الأكاديمية الليبية
The Libyan Academy

The Libyan Academy – Misrata Branch

School of Engineering and Applied Sciences

Department of Information Technology

Improving Web Authentication Using User Drawing Passwords

A Thesis Submitted in Partial Fulfillment of the Requirements

For The Master Degree in Information Technology

By

Abdulmottaleb Mohammed Elabour

(31357016)

The Libyan Academy – Misrata Branch

Fall-2017

Declaration

I declare that this thesis contains no material which has been accepted for the award of any other degree or diploma in my name, in any university or other tertiary institution and, to the best of my knowledge and strongly belief, contains no material previously published or written by another person, except where due reference has been made in the text.

Acknowledgement

I express special thanks to my mother and father, thanks for every moment you spent watching over me. Thanks for support and care. To both of you, I submit this work. May Allah bless you and give you health and long lives.

Also, my thanks go to my wife Hajer, and my children Mohammed and Fatima. Thank you very much for being incredibly understanding and supportive.

Also, I would like to thank my advisor and guide, Dr. Mohammed Elsheh for the continuous support of my thesis, for his patience, motivation, His guidance helped me in all the time of research and writing of this thesis.

Also, my thanks to Dr. Salem Jebriel, Dr. Mohamed Sullabi, Dr. Idris El-Feghi, Husam BinSasi, Fareed Altayesh, Ali Alrewayathi, Jamal Meftah and Mohammed Maafa for providing me assistance and direction whenever I needed it.

Also, my thanks to the participants who took part in experiment study. Their cooperation and feedback were keys to the success of this work.

I would like to thank all the staff and all my colleagues in the department of information technology at the Libyan Academy in Misrata, for their support and help during this work.

Finally, I would like to thank my friends Osama Bala and Ali Almdaini who encouraged me during my study.

Abstract

Authentication is a measure to secure information. Textual passwords are not easy to remember and not safe. Graphical passwords give an alternative solution to textual passwords. It can provide better security and memorability than textual passwords. This study proposed a recognition-based graphical authentication model, where users draw their image passwords on a web page via touch-enabled devices, using their fingers or stylus. Previous studies require an administrator to register the images, or by using external costly tools and take a relatively long time. In this study 103 users were involved. Results show that the average time for drawing images is 3:10 (minutes), the average time length of authentication 1:41(minutes). Meanwhile, 84.78% of users recognize their image passwords.78 users returned a survey which shows that they are satisfied with the usability and memorability of the model.

Table of contents

List of Figures

List of Tables

Chapter One

Introduction

This chapter contains the following subsections: Introduction to user authentication, text passwords and password problem, Graphical passwords, Why using hand-drawn images rather than other images, Motivation, Thesis statement followed by the structure of the thesis.

1.1. Background

Computer applications today uses user authentication as its fundamental security component. Authentication is a process that proves someone's identity. This should be distinguished from deciding what constitutional rights accumulate to the identity (Cheswick, Bellovin, and Rubin, 2003).

The term identification usually means a user ID, which is commonly used to identify the user, whereas the authentication process verifies that the user is the legitimate owner of the ID (Adams and Sasse, 1999).

According to studies in (Zwicky, Cooper, and Chapman, 2000), (K Renaud and Smith, 2001), and (Radack, 2004) authentication is divided into three approaches. These methods depend on the human factors of authentication and answer one of the following:

1. What do you know, which includes traditional textual passwords or PIN?
2. What you have, which includes authentication by smart cards?
3. Who you are, which includes biometric authentication systems like fingerprint?

1.2. Text Passwords and Password Problems

The most common type of authentication is "what you know", and the most common schema we use is textual passwords.

The textual password is a string of printable characters to identify the user. Alphanumeric passwords introduced in the 1960's. Based on (Jadhao and Dole, 2013) the recommendations for creating strong alphanumeric password are:

- The password should be eight characters long at least.
- The password should not be related to the user, such as names, phone numbers, etc.
- The password should not be a word that can be found in the dictionary.
- Ideally, the user should mix upper and lower case letters and digits.

Textual passwords suffer from many problems, the main problem is that memorable textual passwords are not very secure. And strong textual passwords are not easy to remember (Cranor and Garfinkel, 2004).

Also, textual passwords are vulnerable to small dictionary attack (Tao, 2006), in which an attacker searches candidate passwords from "small dictionary". Due to human memory limitation, users frequently choose passwords which are easy to remember.

1.3. Graphical Passwords

Graphical passwords were introduced as an alternative to textual passwords. The main principle of graphical passwords that humans remember visual information more than other types of information (Garfinkel and Lipford, 2014),(Shepard, 1967). From this principle, graphical password comes with the same issue because passwords are expected to have two requirements, namely:

a) The password should be easy to remember.
b) The password should be secure. (Towhidi and Masrom, 2009)

In graphical password systems, a user needs to choose a memorable image. In authentication process user need to recognize his registered image among a set of images, or a user need to reproduce his own image.

Different types of images were used in various graphical password systems, these types of images including face images, objects, and hand-drawn images, but some studies show that hand-drawn images are more suitable for authentication than another type of images (Karen Renaud, 2009).

1.4. Why use hand-drawn images rather than other images?

According to (Karen Renaud, 2009), There are many advantages of hand-drawn images, which make hand-drawing images suitable for use in the authentication process. Some of these advantages are as follows:

- Hand-Drawn Images are quickly produced.
- Hand-Drawn images are very hard to describe.
- The hand-drawn image cannot be duplicated.
- There is a relation between the drawer and his drawings. (Berger and Savage, 2005)

The best feature of hand-drawn images is that most people can use them whether they are educated or not, young or old. (S. M. Jebriel, 2014)

1.5. Problem statement

The main goal of this study is to investigate current problems associated with graphical authentication; and propose a new method for using hand-drawn image passwords in web authentication, which supports usability, memorability, the main research question is:

Can user-drawn passwords on touch-enabled devices support both usability and memorability?

To answer the above question; this study will perform the following tasks which present the thesis objectives as following:

1. To explore the area of graphical passwords.

2. To identify the issues of graphical passwords.
3. To propose a new method which allows users to draw their own image passwords directly during the registration process using finger or stylus.
4. To evaluate the proposed method using questionnaire survey and comparison with other studies.

1.6. Motivation

Nowadays, the primary measure to guarantee information security is authentication, and the most popular method for authentication is textual passwords. However, as result of defects of textual passwords which led to a search for an alternative way for authenticating users. One of alternative way to textual passwords is biometric authentication, but this way is costly. Another alternative for textual passwords is graphical authentication. The primary motivation of graphical authentication is that human brain can remember graphical objects better than text. Also, psychological studies support such assumption (Thorpe and van Oorschot, 2004), (Shepard, 1967). And also with the significant evolution of IT technology, we are moving forward to use touch-based devices such as tablets, smartphones, laptops and desktop computers.

Another motivation of this research is that the design of any technique should take into consideration the ease of use, as well as minimal effort, time and basic equipment(cost).

The model of Govindrajulu and Madhvanath (Govindarajulu and Madhvanath, 2007) requires expensive pieces of equipments, such as a touchpad and a digitizing tablet connected to the computer. And users need to be trained how to use the whole system.

The approach which proposed by Jebriel and Poet (S. Jebriel and Poet, 2014), requires a scanner attached to the computer to scan images drawn by the user on paper and needs external painting program to draw images. To overcome all existing drawbacks; the proposed approach in this research require only touch-enabled device such as laptop, smartphone, tablet or desktop computer.

1.7. Structure of The Thesis

The remaining parts of this thesis is organized as follows:

Chapter Two: discusses various graphical authentication schemes, and different design implementation and security issues.

Chapter Three: describes the methodology of the proposed method for graphical user authentication.

Chapter Four: gives the details of the implementation of data gathering for testing the proposed model.

Chapter Five presents the experiments and results.

Chapter Six conclude the thesis, and suggest further research directions for future works.

Chapter Two

Literature Review

In this chapter, the researcher reviewed prior studies related to usage of graphical passwords in authentication. Also, review of some security issues and vulnerabilities related to graphical passwords. This chapter contains the following subsections:

- Classification of graphical passwords
- Security of graphical passwords
- Usability of Graphical Passwords
- Memorability of Graphical Passwords
- Recognition-based graphical passwords
- Summary

2.1. Classification of Graphical password

There are many classifications for a graphical password; for example, authors in (De Angeli, Coventry, Johnson, and Renaud, 2005) classified graphical passwords into three categories: Cognometrics, Locimetrics, and Drawmetrics. The term Cognometric refers to using human mind abilities to innate cognitive. The Locimetrics refers to techniques which require clicking on specific points on an individual image during the authentication phase, and the term Drawmetric refers to techniques that enforce the user to reproduce a pre-drawn outline drawing, Drawmetric systems located at the borderline between biometrics and graphical mechanisms. According to the study (Tao, 2006), graphical passwords has been divided into two categories: Image-based schemas and Grid-based schemes. Image-based systems use many types of images, including artificial pictures, photo graphics, or any other kind of images as background. According to the number of images displayed, image-based schemes is divided into two subclasses: single-image schemes and multiple-image schemes. In grid-based scheme which proposed by (Jermyn, Mayer, Monrose, Reiter, and Rubin, 1999); it used a grid as background, however, there are many advantages of using a grid as background such as:

- Elimination of store graphical database on the server.
- Unlike image-based schema which requires overhead to transfer images through the network. Grid scheme minimizes the requirement of displays.

The study of (Dirik, Memon, and Birget, 2007) divided schemes of graphical passwords into three systems:

- **Recognition based systems**

  In this kind of systems, users need to recognize their own image passwords when they see them each time they log in. The challenge set contains image password together with some distractor images.
- **Pure recall based systems**

  Users in this kind of systems are required to recreate their image passwords from scratch whenever they log in.

- **Cued recall based systems**

  During authentication, the system provides some help to the user to recreate their own image passwords, including selecting points in an image.

Another survey study of graphical passwords classifications by (Suo, Zhu, and Owen, 2005) divided graphical password schemes into two main categories:

- Recognition based systems
- Recall based systems.

This study focuses on recognition based systems. The advantages of recognition based systems over a recall based systems; including that image easier to recognize when showing it again rather than recreate it (Koriat, Ben-Zur, and Nussbaum, 1990),(Cave, 1997). One disadvantage of recognition based systems is that attacker can see the actual image passwords, and the attacker just needs to guess the correct image from the set of distractor images (S. Jebriel and Poet, 2014).

2.2. Security of Graphical Passwords

As textual passwords, graphical password systems are vulnerable to many attacks, which mentioned by (Poet and Renaud, 2009):

- **Dictionary Attacks:**

Since recognition based systems involve input by mouse instead of input by keyboard, it will be vulnerable to dictionary attack on this type of systems (Suo, 2006). In a dictionary attack, the attacker uses images which can be applied to recognition based systems. In cued recall based systems; the attacker builds a program that can obtain click points on an image.

- **Brute Force Attack**

Brute force attack represents repeating number of trials to get the password. Users are helped in recognition based systems to remember their image passwords; with another set of distractors; which could be vulnerable to brute force attack which helps attackers to try a number of different image choices without restrictions. The system should give the users small number of trials to prevent brute force attack.

- **Denial of Service**

Denial of service is used to prevent an attacker from using a brute force attack to get the password which denies service after a small number of trials. The attacker can deliberately try to log in as another user, this cause failing specific times which led the victim to re-enroll. Thus, re-enrolment is required and should be used with care to avoid a brute force.

- **Intersection Attack**

This kind of attacks targeting recognition based systems, the attack occurs when a recognition system uses a different set of distractors each time the challenge set is displayed. The attacker can keep refreshing the display to see which image of a challenge set not change. This attack can be avoided by fixing the distractors of a challenge set during registration.

- **Shoulder-Surfing:**

In graphical password systems, images are displayed to the user, and the user needs to identify the image, users often choose their own image password by clicking on it with the mouse, so it is possible for someone to monitor which choices have been made. Some recognition-based systems allow users to enter their choice using the keyboard only, and this lead to make it much harder for an observer to identify the target image.

- **Social Engineering**

Users in some graphical password systems can use their own images as password images; Attackers may guess this kind of images if they can relate the image to a particular person. This problem concerned with some images such as photographs but less with other types of images such as sketches and mikons, where the images are created by software and provided by the user. However this kind of images is much less likely to be easily attributed to the artist. According to study of (Suo, 2006), the security threats of recognition-based systems were grouped into three basic security aspects, which summarized as follows:

- Guessability: ability of attacker to guess user's password;
- Observability: ability of attacker being able to observe the password as the user enters it;
- Recordability: an ability of the user to record the password, which makes it easier for an attacker to steal it.

