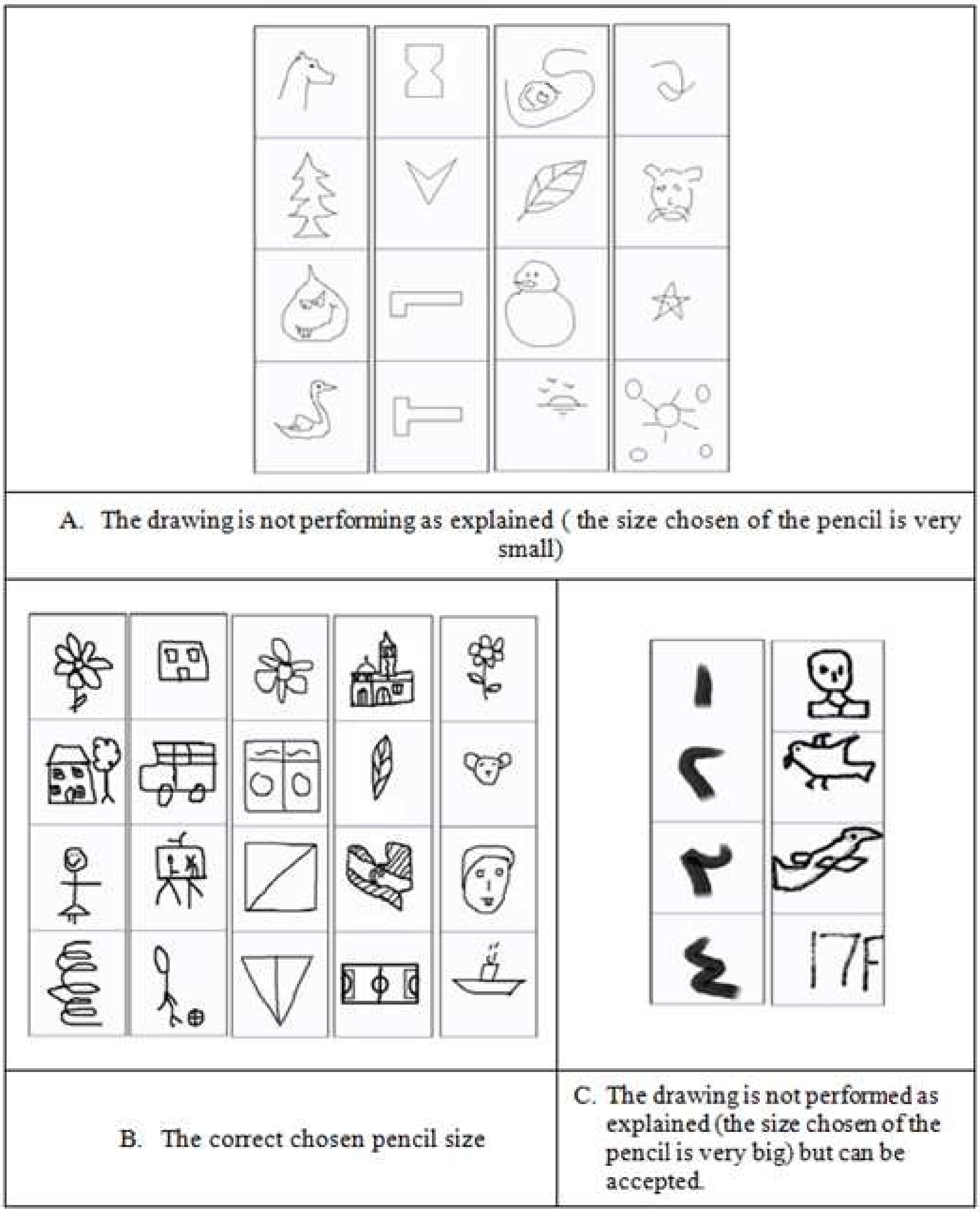


The drawing is not performing as explained (for example using pencil instead of pen and using different colours not black). All these effect the generated of passdoodles.

Figure 5-17 Passdoodles not generated properly

5.6.8.2 Errors during Paint

It was also possible for the participants to generate incorrect images using the Paint tool. Some of these errors are shown in Figure 5-18



A. The drawing is not performing as explained (the size chosen of the pencil is very small)

B. The correct chosen pencil size

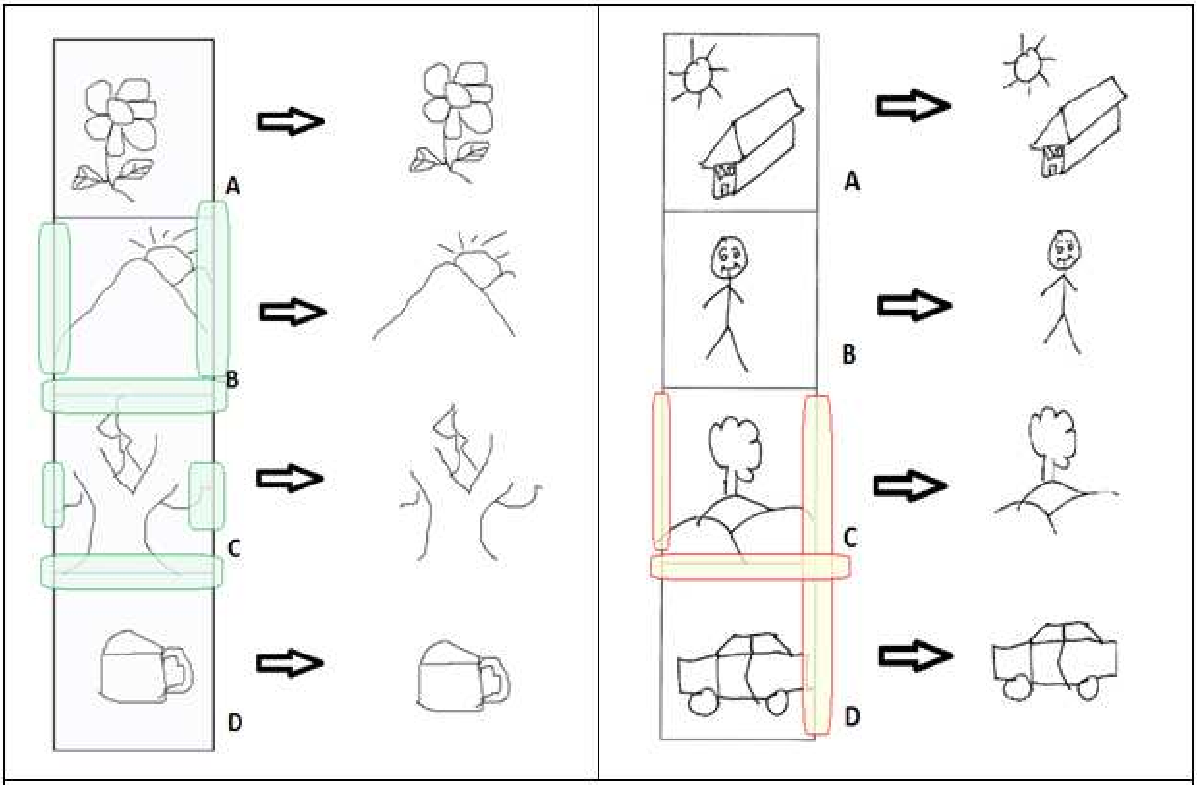
C. The drawing is not performed as explained (the size chosen of the pencil is very big) but can be accepted.

Figure 5-18 Examples of errors caused during paint system

The main error was in the point size of the pencil. Thick lines are fine, but thin lines can cause problems when the images are displayed during the authentication phase. Our software automatically thickened all the lines, and indeed the black regions, of the submitted images, which corrected the problems shown in File (A) of Figure 5-18; also it pointed out some example of passdoodles drawn in three different font sizes. Two of them were accepted, i.e. (B) and (C), but the first were not (A).

5.6.8.3 Errors common to both systems

Another type of error was discovered in both systems. This type of errors does not seriously affect the passdoodles drawings but again highlights the carelessness of some participants in following the drawing instructions. Figure 5-19 shows some examples of passdoodles that were drawn outside the boxes, affecting the final image.



Some of drawing passdoodles are not in the central of the boxes as explained which caused partial passdoodles problem.

Figure 5-19 Samples of passdoodles that were not drawn in the central area

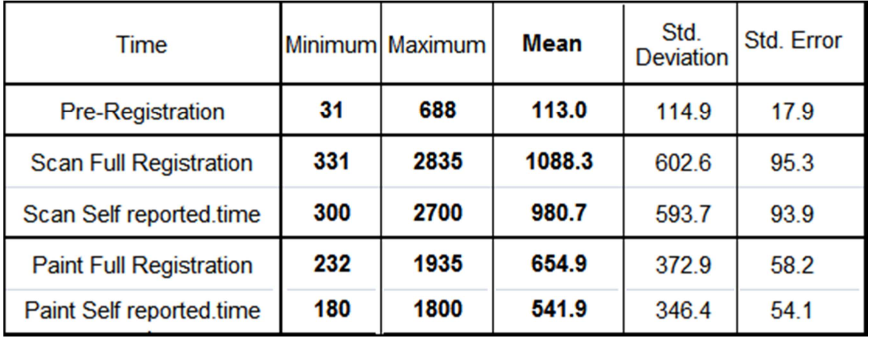
5.6.9 Registration Times

First of all, the null hypothesis to be tested in this section is that:

There is no big difference between the registration times using Scan and Paint.

Table 5-20, below, shows the average time in seconds that were spent to complete the pre-registration and full registration and the time spent by users to draw their passwords for both systems. In addition, it shows the minimum and maximum times achieved by participants for both types. The mean scores provided in Table 5-20clearly show that pre-registration completion times were below two minutes. The full time registration incurred a mean score of 1088 seconds in the scan system whereas it incurred only 654 seconds in the Paint system. Self-reported times were slightly less, at 980 and 541 seconds respectively. The standard deviation was also quite high, showing a lot of variability.

Table 5-20 Registration time



Time	Minimum	Maximum	**Mean**	Std. Deviation	Std. Error
Pre-Registration	**31**	**688**	**113.0**	114.9	17.9
Scan Full Registration	**331**	**2835**	**1088.3**	602.6	95.3
Scan Self reported.time	**300**	**2700**	**980.7**	593.7	93.9
Paint Full Registration	**232**	**1935**	**654.9**	372.9	58.2
Paint Self reported.time	**180**	**1800**	**541.9**	346.4	54.1

The distribution is illustrated by the box plots in Figure 5-20.

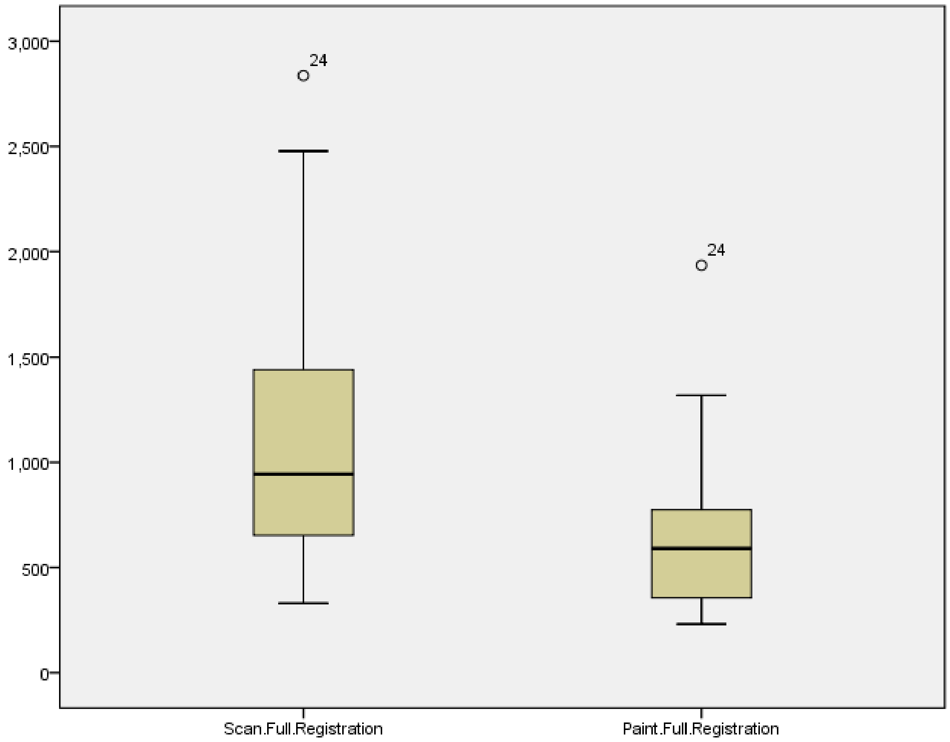
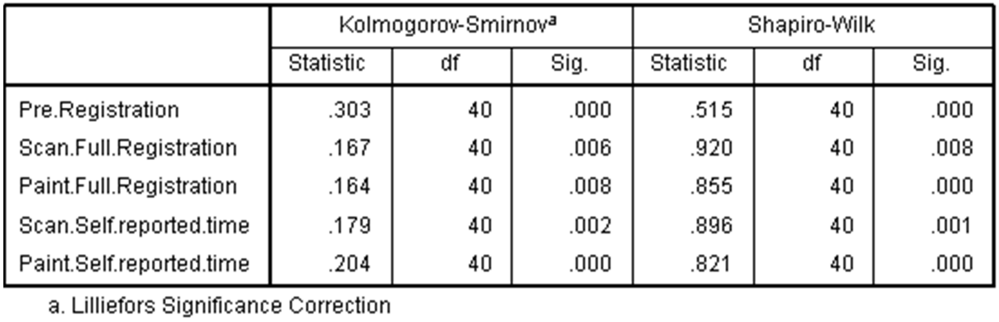


Figure 5-20 Box plot showing the existence of outliers in full registration time (scan &paint)

The null hypothesis that "There is no significant difference between the registration times for scan and Paint systems" will be tested statically. The Kolmogorov–Smirnov and Shapiro–Wilk tests reported in Table 5-21 show that the data was not normally distributed since significance p values were < 0.05. Thus a Wilcoxon Signed Rank test was more appropriate than a t-test.

Table 5-21 Normality test of registration time

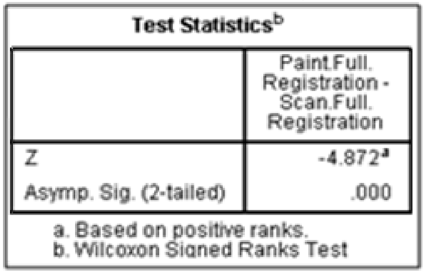


	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
Pre.Registration	.303	40	.000	.515	40	.000
Scan.Full.Registration	.167	40	.006	.920	40	.008
Paint.Full.Registration	.164	40	.008	.855	40	.000
Scan.Self.reported.time	.179	40	.002	.896	40	.001
Paint.Self.reported.time	.204	40	.000	.821	40	.000

a. Lilliefors Significance Correction

The results in Table 5-22show significant differences in registration time between scan and Paint and that the participants took more time to register their password using the Scan method than the Paint method(z=4.87, p<0.05, r=0.76). The null hypothesis was therefore rejected and the registration time for the scan system was shown to be significantly longer than the Paint system.

Table 5-22 Wilcoxon test for registration stage.



Test Statistics[b]

	Paint.Full.Registration - Scan.Full.Registration
Z	-4.872[a]
Asymp. Sig. (2-tailed)	.000

a. Based on positive ranks.
b. Wilcoxon Signed Ranks Test

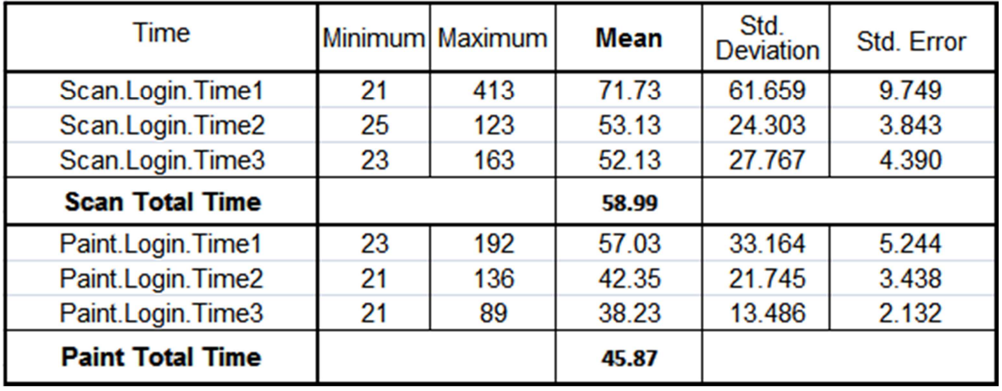
5.6.10 Login Time

The null hypothesis to be tested in this section is that:

There is no difference between the login times using Scan and Paint.

In fact, there should be few differences in login times between scan and Paint systems where both have used the same kinds of images. However, Table 5-23 illustrates a comparison between the two systems in the three login times and it can be observed that the scan type takes a bit longer than the Paint type. Also, Table 5-23 shows the average time spent on login and also the minimum, maximum and stranded deviations for each login as well as the main average time between scan and Paint. The first time login incurred a mean score of 71 seconds in scan system while it incurred a mean score of 57 seconds in the Paint system. There were only one second differences between the second and third login time in the scan system whereas the difference was about 4 seconds in the Paint system. Overall, the difference between scan and Paint systems was only 13 seconds where a mean score of 59 seconds was incurred by the scan system and the Paint system incurred a mean score of 46 seconds.

Table 5-23 Login time in scan and Paint systems



Time	Minimum	Maximum	**Mean**	Std. Deviation	Std. Error
Scan.Login.Time1	21	413	71.73	61.659	9.749
Scan.Login.Time2	25	123	53.13	24.303	3.843
Scan.Login.Time3	23	163	52.13	27.767	4.390
Scan Total Time			**58.99**		
Paint.Login.Time1	23	192	57.03	33.164	5.244
Paint.Login.Time2	21	136	42.35	21.745	3.438
Paint.Login.Time3	21	89	38.23	13.486	2.132
Paint Total Time			**45.87**		

To further investigate the existence of outliers, an exploratory SPSS test was conducted to evaluate the logins individually and to check for outliers using box plot. The results are illustrated in Figure 5-21, below.