2.3. Usability of Graphical Passwords

The International Organization for Standardization (ISO) is the largest developer and publisher of international standards in the world. ISO developed some models to measure usability. ISO 9241 ("usability.org,"), defined 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"*. (Usability Definitions, para. 2). Shneiderman and Ben, 2003 characterized usability of software or interface should involve the following concerns:

- Learn-Ability: the amount of time for typical users to learn the actions relevant to a set of tasks.
- Efficiency: How long does it take users to perform typical tasks?
- Errors: The rate of mistakes made by users when they are performing tasks.

- Memorability: How users can regain their knowledge of the system over time?
- Subjective Satisfaction: How users like the aspects of the system?

2.4. Memorability of Graphical Passwords

The main reason behind investigating graphical password is that text passwords are difficult to remember. Many studies show that human's memory able to retain visual information longer than words or texts (De Angeli et al., 2005), (Goldstein and Chance, 1971). Also, Psychological studies (Thorpe and van Oorschot, 2004), (Shepard, 1967) shows that people can remember pictures more easily than words. The most important design issue for recognition-based graphical systems is how to make it easier for users to remember their images. There are many techniques have been proposed to help users recognize their images; such as grouping images by theme, using images of the human face, or authorizing users to use their images as passwords.

2.5. Recognition Based Graphical Passwords

This section presents several recognition-based systems, the main different between these systems refers to the kind of images used in the system, and whether the users provide their images or they choose images supplied by the system.

2.5.1. D´ej`a Vu Scheme

This scheme was proposed by Dhamija and Perrig (Dhamija and Perrig, 2000) which shown in Figure 2.1. D´ej`a Vu Scheme was built based on Hash Visualization techniques (Perrig and Song, 1999). During portfolio creation phase; users select a specific number of images among a large number of images generated by the system, the system created the images from Andrej Bauer's Random art collection.

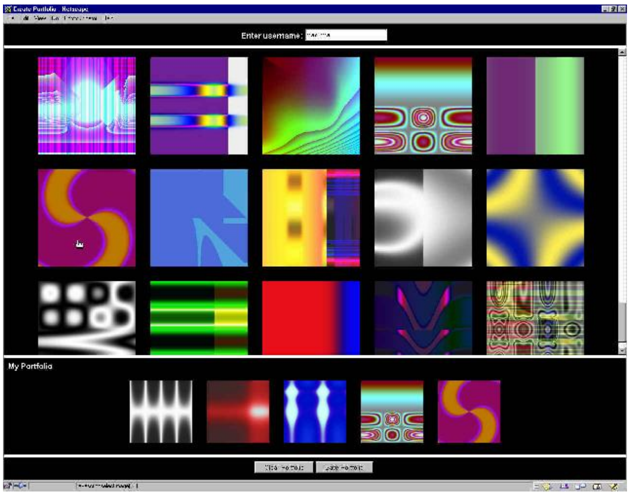


Figure 2.1 D´ej`a Vu Scheme

Later, during authentication phase; users should identify and pass a challenging set which contains their pre-selected images mixed with decoy images. The users will be authenticated if they can identify their images successfully. Results showed that 90% of all participants succeeded in using D´ej`a Vu Scheme. Meanwhile, only 70% succeeded using text-based passwords and PINS. There are several advantages for D´ej`a Vu Scheme; for example, the schema is strongly resistant to a social engineering attack because of using hardly described abstract images. Also, this schema is preventing users from choosing a weak password and disallowing writing the password down and sharing it with other people (S. M. Jebriel, 2014). The main drawbacks of D´ej`a Vu Scheme are, the time required for creating the portfolio. As it needs about sixty seconds which is longer than the time required for creating the textual password (twenty-five seconds). Also, the login phase in this scheme takes longer time than login using textual passwords. The study of (Rittenhouse, Chaudry, and Lee, 2013) reported that D´ej`a Vu scheme is vulnerable to brute force attack.

2.5.2. Passface Scheme

This scheme developed by Real User Corporation (authentication). The system uses faces as an object for a password as shown in Figure 2.2. The main principles of this system based on psychological studies such as the study of Feingold (Feingold, 1914). During enrollment procedure, the users choose four faces from a database which will represent their authentication password in future. Later, in the authentication process, the system displays to the user a grid of nine faces, consisting of eight decoy faces and one face previously chosen by the user. As the user's password contains four faces, so the grid is shown to the user four times. To secure passface combination against detection through shoulder-surfing and packet-sniffing; the faces are ordered randomly in each phase. Also, no grid contains faces found in other ones.

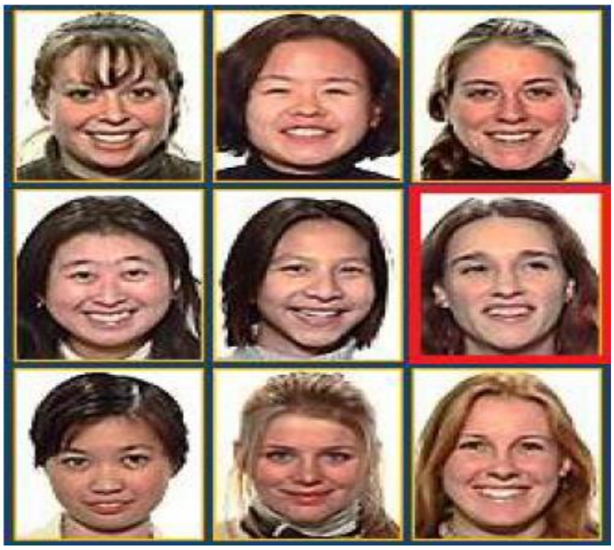


Figure 2.2 Passface Scheme

The study of (Valentine, 1999) which targeted 77 users, found that people could remember their Passfaces password over extended periods of time, with login success rates between 72% and 100% by the third attempt for different time interval up to 5 months. Another 34-user field study (Brostoff and Sasse, 2000) found mixed results. While users made fewer login errors (95% success rate for Passfaces), they tended to log in more rare times than users who log in with text passwords because the login phase took longer (although no login times were reported). The Study of (Davis, Monrose, and Reiter, 2004) invetigated the graphical passwords created using Passface technique; the study found that most users tend to choose faces for people from the same race. Also, the study found that the better-looking faces were more likely to be chosen by users. All of these results make the Passface password quite predictable. This problem may be alleviated by arbitrarily assigning faces to users, but this will make it hard for users to remember the password. However, there are several drawbacks to Passface scheme. Passfaces corporate website (authentication) reports that password creation time takes three to five minutes for a panel of nine faces and five rounds. Also, usage of the mouse to select passface image could affect the threat of shoulder surfing attack. According to studies of (Davis et al., 2004), (Levin, 2000); the images which used in Passface scheme are vulnerable to guessing attack.

2.5.3. Triangle Scheme

Sabrado and Birget (Sobrado and Birget, 2002) designed a graphical authentication technique which deals with shoulder surfing attack. Their method named triangle which is shown in Figure 2.3. In this scheme, the system randomly put a set of N objects which could be a hundred or a thousand of objects. Also, there is a subset of K objects previously chosen by the user; these K objects represent the user password. Then, in login phase; the system will randomly placed of N image objects; then the user must find three of his password image objects, and the user must click on the invisible triangle created by those three image objects or click inside the convex hull of the pass objects that are displayed. Also, for each login, this challenge is repeated a few times using a different display of some of the N objects. Therefore, the probability of randomly clicking on the right region in each challenge is very small.

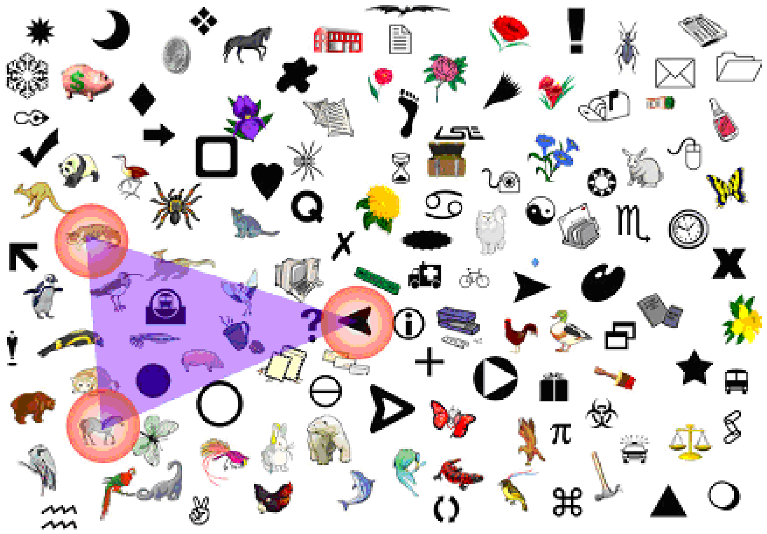
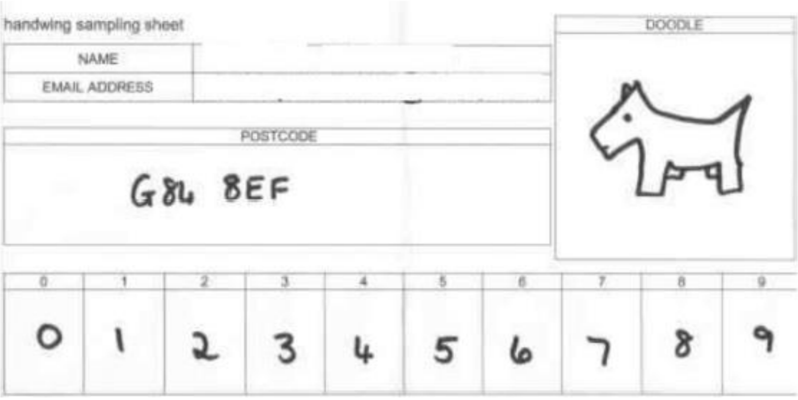


Figure 2.3 Triangle Scheme

Triangle scheme is intended to prevent shoulder surfing and Guessability attacks. However, there are several drawbacks associated with this scheme. The designers of this system suggest usage of a thousand of objects which make the display very crowded and the objects almost indistinguishable. However, by using a small number of objects will lead to a smaller password space and cause the resulting convex hull be massive (Suo et al., 2005).

2.5.4.Handwing Scheme

Renaud in (Karen Renaud, 2006), proposed a web authentication mechanism that uses doodles in one of its authentication phases. This technique called Handwing; This method 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 postcodes on a provided form such as that shown in Figure 2.4.



handwing sampling sheet

NAME

EMAIL ADDRESS

POSTCODE

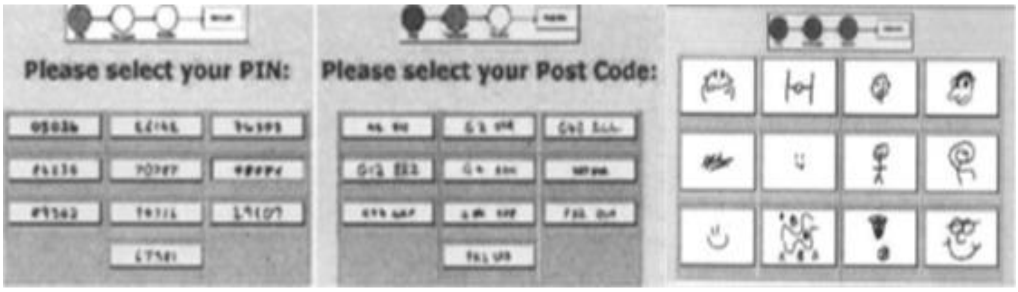
G86 8EF

DOODLE

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

Figure 2.4 Biometric Collection form

Users then obtained their password generated from the information on the form above using 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 handwritten PIN numbers; by recognizing their handwritten digits. Secondly, as similar to first stage, users had to identify their hand-written 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 2.5 shows the three authentication stages. Once users had passed the three phases by choosing all three components correctly, they were allowed to enter the website.



Please select your PIN:

Please select your Post Code:

Figure 2.5 Handwing Scheme

The study of 20 elder users (eleven females and nine males) pointed out that the duration of the experiment (nine months), only one authentication failure happened as a result of selecting the wrong doodles. This scheme demonstrated some security drawbacks such as the probability of recognition of the users' handwriting digits by people who knew them. Also, the observability of the system is very high. Additionally, the PINs and the postcodes could easily be recorded, whereas doodles are difficult to guess because the system used over 200 doodles and many of them were similar to the user's drawings.