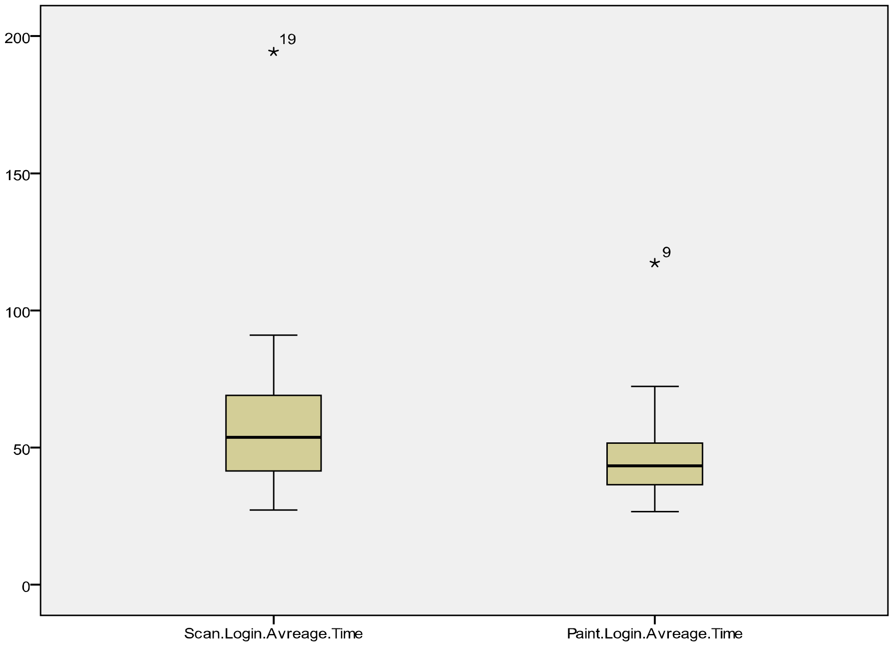
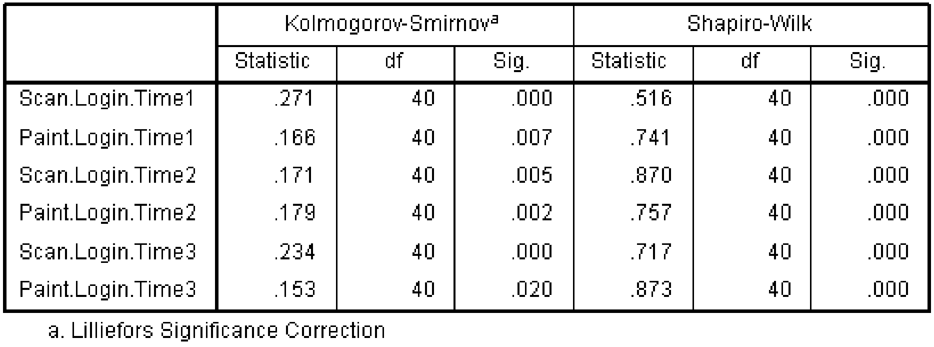


Figure 5-21 Box plot showingthe existence of outliers in logintimesfor both (scan &Paint)

Figure 5-21clearly shows the existence of outliers above 70 seconds, with one extreme score (case 19) in the scan system. Moreover, the figure shows the existence of outliers above 50 seconds with one extreme score (case 9) in the Paint system. Overall, neither of the systems incurred a login time of more than 3.25 minutes (194 seconds). However, the distribution of the data was not normal and the data was measured to cheek the normality by using a Shapiro test, as shown in Table 5-24and therefore, the Wilcoxon test was selected.

Table 5-24 Normality test of login time

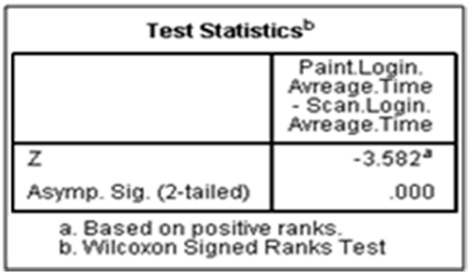


	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
Scan.Login.Time1	.271	40	.000	.516	40	.000
Paint.Login.Time1	.166	40	.007	.741	40	.000
Scan.Login.Time2	.171	40	.005	.870	40	.000
Paint.Login.Time2	.179	40	.002	.757	40	.000
Scan.Login.Time3	.234	40	.000	.717	40	.000
Paint.Login.Time3	.153	40	.020	.873	40	.000

a. Lilliefors Significance Correction

It was found that the mean time taken at the authentication stage was greater in the scan system than in the Paint system, as shown in Table 5-25. The results of the Wilcoxon signed rank test showed that the participants had significantly shorter authentication times in the Paint system than in the scan system (z=3.58, p<0.05, r=0.55).

Table 5-25 Wilcoxon test for the authentication stage.



Test Statistics^b

	Paint.Login. Avreage.Time - Scan.Login. Avreage.Time
Z	-3.582^a
Asymp. Sig. (2-tailed)	.000

a. Based on positive ranks.
b. Wilcoxon Signed Ranks Test

5.7 Discussion

Many of the studies mentioned in Chapter Two used hand drawn images (doodles) as graphical passwords [20], [21], [29], [95]. Doodles had been used in Cognometric schemes [193] and Drawmetric schemes. Most of the Cognometric studies focused on memorability and the success rate of the approach but none of them had reported the registration time as a self-performed task. In the results of the present experiment it is clear that the registration time was a little high on both systems compared to other systems that use such images, for example in study [193]. In the study, where the system provided the users with doodles to choose as passwords, it took an average of 39 seconds to enrol in the system. On another study, using Passface [194], the mean timings differed a little between the three groups: 155 seconds for the random groups, 152 seconds for the visual groups, and149 seconds for the verbal groups. In our system, it took on average about 10 minutes to complete registration in Paint and about 18 minutes for the scan process. This is understandable as the users had to achieve many steps to register their drawings and the time obviously depends on the number of the steps required by the users for each system.

Again, most of the graphical password studies which have used doodles, as mentioned in Chapter Two, did not report the login time. They either concerned themselves with security issues or usability in terms of memorability. However, a comprehensive study of frequency, interference, and training of multiple graphical passwords which used PassFaces [195] reported login times for one of the study groups who had used different for logins, with a mean score of 47.27 seconds. Similarly, a comprehensive study of the usability of multiple graphical passwords by Chowdbury et al. [196] reported that the mean login time for a doodle graphical password was 22.16 seconds and 48 seconds in a study comparing the usability of doodle and Mikon images by the same author [193]. Our results for the use of hand writing images showed that there was a slight difference between scan and paint in using doodles as a graphical password.

Finally, unforeseen environmental and personal factors (e.g., answering a phone call, discussing an urgent issue with a colleague, a sudden power shut-down, having a cup of coffee, and so on) may affect completion-time measured in online-based experiments [197]. The efficiency hypothesis was supported in relation to all the arguments covered in this section. Moreover, also it can be observed that this hypothesis of efficiency is more supported in scan than in Paint.

5.8 Conclusions

In this chapter, the results of two usability studies of using hand drawn images in authentication graphical passwords have been presented. It is now the appropriate point at which to revisit the questions asked at the start of the research.

How effectively can users be guided through the registration process?

95% of the participants who registered a pass-image completed the experiment. However, 21% created an account and then did not submit a pass image. The reasons for dropping out could not be determined. It could be that they were not very committed to using the website because it did not house any useful content. Alternatively, they may have found the instructions confusing. However, 79% did complete the registration stage successfully.

How effective is the image analysis software?

The software worked very well and was able to detect and correct almost all of the errors that users made when submitting their scanned file. The software worked equally well with scanned images and with those produced by a Paint program.

Which method of providing their images did users prefer?

The main conclusion of this research is that the participants would prefer to use a Paint based system rather than a pencil and paper to generate their pass images.

Implications

Graphical passwords are beginning to be deployed on smart phones and this research is relevant in this context. Smart phones have a camera which can be used to take a picture of the drawings and upload it to an app. This replaces the scanner, and is more convenient to use. Users may tend to make the same mistakes and so the same image analysis software can be used to detect and correct them. There is one additional error that would probably be common in the context of camera use; that of perspective distortion caused by the camera not being exactly square onto the paper. This can be detected from the distorted shape of the boxes on the supplied form, which would have to be printed, and then corrected. There are many drawing apps available on phones, with the user's finger replacing a mouse. These would replace the Paint program in our experiment. Our study indicated that users would prefer to use a drawing app to construct their pass images, rather than to draw them onto paper and take a photograph.

5.9 Chapter Summary

This chapter has outlined the following topics:

1. **An automated registration technique of graphical password**. This highlighted the software which was used to solve the many problems which accrued during or after drawing hand writing images to be registered as graphical passwords.
2. **An overview of the website used to meet the hypotheses behind this research**. This depicted its implementation and the related database used to keep the information of the experiment.
3. **Experiment details**. Clear information on the experiment was given, including experiment procurers, participants, roles, etc.
4. **Results and discussion**. This section presented the results obtained from the experiment and assessed the benefit of using such systems. It explained different preliminary analyses including data preparation and screening, and usability was tested based on the three usability metrics: *effectiveness*, *efficiency* and *satisfaction*.
5. **An overview of the errors made by users in drawing images during the experiment.** This highlighted many errors which appeared during drawing and scanning the forms into both systems.

Chapter Six
Shoulder Surfing and Recognition-Based Graphical Passwords

This chapter describes an experiment which detected the vulnerability of recognition based graphical authentication systems to shoulder surfing while using hand-drawn images. The experiment was conducted with teams of two, a user logging into such a system and an observer who was trying to spot the user's pass-image.

6.1 Introduction

Graphical passwords are still far from being perfect. For example, a password supplied for authentication by a user in a public place, if it is not properly protected, can be stolen by a bystander who observes it over the user's shoulder. A potential drawback of graphical password schemes is that they are more vulnerable to shoulder surfing than conventional alphanumeric text passwords [198]. Indeed, shoulder surfing was classified as one of the threat models affecting recognition-based graphical passwords under the area of observability[147]. A definition of shoulder surfing graphical passwords is that it is the process of observing authentication sessions and noting the images selected in order to use them to impersonate the user at a later time[199].

Since many graphical password studies and techniques are based on clicking on the password [71, 76, 93, 94]. The present experiment will determine the most user-friendly way to enter a doodle password (i.e. by typing or clicking) on the one hand and which is the most usable keyboard-based proposed method on the other hand. The results of the experiment were used in the experiment website which was described in Chapter Five, for the authentication screens for both of the scan and Paint systems.

6.2 Recognition-Based Graphical Authentication

The common feature of recognition-based graphical authentication systems is that the user is shown their pass-image, together with a number of distracter images when they log in. In this way they simply need to recognize their image when they see it. This is in contrast with password systems where the user must recall their exact password without any help provided by the system. Examples of such systems are: PassFace [71], Pass-Go [37] and Mikons [68]. If the challenge set consists of 16 images, the target image and 15 distracters, then the chance of guessing the right image is 1/16, which is too high for the system to offer much security. Because of this, in practice, several pass-images need to be selected before authentication can be completed. One problem with these systems is shoulder surfing. If the pass-image is selected using a mouse, then an observer could observe the position of the cursor when the mouse was clicked and could there by discover the pass-image. This could be easier than observing the character type, as would be the case with a password. With this in mind, we conducted an experiment with four different ways of entering the selected image. These were:

- Numeric - each image has a number.
- Numeric and alphabetic -each image has a number or letter.
- Row or column identifier.
- Mouse Clicks.

The usability of the four different methods of selecting a pass-image was also investigated. There may well be a tradeoff between usability on the one hand and security from shoulder surfing on the other. It has been observed that users will usually choose the easier approach, even if it is less secure. Thus, our goal is to find a method of choosing a pass-image that is both usable and as resistant to shoulder surfing as possible.

6.3 Experiment Details

The system used in this experiment used doodles as pass-images. The challenge set contained 16 doodles; the target doodle and 15 distracters. The system was run on both a laptop and a desktop with a high resolution monitor and 40 participants were divided into 20 teams with two people each, a user and an observer. Most of the participants who conducted this experiment were students from different departments and schools at Glasgow University.

Each user was given a sheet of paper containing their username and four doodle passwords, one for each method of selecting the pass-image. The user was asked to enter their username to start the experiment and then the four section methods sequentially presented themselves, with a period of preparation time for each. The order in which they were presented was chosen at random. After that they filled out a user questionnaire (see Appendix E).

The observer took a seat near the user, in the region of about one metre from the user. This is similar to the distances encountered in an internet café. The observer's task was to try to identify the entered pass-image and they were given a sheet of paper to record their choice. After that, they filled out an observer questionnaire. When the experiment was over, the user and observer swapped roles and reported the experiment. In addition, each user was given a sheet of paper with different doodle passwords from the previous user sheet.

While the experiment was taking place, the system recorded how long it took for each user to make a selection with each method. This is the time between displaying the challenge set and getting a user response. Also, the experimenter observed and took notes on how the experiment proceeded. The next sections explain the methods used in selecting the pass-images in detail.

6.3.1 Numeric type

In this model the user is asked to type the number of the provided doodle password which appears on the screen. These numbers range from 1-16, as illustrated in Figure 6-1. The password space will have a size of 1/16.

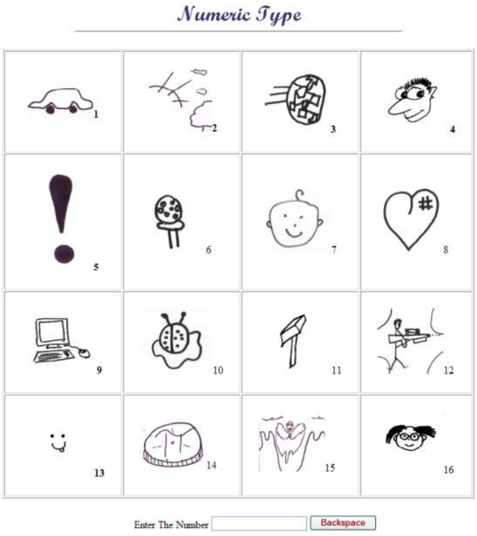


Figure 6-1 Numeric type

6.3.2 Numeric and alphabetic type

The user is asked to select and enter one of the characters provided on the screen which contains numbers and letters (1...9, a...g) as an identifier. This identifier must match the provided doodle password, as shown in Figure 6-2. Moreover, the password space will be 1/16.

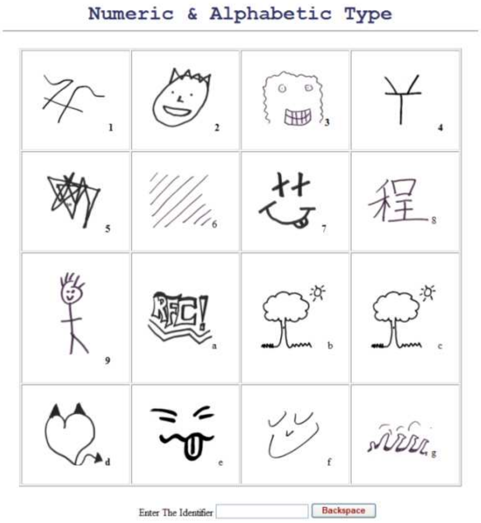


Figure 6-2 Numeric and alphabetic type

6.3.3 Columns and rows type (matrix)

In this model, the user must type either the column's letter (a…d) or the row's number (1…4) to express the location of the provided doodle password. Figure 6-3 illustrates this model. This model provides more security as the number of the password is difficult to predict. Furthermore, the password space size of this type will be 1/4.

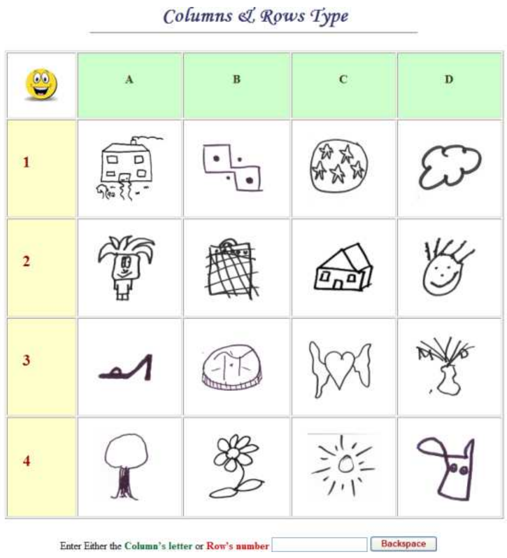


Figure 6-3 Columns and rows type (matrix)

6.3.4 Clicking Type

This model is totally different from the three previous models which have just been outlined. The previous models require the user to enter the number of the provided doodle password by typing the number or the letter according to the model. In this model, the user needs to select the exact provided doodle password from the screen by clicking the mouse button, as shown in Figure 6-4. The password space will have a size of 1/16.

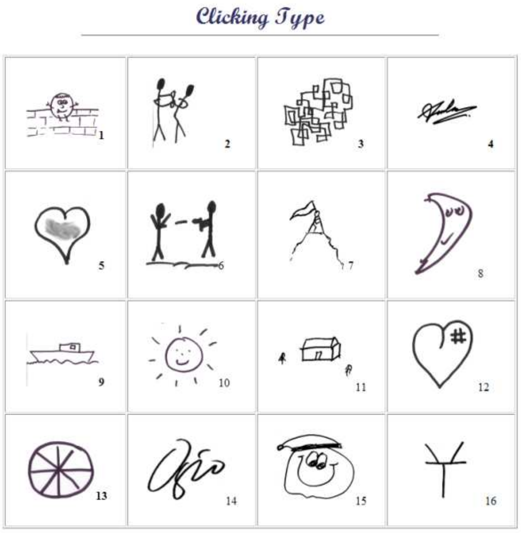


Figure 6-4 Clicking type

6.4 Evaluation assessments

Four elements were included to assess the four models of the experiment. First, the user and the observer were used to perform the assessment by the researcher, as mentioned before. Second, the third element of the assessment procedure was the running time of each model for each user which was recorded into a database of the experiment; this running time was calculated from the screen display for the user until he typed or clicked the password. Finally, the last element of the assessment procedure was the administrator of the experiment who was required to provide his notes and observations for each model.

6.5 Results

The results of this experiment were measured using two data collection methods. Firstly, the participants completed two sheets of paper. A Likert-scale questionnaire for the user and an observation form for the observer as shown in Appendix E, were distributed to the teams. Secondly, the time measurements were calculated by the system.

6.5.1 Questionnaire responses

The first nine questions asked about the usability of the experimental system. As mentioned in the previous section, the participants used a Likert system with five categories from 'strongly agree' to 'strongly disagree'. It can be seen that the average responses in support of using the system were higher than those against. The next three questions asked the users to compare the various methods against each other. Each question asked the user to select one stage as an answer. These stages were than translated into the actual method, since the actual methods used by each user appeared in a random order.