2.5.5.Jebriel and Poet Scheme

Jebriel and Poet in (S. Jebriel and Poet, 2014) proposed a recognition based method for authentication based on user-drawn passwords which is shown in Figure 2.6. The idea suggested that users provide their images passwords as simple drawings. Previous recognition based schemes have relied on a human administrator to register the images with the system. They replaced the system administrator with software which guides the user through the registration process. Also, the software automatically corrects any errors in the image files which submitted by the users to the system. A study of 40 users; each user provided four different images for each of the scans, and paint programs, leading to a total of eight images. In each case was prevented with four challenge sets, each set consists of one of their provided image password and 15 decoy images when they logged in. The users must select all four pass images to log in correctly. To avoid any bias between pass and decoy images; the decoy images were selected randomly with actual pass images from other users.

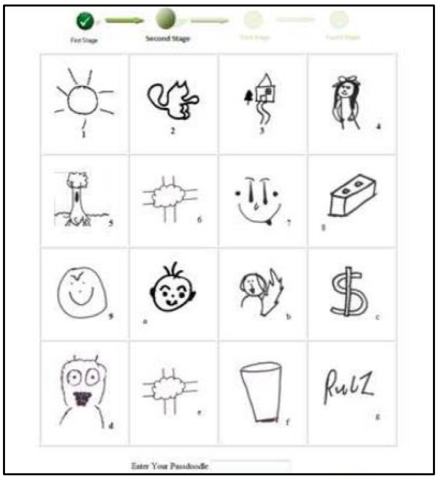


Figure 2.6 Jebriel and Poet Scheme

The study pointed out that 84% of users strongly preferred to submit their image passwords using paint programs, and 16% of users preferred using scan system. Also, the study shows that 92.80% of the users who used paint system was successfully logged into the system. Meanwhile, 91.16% of the users who uses scan system successfully authenticated. Neverthless, this method has several drawbacks; Firstly the study reports that the average time for registration using scan is 16 minutes, and registration using paint program took nine minutes which is longer than creating textual passwords. Another drawback of this system, that users need external tools such as a scanner to draw their passwords which makes the system costly.

2.6. Summary

This chapter mentioned some prior studies related to recognition-based graphical passwords. In D´ej`a Vu, passface, and triangle schemes; the users choose their pass images from a system supplied collection. This study proposed a method that allows users to create and draw their own image passwords, since user performed tasks are easier to remember than system provided graphical passwords, and system provides pass images may be less personal and thus less memorable

(Jebriel, 2014). The study of (Rittenhouse, Chaudry, and Lee, 2013) reports that D´ej`a Vu scheme is vulnerable to brute force attack. However, in this study the proposed model allows users to try login to the system three attempts only, that protect the system from brute force attack. The usage of the mouse in passface scheme to select pass image could make the system vulnerable to shoulder-surfing attack, this proposed model overcome this issue by allowing the users to choose their image password by entering the number of the pass image using keyboard only in textbox password mode, so the entered number will appear as stars. Also, the password creation time using passface scheme takes five minutes which quite long. However, this study proposed a method that may reduce the time of registration by allowing the users to draw their own image passwords directly on touch-enabled devises.

The display of challenge set in Triangle system is very crowded and indistinguishable, due to the usage of a thousand of objects. To tackle this drawbacks, this study suggested a technique which shows 64 decoy images in four challenge sets; each set contains 16 decoy images. The observability of Handwing scheme is high. Also, the PINs and postcodes could easily be recorded. However, this study proposed a technique that allows the user to draw four image passwords during the registration at the first time. During login phase, the display of decoy images on a challenge set is displayed randomly, and the entry of choice of image password is only allowed by keyboard in textbox password character mode; which avoiduing observability and recording of user choice. The system of Jebriel and Poet (S. Jebriel and Poet, 2014) required some external tools such as scanner if the user chooses to draw password on paper, which may not be available to all users, and this made the system is costly and less usable. As a result of wide spreading of touchscreen devices such as smartphone, tablets, laptops and desktop computers; this study proposes a system which only need the touch-enabled device, which allows users to draw their own pass images directly into the system using their finger or stylus. This leads to reduce the cost and time of registration. Although, the main focus in this research on touch-enables devices; the proposed system still deals with non-touch-enables devices by allowing the users to draw their own pass images using mouse.

Chapter Three

The proposed system

This thesis focuses on recognition-based authentication systems. The advantage of recognition-based over recall-based authentication is that it is easier to recognize an image password when showing it again, rather than recall-based authentication which requires reproducing the image password again from scratch (Koriat et al., 1990),(Cave, 1997).

To overcome all drawbacks of previous models (S. Jebriel and Poet, 2014),(authentication),(Sobrado and Birget, 2002),(Dhamija and Perrig, 2000); this study proposed a recognition-based approach for authentication. The approach in this research suggested users will draw their own image passwords using finger or stylus during the registration phase, without any external tools such as painting programs or papers. Simple drawings which drawn by the user using their fingers or stylus are simpler than drawings which system-issued images or personal photos, also personal photos have many problems which make them unsuitable for security issues (Karen Renaud, 2009). The creative effort involved makes user drawings easier to recognize than another type of drawings(Knoblich and Prinz, 2001).

Following the registration stage; in authentication phase; password image is displayed for users on a screen with another number of images which drawn by other users. The users need to identify and recognize the password image they have drawn earlier.

the proposed system will go through three phases:

1.Registration phase.

2.Authentication phase.

3.The final phase is evaluation phase, which relies on questionnaire survey to identify user's satisfaction and reliability of the proposed model.

3.1. Registration Phase

As shown in Figure 3.1, the user enters some personal information such as email, phone number, age, education level and device type; then the user is asked to draw four image passwords on a web page using his/her finger or stylus. The user information and image passwords are collected and stored in a database. Also, the elapsed time of registration and drawing images for each user will be saved in the system.

3.2. Authentication phase

As shown in Figure 3.2; each user login to the system by entering his email or phone number, then the system displays four screens in sequence to the user, each screen contains 15 images which chosen randomly by the system and one target image, and each image occupied a different position in 4x4 grid each time. One of the key security aspects of recognition-based graphical passwords is the probability of guessing the correct images for a whole challenge session; researchers often report a chance of guessing as shown in equation below where *x* is the number of images displayed on a challenge screen, and *n* is the number of challenge screens(English, 2012).

$$\text{P(guess)}=\frac{1}{X^{n}}$$

Based on the above formula, the chance of guessing in the proposed method is:

$$\text{P}=\frac{1}{16^{4}}=\frac{1}{65536}=0.0000152587890625$$

Users will be authenticated if they selected their four image passwords and completed the login process without any errors. Otherwise, the system gives the user three more chances to log into the system. To enhance security; the system gives the user an opportunity to select the image password within two minutes. Also, some information for each trial for login were stored in a database such as elapsed time for login, the number of correct and fault choices, this information will be used during the evaluation of the proposed model.

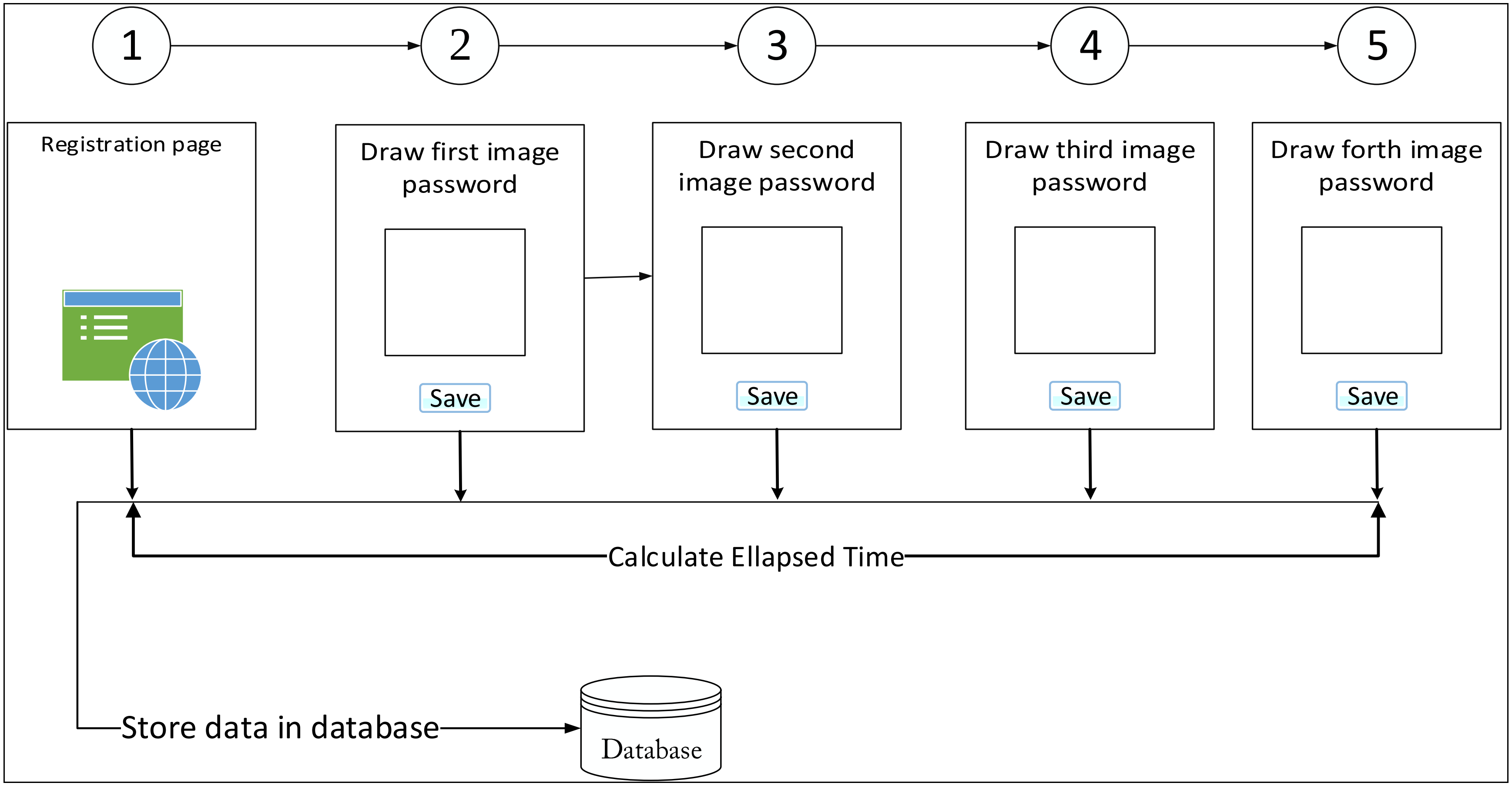
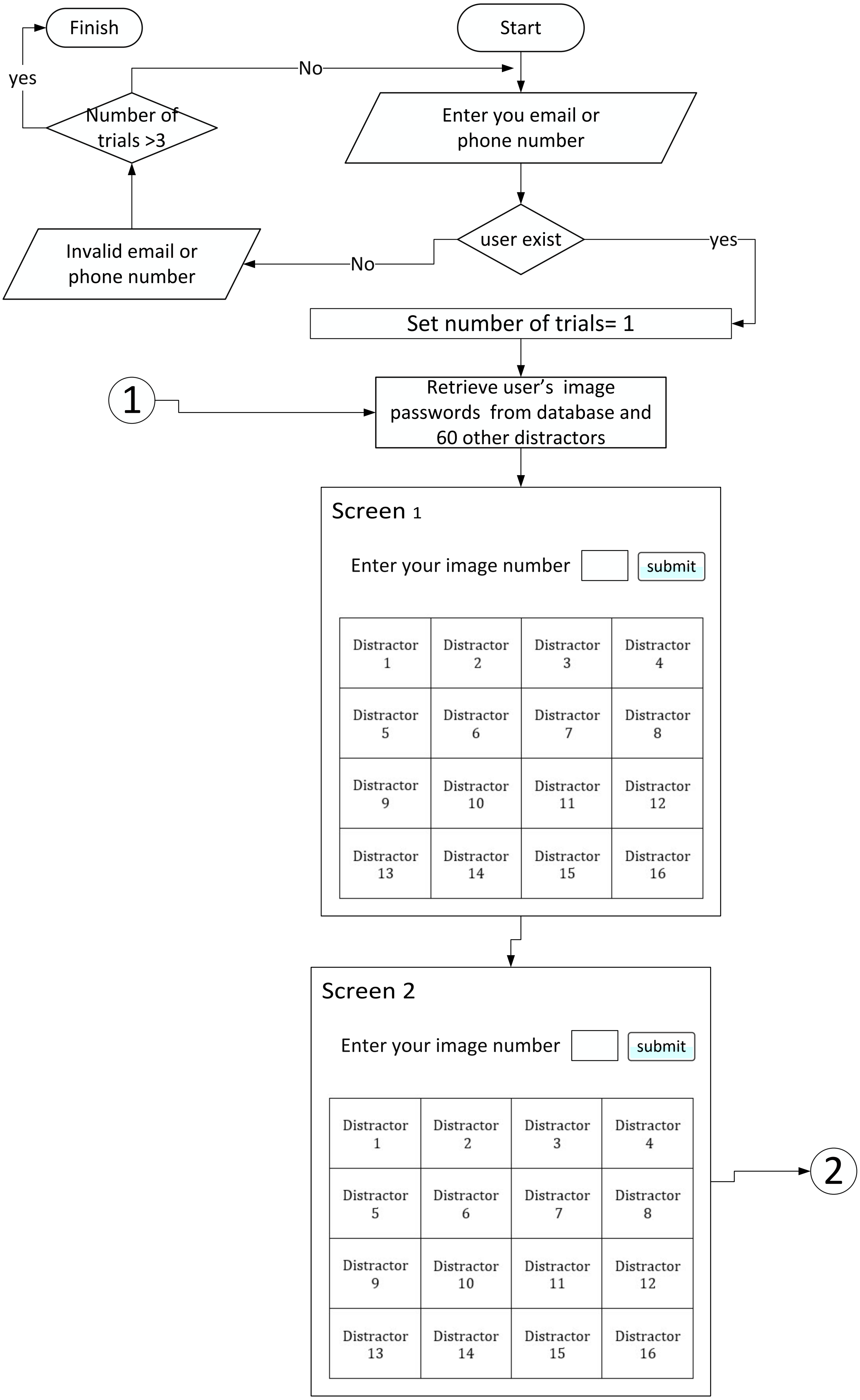