The below summary given in Table 6-1**,** shows the mean responses in each of the five categories, from strongly disagree to strongly agree. It can be noted that overall, the averaged responses in support of using the system were higher than those against. These pieces of information were drawn from nine different questions used in the usability questioner. Moreover, another five questions were asked and the answers are discussed later in this chapter.

Table 6-1 Summary of usability questions

	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
Ease of use this system	42.5%	45.0%	12.5%	0.0%	0.0%
Simple to use this system	55.0%	37.5%	7.5%	0.0%	0.0%
I feel comfortable using this system	35.0%	40.0%	7.5%	15.0%	2.5%
Easy to learn to use this system	42.5%	47.5%	5.0%	5.0%	0.0%
Easy to understand the provided information	40.0%	50.0%	7.5%	2.5%	0.0%
The organization of information on screens is clear	30.0%	57.5%	5.0%	7.5%	0.0%
The interface of this system is pleasant	17.5%	60.0%	17.5%	5.0%	0.0%
I like using the interface of this system	15.0%	67.5%	5.0%	12.5%	0.0%
Overall, I am satisfied with this system	22.5%	67.5%	5.0%	2.5%	2.5%

Figure 6-5 shows the average times spent on each type of model by participants in the experiment. As seen in the chart, there is not much time difference between the models; approximately 8 seconds' difference between the lowest average time spent on the mouse type and the highest average time spent on the matrix type.

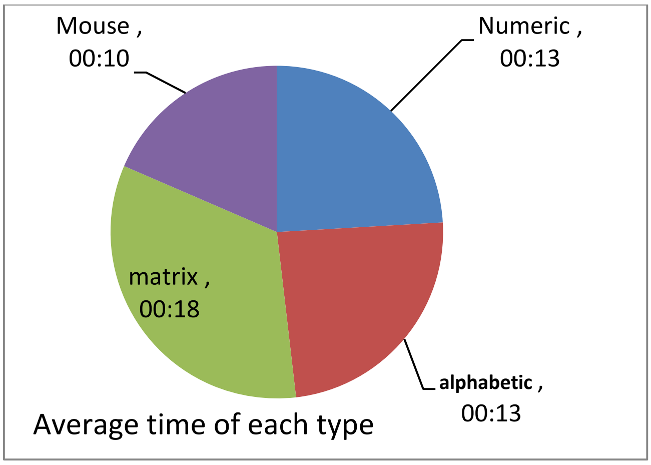


Figure 6-5 Average time spent on each type

Moreover, just under a half of the total 40 users agreed that the matrix is more secure than other types while about 30% pointed out that the alphabetical type is secure, as illustrated in Figure 6-6. In addition, Figure 6-7 shows that more than a third of users were satisfied with the matrix type and said they felt more comfortable with it than with other types. Furthermore, about half of the users believed it was important for security to try to ensure that no others to see their selection, by using the mouse type as seen in Figure 6-8.

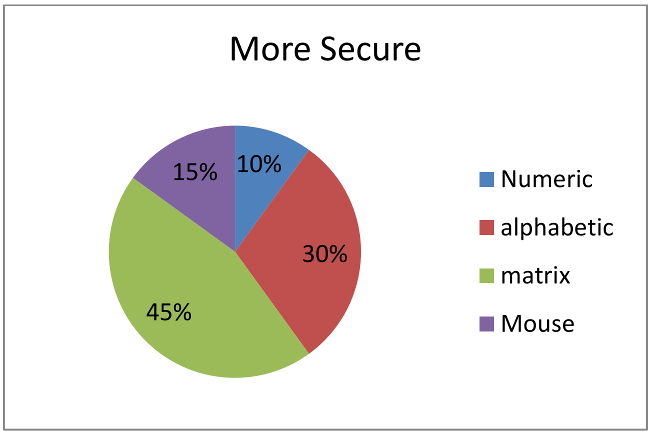


Figure 6-6 Priority of security

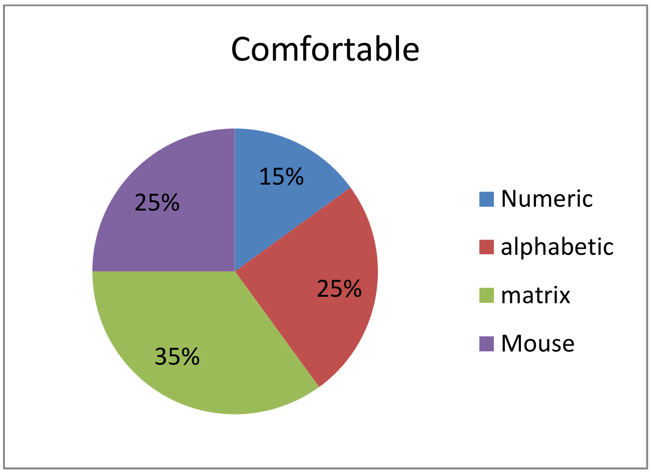


Figure 6-7 Comfort of the types

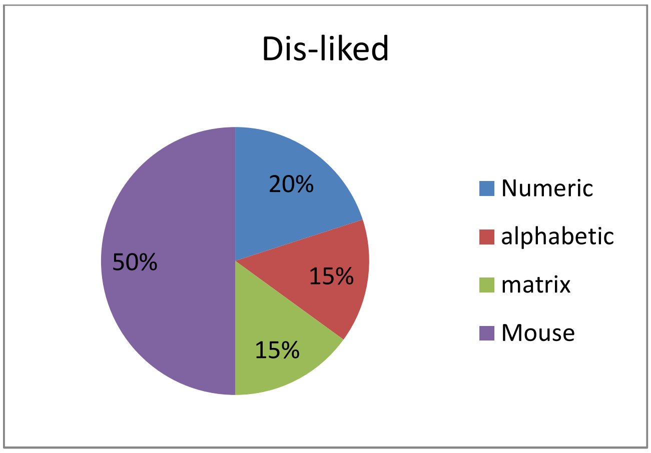


Figure 6-8 Unsatisfying types

6.5.2 Effectiveness of the observers

Figure 6-9 shows how effective the observers were in guessing the passimage. Overall, the attackers were quite effective and guessed the correct passimage. They were most successful at guessing the position of the mouse click, being able to record it over three quarters of the time. The three methods using the keyboard were slightly more secure. It can be seen also from Figure 6-9 that types 2 and 3 are types which are liable to more disclosure to observers, at about 47% ≈ 19 people for each type.

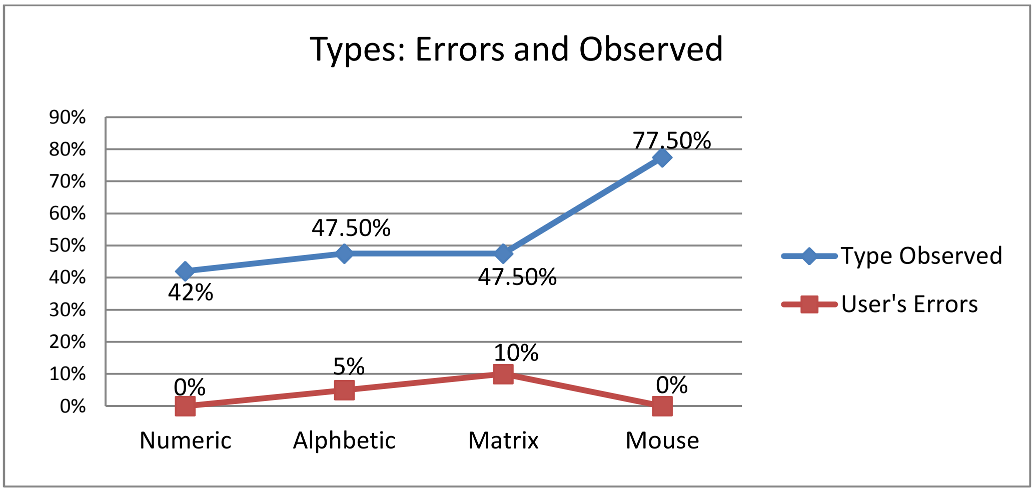


Figure 6-9 User errors and types observed

6.5.3 Time to enter data

As can be seen in the graph in Figure 6-10, there were four ways to enter the passdoodles. The graph shows the relationships between the time spent to enter the characters of the passdoodles and the users for all types. It can be seen from the graph, users fluctuated between a low of 3 seconds and a peak of 36 seconds in the Numeric type. In addition, users fluctuated between a low of 3 seconds and a peak of 52 seconds in the Numeric and Alphabetic types.

Moreover, users fluctuated between a low of 4 seconds and a peak of 59 seconds in the Matrix type. Furthermore, users fluctuated between a low of 2 seconds and a peak of 36 seconds in the Clicking type. This fluctuation occurred as a result of several factors which will be mentioned in the next section.

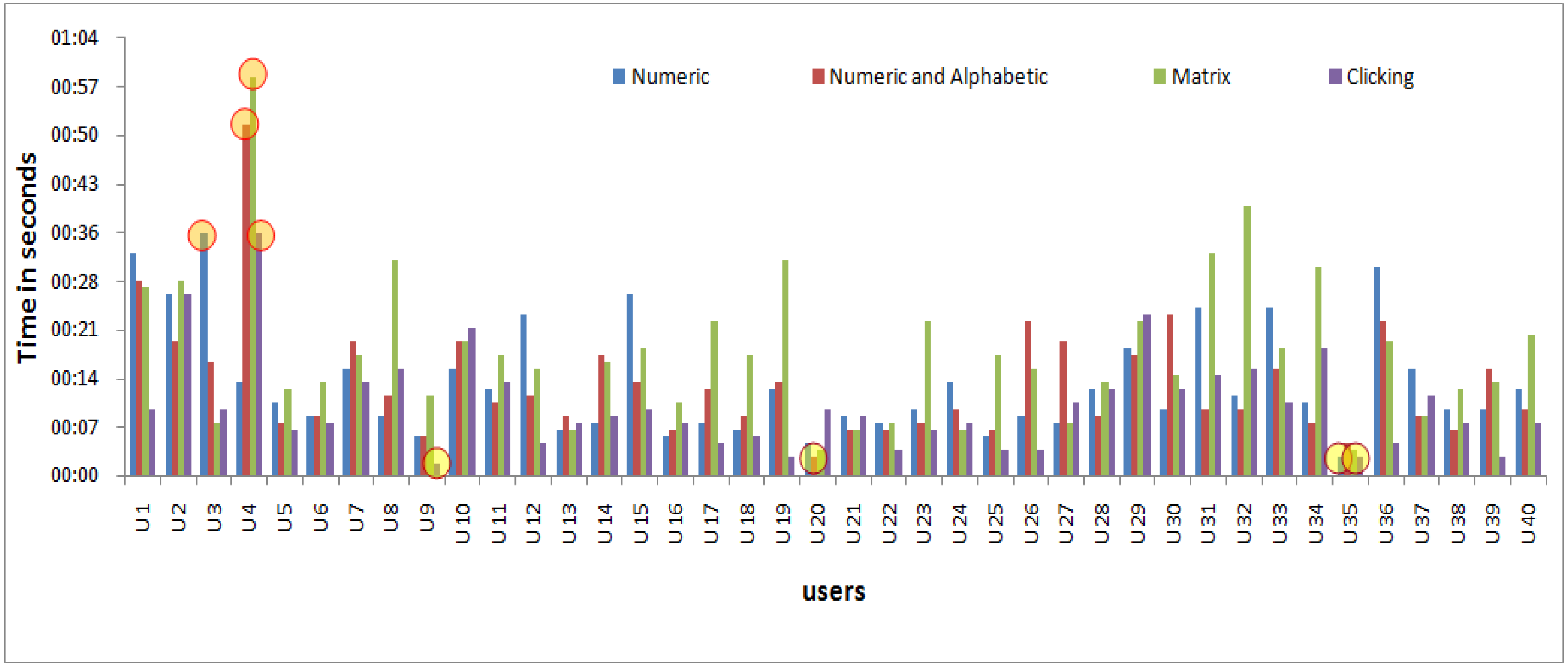


Figure 6-10 Time spent on each type by the all 40 users

6.6 Discussion

The main purpose of this study was to determine which type of the four modules of the experiment was the most usable and effective type for people to select and securely enter their passdoodles. The four discussion topics will be described individually which regarding to the modules of this experiment.

6.6.1 Numeric and Numeric & Alphabetic types

The majority of users who selected the Numeric and Alphabetic types felt that they were easy to use, with differences which can briefly be described into two points: first, that it would be more complicated for the observer to determine the identifier of numbers and characters rather than the numbers only. The second point concerned solitary entering, in other words, where it was only required to enter only one character to select the passdoodles.

“I do not really see a difference between the three ways of typing”.

“I feel that the combination of numbers and letters offer more security particularly when entering a single character”.

“I like type 2 which offers more security by single pressing”.

However, the alphabetic type was slightly error prone, with a 5% error rate.

6.6.2 Matrix Type

Most users liked the matrix type. Some of them attributed this to the ease of use, others to the confidentiality afforded by this type. The recognition of the entered character did not give the observer any indication of the user’s passdoodles. On the other hand, if the observer identifiers the entered character, he still needs to define which one from the options is the user’s exact passdoodle. Each character in this type has four displayed doodles which will make it very difficult to determine the exact one.

“I feel this type is more comfortable because it does not give the observer any idea of the password selected”. . *“It is hard to recognize”*.

Of course, the user would have to use the matrix method twice to locate the correct pass doodle. The attacker would however have to correctly observe the entries. The matrix method was also more error prone, with a 10% error rate.

6.6.3 Mouse type

Although the mouse type of login may overcome some of the problems found in previous studies [37], [39], [200] and the changing of the shape of the mouse cursor to a 'cross ship' could be one of possible solutions of the problem of observation which make the courser too small and hard to be observed. Therefore, in this experiment it is noted that the mouse type is more discovered than other types at about 77% compared to the other keyboard types, which were discovered 42%, 47.5% and 47.5%. It is suggested that in future studies in the field, a different mouse cursor such as a dot (.) could be used to increase the level of security.

6.7 Conclusion and future work

One clear result of this work is that it has shown that it is easier to observe a mouse click than data entered via a key board. One surprising result is that while the three key board based methods were more secure than using the mouse, they were not very different from each other. In particular, the matrix method was correctly observed nearly half of the time even though observing a single key press still left the observer with a one in four guess. One possible explanation is that the user may have been unconsciously indicating which keys were needed to determine the passimage, perhaps by hovering their fingers over both keys before deciding which one to press. One indication that this might be the case is that the time needed to enter data in the matrix case was, on average, five seconds longer. Additionally, using identifiers for the images that had been mixed up by characters and numbers is more secure than the other proposed keyboard types. It would be of benefit to conduct a further experiment where the users were given time to practice the various form of choice indication before being observed. The observers could also be given the chance to explain how they had worked out which was the chosen image. The clicking model was the easiest and fastest way of all, but this method lacked security and could be used more effectively in the future if the mouse cursor was changed to a small point such as dot (.). There would also be a need to do some testing to check how easy it is to identify the location of the cursor on the screen and therefore such experiments are strongly advised, as their success might open up horizons for the use of a mouse-pointer in graphical passwords.

Chapter Seven
Conclusions and future work

7.1 Introduction

This chapter summarises the contributions made by this research. The chapter also offers conclusions in terms of the original research questions as well as the overall aims of the research and offers recommendations for the potential applications of the results of the passdoodles system. In closing, we discuss possible future research directions which could be based on this work, and offer concluding remarks.

7.2 Research Contributions and Achievements

This research has produced several original contributions to the research into the security and usability of graphical password authentication. The following table shows the major contributions of this research:

Table 7-1 Original Research

Chapter	Original Research
Chapter 3	An empirical study of the relative comprehensibility of cross-cultural influences in drawing doodles between Scottish, Libyan and Nigerian participants.
Chapter 4	An empirical study highlighted the guessability of hand-drawn images based on cultural knowledge.
Chapter 5	Demonstration, via automatic registration of hand drawn images as graphical passwords and an empirical study of usability, of the use of a hand-drawn images technique vs. the use of a program-based drawing technique.
Chapter 6	An empirical study on preventing shoulder surfing when selecting pass-images in a challenge set revealed the most secure ways of doing so and suggested further improvements.

7.3 Thesis Summary

The choice of hand-drawn images is affected by a user's culture, and this can have an impact on their usability and security. In addition, it is possible to build a system that allows a user to submit their own hand-drawn images without the need for an administrator, making the system more scalable.

This research has had the aims of investigation of cultural aspects of user drawn images for authentication was carried out and a comparison was made between Westerners (represented by Scots), Africans (represented by Nigerians) and Arabs (represented by Libyans). Additionally, another major aim behind this research is investigating whether user-drawn pictures are easier to use than user created program-drawn ones and to create a simple method for using hand-drawn images as graphical password by making it easier for users to register them. Finally, a part of this research has concerned itself with two of the well-known security issues that are related to graphical passwords: guessability and shoulder surfing.

A number of research questions were posed at the start of this thesis. Summaries of the answers are given below:

Q1. Does culture play an important role in the selection of pictures by Scottish, Libyan and Nigerian users? Can we quantity this effect?

To answer this question, Chapter three introduced a study that was conducted to evaluate the effects of culture on drawings. To achieve the aim of this study, an investigation was carried out in two different countries: Scotland, as a 'Western' country, and Libya as an 'Arab' country. Many doodles may be influenced by the users' culture, which makes them easier to guess. Thus, it follows that the culture of the drawers of many doodles can be guessed. We also found that it was possible to guess the gender of the drawer based on the type of doodle drawn. Some simple guidelines, such as not including text or drawing flags and maps can have a large effect on the level of guessability of doodles.

Q2 .Is it possible to guess other people's hand-drawn image passwords depending on his/her personality characteristics, such as cultural features or nationality?

One clear result of the work presented in Chapter four is that it is apparently highly possible to guess other people’s pass images if they contain cultural characteristics, especially religious marks.

Q3. Is it possible to automate the registration of hand drawn images?

Chapter five introduced image analysis software created by researcher, that was able to correct almost all common user mistakes. The software can be generalised to correct perspective effects if photos of the image passwords, perhaps generated by a Smartphone, are provided.

Q4. How does the usability compare between registering hand-drawn images by scan and hand-drawn images created with paint?