1
2
3
4
5
Registration page
Draw first image password
Save
Draw second image password
Save
Draw third image password
Save
Draw forth image password
Save
Calculate Ellapsed Time
Store data in database
Database

Figure 3.1 Design of Registration phase


Finish
Start
yes
No
Number of trials >3
Enter you email or phone number
user exist
yes
No
Invalid email or phone number
Set number of trials= 1
1
Retrieve user's image passwords from database and 60 other distractors
Screen 1
Enter your image number
submit
Distractor 1
Distractor 2
Distractor 3
Distractor 4
Distractor 5
Distractor 6
Distractor 7
Distractor 8
Distractor 9
Distractor 10
Distractor 11
Distractor 12
Distractor 13
Distractor 14
Distractor 15
Distractor 16
Screen 2
Enter your image number
submit
Distractor 1
Distractor 2
Distractor 3
Distractor 4
Distractor 5
Distractor 6
Distractor 7
Distractor 8
Distractor 9
Distractor 10
Distractor 11
Distractor 12
Distractor 13
Distractor 14
Distractor 15
Distractor 16
2

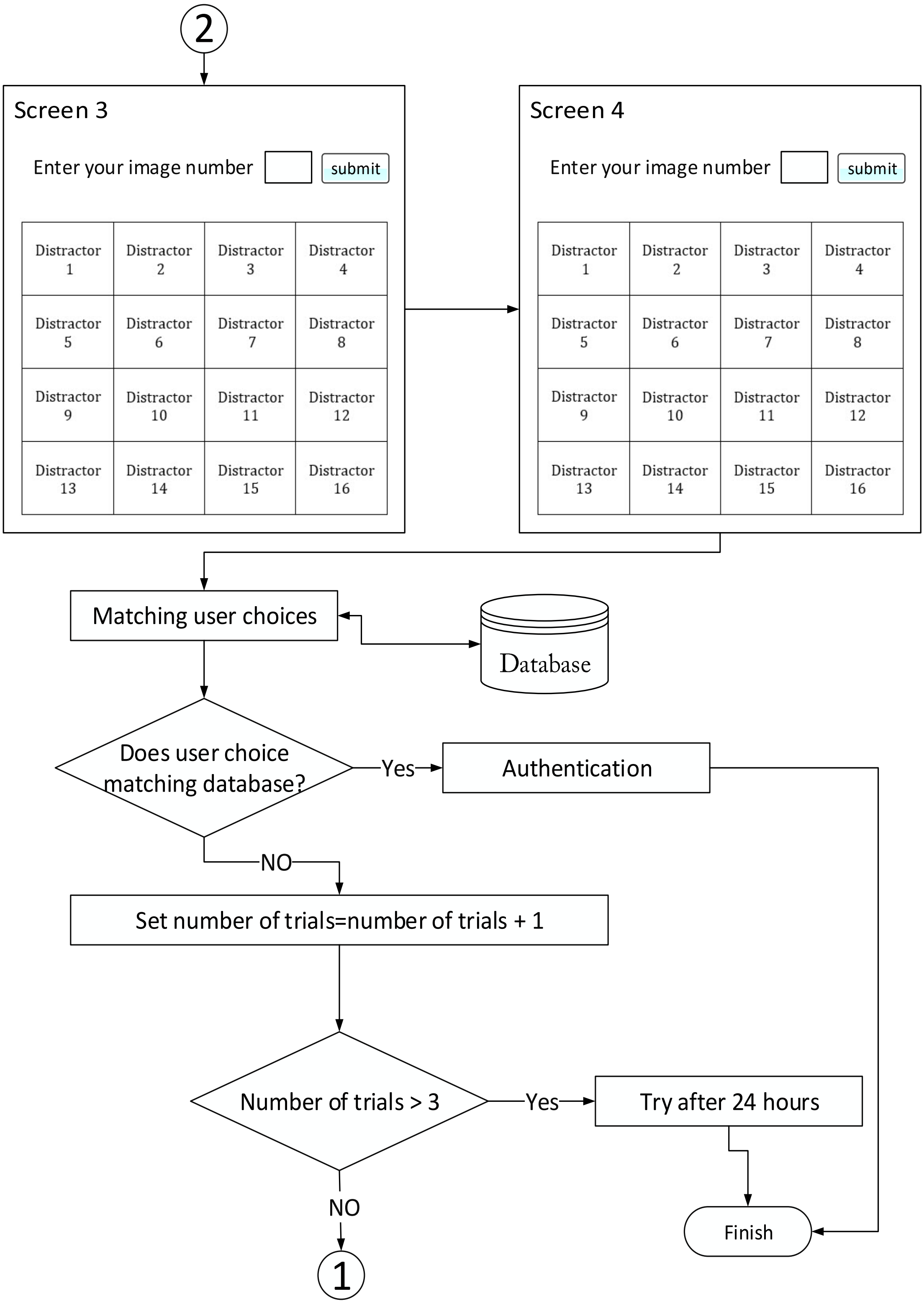


Figure 3.2 Design of authentication phase

3.3. Summary

In this chapter; the proposed model for a recognition-based graphical password has been explained and clarified.

Chapter Four

Implementation

The proposed method implemented with the following technologies:

- ASP.NET with C# language as core programming tool.
- SQL Server for database storage.
- CSS, JavaScript, and AJAX.

4.1. Database Design

This study aims to develop a new model of hand-drawn graphical passwords for web authentication. To evaluate the proposed system; some data is needed to be collected from users to justify their satisfaction. Good database design leads to ease of storing, retrieving and processing of data, and vice versa. The prototype system manages data which is stored in relational database schema as shown in Figure 4.1. More details about database tables could be found in appendix A.

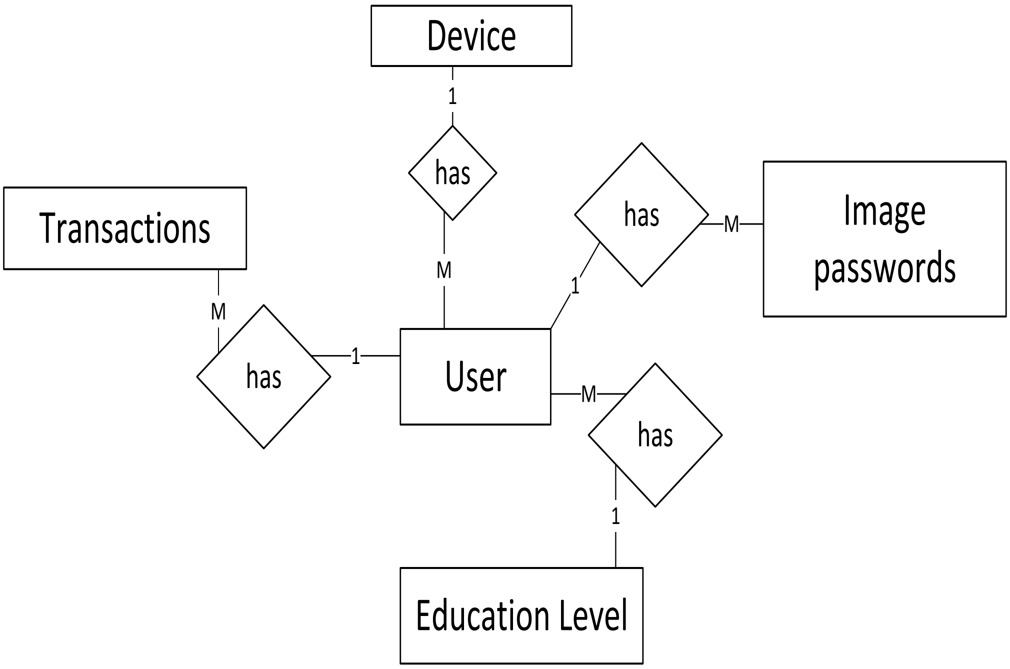
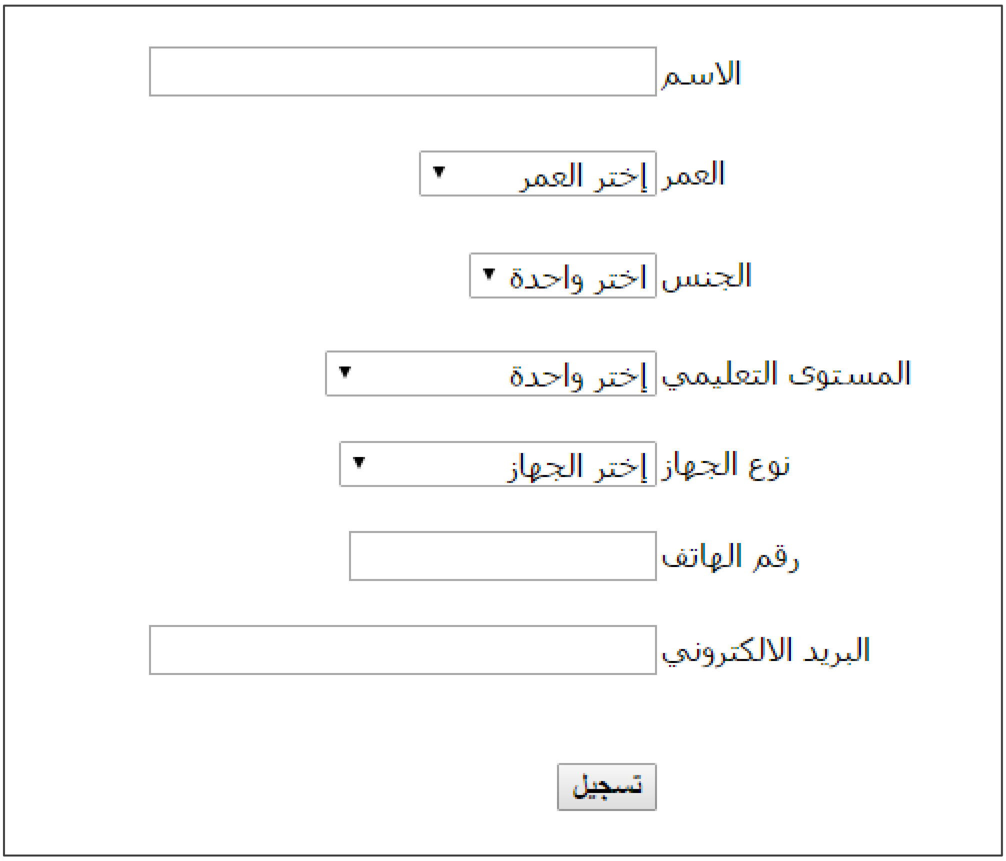


Figure 4.1 ER diagram for the proposed mode

4.2 Layout Design for Registration Phase

A web based application was built using some technologies which mentioned earlier. The application pages are developed with Microsoft Visual Studio 2015 Enterprise development environment.

The home page of the application is registration page, which asks the users to enter basic information such as name, phone, age, device type, education level and email address which shown in Figure 4.2



الاسم

العمر إختر العمر ▼

الجنس اختر واحدة ▼

المستوى التعليمي إختر واحدة ▼

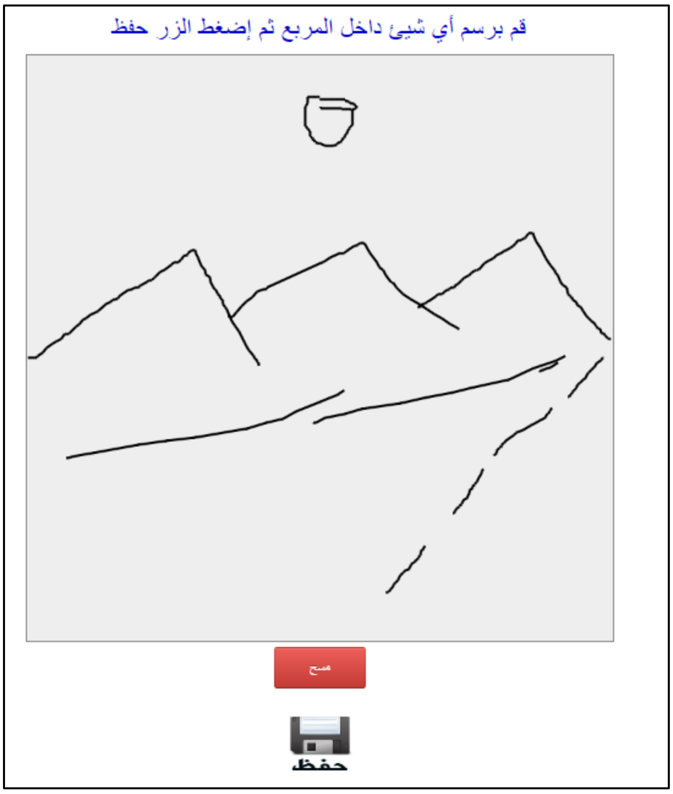
نوع الجهاز إختر الجهاز ▼

رقم الهاتف

البريد الالكتروني

Figure 4.2 Registration Page

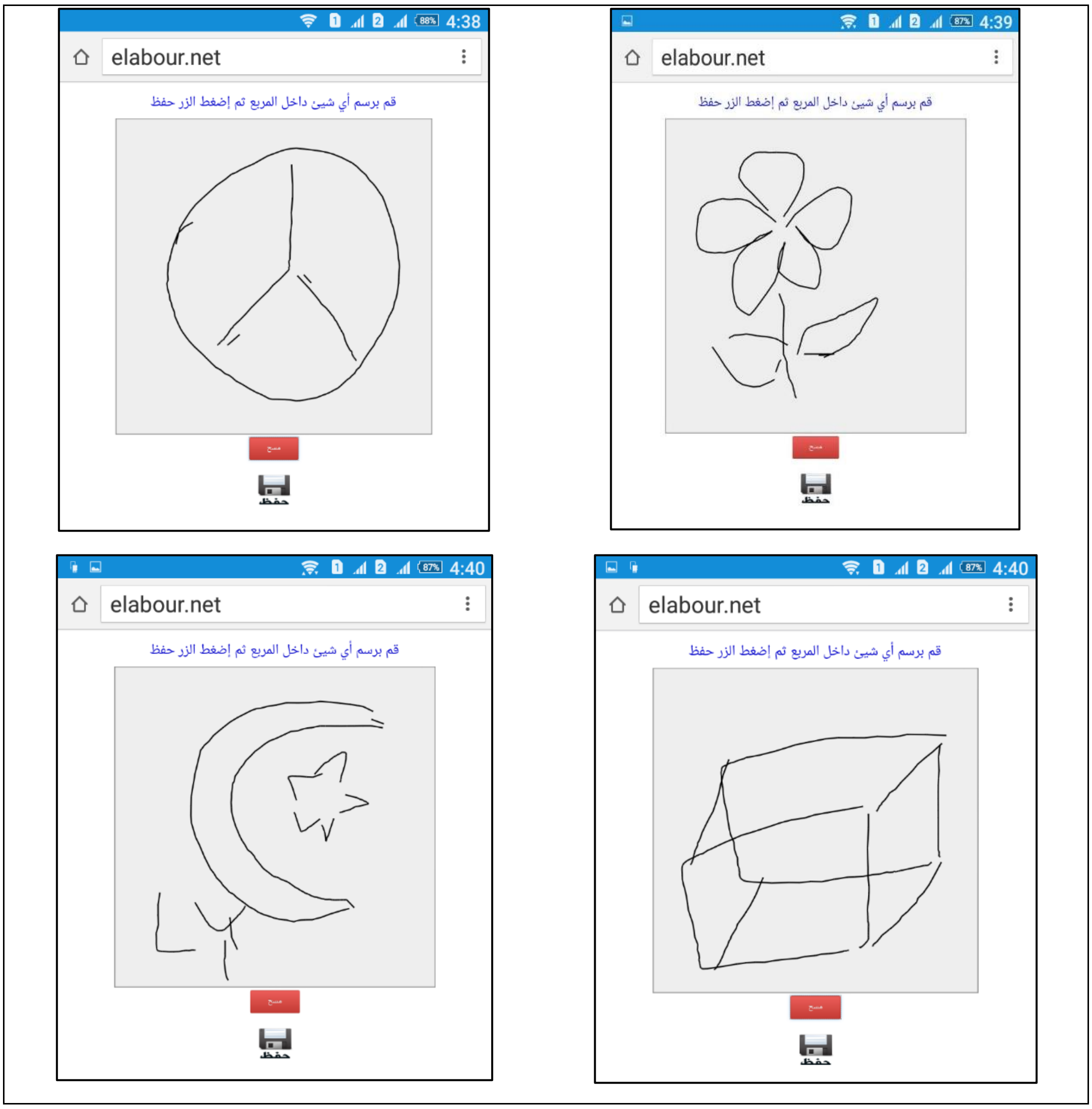
Following entering and validating of user's data; data will be stored in database. Then the user will be redirected to the drawing page, which allows him to create his/her image passwords using fingers or stylus as shown in Figure 4.3



قم برسم أي شيئ داخل المربع ثم إضغط الزر حفظ

Figure 4.3 Drawing of image password page

In each time when the user draws his/her password on the web page, the image will be stored in the database. Also, the elapsed time of drawing the image is saved in the database. Since every user is required to draw four pictures; the previous task is repeated four times in a single session. Figure 4.4 shows an example of image passwords were drawn using a smartphone browser.



قم برسم أي شيئ داخل المربع ثم إضغط الزر حفظ

قم برسم أي شيئ داخل المربع ثم إضغط الزر حفظ

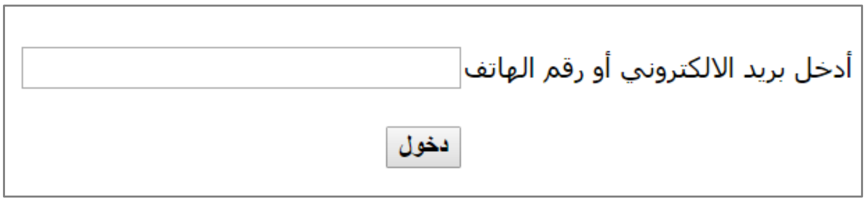
قم برسم أي شيئ داخل المربع ثم إضغط الزر حفظ

قم برسم أي شيئ داخل المربع ثم إضغط الزر حفظ

Figure 4.4 Image passwords drawn using smartphone

4.3 Layout Design for Authentication Phase

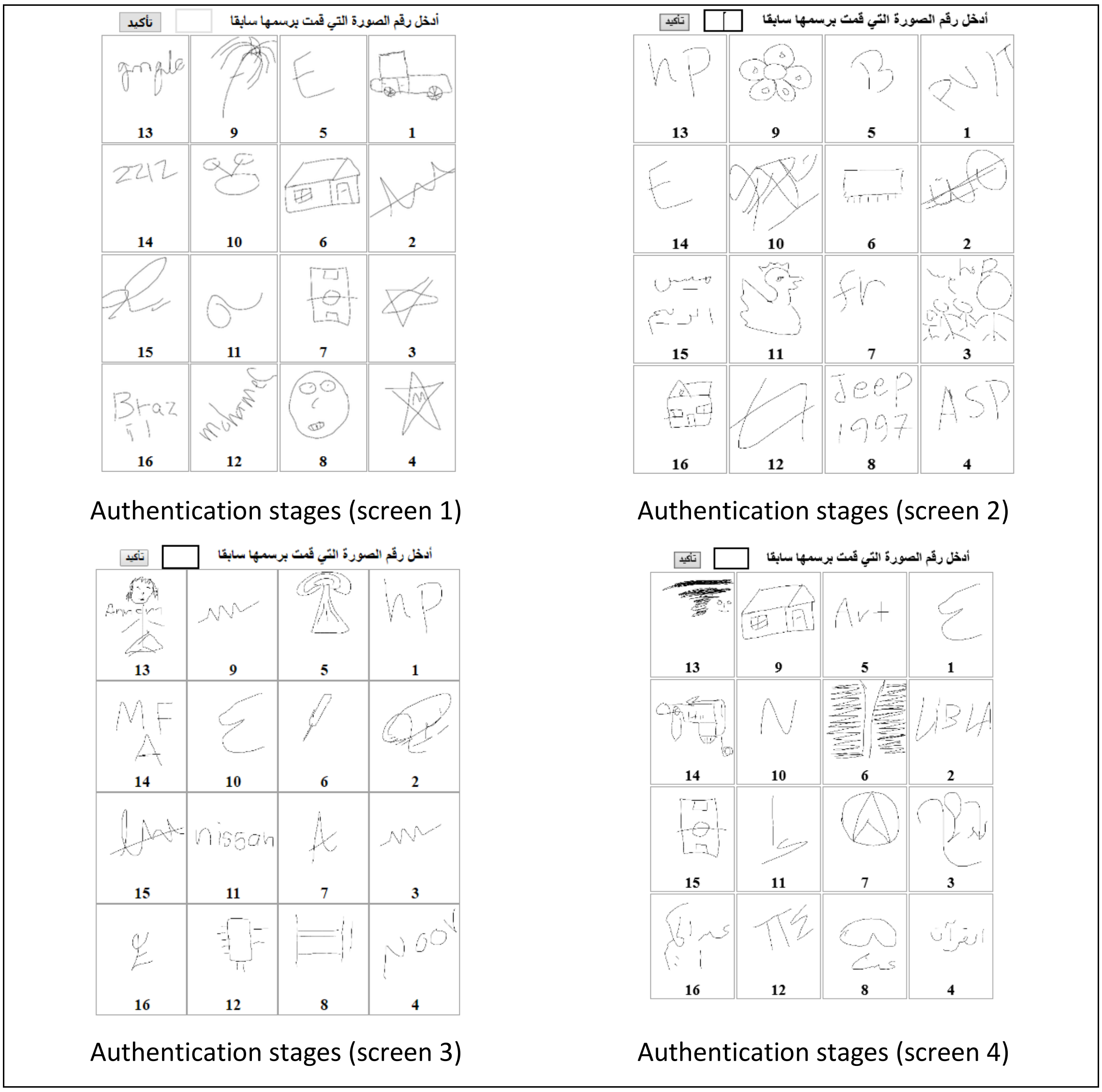
After finishing the registration process; each user must log in to the system using his/her phone number or email address, as shown in Figure 4.5



أدخل بريد الالكتروني أو رقم الهاتف

Figure 4.5 Login Page

Following success login; users will be directed to the authentication screens; Users were only authenticated if they passed all four authentication screens by selecting the right images. The application displays four screens in sequence, each containing 15 random distractors selected randomly among hundreds of images was drawn by other users, and one target image, as shown in Figure 4.6



Authentication stages (screen 1)

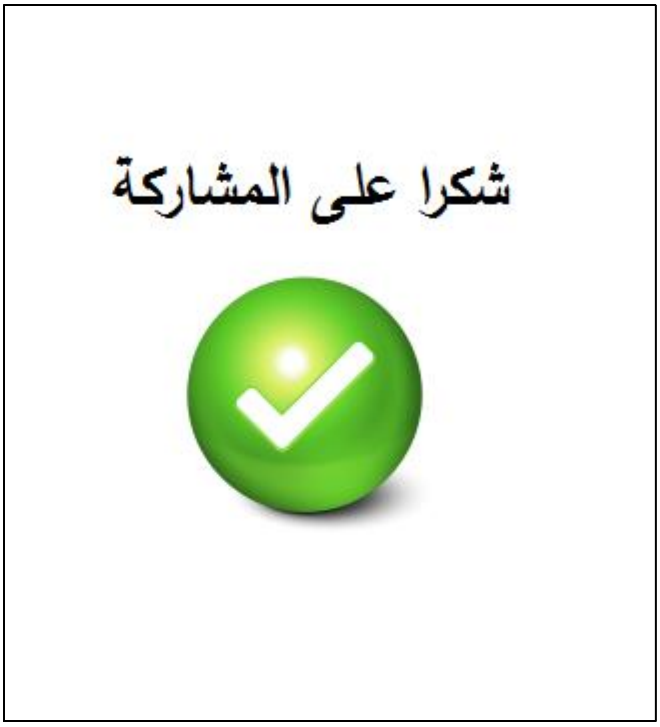
Authentication stages (screen 2)

Authentication stages (screen 3)

Authentication stages (screen 4)

Figure 4.6 Authentication Phase

After the user completes the authentication phase; the user will be redirected to the final page as shown in Figure 4.7



شكرا على المشاركة

Figure 4.7 Thanks page

4.4 Summary

This chapter explained the implementation of the proposed model for a recognition-based graphical password. A web aplication for the proposed model has been designed using ASP.NET and SQL server databases.