To answer the above questions, Chapter five introduced an empirical study that was conducted to evaluate the usability of hand–drawn passimage systems. Each user was asked to create accounts and login to both of the systems, scan and Paint. This study was conducted to compare between a hand-drawing technique using the scan method and a program-based drawing technique using the Paint method. The study measured all usability terms for both systems and recorded the issues that arose during the experiment. It was clearly demonstrated that using the Paint system was easier, faster and more acceptable to users than the scan system. The memorability of both systems was roughly equal. Users preferred the Paint system over the scan system by a factor of 4 to 1. Users were quicker at logging in using the Paint system than they were with the scan system. This would indicate that they remembered the paint images more than the scanned ones also login success rate showed the memorability rate were high which is around 95%.

Q5. What is the safest way of selecting hand-drawn image passwords?

In chapter six an experiment was performed that showed that using a single key stroke (mixed letters and numbers) to select a doodle is the safest way to avoided shoulder surfing. Also, the flinging from the experiment conducted in Chapter six confirmed that using mouse clicking for selecting passimage is less secure than using keyboard strokes.

7.4 Future Work

During the work reported in this dissertation, many ideas arose which could be suitable for the future development of the area of research. This thesis has contributed to understanding issues of security, and the improved usability of the use of hand-drawn images as graphical passwords. Moreover, part of this research has contributed to understanding cross-cultural influences in drawing images. However, it has also raised new research directions. These research opportunities will be discussed in the following sub sections.

7.4.1 Future work suggestion in Chapter 3 and Chapter 4

It would be good to develop a quantitative measure of how easier it is to guess the culture and gender varies types of user drawn as the further research of this work.

7.4.2 Future work suggestion in Chapter 5

The hand-drawn Paint system was found to be more usable than the scan system. Unfortunately, the Paint system still has drawbacks in its drawings, as mentioned in section 5.6.8.2 and 5.6.8.3. As an improvement to this system, we suggest building up very simple drawing tools that use one size of bold pen and an automatically focused drawing box and then integrating all these together into the subject website or Smartphone app.

Nowadays, graphical passwords are beginning to be deployed on smart phones and this research is relevant in this context. Smart phones have a camera which can be used to take a picture of the drawing and upload it to an app. This replaces the scanner, and is more convenient to use. Users may tend to make the same mistakes and so the same image-analysis software can be used to detect and correct them. Many drawing apps are available on phones, with the user’s finger replacing a mouse. These could replace the paint program in our experiment. Our study indicated that the majority of users would prefer to use a drawing app to construct their pass images, rather than to draw them on paper and take a photograph.

7.4.3 Future work suggestion in Chapter 6

The mouse clicking model was the easiest and fastest way of all, but this method lacked security. Can we use this method in the future in a more effective way, if the mouse cursor has been changed to a small point, such as a dot (.)?Tests are also advised to check how easy it is to identify the location of the cursor on the screen, the success of which will open up possibilities for the use of the mouse-pointer in logging in with graphical passwords.

Bibliography

[1] W. R. Cheswick and S. M. Bellovin, *Firewalls and Internet Security:Repelling the Wily Hacker*, First ed.: AT&T and Lumeta Corporation, 1994.

[2] A. Adams and M. A. Sasse, "Users are not the enemy," *Commun. ACM,* vol. 42, pp. 40-46, 1999.

[3] M. N. Roger and D. S. Michael, "Using encryption for authentication in large networks of computers," *Commun. ACM,* vol. 21, pp. 993-999, 1978.

[4] A. Patrick, "Human factors of security systems: A brief review. ," ed, 2002.

[5] A. Adams and A. Blandford, "Security and Online learning: to protect or prohibit," in *Usability Evaluation of Online Learning Programs*, Claude, Ed., ed: UK: IDEA, 2003, pp. 331-359.

[6] W. Hugh and M. L. Lorie, "Using Fingerprint Authentication to Reduce System Security: An Empirical Study," presented at the Proceedings of the 2011 IEEE Symposium on Security and Privacy.

[7] D. B. Chapman and E. D. Zwicky. (1995, 6/2008). *Building Internet Firewalls.* Available: http://www.unix.com.ua/orelly/networking/firewall/index.htm

[8] K. Renaud and E. Smith, "Jiminy: helping users to remember their passwords," presented at the Annual Conference of the South African Institute of Computer Scientists and Information Technologists, Pretoria, South Africa, 2001.

[9] S. Radack. (2004) Electronic Authentication: Guidance For Selecting Secure Techniques. *National Institute of Standards and Technology*.

[10] J. Brainard, A. Juels, R. L. Rivest, M. Szydlo, and M. Yung, "Fourth-factor authentication: somebody you know," presented at the Proceedings of the 13th ACM conference on Computer and communications security, Alexandria, Virginia, USA, 2006.

[11] M. D. H. Abdullah, A. H. Abdullah, and N. Ithnin, "Graphical Password: Security and Usability Issues," *PARS’07,* 3-4 July 2007.

[12] P. Elftmann, "Secure Alternatives to Password-based Authentication Mechanisms," Diploma, Laboratory for Dependable Distributed Systems, RWTH Aachen University, Aachen, Germany, 2006.

[13] P. C. v. Oorschot and J. Thorpe, "On predictive models and user-drawn graphical passwords," *ACM Trans. Inf. Syst. Secur.,* vol. 10, pp. 1-33, 2008.

[14] F. L. Francis, "Handwriting Authentication by Envelopes of Sound Signatures," presented at the Proceedings of the Pattern Recognition, 17th International Conference on (ICPR'04) Volume 1 - Volume 01, 2004.

[15] G. E. Blonder, "Graphical password," *U.S. Patent 5,559,961*, 1996.

[16] R. N. Shepard, "Recognition Memory for Words, Sentences, and Pictures," *Journal of Verbal Learning and Verbal Behavior,* vol. 6, pp. 156-163, 1967.

[17] A. De Angeli, L. Coventry, G. Johnson, and K. Renaud, "Is a picture relly worth a thousand words? Exploring the feasibility of graphical authentication systems," *International Journal of Human-Computer Studies,* vol. 63, pp. 128-152, 2005.

[18] F. M. a. M. K. Reiter., *Graphical Passwords* vol. 9. O'Reilly, 2005.

[19] searchsecurity.techtarget.com, "graphical password," ed, 2008.

[20] K. Renaud, "A Visuo-Biometric Authentication Mechanism for Older Users " in *People and Computers XIX - The Bigger Picture*, ed: Springer London, 2006, pp. 167-182.

[21] J. Goldberg, J. Hagman, and V. Sazawal, "Doodling Our Way to Better Authentication," USA Patent ACM 1-58113-454-1/02/0004., 2002.

[22] N. S. Govindarajulu and S. Madhvanath, "Password management using doodles," presented at the Proceedings of the 9th international conference on Multimodal interfaces, Nagoya, Aichi, Japan, 2007.

[23] B. Sidis and S. P. Goodhart, *Multiple personality: An experimental investigation into human individuality*. New York: New York : D. Appleton and Company, 1905.

[24] B. Russell, *The Analysis of Mind.*: 2007 BiblioBazaar, 1921.

[25] G. Mandler, "Familiarity Breeds Attempts: A Critical Review of Dual-Process Theories of Recognition," *Perspectives on Psychological Science*, vol. 3, pp. 390-399, September 1, 2008 2008.

[26] M. M. Langley, "An event-related potential investigation of the neural representations that support familiarity-based picture recognition.," Doctor of Philosophy, Psychology, Iowa State University of Science and Technology, Iowa State University, 2010.

[27] A. P. Yonelinas, "Receiver-operating characteristics in recognition memory: evidence for a dual-process model," *J Exp Psychol Learn Mem Cogn*, vol. 20, pp. 1341-54, Nov 1994.

[28] A. P. Yonelinas, "The Nature of Recollection and Familiarity: A Review of 30 Years of Research," *Journal of Memory and Language*, vol. 46, pp. 441-517, 2002.

[29] K. Renaud, "On user involvement in production of images used in visual authentication," *Journal of Visual Languages & Computing*, vol. 20, pp. 1-15, 2009.

[30] J. Berger, *Berger on Drawing*: Occasional Press, 2005.

[31] J. Thorpe and P. C. Van Oorschot, "Towards secure design choices for implementing graphical passwords," *The 20th Annual Computer Security Applications Conference (ACSAC'04)*, vol. 1063-9527, pp. 50- 60, 2004.

[32] G. Ford and P. Kotz, "Designing usable interfaces with cultural dimensions," presented at the Proceedings of the 2005 IFIP TC13 international conference on Human-Computer Interaction, Rome, Italy, 2005.

[33] M. Anandarajan, M. Igbaria, and U. P. Anakwe, "IT acceptance in a less-developed country: a motivational factor perspective," *International Journal of Information Management*, vol. 22, pp. 47-65, 2002.

[34] D. Casasanto and K. Dijkstra, "Motor action and emotional memory," *Cognition*, vol. 115, pp. 179-185, 2010.

[35] J. Engelkamp, H. Zimmer, G. Mohr, and O. Sellen, "Memory of self-performed tasks: Self-performing during recognition," *Memory & Cognition*, vol. 22, pp. 34-39, 1994.

[36] A. Koriat, H. Ben-Zur, and A. Nussbaum, "Encoding information for future action: Memory for to-be-performed tasks versus memory for to-be-recalled tasks," *Memory & Cognition*, vol. 18, pp. 568-578, 1990.

[37] HaiTao, "Pass-Go, a New Graphical Password Scheme," Master of Applied Science, Electrical and Computer Engineering, University of Ottawa, Canada, 2006.

[38] X. Suo, Y. Zhu, and G. S. Owen, "Graphical Passwords: A Survey," *acsac*, 2005.

[39] A. E. Dirik, N. Memon, and J.-C. Birget, "Modeling user choice in the PassPoints graphical password scheme," presented at the Proceedings of the 3rd symposium on Usable privacy and security, Pittsburgh, Pennsylvania, 2007.

[40] R. Poet and K. Renaud, "An algorithm for automatically choosing distractors for recognition based authentication using minimal image types," *Open Ergonomics Journal*, vol. 2, pp. 178-184, 2009.

[41] K. D. Mitnick and W. L. Simon, *The Art of Deception: Controlling the Human Element of Security*: Wiley, 2002.

[42] R. G. Rittenhouse, J. A. Chaudry, and M. Lee, "Security in Graphical Authentication," *Security in Graphical Authentication*, vol. 7, May 2013 2013.

[43] A. D. Angeli, L. Coventry, G. Johnson, and K. Renaud, "Is a picture relly worth a thousand words? Exploring the feasibility of graphical authentication systems," *International Journal of Human-Computer Studies*, vol. 63, pp. 128-152, 2005.

[44] K. Renaud, "A process for supporting risk-aware web authentication mechanism choice," *Reliability Engineering & System Safety*, vol. 92, pp. 1204-1217, 2007.

[45] R. Biddle, S. Chiasson, and P. C. V. Oorschot, "Graphical Passwords: Learning from the First Twelve Years," *ACM*, 2010.

[46] usabilitynet.org. (1998, 04-08). *Usability definitions*. Available: http://www.usabilitynet.org/tools/r_international.htm#9241-1

[47] M. A. Sasse, "Usability and trust in information systems," in *Cyber Trust & Crime Prevention Project*, U. C. London, Ed., ed: Cyber Trust & Crime Prevention Project, 2004, p. 18.

[48] M. V. Welie, G. v. d. Veer, and A. Elins, "Breaking down Usability," in *Proceedings of Interact '99*, ed. Edinburgh, Scotland, 1999.

[49] E. E. Schultz, R. W. Proctor, M.-C. Lien, and G. Salvendy, "Usability and Security An Appraisal of Usability Issues in Information Security Methods," *Computers & Security*, vol. 20, pp. 620-634, 2001.

[50] K. Renaud and A. De Angeli, "My password is here! An investigation into visuo-spatial authentication mechanisms," *Interacting with Computers*, vol. 16, pp. 1017-1041, 2004.

[51] C. Braz and J. M. Robert, "Security and usability: the case of the user authentication methods," presented at the Proceedings of the 18th International Conferenceof the Association Francophone d'Interaction Homme-Machine, Montreal, Canada, 2006.

[52] R. S. Sollie, "Security and usability assessment of several authentication technologies," Master of Science in Information Security, Computer Science and Media Technology, Gjøvik University College, Norway, 2005.

[53] D. Davis, F. Monrose, and M. K. Reiter, "On user choice in graphical password schemes," presented at the Proceedings of the 13th conference on USENIX Security Symposium - Volume 13, San Diego, CA, 2004.

[54] P. Harsh and R. E. Newman, "Usability and Acceptance of an Image-based Authentication System," 2006.

[55] M. D. Hafiz, A. H. Abdullah, N. Ithnin, and H. K. Mammi, "Towards Identifying Usability and Security Features of Graphical Password in Knowledge Based Authentication Technique," in *Modeling & Simulation, 2008. AICMS 08. Second Asia International Conference on*, 2008, pp. 396-403.

[56] A. Goldstein and J. Chance, "Visual recognition memory for complex configurations," *Perception & Psychophysics,* vol. 9, pp. 237-241, 1971.

[57] R. N. Shepard, "Recognition Memory for Words, Sentences, and Pictures," *Journal of Verbal Learning and Vei~Bal Behavior,* vol. 6, pp. 156-163, 1967.

[58] R. Dhamija and A. Perrig, "Déjà Vu: a user study using images for authentication," presented at the Proceedings of the 9th conference on USENIX Security Symposium - Volume 9, Denver, Colorado, 2000.

[59] J. Andrade, "What does doodling do?," *Applied Cognitive Psychology,* vol. 24, pp. 100-106, 2009.

[60] L. Nyberg, L. G. Nilsson, and L. Bäckman, "Recall of actions, sentences, and nouns: Influences of adult age and passage of time," *Acta Psychologica,* vol. 79, pp. 245-254, 1992.

[61] G. Knoblich and W. Prinz, "Recognition of self-generated actions from kinematic displays of drawing," *Journal of Experimental Psychology: Human Perception and Performance,* vol. 27, pp. 456-65, 2001.

[62] P. A. Leynes, J. A. Grey, and J. T. Crawford, "Event-related potential (ERP) evidence for sensory-based action memories," *International Journal of Psychophysiology,* vol. 62, pp. 193-202, 2006.

[63] M. Longcamp, J.-L. Anton, M. Roth, and J.-L. Velay, "Visual presentation of single letters activates a premotor area involved in writing," *NeuroImage,* vol. 19, pp. 1492-1500, 2003.

[64] B. H. Repp and G. Knoblich, "Perceiving action identity: how pianists recognize their own performances," *Psychological science,* vol. 15, p. 9, 2004.

[65] R. Flach, G. Knoblich, and W. Prinz, "Recognising one’s own clapping: The role of temporal cues," *Pscyhological Research,* vol. 69, pp. 147-156, 2004.

[66] F. Loula, S. Prasad, K. Harber, and M. Shiffrar, "Recognizing People From Their Movement," *Journal of Experimental Psychology. Human Perception & Performan,* vol. 31, p. 210, 2005.

[67] J. Engelkamp and H. D. Zimmer, "Similarity of movement in recognition of self-performed tasks and of verbal tasks," *British Journal of Psychology,* vol. 86, pp. 241-252, 1995.

[68] K. Renaud, "Web Authentication Using Mikon Images," in *Privacy, Security, Trust and the Management of e-Business, 2009. CONGRESS '09. World Congress on*, 2009, pp. 79-88.

[69] Mohammad A. Alia, A. A. Hnaif, H. K. Al-Anie, and A. A. Tamimi, "Graphical Password Based On Standard Shapes," *Science Series Data Report,* vol. 4, Feb 2012 2012.

[70] G. A. Feingold, "Influence of Environment on Identification of Persons and Things," *HeinOnline -- 5 J. Am. Inst. Crim. L. & Criminology,* pp. 39-51, 1914.

[71] R. U. Corporation, "The Science Behind Passfaces," June 2004.

[72] S. Brostoff and M. A. Sasse, "Are Passfaces more usable than passwords? A field trial investigation," in *HCI 2000,* 2000.

[73] P. Corporation, "About Passfaces ", ed, 2005-2007.

[74] D. T. Levin, "Race as a Visual Feature: Using Visual Search and Perceptual Discrimination Tasks to Understand Face Categories and the Cross-Race Recognition Deficit," *Experimental Psychology: General,* vol. 129, pp. 559-574, 2000.

[75] J. H. Langlois, L. Kalakanis, A. J. Rubenstein, A. Larson, M. HaUam, and Monica'Smoot, "Maxims or Myths of Beauty? A Meta-Analytic and Theoretical Review," *Psychological Bulletin,* vol. 126, pp. 390-423, 2000.

[76] L. Sobrado and J.-C. Birget, "Graphical passwords," *The Rutgers Scholar, An Electronic Bulletin for Undergraduate Research,* vol. 4, 2002.

[77] W. Jansen, S. Gavrila, V. Korolev, R. Ayers, and R. Swanstrom, "Password: A Visual Login Technique for Mobile Devices," C. S. Division, I. T. Laboratory, and N. I. o. S. a. Technology, Eds., ed, 2003.

[78] F. A. Alsulaiman and A. E. Saddik, "A Novel 3D Graphical Password Schema," *IEEE International Conference on Virtual Environments, Human-Computer Interfaces, and Measurement Systems,* 10-12 July 2006.

[79] N. Fraser, "The usability of picture passwords," Tricerion Group plc 2006.

[80] O. L. S. S. Steven, Davis, Nicholas A., Sontag, James L. and Norvell, Joel, "Methods And Systems For Graphical Image Authentication," United States Patent, 2008.

[81] L. Phen-Lan, W. Li-Tung, and H. Po-Whei, "Graphical Passwords Using Images with Random Tracks of Geometric Shapes," presented at the Proceedings of the 2008 Congress on Image and Signal Processing, Vol. 3 - Volume 03, 2008.

[82] H. Eiji, D. Rachna, C. Nicolas, and P. Adrian, "Use Your Illusion: secure authentication usable anywhere," presented at the Proceedings of the 4th symposium on Usable privacy and security, Pittsburgh, Pennsylvania, 2008.

[83] A. M. Eljetlawi and N. Ithnin, "Graphical Password: Prototype Usability Survey," in *Advanced Computer Theory and Engineering, 2008. ICACTE '08. International Conference on*, 2008, pp. 351-355.

[84] P. C. Ven Oorschot and T. Wan, "TwoStep: An Authentication Method Combining Text and Graphical Passwords," in *E-Technologies: Innovation in an Open World*. vol. 26, ed Ottawa, Canada: Springer Berlin Heidelberg, 2009, pp. 233-239.

[85] I. Jermyn, A. Mayer, F. Monrose, M. K. Reiter, and A. D. Rubin, "The design and analysis of graphical passwords," presented at the Proceedings of the 8th conference on USENIX Security Symposium - Volume 8, Washington, D.C., 1999.