Chapter Five
Results and Discussion

In this chapter, the experiments and the results of the proposed model will be explained. Also, the experiment results will be discussed and compared with other studies.

5.1. Pilot Study

A pilot study was implemented to solve any problems before the real test was conducted. The participants were 11 students in the Libyan Academy at Misrata city. The participants tested the proposed model over the internet, and They provided valuable comments about the system. This ensured that the prototype system worked well with different types of devices such as smartphones, tablet, laptop and desktop computers. Also, the participants made sure that all the correct data was logged and collected.

5.2. The Experiment

Participants were recruited from various genders, ages, and

education levels in Misrata city, the experiment took place between 21st March and 11th June 2016. 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.
2. During this process; the researcher sent the website link to participants to create their accounts. They also provided their basic personal information.
3. The participants created and registered four image passwords.
4. The participants logged into the system two times, firstly two weeks after registration, then after another four weeks from registration. The researcher sent SMS and Facebook message reminders at the appropriate times.
5. The participants filled in the questionnaire survey.

5.3. Experiment Results

A total of 103 participants were conducted for the experiment, they create their accounts and provide some basic personal information such as name, gender, age,email, and education level. Then they were drawn four image passwords. 92 participants logged into their systems two times. Finally, 78 participants filled the questionnaire. The participants were 25 females and 78 males as shown in Figure 5.1

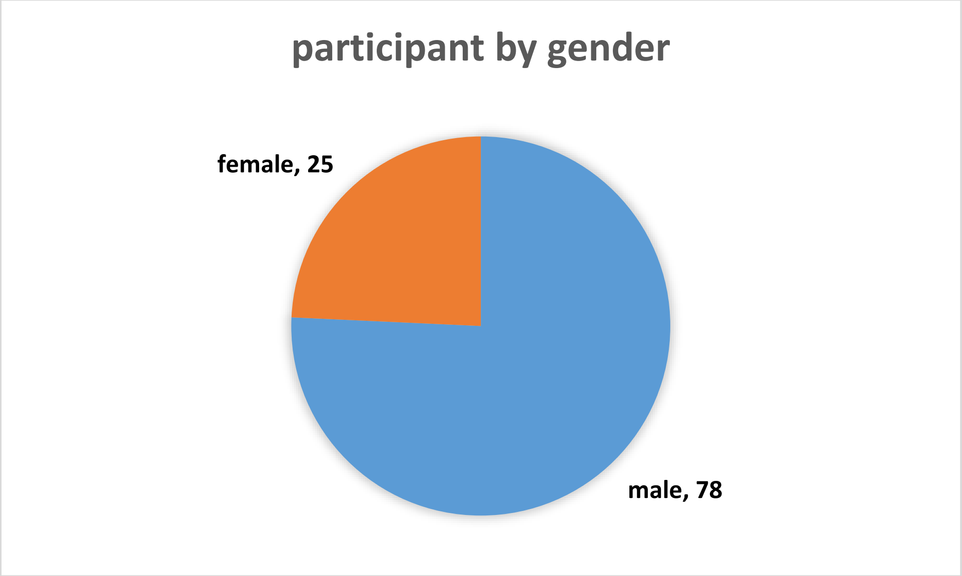


Figure 5.1 Participants by gender

The ages of participants were between 15 and 64 years as illustrated in figure 5.2

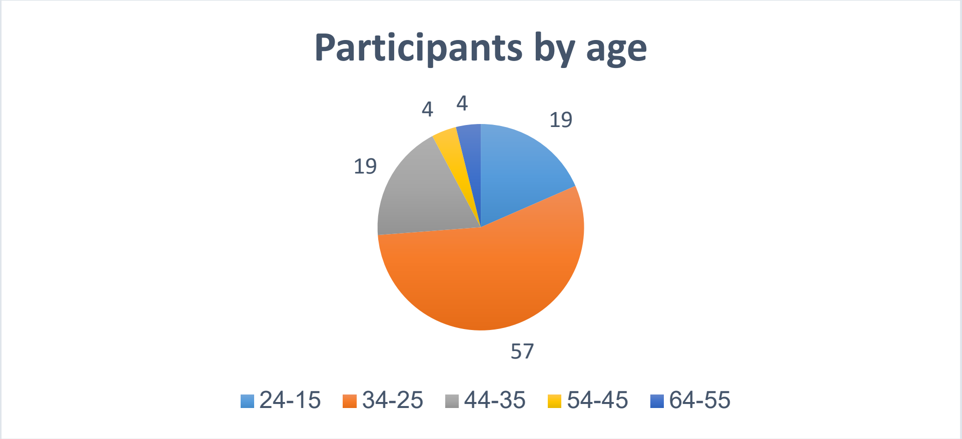


Figure 5.2 Participants by age group

As shown in Figure 5.3. The qualifications of the participants in this study are vary, 71 of participants were undergraduate, 11 of them hold a master degree, where 14 of participants hold a high school qualification, and seven participants hold a primary school certificate.

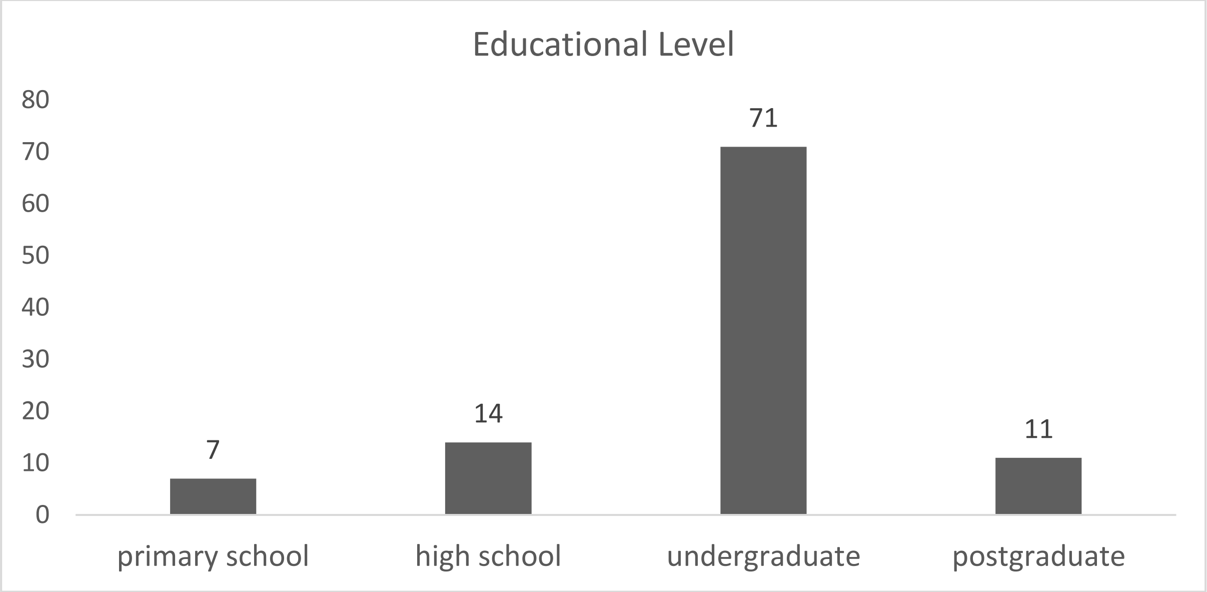


Figure 5.3 Participants by educational level

In this experiment, most of the participants use a smartphone device as shown in figure 5.4, where seven participants use tablet devices, and 10 participants use laptop and desktop computers.

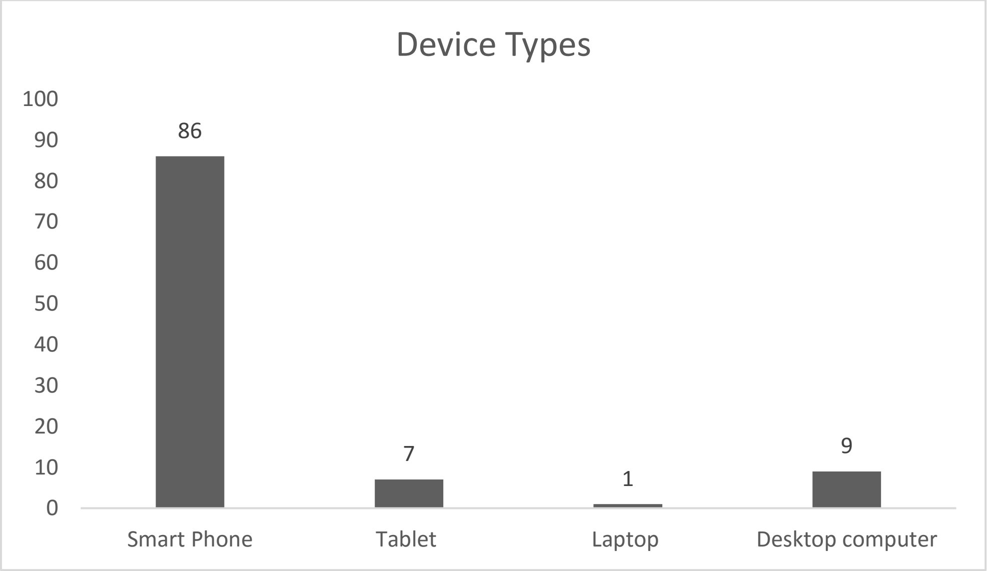


Figure 5.4 Participants by device types

According to the extensive spreading of Android based smartphones, which came with pre-installed Google chrome browser, most participants favor to google chrome browser, also in this experiment; participants who own iPhone or iPad favor to use Safari web browser, whereas only seven participants use a Mozilla Firefox internet browser.