[86] H. Gao, X. Guo;X. Chen; L. Wang;X. Liu; , "YAGP: Yet Another Graphical Password Strategy.," presented at the Computer Security Applications Conference,ACSAC 2008,Annual, Anaheim, CA 2008.

[87] C. Varenhorst, "Passdoodles; a Lightweight Authentication Method," Research Science Institute2004.

[88] N. SundarG and S. Madhvanath, "Password Management Using Doodles," *ACM*, pp. 12–15, 2007.

[89] A. De Luca, R. Weiss, H. Hußmann, and X. An, "Eyepass - eye-stroke authentication for public terminals," presented at the CHI '08 extended abstracts on Human factors in computing systems, Florence, Italy, 2008.

[90] M. Yves, St, O. phane, and H. Olivier, "Recall-a-story, a story-telling graphical password system," presented at the Proceedings of the 5th Symposium on Usable Privacy and Security, Mountain View, California, 2009.

[91] F. A. Alsulaiman and A. E. Saddik, "Three-Dimensional Password for More Secure Authentication," *IEEE TRANSACTIONS ON INSTRUMENTATION AND MEASUREMENT,* February 6, 2008 2008.

[92] S. Wiedenbeck, J. Waters, J.-C. Birget, A. Brodskiy, and N. Memon, "PassPoints: Design and longitudinal evaluation of a graphical password system," *International Journal of Human-Computer Studies,* vol. 63, pp. 102-127, 2005.

[93] L. D. Paulson, "Taking a Graphical Approach to the Password," *IEEE,* vol. 35, p. 1, 2002.

[94] viskey, "User Manual visKey," 2005.

[95] P. Dunphy and J. Yan, "Do background images improve "draw a secret" graphical passwords?," presented at the Proceedings of the 14th ACM conference on Computer and communications security, Alexandria, Virginia, USA, 2007.

[96] S. Chiasson, P. C. v. Oorschot, and R. Biddle, *Graphical Password Authentication Using Cued Click Points* vol. 4734/2007: Springer Berlin / Heidelberg, 2007.

[97] S. Alireza Pirayesh and S. Angelos, "Universal Multi-Factor Authentication Using Graphical Passwords," presented at the Proceedings of the 2008 IEEE International Conference on Signal Image Technology and Internet Based Systems, 2008.

[98] G. a. Z. Haichang, Ren and Xiuling, Chang and Xiyang, Liu and Aickelin, Uwe "A new graphical password scheme resistant to shoulder-surfing," presented at the International Conference on CyberWorlds, , Singapore, 2010.

[99] A. H. Lashkari, A. Gani, L. G. Sabet, and S. Farmand, "A new algorithm on Graphical User Authentication (GUA) based on multi-line grids," *Scientific Research and Essays (SRE),* vol. 5, pp. 3865 - 3875, 18 December 2010 2010.

[100] P. R. Devale, S. M. Deshmukh, and A. B. Pawar, "Persuasive Cued Click Points with Click Draw Based Graphical Password Scheme," *International Journal of Soft Computing and Engineering (IJSCE),* vol. 3, may 2013 2013.

[101] J. Thorpe, B. MacRae, and A. Salehi-Abari, "Usability and Security Evaluation of GeoPass: a Geographic Location-Password Scheme," in *Symposium on Usable Privacy and Security (SOUPS),* Newcastle, UK, July, 2013.

[102] K. Renaud and J. Ramsay, "Now what was that password again? A more flexible way of identifying and authenticating our seniors," *Behav. Inf. Technol.,* vol. 26, pp. 309-322, 2007.

[103] R. Poet and K. Renaud, "A Mechanism for Filtering Distractors for Doodles Passwords," in *Conference of the International Graphonomics Society*, Australia, 2007, pp. 129-132.

[104] H. Cherifi, J. M. Zain, E. El-Qawasmeh, A. H. Lashkari, A. Abdul Manaf, M. Masrom, and S. M. Daud, "Security Evaluation for Graphical Password," in *Digital Information and Communication Technology and Its Applications*. vol. 166, ed: Springer Berlin Heidelberg, 2011, pp. 431-444.

[105] K. Saranga and R. H. Dugald, "Order and entropy in picture passwords," presented at the Proceedings of graphics interface 2008, Windsor, Ontario, Canada, 2008.

[106] M. Hasegawa, Y. Tanaka, and S. Kato, "A study on an image synthesis method for graphical passwords," in *Intelligent Signal Processing and Communication Systems, 2009. ISPACS 2009. International Symposium on*, 2009, pp. 643-646.

[107] M. Sreelatha, M. Shashi, M. R. Teja, M. Rajashekar, and K. Sasank, "Intrusion prevention by image based authentication techniques," in *Recent Trends in Information Technology (ICRTIT), 2011 International Conference on*, 2011, pp. 1239-1244.

[108] F. Tari, A. A. Ozok, and S. Holden, H. , "A comparison of perceived and real shoulder-surfing risks between alphanumeric and graphical passwords," presented at the Proceedings of the second symposium on Usable privacy and security, Pittsburgh, Pennsylvania, 2006.

[109] M. K. Rao and S. Yalamanchili, "Novel Shoulder Surfing Resistant Authentication Schemes using TextGraphical Passwords," *International Journal of Information and Network Security (IJINS),* vol. 1, pp. 163-170, 2012.

[110] Y. L. Chen, W. C. Ku, Y. C. Yeh, and D. M. Liao, "A simple text-based shoulder surfing resistant graphical password scheme," in *Next-Generation Electronics (ISNE), 2013 IEEE International Symposium on*, 2013, pp. 161-164.

[111] G. Hofstede, *Culture's Consequences: International differences in work related values*. Newbury Park: Sage Publications, 1980.

[112] E. B. Tylor, *Primitive culture: researches into the development of mythology, philosophy, religion, art, and custom*. London: J. Murray, 1871.

[113] R. A. Shweder and R. A. LeVine, *Culture Theory: Essays on Mind, Self and Emotion*: Cambridge University Press, 1984.

[114] G. H. Hofstede and G. Hofstede, *Culture's Consequences: Comparing Values, Behaviors, Institutions and Organizations Across Nations*: SAGE Publications, 2001.

[115] D. O'Neil. (2012, 18/06/2014). *HUMAN CULTURE:An Introduction to the Characteristics of Culture and the Methods used by Anthropologists to Study It*. Available: http://anthro.palomar.edu/culture/DEFAULT.HTM

[116] F. Monrose and M. K. Reiter, "Graphical Passwords," in *Security and Usability*, I. L. C. a. S. Garfinkel, Ed., ed: O'Reilly, 2005, pp. 147-164.

[117] S. Wallace and H.-C. Yu, "The Effect of Culture on Usability: Comparing the Perceptions and Performance of Taiwanese and North American Mp3 Player Users," *Journal of Usability Studies,* vol. 4, pp. 136-146, 2009.

[118] F. D. Davis, "User acceptance of information technology: system characteristics, user perceptions and behavioral impacts," *International Journal of Man-Machine Studies,* vol. 38, pp. 475-487, 1993.

[119] V. Venkatesh, M. G. Morris, B. D. Gordon, and F. D. Davis, "User Acceptance of Information Technology: Toward a Unified View," *MIS Quarterly,* vol. 27, pp. 425-478, 2003.

[120] D. Straub, M. Keil, and W. Brenner, "Testing the technology acceptance model across cultures: A three country study," *Information & Management,* vol. 33, pp. 1-11, 1997.

[121] A. B. Zakour, "Cultural differences and information technology acceptance," in *Proceedings of the 7th annual conference of the Southern Association for Information Systems*, Savannah, GA, USA, 2004, pp. 156-161.

[122] M. Srite and E. Karahanna, "The Role of Espoused National Cultural Values in Technology Acceptance," *MIS Quarterly,* vol. 30, pp. 679-704, 2006.

[123] S. McCoy, D. F. Galletta, and W. R. King, "Applying TAM across cultures: the need for caution," *European Journal of Information Systems,* vol. 16, pp. 81-90, 2007.

[124] G. Ford, "Researching the effects of culture on usability," M.Sc Dissertation, University of South Africa, 2005.

[125] E. Vockell. (2001, 29 June 2014). *Educational psychology: A practical approach*. Available: http://education.purduecal.edu/Vockell/EdPsyBook/

[126] R. E. Mayer and R. Moreno, "Nine Ways to Reduce Cognitive Load in Multimedia Learning," *Educational Psychologist,* vol. 38, pp. 43-52, 2003/03/01 2003.

[127] A. Paivio, *Mental Representations: A Dual Coding Approach*: Oxford University Press, 1986.

[128] R. Nisbett, Peng, K., Choi, I., and Norenzayan, A., "Culture and systems of thought: holistic versus analytic cognition. ." *Psychological Review,* vol. 108, , pp. 291-310, 2001

[129] A. Boduroglu, P. Shah, and R. E. Nisbett, "Cultural Differences in Allocation of Attention in Visual Information Processing," *J Cross Cult Psychol,* vol. 40, pp. 349-360, 2009.

[130] H. F. Chua, J. E. Boland, and R. E. Nisbett, "Cultural variation in eye movements during scene perception," *Proceedings of the National Academy of Sciences of the United States of America,* vol. 102, pp. 12629-12633, 2005.

[131] A. Gutchess, R. Welsh, A. Boduroĝlu, and D. Park, "Cultural differences in neural function associated with object processing," *Cognitive, Affective, &amp; Behavioral Neuroscience,* vol. 6, pp. 102-109, 2006.

[132] C. S. Huntsinger, J. Schoeneman, and W.-D. Ching, "A Cross-Cultural Study of Young Children's Performance on Drawing and Handwriting Tasks," Chicago1994-05-00 1994.

[133] T. Masuda and R. E. Nisbett, "Attending Holistically Versus Analytically: Comparing the Context Sensitivity of Japanese and Americans," *Journal of Personality and Social Psychology,* vol. 81, pp. 922-934, 2001.

[134] S. G. Goto, Y. Ando, C. Huang, A. Yee, and R. S. Lewis, "Cultural differences in the visual processing of meaning: Detecting incongruities between background and foreground objects using the N400," *Social Cognitive and Affective Neuroscience,* vol. 5, pp. 242-253, June 1, 2010 2010.

[135] K. A. Abbott, *Hormone and individualis*. Taipei: Orient Cultural Service, 1970.

[136] C. H. Hwang, "Studies in Chinese personality: A critical review," *Bulletin of Educational Psychology,* vol. 15, pp. 227-240, 1982.

[137] J. O. Goh, M. W. Chee, J. C. Tan, V. Venkatraman, A. Hebrank, E. D. Leshikar, L. Jenkins, B. P. Sutton, A. H. Gutchess, and D. C. Park, "Age and culture modulate object processing and objectscene binding in the ventral visual area," *Cognitive Affective Behavioral Neuroscience,* vol. 7, pp. 44-52, 2007.

[138] C. Chen, J. Kasof, A. J. Himsel, E. Greenberger, Q. Dong, and G. Xue, "Creativity in Drawings of Geometric Shapes," *Journal of Cross-Cultural Psychology,* vol. 33, pp. 171-187, March 1, 2002 2002.

[139] R. Richards, D. K. Kinney, M. Benet, and A. P. Merzel, "Assessing everyday creativity: Characteristics of the Lifetime Creativity Scales and validation with three large samples," *Journal of Personality and Social Psychology,* vol. 54, pp. 476-485, 1988.

[140] D. K. Simonton, "Creativity. Cognitive, personal, developmental, and social aspects," *Am Psychol,* vol. 55, pp. 151-8, Jan 2000.

[141] M. K. Raina, "Cross-cultural differences," in *Encyclopedia of creativity*, M. A. Runco and S. R. Pritzker, Eds., ed San Diego: Academic Press, 1999, pp. 453-464.

[142] R. J. Sternberg and T. I. Lubart, *Defying the Crowd: Cultivating Creativity in a Culture of Conformity*: Free Press, 1995.

[143] R. S. Sobel and A. Rothenberg, "Artistic creation as stimulated by superimposed versus separated visual images.," *Journal of Personality & Social Psychology,* vol. 39, pp. 953-961, 1980.

[144] D. Solar, D. Bruehl, and J. Kovacs, "The Draw-A-Person Test: Social conformity or artistic ability?," *Journal of Clinical Psychology,* vol. 26, pp. 524-525, 1970.

[145] F. Pine and R. R. Holt, "Creativity and primary process: A study of adaptive regression," *The Journal of Abnormal and Social Psychology,* vol. 61, pp. 370-379, 1960.

[146] C. S. Huntsinger, P. E. Jose, D. B. Krieg, and Z. Luo, "Cultural differences in Chinese American and European American children's drawing skills over time," *Early Childhood Research Quarterly,* vol. 26, pp. 134-145, 2011.

[147] R. English, "Modelling the security of recognition-based graphical password schemes," PhD Thesis, School of Computing Science, University of Glasgow., Glasgow, 2012.

[148] Levin, "Race as a visual feature: using visual search and perceptual discrimination tasks to understand face categories and the cross-race recognition deficit.," *J Exp Psychol Gen,* vol. 129, pp. 559-74, 2000.

[149] P. Walker and W. Tanaka, "An encoding advantage for own-race versus other-race faces.," *Perception,* vol. 23, pp. 1117-1125, 2003 2003.

[150] H. M. Aljahdali and R. Poet, "The affect of familiarity on the Usability of Recognition-based graphical Password Cross cultural Study Between Saudi Arabia and the United Kingdom," in *The 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (IEEE TrustCom-13)*, Melbourne, Australia, 2013.

[151] H. Liang and Y. L. Xue, "Understanding Security Behaviors in Personal Computer Usage: A Threat Avoidance Perspective," *Journal of the Association for Information Systems,* vol. 11, pp. 394-413, 2010.

[152] J. G. Snodgrass and M. Vanderwart, "A standardized set of 260 pictures: Norms for name agreement, image agreement, familiarity, and visual complexity," *Journal of Experimental Psychology: Human Learning and Memory,* vol. 6, pp. 174-215, 1980.

[153] Y. M. Cycowicz, D. Friedman, M. Rothstein, and J. G. Snodgrass, "Picture Naming by Young Children: Norms for Name Agreement, Familiarity, and Visual Complexity," *Journal of Experimental Child Psychology,* vol. 65, pp. 171–237, 1997 1997.

[154] F. X. Alario and L. Ferrand, "A set of 400 pictures standardized for French: Norms for name agreement, image agreement, familiarity, visual complexity, image variability, and age of acquisition," *Behavior Research Methods, Instruments, & Computers,* vol. 31, pp. 531-552, 1999.

[155] N. Janssen, P. Pajtas, and A. Caramazza, "A set of 150 pictures with morphologically complex English compound names: Norms for name agreement, familiarity, image agreement, and visual complexity," *Behavior Research Methods,* vol. 43, pp. 478-490.

[156] P. M. Greenfield, "You Can't Take It With You: Why Ability Assessments Don't Cross Cultures," *American Psychologist*, vol. 52, pp. 1115-1124, 1997.

[157] A. Gutchess, R. Welsh, A. Boduroĝlu, and D. Park, "Cultural differences in neural function associated with object processing," *Cognitive Affective Behavioral Neuroscience,* vol. 6, pp. 102-109, 2006.

[158] L. J. Jenkins, Y.-J. Yang, J. Goh, Y.-Y. Hong, and D. C. Park, "Cultural differences in the lateral occipital complex while viewing incongruent scenes," *Social Cognitive and Affective Neuroscience,* vol. 5, pp. 236-241, June 1, 2010 2010.

[159] InternetWorldStats. (21/03/2011). *Internet Usage Statistics for Africa*. Available: http://www.internetworldstats.com/stats1.htm

[160] D. V. Klein, ""Foiling the cracker": A Survey of, and Improvements to,Password Security," *In Proceedings of the 2nd USENIX Security Workshop*, pp. 5-14, 1990.

[161] S. Gaw and W. E. Felten, "Password management strategies for online accounts," presented at the Proceedings of the second symposium on Usable privacy and security, Pittsburgh, Pennsylvania, 2006.

[162] A. De Angeli, M. Coutts, L. Coventry, G. I. Johnson, D. Cameron, and M. H. Fischer, "VIP: a visual approach to user authentication," presented at the Proceedings of the Working Conference on Advanced Visual Interfaces, Trento, Italy, 2002.

[163] E. Hayashi, J. Hong, and N. Christin, "Security through a different kind of obscurity: evaluating distortion in graphical authentication schemes," presented at the Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, Vancouver, BC, Canada, 2011.

[164] R. English and R. Poet, "Measuring the revised guessability of graphical passwords," in *Network and System Security (NSS), 2011 5th International Conference on*, 2011, pp. 364-368.

[165] "PASSWORD MANAGEMENT," Hong Kong Special Administrative Region, Ed., ed: The Government of the Hong Kong Special Administrative Region, February 2008.

[166] A. Huth, M. Orlando, and L. Pesante, "Password Security, Protection, and Management," US-CERT a government organization USA, Ed., ed: Carnegie Mellon University, 2012, p. 5.

[167] L. F. Cranor and S. Garfinkel., "Secure or Usable?," *IEEE Privacy and Security*, vol. 2, pp. 16-18, 2004.

[168] K. Pezdek, R. Maki, D. Valencia-Laver, T. Whetstone, J. Stoeckert, and T. Dougherty, "Picture memory: recognizing added and deleted details.," *Journal of Experimental Psychology: Learning, Memory, and Cognition,* vol. 14, pp. 468-476, 1988.

[169] C. B. Cave, "Very Long-Lasting Priming in Picture Naming," *Psychological Science,* vol. 8, pp. 322-325, July 1, 1997 1997.

[170] F. Towhidi and M. Masrom, "A Survey on Recognition Based Graphical User Authentication Algorithms " *International Journal of Computer Science and Information Security,* vol. 6, 2009.

[171] S. Chiasson, C. Deschamps, E. Stobert, M. Hlywa, B. F. Machado, A. Forget, N. Wright, G. Chan, and R. Biddle, "The MVP Web-Based Authentication Framework," in *Financial Cryptography*, ed, 2012, pp. 16-24.

[172] Passfaces.com, "Passfaces as a Countermeasure for Phishing and Malware " 2006.

[173] A. De Luca, R. Weiss, and H. Hussmann, "PassShape: stroke based shape passwords," presented at the Proceedings of the 2007 conference of the computer-human interaction special interest group (CHISIG) of Australia on Computer-human interaction: design: activities, artifacts and environments, Adelaide, Australia, 2007.