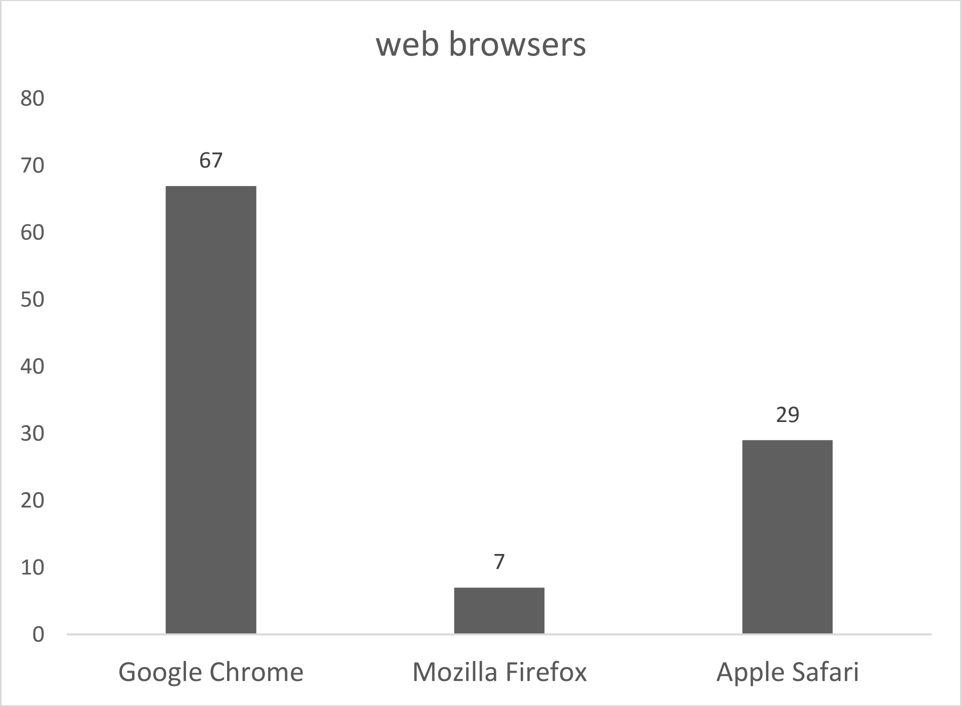


Figure 5.5 Participants by web browser

5.3.1. Dropout Participants

Some participants dropped out at various phases during the experiment. two participants (1.94%) dropped out at the first authentication phase which appointed after two weeks of the registration phase. In second authentication phase which appointed after four weeks from registration phase; nine participants (8.91%) dropped out. Finally, among 92 participants who completed the authentication phases; 14 participants (15.21%) failed to submit a questionnaire, leaving 78 participants who completed all stages of the experiment. Most of the dropouts occurred during the second authentication phase. The researcher sends messages to the participants via SMS and Facebook Messenger; The reasons for dropping out could not be determined. It could be related to an internet connection, or because they lost interest in completing the experiment.

5.3.2. Effectiveness of the model

In this proposed model; The effectiveness was evaluated by the number of participants who have completed all the phases of the experiment without dropping out. Table 5.1 shows the number of participants who have completed each stage of the experiment.

Table 5.1 Phase Completion

Phase	Number
Creating account	103
Drawing image passwords	103
First authentication phase	101
Second authentication phase	92
Return Questionnaire	78

5.3.3. Efficiency of the model

The model efficiency is measured by the time required to complete each stage. The model is efficient if the participant can complete tasks in a reasonable amount of time. This experiment measured the time of each stage of the experiment as shown in Table 5.2

Table 5.2 Average Times Of Task Completion

Phase	Time(min:sec)
Creating accounts	1:05
Drawing image passwords	3:10
First authentication phase	1:55
Second authentication phase	1:28

5.3.4. Security of the model

Graphical password systems are vulnerable to many attacks. Table 5.3 describes the procedures which implemented to prevent attacks on the proposed model.

Table 5.3 implemented procedures against security attacks

Security Attack	Procedure
Dictionary	The user can only input the password choice by keyboard only.
Brute Force	The model gives the users three trials only of authentication
Intersection	The model prevents the user from refreshing the web page
Shoulder-Surfing	Users can only enter their choices by keyboard in textbox password mode, to avoid the observation of other people.
Social Engineering	The model does not allow users to choose their photos as password. Also the users has been urged to avoid drawing things related to them.

5.3.5. Authentication Rates

The authentication rates are shown in Tables 5.4. This study used data from users who completed each login phase. The first authentication phase was after two weeks from registration, and the second phase of authentication was after six weeks from registration.

Table 5.4 Authentication Rates

Phase	Participants	Success	Fail	Success rate
First authentication	101	85	16	84.15%
Second authentication	92	78	14	84.78%

Success and failed authentication rates which categorized by the property are shown in Table 5.5. This study used data from 92 participants who completed all authentication stages.

Table 5.5 Authentication-Results by property

Property	success	failed
Gender		
Male	59	11
Female	19	3
Age group		
15-24	14	3
25-34	43	9
35-44	15	1
45-54	3	1
55-65	3	0
Education Level		
Primary School	2	0
High School	15	3
Undergraduate	53	10
Postgraduate	8	1
Device Type		
Smartphone	65	12
Tablet	7	0
Laptop	1	0
Desktop computer	5	2
Browser		
Google Chrome	50	9
Mozilla Firefox	5	2
Apple Safari	23	3

5.3.6. Evaluation of the proposed model

In order to evaluate the proposed model; participants who used the proposed system filled an online questionnaire survey. This study used a questionnaire in closed forms of questions; these questions asked participants about their experience of using the proposed system, and how usable they thought it was. The questions were based on previous studies (Tullis and Stetson, 2004), (Lewis, 1995), These questions were based on the System Usability Scale (SUS), which developed by Digital Equipment Corp. This scale can be used for global assessments of systems usability. SUS (System Usability Scale) consists of ten questions. Each question on this scale is a statement, and each question has a rating on a five-point scale of “Strongly Disagree” to “Strongly Agree”. This scale is adapted by replacing the word “system” in every question with “website”.

The SUS questions 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 5 point Likert scale, which shown in Table 5.6

Table 5.6 Likert Scale

Strongly Disagree	Disagree	Neither	Agree	Strongly Agree
1	**2**	**3**	**4**	**5**

The questions have been translated into the Arabic language to allow none English speaker to understand the questionnaire. 78 participants who represent (84.78%) from participants who completed all authentication phases; answered all ten questions. The results are shown in Table 5.7.

Table 5.7 Questionnaire Results

Usability Questions		Weighted Average	Mode	Std.Deviation
1.	I think that I would like to use this website frequently.	3.99	4	0.693
2.	I found the website unnecessarily complex.	1.91	2	0.776
3.	I thought the website was easy to use.	4.10	4	0.799
4.	I think that I would need the support of a technical person to be able to use this website.	1.97	2	0.738
5.	I found the various functions in this website were well integrated.	3.81	4	0.646
6.	I thought that there was too much inconsistency in this website.	1.99	2	0.592
7.	I would imagine that most people would learn to use this website very quickly.	3.81	4	0.740
8.	I found the website very cumbersome to use.	1.79	2	0.567
9.	I felt very confident using the website.	3.95	4	0.737
10.	I needed to learn a lot of things before I could get going with this website.	2.04	2	0.813

It can be noted that the lowest weighted average and mode was for the only negative-type questions (2,4,6,8,10). i.e.: ' I found the website very cumbersome to use,' with a weighted average score of 1.79 (mode=2). It is also clear that the top variables scoring the highest weighted average of 4.10 (mode = 4) were 'I thought the website was easy to use' and the variable scoring the second highest a weighted average of 3.99 (mode = 4) was 'I think that I would like to use this website frequently.'. These figures indicate that online users found the proposed method mechanism was usable. However, questions (1,3,5,7,9) scored highly, and all the negative questions (2,4,6,8,10) had low scores. Thus, the participants were satisfied with the website of the proposed method. More details about survey results can be found in appendix B.

5.4. Statistical Analysis

Each question results of the questionnaire has been analyzed using one sample t-test. A one-sample t-test is used to determine whether a population mean is significantly different from some hypothesized value. Table 5.8, 5.9 shows the results of the statistical analysis.

Table 5.8 One-Sample Statistics

	N	Mean	Std. Deviation	Std. Error Mean
Q1	78	3.99	.693	.078
Q2	78	1.91	.776	.088
Q3	78	4.10	.799	.090
Q4	78	1.97	.738	.084
Q5	78	3.81	.646	.073
Q6	78	1.99	.592	.067
Q7	78	3.81	.740	.084
Q8	78	1.79	.567	.064
Q9	78	3.95	.737	.083
Q10	78	2.04	.813	.092

Table 5.9 Results on one sample t-test

Question	Test Value = 2.5					
	t	df	P-value	Mean Difference	95% Confidence Interval of the Difference	
					Lower	Upper
Q1	18.951	77	.000	1.487	1.33	1.64
Q2	-6.712	77	.000	-.590	-.76	-.41
Q3	17.710	77	.000	1.603	1.42	1.78
Q4	-6.290	77	.000	-.526	-.69	-.36
Q5	17.883	77	.000	1.308	1.16	1.45
Q6	-7.650	77	.000	-.513	-.65	-.38
Q7	15.616	77	.000	1.308	1.14	1.47
Q8	-10.991	77	.000	-.705	-.83	-.58
Q9	17.367	77	.000	1.449	1.28	1.61
Q10	-5.014	77	.000	-.462	-.64	-.28

The sample has been tested with the following hypothesis:

11. Null hypothesis H_0: there is no significance difference between usability and useless of the model.
12. Alternative hypothesis H_1: there is significance difference between usability and useless of the model.

The value of alpha (the significance level) is typical to let alpha be 0.05.

From Table 5.9, the P-value of questions (1,3,5,7,9) is smaller than 0.05, which lead to rejecting the null hypothesis H0 and accept the alternative hypothesis H1, and the mean of these questions is greater than 2.5 which mean that there is satisfaction about these questions. Also, the P-value of questions (2,4,6,8,10) is smaller than 0.05; this is rejecting the null hypothesis H0 and accept the alternative hypothesis H1. The mean of these questions is lower than 2.5 which mean that there is dissatisfaction about these questions.

5.5. Discussion

The result of the proposed model was compared with the system of Jebreil and Poet (Jebriel and Poet, 2014). The system used two types of drawing, drawing using paper and scanner, and using computer paint program. In the proposed system; the average time for drawing pass images is 3 minutes and 10 seconds, where drawing images using paint programs in the system of Jebreil and Poet is 9 minutes which caused by using of external paint programs for drawing graphical passwords. In the authentication phase; the average time is 1 minute and 43 seconds in the proposed model, and 43 seconds in the system of Jebreil and Poet. This difference may refer to the skills of typing, and the various cultures of participants. The results of comparison with the proposed model are shown in Table 5.10.

Table 5.10 Comparison Between System Of Jebriel And The Proposed Model

Task	Jebriel & Poet System	The proposed model
	Time(min:sec)	Time(min:sec)
Creating account	1:46	1:05
Drawing images using scanner	16:00	3:10
Drawing images using paint program	9:00	
Login using scan system	1:07	1:43
Login using paint program	0:47	
Login success rates after two weeks(scan)	94%	84.15%
Login success rates after two weeks (paint)	91%	
Login success rates after four weeks (scan)	94%	84.78%
Login success rates after four weeks (paint)	94%	

Also, the study compared the registration phase of the proposed model with the passface scheme as shown in Table 5.11. According to ("Two Factor Authentication, Graphical Passwords - Passfaces," n.d.); that password creation time takes three to five minutes, on another hand in the proposed model, it takes 3 minutes and 10 seconds on average.

Table 5.11 creating image password using Passface and the proposed model

Task	Passface Scheme	The proposed model
	Time(min:sec)	Time(min:sec)
Average time for Creating image password	3:00 to 5:00	3:10

5.6. Summary

In this chapter, the results of the proposal method has been displayes and explained. Aslo, the reults has been compared with other studies.

Chapter Six

Conclusion and Future Works

This chapter conclude the thesis, and mention some proposals for future works.

6.1 Conclusion

This study investigated graphical passwords and problems related to graphical passwords. Also this thesis presented a recognition-based graphical authentication model as an alternative to replace text-based authentication systems. In this model, the users draw four image passwords using finger or stylus on touch-enabled devices. During Authentication, the users must recognize their image passwords from four challenge sets; each set contains 15 images selected randomly by the system and one target image. A prototype of the proposed model was implemented on a web platform using ASP.NET.

In chapter one, there are a question has been asked:

Can user-drawn passwords on touch-enabled devices support both usability and memorability?

103 participants who created accounts and drew images passwords, 11 participants (10.67%) dropped out during the authentication stages, the reasons for dropping out could not be determined, but it could be related to an internet connection. From 92 participants who completed the authentication phases; 84.78% of participants recognize their image passwords and successfully authenticated. 78 of participants who completed all experiment stages and returned a questionnaire. The results show that the users are satisfied with the website. That means the proposed model is usable and memorable.

6.2 Future work

This study proposed a web-based graphical authentication method and tried to make this model secure against some graphical password attacks. Much more research are necessary for testing this proposed model against all possible graphical password and internet attacks.

Also, this study unified the image drawing space by restricting the user for drawing image passwords by finger or stylus using a black pen on white background. More studies are required to investigate the memorability, usability, and security of multi-color image passwords. Also, in this study some users accessed the proposed model via internet browsers on their smartphones, which suffers from incompatibility in some web standards, more studies are required to investigate the usability and security of the proposed model via built-in application cross-smartphone platforms such as Android, iOS, and Windows phone.