[174] W. Fulton. (1997-2008 A few scanning tips. Available: http://www.scantips.com/basics09.html

[175] J. F. Blinn, "A scan line algorithm for displaying parametrically defined surfaces," *SIGGRAPH Comput. Graph.,* vol. 12, pp. 1-7, 1978.

[176] R. English and R. Poet, "The Effectiveness of Intersection Attack Countermeasures for Graphical Passwords," in *Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on*, 2012, pp. 1-8.

[177] N. Schmitt, R. J. Klimoski, G. R. Ferris, and K. M. Rowland, *Research methods in human resources management*. Cincinnati: South-Western Pub. Co., 1991.

[178] H. Sharp, Y. Rogers, and J. Preece, *Interaction Design: Beyond Human-computer Interaction*, 2nd edition ed.: John Wiley & Sons, 2007.

[179] V. Anderson, "Approaches to gathering data in HR research," in *Research Methods in Human Resource Management*, 2nd Edition ed: CIPD, 2009, p. 400.

[180] T. Tullis and J. Stetson, "A Comparison of Questionnaires for Assessing Website Usability," *Usability Professional Association Conference,* pp. 1-12, 2004.

[181] R. L. James, "IBM computer usability satisfaction questionnaires: psychometric evaluation and instructions for use," *Int. J. Hum.-Comput. Interact.,* vol. 7, pp. 57-78, 1995.

[182] Student, "The probable error of a mean," *Biometrika,* vol. 6, pp. 1-25, March 1, 1908 1908.

[183] J. H. McDonald, *Handbook of Biological Statistics*, Second Edition ed. Maryland, USA: Sparky House Publishing, 2009.

[184] D. C. Howell, "Chi-Square Test-Analysis of contingency table s," *Women* vol. 35, pp. 28-83, 2009.

[185] J. Pallant, *SPSS Survival Manual: A Step by Step Guide to Data Analysis Using SPSS,* 3ed ed. Sydney, Australia: McGraw-Hill Education, 2007.

[186] T. A. Myers, "Goodbye, Listwise Deletion: Presenting Hot Deck Imputation as an Easy and Effective Tool for Handling Missing Data," *Communication Methods and Measures,* vol. 5, pp. 297-310, 2011 2011.

[187] A. R. Donders, G. J. van der Heijden, T. Stijnen, and K. G. Moons, "Review: a gentle introduction to imputation of missing values," *J Clin Epidemiol,* vol. 59, pp. 1087-91, Oct 2006.

[188] B. G. Tabachnick and L. S. Fidell, *Using multivariate statistics (5th ed.)*. Boston, MA: Allyn & Bacon/Pearson Education, 2007.

[189] W. Outhwaite and S. P. Turner, *The SAGE handbook of social science methodology*. Los Angeles ; London: SAGE, 2007.

[190] Y. L. He, "Missing Data Analysis Using Multiple Imputation Getting to the Heart of the Matter," *Circulation-cardiovascular Quality and Outcomes,* vol. 3, pp. 98-U145, 2010.

[191] M. Zviran and W. J. Haga, "Password Security: An Empirical Study," *Journal of Management Information Systems* vol. 15, pp. 161-185, 1999.

[192] J. Thomason. Password Security [Online]. Available: http://www.oucs.ox.ac.uk/registration/passwords/password_security.xml.ID=body.1_div.2

[193] S. Chowdhury and R. Poet, "Comparing the usability of doodle and Mikon images to be used as authenticators in graphical authentication systems," presented at the International Conference on User Science and Engineering (i-USEr), Kuala Lumpur, Malaysia, 2011.

[194] D. Paul, N. James, and O. Patrick, "Securing passfaces for description," presented at the Proceedings of the 4th symposium on Usable privacy and security, Pittsburgh, Pennsylvania, 2008.

[195] M. E. Katherine, B. Tanya, F. James, and K. Tadayoshi, "A comprehensive study of frequency, interference, and training of multiple graphical passwords," presented at the Proceedings of the 27th international conference on Human factors in computing systems, Boston, MA, USA, 2009.

[196] S. Chowdhury, R. Poet, and L. Mackenzie, "A comprehensive study of the usability of multiple graphical password," in *Interact 2013*, South Africa, 2013.

[197] M. A. S. Al-Fairuz, *An Investigation Into the Usability and Acceptability of Multi-channel Authentication to Online Banking Users in Oman*: University of Glasgow.

[198] X. SUO, "A DESIGN AND ANALYSIS OF GRAPHICAL PASSWORD," Master of Science, College of Arts and Sciences, Georgia State University, USA, 2006.

[199] W. Susan, W. Jim, S. Leonardo, and B. Jean-Camille, "Design and evaluation of a shoulder-surfing resistant graphical password scheme," presented at the Proceedings of the working conference on Advanced visual interfaces, Venezia, Italy, 2006.

[200] J. C. Birget, H. Dawei, and N. Memon, "Graphical passwords based on robust discretization," *Information Forensics and Security, IEEE Transactions on,* vol. 1, pp. 395-399, 2006.

Appendix A

Cross Culture Experiment Instructions and Questionnaire

Cross Culture Experiment

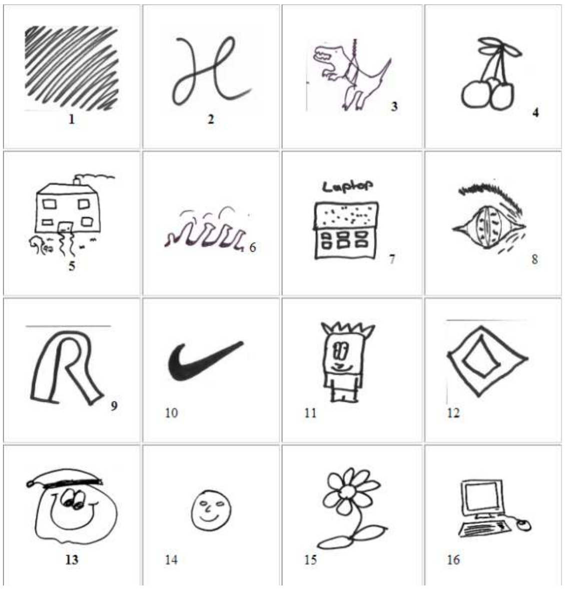
What is the idea behind this experiment?

Password security often fails in practice because users select predictable passwords .secure passwords are hard to remember. As an alternative, many studies have found that graphical passwords are more usable than ordinary passwords. In this experiment we will use a handwriting technique called doodling, and we will use these doodles as the password.

The aim: In this experiment we will study how culture might affect our use of drawn doodles as passwords.

What is a doodle?

As well definite on Wikipedia at http://en.wikipedia.org/wiki/Doodle **"**A **doodle** is a type of sketch, an unfocused drawing made while a person's attention is otherwise occupied. Doodles are simple drawings that can have concrete representational meaning or may just be abstract shapes." Here are some examples:



Gender: Male □ Female □

Age: (10-20) □ (21-30) □ (31-40) □ (41-50) □ (51-60) □ (>60) □

How would you classify yourself?

African	Arab	Asian	Australian	European	Hispanic	other

Nationality ……………………………………………………..

Level of education:

Primary school □ High school □ Undergraduate □ Postgraduate □ Un-educated □

Number of different computer accounts such as Internet banking

(0) □ (1-5) □ (6-10) □ (11-20) □ (>20) □

Number of different passwords

(0) □ (1-3) □ (4-8) □ (9-15) □ (>15) □

How often do you use the computer? …………….per day

How often do you use the the internet? …………….per day

How often do you have to use a password? …………….per day

Do you like a drawing: Yes □ No □

If **No** can you provide the reason:

………

………

Have you constructed drawing using a computer: Yes □ No □

Would you be happy to provide doodles as passwords?

Yes □ No □ don’t know □

Please draw four doodles in the boxes below Assuming that these doodles will representing your passwords:

Doodle 1	Doodle 2
Doodle 3	Doodle 4

How long did that take you?

………

How much did you enjoy making the drawings?

1 (Not at all)	2	3	4	5	6	7	8	9	10 (a lot)

Do you think a friend could guess your doodle when shown a collection of doodles?

1 (Never)	2	3	4	5	6	7	8	9	10 (very likely)

Thank you *very much for your cooperation and your participation.*

"Some people make the world SPECIAL just by being in it"

Appendix B

Guessability of Hand-Drawn Images Based on Cultural Characteristics

Experimental website

The web site contained a total of seven screens, which were as follows:

- **Homepage:** this was the first screen, displaying information about the experiment and the start button.
- **Registration page**: the second screen asked participants to fill in the required information.
- **3,4,5,6 Screens**: these were screens for the main purpose of this experiment; more detail is given in the next section.
- **Completed page**: this is the last page which is displayed after the participant completed all tasks.

Main task screens

Four screens were displayed in sequence to every participant, each screen contained five elements. The main element which was contained were 16 hand drawn images ready to be dragged and dropped into one of the four small boxes, each box representing one category. All images were coded and some of them represented cultural aspects; more details about the images will be discussed in the next section. Moreover, each image put by the participants into the selected categories was stored as an array in the database. The last element was the **Next** button which transferred the user to the next page.

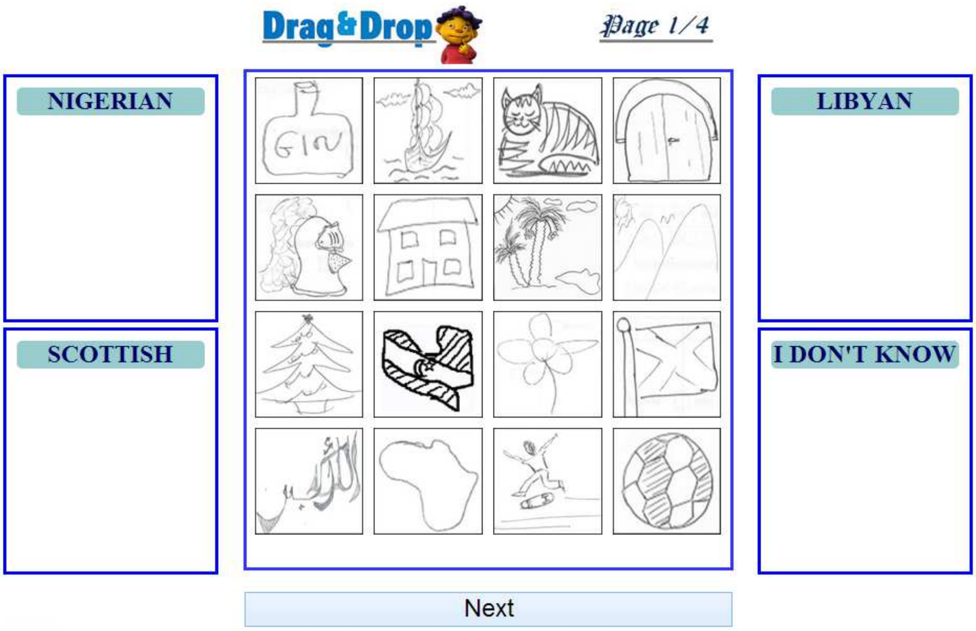


Figure 1 One of the displayed screens used in the experiment (Drag& Drop)

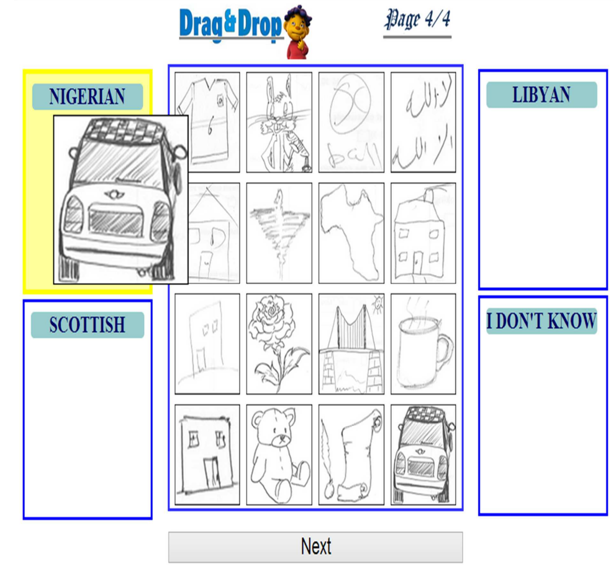
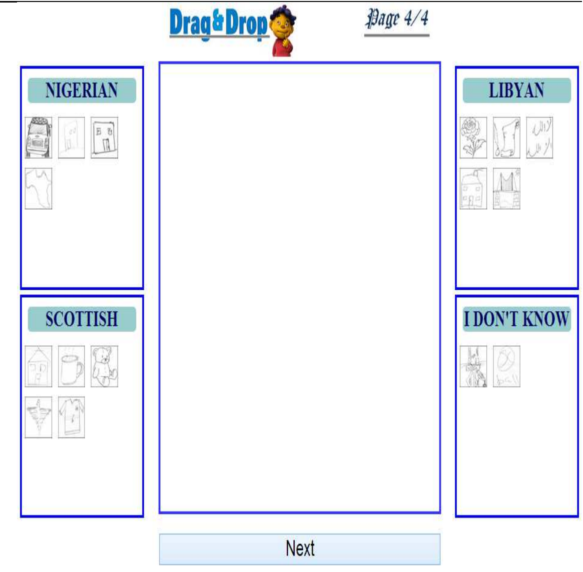
	
Screen During Dragging & Dropping selected images	Screen after finishing all Dragging & Dropping of images

Figure 2 Screen during and after completion of the task

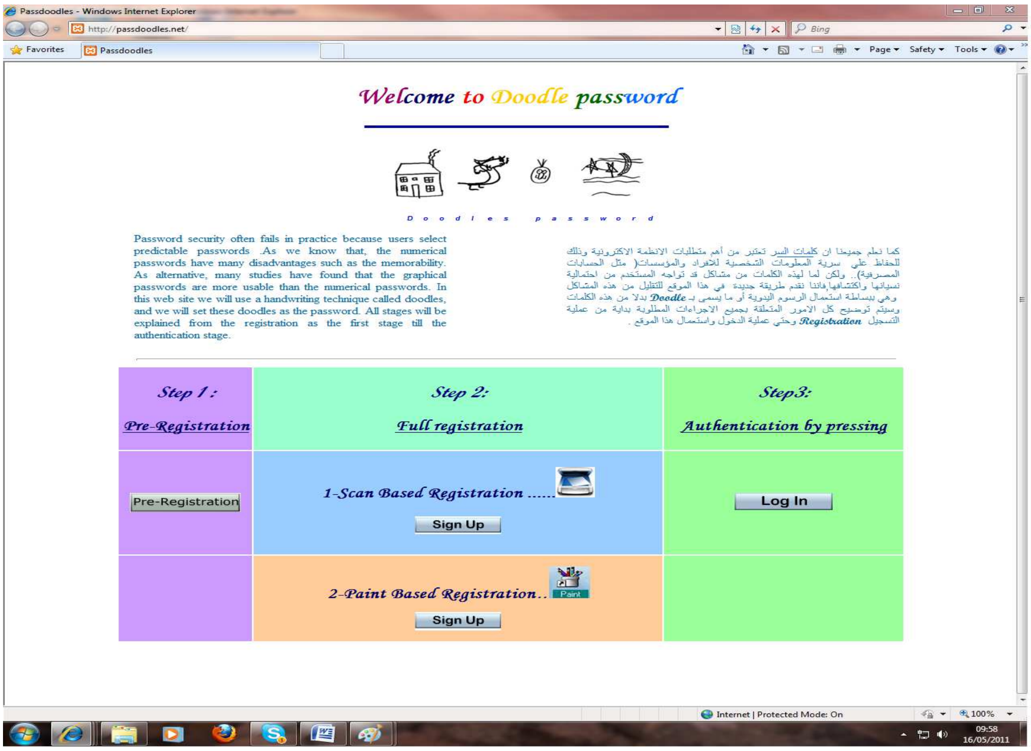
Appendix C

Automatic Registration of User Drawn Graphical Passwords

The Website

1. Website Pages

A user of the online doodles system passes through several stages starting with a pre-registration stage and ending with the authentication stage (the main homepage shown in Figure 1). Figure 2 and Figure 3; illustrate all the registration processes on both sides of this system, the client and server side. The pre-registration and full registration steps can be done together in a single session or split into two sessions. This lets the user take time to create their images between the two sessions.



Welcome to Doodle password

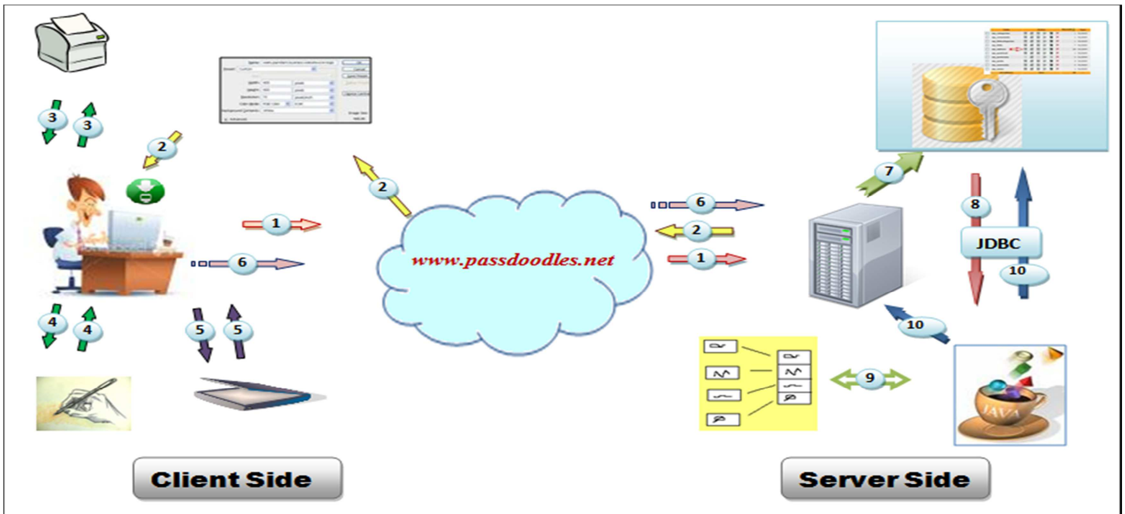
Doodles password

Password security often fails in practice because users select predictable passwords .As we know that, the numerical passwords have many disadvantages such as the memorability. As alternative, many studies have found that the graphical passwords are more usable than the numerical passwords. In this web site we will use a handwriting technique called doodles, and we will set these doodles as the password. All stages will be explained from the registration as the first stage till the authentication stage.

كما نعلم جميعنا ان كلمات السر تعتبر من أهم متطلبات الانظمة الاكترونية وذلك للحفاظ علي سرية المعلومات الشخصية للافراد والمؤسسات(مثل الحسابات المصرفية).. ولكن لما لهذه الكلمات من مشاكل قد تواجه المستخدم من احتمالية نسيانها واكتشافها,فاننا نقدم طريقة جديدة في هذا الموقع للتقليل من هذه المشاكل وهي ببساطة استعمال الرسوم اليدوية أو ما يسمى بـ Doodle بدلا من هذه الكلمات وسيتم توضيح كل الامور المتعلقة بجميع الاجراءات المطلوبة بداية من عملية التسجيل Registration وحتى عملية الدخول واستعمال هذا الموقع .

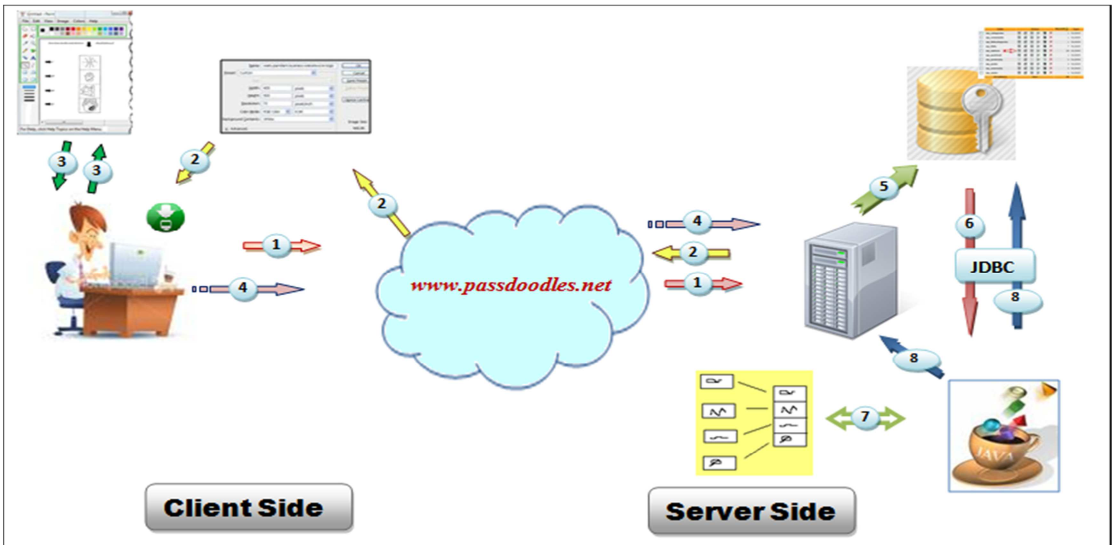
Step 1 : Pre-Registration	Step 2: Full registration	Step3: Authentication by pressing
Pre-Registration	1-Scan Based Registration ...... Sign Up	Log In
	2-Paint Based Registration.. Paint Sign Up	

Figure 1 Passdoodles website



1. Connect to http://www.passdoodles.net
2. Pre-Registration page and filling the required information and send them to the server for saving (need for full registration).
3. Complete the full registration by downloading the Form and printing out drawing Form.
4. Draw 4 passdoodles.
5. Scan the Form and upload the Form &complete entering data.
6. Sending the information.
7. Store collection data in MySQL database.
8. Sending information of user's passdoodles location.
9. JAVA code for extract the original Form into four passdoodles.
10. Store location of passdoodles and save passdoodles in the server.

Figure 2 Registration processes by scan based registration



1. Connect to http://www.passdoodles.net
2. Pre-Registration page and filling the required information and send them to the server for saving (need for full registration).
3. Complete the full registration using Paint based registration and:
   - Downloads the Form
   - Open it with paint software and
   - Draw 4 passdoodles.
4. Sending the information.
5. Store collection data in MySQL database.
6. Sending information of user's passdoodles location.
7. JAVA code for extract the original Form into four passdoodles.
8. Store location of passdoodles and save passdoodles in the server.

Figure 3 Registration processes by Paintbased registration

Finally, Figure 4 illustrates all the authentication processes on both sides of this system, i.e. the client side and the server side.

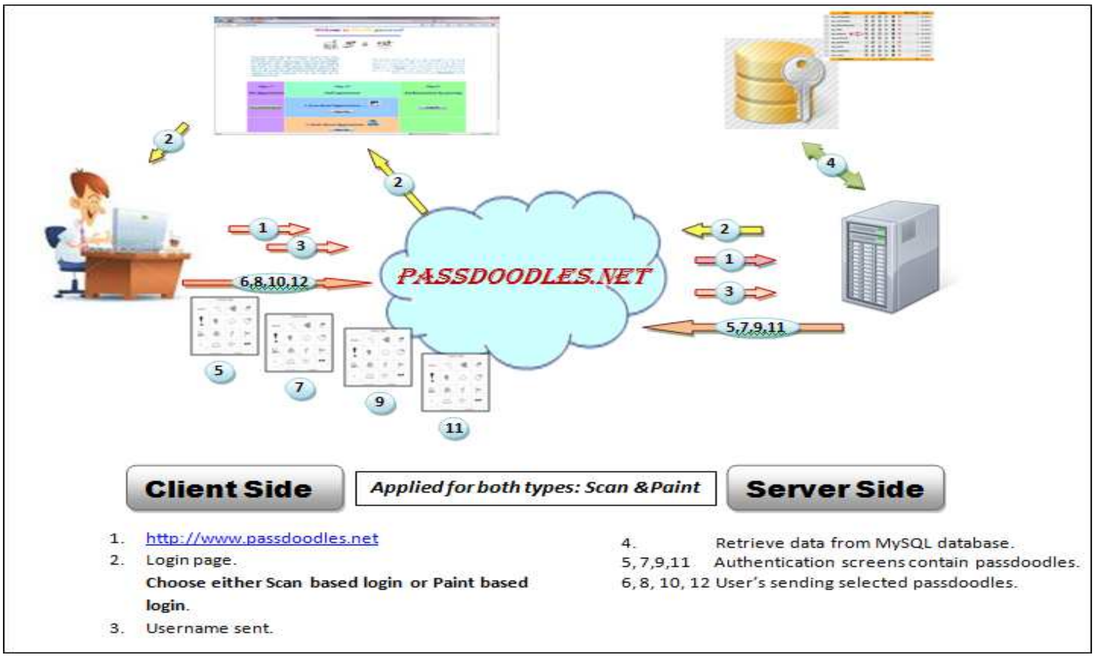

2
2
4
1
3
6,8,10,12
PASSDOODLES.NET
2
1
3
5,7,9,11
5
7
9
11
Client Side
Applied for both types: Scan & Paint
Server Side
1. http://www.passdoodles.net
2. Login page.
Choose either Scan based login or Paint based login.
3. Username sent.
4. Retrieve data from MySQL database.
5, 7,9,11 Authentication screens contain passdoodles.
6, 8, 10, 12 User's sending selected passdoodles.

Figure 4 the authentication stage

2 User Views of the Website

2.1 Pre - registration

All users are required to login to passdoodles.net and then to sign up for pre-registration. The pre-registration page will ask the user to provide some personal information. The information requested is: their first name, last name, gender, age, nationality, occupation, experience in computing security, any vision problems the user may have, and their email address. Also, the user has to select a unique username which will be used to complete his/her full registration stages in both systems and also for the login stage. The server will send the collected information to the database and save it to the user's profile.

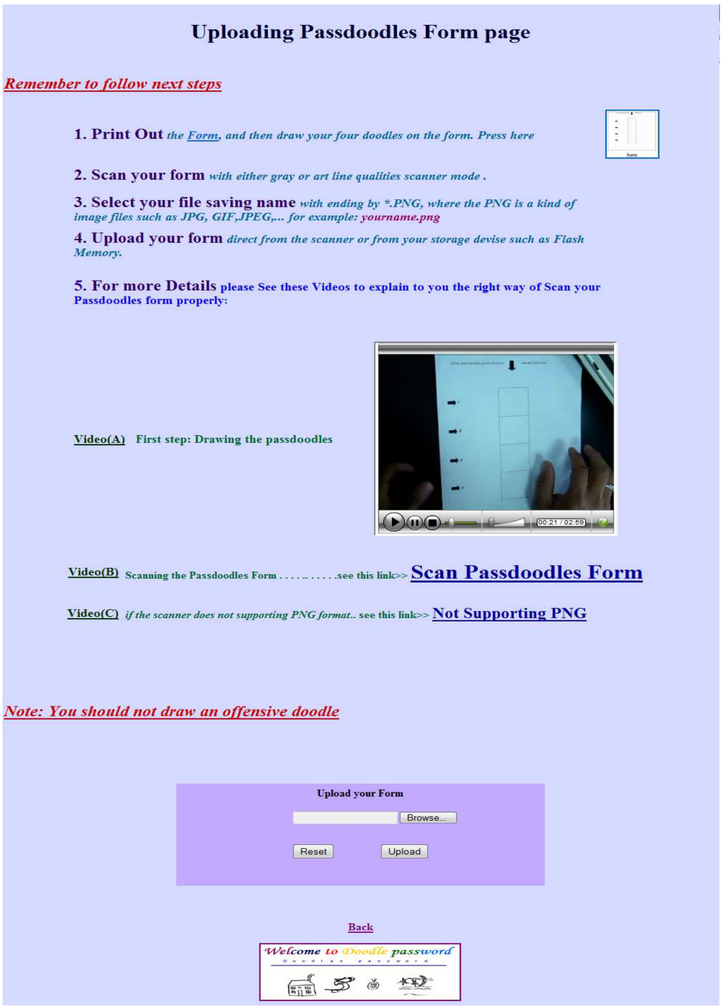
2.2 Scan based registration

In the scan based registration, the user has to download and print out the form on which to draw his four image password from the website and then scan it with two conditions: in PNG format and either gray or art line scanning quality. The webpage provides full details of how to do this correctly and explains the instructions as shown in Figure 6. The Passdoodles website is provided with several videos demonstrating every step in registering the drawing images and explaining how to use the website correctly. These videos are in both English and Arabic and their focuses are as follows:

Video A: explains the correct way of drawing passdoodles including the correct pen colour, type and size, and the right A4 paper colour.

Video B: explains how to scan the drawing form properly by using the correct scanned format and scanning quality.

Video C: shows how to convert the image format if the scanner does not support the PNG format.



Uploading Passdoodles Form page

Remember to follow next steps

1. **Print Out** *the Form, and then draw your four doodles on the form. Press here*
2. **Scan your form** *with either gray or art line qualities scanner mode .*
3. **Select your file saving name** *with ending by *.PNG, where the PNG is a kind of image files such as JPG, GIF,JPEG,... for example: yourname.png*
4. **Upload your form** *direct from the scanner or from your storage devise such as Flash Memory.*
5. **For more Details** please See these Videos to explain to you the right way of Scan your Passdoodles form properly:

Video(A) First step: Drawing the passdoodles

Video(B) Scanning the Passdoodles Form . . . . .see this link>> Scan Passdoodles Form

Video(C) *if the scanner does not supporting PNG format..* see this link>> Not Supporting PNG

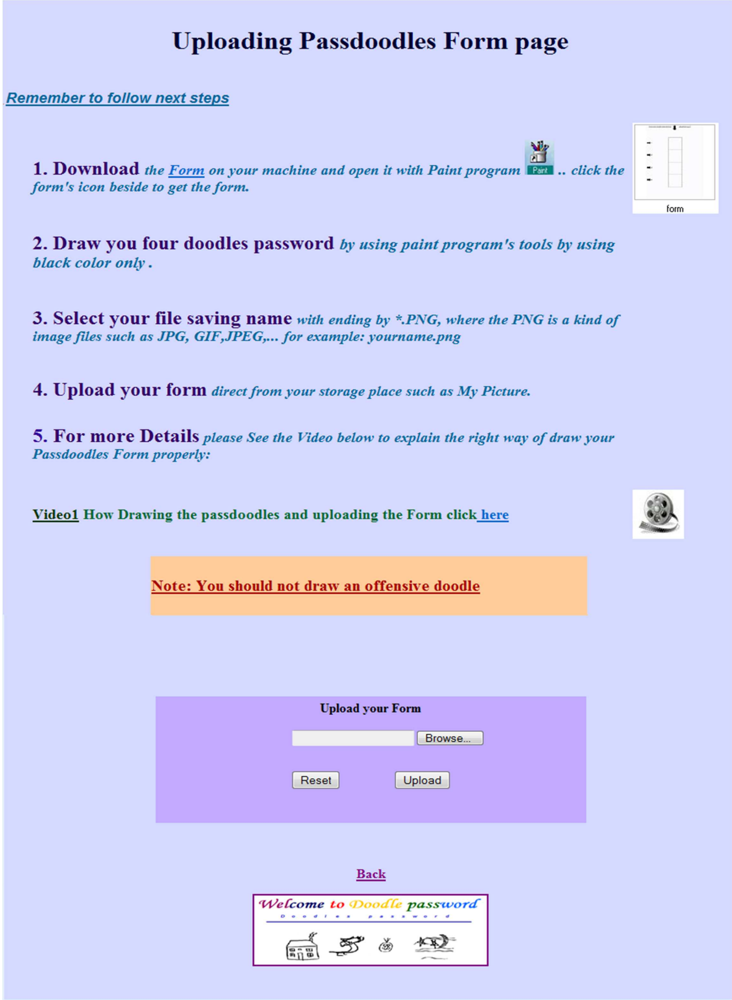
Note: You should not draw an offensive doodle

Upload your Form

Figure 6 Scan based registration

2.3 Paint based registration

In the Paint based registration process, the users have to download the form onto their computer and open the form with a Paint program, then draw their images using the tools and then submit the form. Similar to the scan based registration process, the Paint based registration web page provided a single video explaining how to register correctly, as shown in Figure 7.



Uploading Passdoodles Form page

Remember to follow next steps

1. **Download** *the Form on your machine and open it with Paint program .. click the form's icon beside to get the form.*

2. **Draw you four doodles password** *by using paint program's tools by using black color only .*

3. **Select your file saving name** *with ending by *.PNG, where the PNG is a kind of image files such as JPG, GIF,JPEG,... for example: yourname.png*

4. **Upload your form** *direct from your storage place such as My Picture.*

5. **For more Details** *please See the Video below to explain the right way of draw your Passdoodles Form properly:*

Video1 How Drawing the passdoodles and uploading the Form click here

Note: You should not draw an offensive doodle

Upload your Form

Figure 7 Paint based registration

Once the registration stage was completed, each user received an account activation email for both types (scan and Paint) within 24 hours. That email asked the user to use the system and login (this point will be discussed in more detail in the next section).

2.4 Finishing the registration

To complete the scan based registration, the user required two pieces of equipment, a printer and a scanner, while to complete the Paint based registration the user only had to have access to the Paint software, which is available and free to all computers users. After the users completed their forms either by scanning or painting, they could use the text box to enter the location of the user's drawing form and press the submit button to send the form to the server to be saved in the database. Each page had the same submitting button which could be used to send the form.

Once they have finished, they were asked to press the 'create account' button. If all the required data was complete, a congratulations message appeared and an automated email was sent to the users letting them know of the next step (they could use the system after 24 hours for the authentication stage); otherwise, a warning message was displayed for missing or invalid data.

During the next 24 hours, the user's entered drawing form was checked. If any problems were apparent with the forms or if there were any offensive doodles, a warning message was issued and sent to the user asking them to resubmit the forms. Java code was responsible for extracting the images form into four PNG files as explained in section 5.2. The files were then used at the authentication stage. This is repeated for both the scan and Paint based registrations.

3. Website Implementation

A collection of scripting languages and website component tools were used, and before detailing the implementation of the website, some of the features of these tools will now be briefly described in the paragraphs which follow.

The Passdoodle system was built using XAMPP. It is *"a free and open source cross-platform web server package, consisting mainly of the Apache HTTP Server, MySQL database, and interpreters for scripts written in the PHP and Perl programming languages"*[4].

The main scripting language used to build the website was PHP. *"PHP is a server-side scripting language designed for Web development but can also be used as a general-purpose programming language"*[5].

MySQL database is one of the most popular database management systems used with web servers. MySQL database is also extremely powerful and exceptionally fast (as cited in Nixon, 2012, p. 161)[6]. Moreover, it is free under the open source GPL license and very easy to use for all programmers and web developers. MySQL can be run on many operating systems, such as Windows, Linux, Mac OS and others and this make it flexible. Additionally, large bases of users provide free support through mailing lists. Finally, it is

[4] *C. Wiedmann, "Apache Friends, Imprint," 2009.*

[5] *D. S. a. A. Trachtenberg, "What is PHP?," 2003.*

[6] *R. Nixon, Learning PHP, MySQL, JavaScript, and CSS: A Step-by-Step Guide to Creating Dynamic Websites, 2 ed.: O'Reilly Media, Incorporated, 2012.*

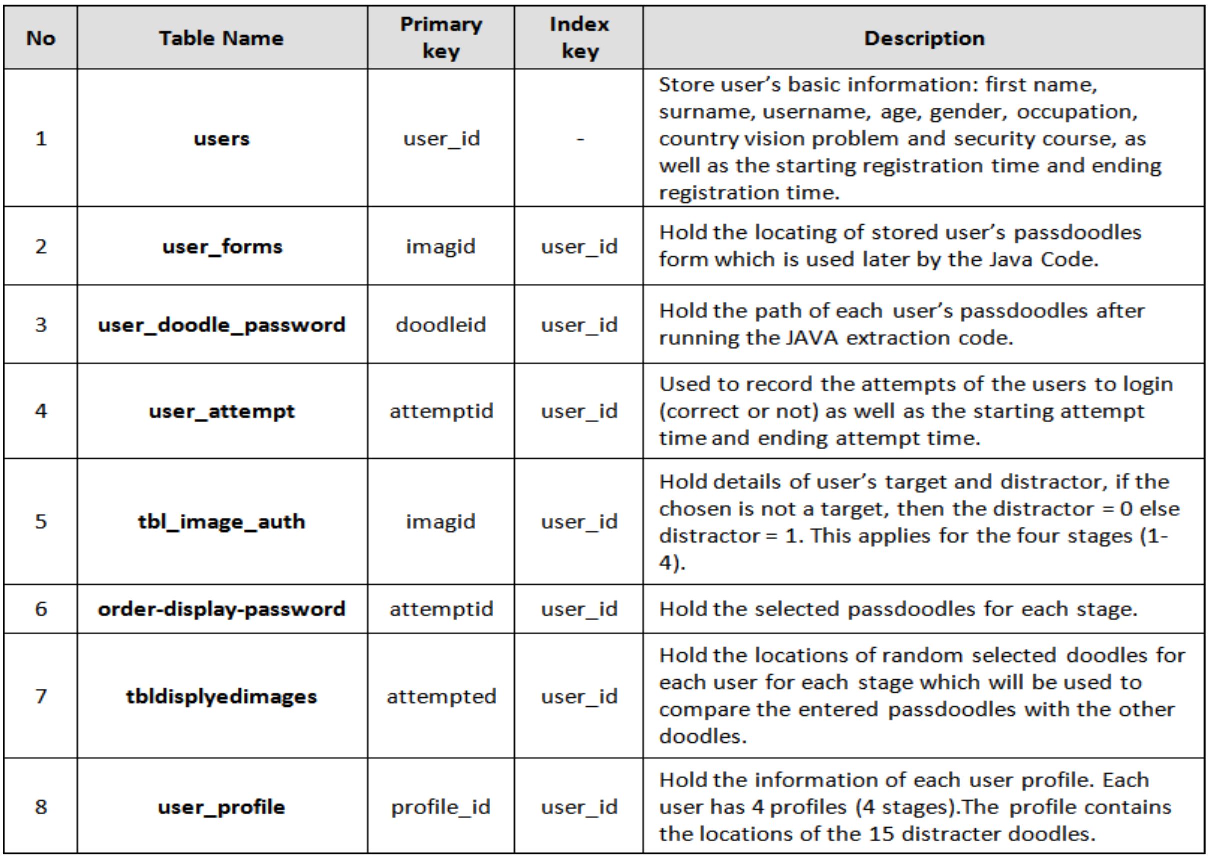
secure, with MySQL's flexible system of authorization which allows some or all database privileges (such as the privilege to create a database or table or delete data) to be given to specific users or groups of users and passwords within it are encrypted.

Another component used in the implementation of the passdoodle website was JavaScript. *"JavaScript is an interpreted programming language with object-oriented capabilities"*[7]. While PHP runs on the server and has the main function of producing HTML code for the browser to read, JavaScript runs on the browser and executes specific local tasks.

3.1 The Passdoodles system database tables

The passdoodles system uses eight tables, which are listed and described in Table 1.

Table 1 Doodles System Database tables



No	Table Name	Primary key	Index key	Description
1	**users**	user_id	-	Store user's basic information: first name, surname, username, age, gender, occupation, country vision problem and security course, as well as the starting registration time and ending registration time.
2	**user_forms**	imagid	user_id	Hold the locating of stored user's passdoodles form which is used later by the Java Code.
3	**user_doodle_password**	doodleid	user_id	Hold the path of each user's passdoodles after running the JAVA extraction code.
4	**user_attempt**	attemptid	user_id	Used to record the attempts of the users to login (correct or not) as well as the starting attempt time and ending attempt time.
5	**tbl_image_auth**	imagid	user_id	Hold details of user's target and distractor, if the chosen is not a target, then the distractor = 0 else distractor = 1. This applies for the four stages (1-4).
6	**order-display-password**	attemptid	user_id	Hold the selected passdoodles for each stage.
7	**tbldisplyedimages**	attempted	user_id	Hold the locations of random selected doodles for each user for each stage which will be used to compare the entered passdoodles with the other doodles.
8	**user_profile**	profile_id	user_id	Hold the information of each user profile. Each user has 4 profiles (4 stages).The profile contains the locations of the 15 distracter doodles.

3.2 Table relationships

Most relationships between passdoodles database tables are on a one to many bases, as shown in Figure 8. The relationships are:

[7] *D. Flanagan, JavaScript: The Definitive Guide, 6th ed. USA: O'Reilly Media, Inc, 2011.*

Table 2 The relationships between passdoodles tables

Table1 → Table 2	Type of Relation	Description
user →user_forms	**1-1**	Each user has one submitted form and that form only belongs to that user only.
user →user_profile	**1-N**	Each user has four profiles and these profiles are related to the specific user.
user →user_attempt	**1-N**	Each user can have many attempts.
user →tbldisplyedimages	**1-N**	Each user has four stages, each stage containing the selected images during the experiments.
user →tbl_image_auth	**1-N**	Each user has four stages, each stage containing a selected image.
user → order-display-password	**1-N**	Each user has four records and each record has an order of 16 images.
user →user_doodle_password	**1-N**	Each user has four pass images.

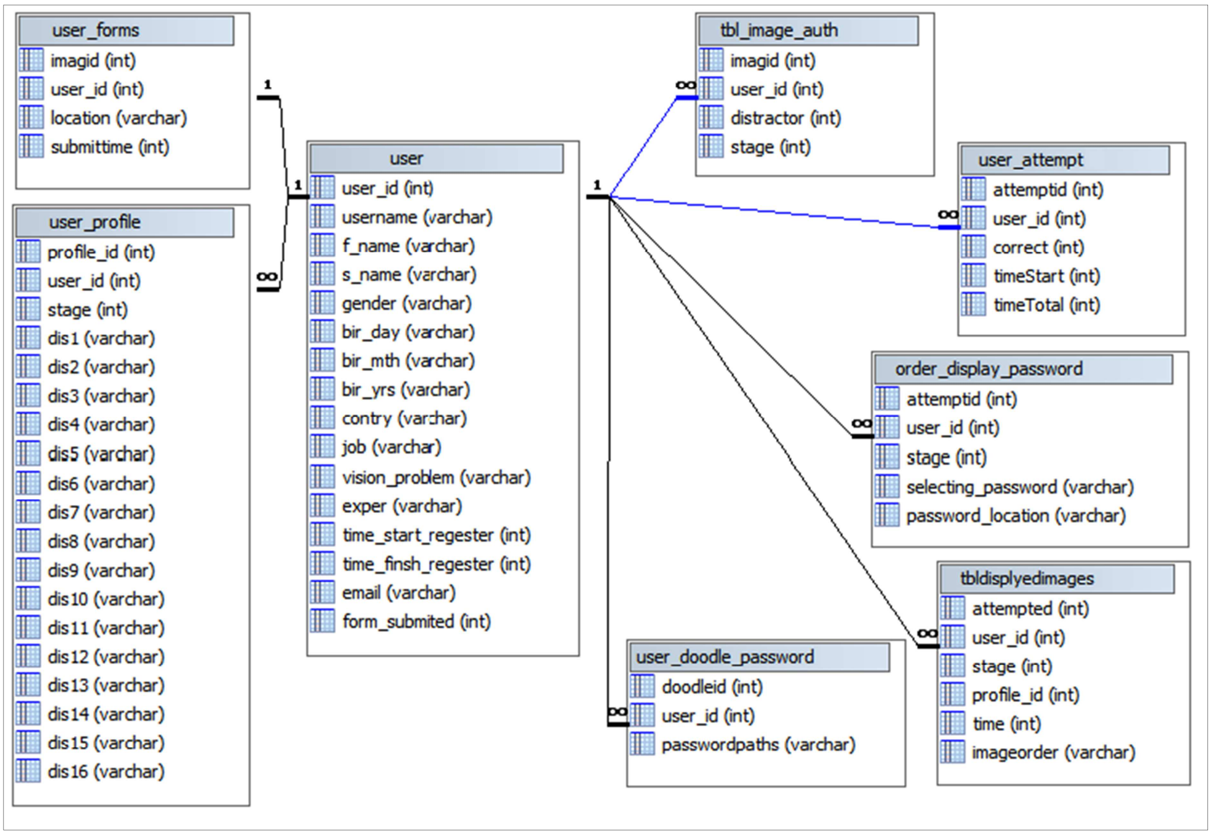


Figure 8 The relationship between the database system tables

4. Passdoodles system PHP components

More than twenty-five PHP code files have been used in the doodles system. In addition, ten screens were designed for the doodles system, starting with the home page. The most important php program scan is described as follows:

passdoodles.php: This program displays the main screen of the passdoodles system (Home page) which contains three steps: pre-registration, full registration (scan based registration and Paint based registration).

register.php: This program displays the registration screen of the doodles system (**registrationpage**) which contains two buttons (**create my account and cancel**). In this screen, the users have to enter their personal data such as their first name, surname and valid username or user ID. By pressing the 'create my account' button, the next php file (**addinfo.php**) is loaded and then a pre-account record is created for the user.

addinfo.php: This program is responsible for two things, firstly to verify the integrity of the data transmitted from the previous step, and secondly to establish contact with the doodle database. If all information has been entered successfully, a congratulations page will be displayed and then the entered data will be added to the database table (user table).

submitionFormPage.php: This program presents the screen for completing the full registration for both types. Effectively, (**submitionFormPageScan.php**) presents the drawing form page that allows users to upload their scanned passdoodles form while (**submitionFormPagePaint.php**) presents the drawing form page that allows users to upload their painted passdoodles form. In practical terms, to use both pages (submission scan form page and submission Paint form page) the user has to be verifying by entering their username where selected in the first stage and their email address. However, the next code (**checked.php**) checks whether the user has been pre-registered or not. Moreover, users need to print out the passdoodles form (for the scan type) or download it (for the Paint type) by pressing the **Form** link coloured in blue in the instruction messages, and then to insert the location of their saved passdoodles forms in the doodles system. These pages contain two buttons **(Reset and Upload).** By pressing the upload button, the next file (**checked.php**) will be run.

checked.php: This program is one of the most important in the doodles system. It checks whether or not they entered user ID and email address exist on the system by establishing a connection to the doodle database and comparing it with the usernames from the table of users. If the username exists then it will recall three php programs which are: **inser_into_user_attempt.php**, **Pathes_file.php** and **password.php**. The first two programs add and retrieve data to the database, and the third code is used to display the authentication screens, as will be explained in more detail below.

login.php: This program presents the login screen which asks users to choose one of the two types of login, i.e. either scan or Paint. Once the user makes a selection, the following screen is displayed and asks the user to input their user ID. This page contains two buttons (**Reset and Next**). By pressing the **Next** button, the next files (**rcordandcheking.php**) will be run.

recordandcheking.php: The **recordandcheking** program and **stages** programs which are explained below are repeated four times. The **recordandcheking** program checks the correctness of the user's passdoodles. If all of the passdoodles entered match the original passdoodles then the user is authenticated and the success screen will be displayed, otherwise the failure screen is displayed. Additionally, all information including either correctly or wrongly entered images and the time taken will be added to database.

Stage1.php, Stage2.php, Stage3.php, and Stage4.php: These programs display screens containing 16 doodles; one of these is the user's passdoodles (target) and the others are distracters. Each program is responsible for displaying the screen that represents one of the passdoodles stages. These screens are displayed four times, each time the user enters the character (1 -9, a-g) of his passdoodles by inserting it into the textbox. By pressing on the character that represents the passdoodles, the previous php file (**recordandcheking.php**) is run again and this is repeated four times.

Appendix D

Experimental Instructions and Questionnaire of the Automatic Registration of User Drawn Graphical Passwords

Instructions for Performing Doodles Experiment

What is the idea behind this experiment?

Password security often fails in practice because users select predictable passwords. Secure passwords are hard to remember. As an alternative, many studies have found that graphical passwords are more usable than ordinary passwords. In this experiment we will use a handwriting technique called doodling, and we will use these doodles as the password.

The aim: In this experiment we will study how culture might affect our use of drawn doodles as passwords.

What is a doodle?

"A doodle is a type of sketch, an unfocused drawing made while a person's attention is otherwise occupied. Doodles are simple drawings that can have concrete representational meaning or may just be abstract shapes." (Source: http://en.wikipedia.org/wiki/Doodle)

Instructions for performing Doodles experiment:

1. The URL of doodles's website is www.passdoodles.com
2. There are three options: **Pre-Registration, Full Registration** and **login**.
3. **Pre-Registration:** this is the first step which is required for the all users.
4. The first step allows you to create a semi account and now you have to complete your full registration which divided into two types: **Scan Based Registration** and **Paint Based Registration.**

Firstly

5. By pressing **Scan Based Registration's sign in** button, a screen will appear which ask you to enter the email address and chosen (user Id).
6. A submit form page by scan will be displayed and you must follow the instructions displayed on the screen carefully. The website provides a simple video that explaining every single point of the registration including the correct way of drawing the doodles on the form and how to scan and submit them.

<u>Secondly</u>

7. By pressing **Paint Based Registration's sign in** button, a screen will appear which ask you to enter the email address and chosen (<u>user Id</u>) as previously done in step 5.
8. A <u>submit form page by paint</u> will be displayed and you must follow the instructions displayed on the screen carefully. Again, the website provides a simple video explaining every single point of the correct way of drawing the doodles on the form by using Microsoft Paint program and how to submit them.

9. During three working days, you will receive a conformation email of completion registration and once you receive that email you will ask to login the website with your doodles passwords for each types **Scan** and **Paint**.

   - **Login process:** To logging in into passdoodles.com you need your <u>user Id</u> and then select one of the 16 doodles displayed on the screen. This login process will be repeated four times. Each time one of the user drawing doodles will be presented together with 15 distracters doodles. If you select your doodles correctly for the all stages then a congratulations message will appear with the imaging gift.

10. You must remember your drawing doodles and note of any difficulties that may be encountered during the experiment.
11. You will be asked by email to log in the website three times for both types Scan and Paint:
    1. After you have finished the full registration.
    2. After two weeks.
    3. After one month.
12. At the end, a questionnaire will be distributed to the participants.

Good Luck!

Evolution of using Doodles website

Part 1:

1- **User Id:**

…………………………………………………………………………………………
……………………..

2- Level of education:

Primary school □ High school □ Undergraduate□ Postgraduate□

Un-educated □

Part 2:

3- Do you create an account with passdoodles.com Yes □ No □

*If (**No**) Can you tell us the reasons of not creating the account (including the difficulties you have faced)

……
……
……
……
……
……
……
………………………………………………………………………………

4-Please answer all Usability questions about the website in the next table:

		strongly disagree(**1**)................ strongly agree(**7**)							
		1	2	3	4	5	6	7	N/A
1	I think that I would like to use this website frequently								
2	I found the website unnecessarily complex								
3	I thought the website was easy to use								

4	I think that I would need the support of a technical person to be able to use this website.								
5	I found the various functions in this website were well integrated								
6	I thought there was too much inconsistency in this website								
7	I would imagine that most people would learn to use this website very quickly								
8	I found the website very cumbersome to use								
9	I felt very confident using the website								
10	I needed to learn a lot of things before I could get going with this website								

5- Do you logged in to passdoodles.com Yes □ No □

*If (**No**) Can you tell us the difficulties which prevented you from logging in:

....

....

....

....

....

....

....

....

Part 3: Registration Based Scan

6- Do you complete full registration with scan type: Yes □ No □

If no, Can you tell us the reasons :

....

....

....

....

....

....

....

....

7- How long did you spend to finsh your drawing , scan and submit the form(Estemated Time in minutes)

....

8- Can you tell us what did you do with the Form after you scanned:

Keep it □ through it □ secure disposal (Ex: burned, rip,..) □

Part 4: Registration Based Paint

9- Do you complete full registration with paint type: Yes □ No □

If no, Can you tell us the reasons :

....
....
....
....
....
....
....
....
....

10- How long did you spend to finsh your drawing and submit the form (Estemated Time in minutes)

....

11- Can you tell us what did you do with the Form after you submitted:

Saved it on the computer □ delete it □ Saved it with secure method (Ex: encrypt the file, saved with password,..) □

Part 5: Summary

12- Can you tell us which type do you liked more:

Scan type □ Paint type □

Scan type (please tick)

1 (Not at all)	2	3	4	5 (a lot)

Paint type (please tick)

1 (Not at all)	2	3	4	5 (a lot)

Could you please provide us with your opining about:

13- Advantages and disadvantages of using Scan type :

………
………
………
………
………
…………………………

14- Advantages and disadvantages of using Paint type :

………
………
………
………
………
…………………………

15- Can you tell us have you used one of the Forms to help your memorability to login:

Yes □ No □

Which type: Scan type □ Paint type □ Both □

16- Could you please provide us with any extra suggestions or further notes that can help us to develop the website:

………
………
………
………
………
………
……………………………….

Thank you *very much for your cooperation and your participation.*

"Some people make the world SPECIAL just by being in it"

Appendix E

Preventing Shoulder-Surfing Instructions and Questionnaire

Instructions

Thank you for agreeing to participate in today’s experiment. You are about to participate in an experiment to test the use of doodles as passwords. Today’s experiment will consist of four stages. Each stage represents different ways of choosing the pass doodle. This experiment will be performed by a team. Each team contains one user and one observer. Please take your time to read the instructions below to understand both roles.

<u>User participant:</u>

1. The user will be given 4 doodle passwords before starting the experiment, one doodle for each stage.
2. Register your username to start the experiment.
3. 16 doodles will be displayed on the screen for each stage and one of these doodles is the password.
4. For the first three stages, you have to enter the number or the letter that matches the given password for each stage. **<u>You do not use the mouse for these three stages</u>**.

   (Once you finish typing the number or the letter press the **Enter** key ↵)
5. In the final stage, <u>you need to use the mouse</u> to select (click) the password of this stage.
6. After you have finished this experiment there is a small questionnaire to answer.

<u>Observer participant:</u>

1. The user will be given 4 doodle passwords before starting the experiment, one doodle for each stage.
2. 16 doodles will be displayed on the screen for each stage and one of these doodles represents the given password of the user.
3. The observer will be given a form what you think the password is for all experimental stages.
4. You need to try and observe the password that the user entered for all stages.
5. Your observations can be recorded by either drawing the expect password or writing the number or the letter of the expect password down on the form given.

Doodles Questionnaire

Team

User…………………………………….. Observer…………………………

		strongly disagree	1	2	3	4	5	6	7	strongly agree	N/A
1	Overall, I am satisfied with how easy it is to use this system										
2	It was simple to use this system										
3	I feel comfortable using this system										
4	It was easy to learn to use this system										
5	The information provided for the system is easy to understand										
6	The organization of information on the system screens is clear										
7	The interface of this system is pleasant										
8	I like using the interface of this system										
9	Overall, I am satisfied with this system										

10	*I feel more comfortable using stage(type) number:	①	②	③	④
11	*I do not like to use stage (type) number:	①	②	③	④
12	I feel stage (type) number : is more secure	①	②	③	④

*10 why I feel this type is more comfortable:

----

*11 why I do not like this type:

____

List the most **negative** aspect(s):

List the most **positive** aspect(s):

____

Thank you for your time! Please return completed questionnaires

Observer form

*Draw the expect password or write down the number or the letter of it for each stage.

Stage 1	Stage 2
Stage 3	**Stage 4**