References

Adams, A., & Sasse, M. A. (1999). Users are not the enemy. *Communications of the ACM, **42***(12), 40-46.

Berger, J., & Savage, J. (2005). *Berger on drawing*. Occasional Press Cork: Ireland.

Brostoff, S., & Sasse, M. A. (2000). Are Passfaces more usable than passwords? A field trial investigation. *People and Computers XIV—Usability or Else!* (pp. 405-424): Springer.

Cave, C. B. (1997). Very long-lasting priming in picture naming. *Psychological science, 8*(4), 322-325.

Cheswick, W. R., Bellovin, S. M., & Rubin, A. D. (2003). Firewalls and Internet security: repelling the wily hacker.

Cranor, L. F., & Garfinkel, S. (2004). Guest Editors' Introduction: Secure or Usable? *IEEE security & privacy, 2*(5), 16-18.

Davis, D., Monrose, F., & Reiter, M. K. (2004). *On User Choice in Graphical Password Schemes.* Paper presented at the USENIX Security Symposium.

De Angeli, A., Coventry, L., Johnson, G., & Renaud, K. (2005). Is a picture really worth a thousand words? Exploring the feasibility of graphical authentication systems. *International Journal of Human-Computer Studies, 63*(1), 128-152.

Dhamija, R., & Perrig, A. (2000). *Deja Vu-A User Study: Using Images for Authentication.* Paper presented at the USENIX Security Symposium.

Dirik, A. E., Memon, N., & Birget, J.-C. (2007). *Modeling user choice in the PassPoints graphical password scheme.* Paper presented at the Proceedings of the 3rd symposium on Usable privacy and security.

English, R. (2012). *Modelling the security of recognition-based graphical password schemes.* University of Glasgow.

Feingold, G. A. (1914). Influence of environment on identification of persons and things. *J. Am. Inst. Crim. L. & Criminology, 5*, 39.

Garfinkel, S., & Lipford, H. R. (2014). Usable security: History, themes, and challenges. *Synthesis Lectures on Information Security, Privacy, and Trust, 5*(2), 1-124.

Goldstein, A. G., & Chance, J. E. (1971). Visual recognition memory for complex configurations. *Perception & Psychophysics, 9*(2), 237-241.

Govindarajulu, N. S., & Madhvanath, S. (2007). *Password management using doodles.* Paper presented at the Proceedings of the 9th international conference on Multimodal interfaces.

Jadhao, P., & Dole, L. (2013). Survey on Authentication Password Techniques. *International Journal of Soft Computing and Engineering (IJSCE), 3*(2).

Jebriel, S., & Poet, R. (2014). *Automatic registration of user drawn graphical passwords.* Paper presented at the Computer Science and Information Technology (CSIT), 2014 6th International Conference on.

Jebriel, S. M. (2014). *Empirical approach towards investigating usability, guessability and social factors affecting graphical based passwords security.* ((Doctoral Dissertation)), University of Glasgow.

Jermyn, I., Mayer, A. J., Monrose, F., Reiter, M. K., & Rubin, A. D. (1999). *The Design and Analysis of Graphical Passwords.* Paper presented at the Usenix Security.

Knoblich, G., & Prinz, W. (2001). Recognition of self-generated actions from kinematic displays of drawing. *Journal of Experimental Psychology: human perception and performance, 27*(2), 456.

Koriat, A., Ben-Zur, H., & Nussbaum, A. (1990). Encoding information for future action: Memory for to-be-performed tasks versus memory for to-be-recalled tasks. *Memory & Cognition, 18*(6), 568-578.

Levin, D. T. (2000). Race as a visual feature: using visual search and perceptual discrimination tasks to understand face categories and the cross-race recognition deficit. *Journal of Experimental Psychology: General, 129*(4), 559.

Lewis, J. R. (1995). IBM computer usability satisfaction questionnaires: psychometric evaluation and instructions for use. *International Journal of Human*‐*Computer Interaction, 7*(1), 57-78.

Perrig, A., & Song, D. (1999). *Hash visualization: A new technique to improve real-world security.* Paper presented at the International Workshop on Cryptographic Techniques and E-Commerce.

Poet, R., & Renaud, K. (2009). An algorithm for automatically choosing distractors for recognition based authentication using minimal image types. *Ergonomics Open Journal, 2*, 178-184.

Radack, S. (2004). Electronic authentication: Guidance for selecting secure techniques. *ITL Bulletin. Gathersburg: National Institute of Standards and Technology*.

Renaud, K. (2006). A visuo-biometric authentication mechanism for older users *People and Computers XIX—The Bigger Picture* (pp. 167-182): Springer.

Renaud, K. (2009). On user involvement in production of images used in visual authentication. *Journal of Visual Languages & Computing, 20*(1), 1-15.

Renaud, K., & Smith, E. (2001). *Jiminy: helping users to remember their passwords.* Paper presented at the Annual Conference of the South African Institute of Computer Scientists and Information Technologists. SAICSIT.

Rittenhouse, R. G., Chaudry, J. A., & Lee, M. (2013). Security in graphical authentication. *International Journal of Security & Its Applications, 7*(3), 347-356.

R. U. Corporation. (2004). The science behind passfaces. Retrieved from http://www.realuser.com/published/ScienceBehindPassfaces.pdf

Shepard, R. N. (1967). Recognition memory for words, sentences, and pictures. *Journal of verbal Learning and verbal Behavior, 6*(1), 156-163.

Shneiderman, B., & Ben, S. (2003). Designing the user interface: Pearson Education India.

Sobrado, L., & Birget, J.-C. (2002). Graphical passwords. *The Rutgers Scholar, an electronic Bulletin for undergraduate research, 4,* 2002.

Suo, X. (2006). A design and analysis of graphical password.

Suo, X., Zhu, Y., & Owen, G. S. (2005). *Graphical passwords: A survey.* Paper presented at the 21st Annual Computer Security Applications Conference (ACSAC'05).

Tao, H. (2006). *Pass-Go, a new graphical password scheme.* (Master thesis), University of Ottawa (Canada).

Thorpe, J., & van Oorschot, P. C. (2004). *Towards secure design choices for implementing graphical passwords.* Paper presented at the Computer Security Applications Conference, 2004. 20th Annual.

Towhidi, F., & Masrom, M. (2009). A Survey on Recognition Based Graphical User Authentication Algorithms. *arXiv preprint arXiv:0912.0942*.

Tullis, T. S., & Stetson, J. N. (2004). *A comparison of questionnaires for assessing website usability.* Paper presented at the Usability Professional Association Conference.

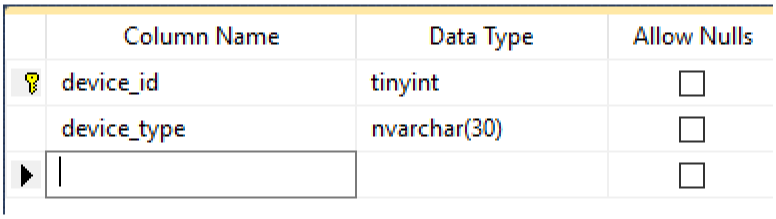
usability.org. 2016, from http://www.usabilitynet.org/tools/r_international.htm#9241

Valentine, T. (1999). An evaluation of the Passface personal authentication system, Goldsmith College Univ: of London, Tech. Report.

Zwicky, E. D., Cooper, S., & Chapman, D. B. (2000). Building internet firewalls.

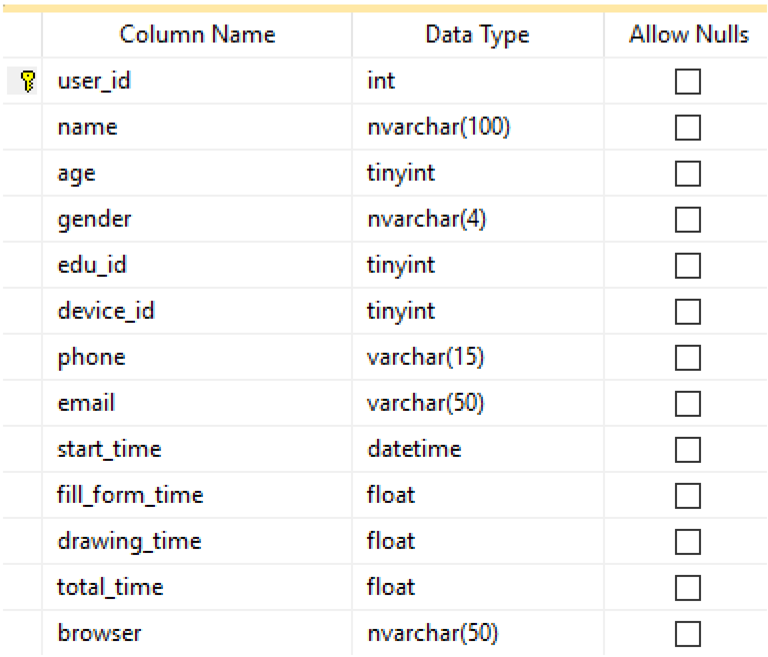
Appendix A

A.1Model database tables



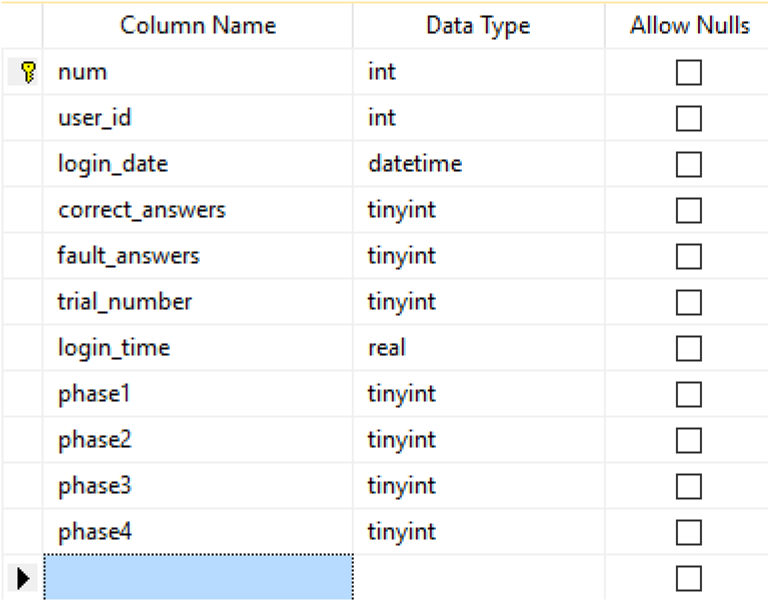
	Column Name	Data Type	Allow Nulls
🔑	device_id	tinyint	□
	device_type	nvarchar(30)	□
▶			□

Figure 1 Devices table



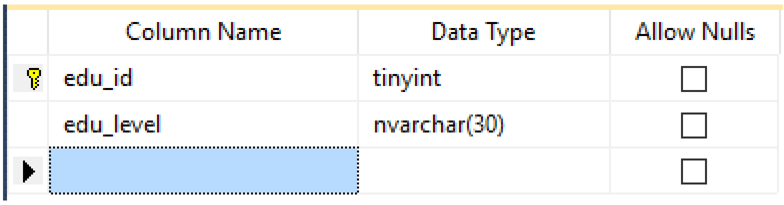
	Column Name	Data Type	Allow Nulls
🔑	user_id	int	□
	name	nvarchar(100)	□
	age	tinyint	□
	gender	nvarchar(4)	□
	edu_id	tinyint	□
	device_id	tinyint	□
	phone	varchar(15)	□
	email	varchar(50)	□
	start_time	datetime	□
	fill_form_time	float	□
	drawing_time	float	□
	total_time	float	□
	browser	nvarchar(50)	□

Figure 2 Users table



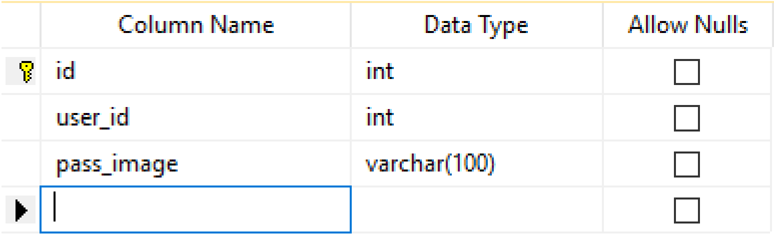
	Column Name	Data Type	Allow Nulls
🔑	num	int	□
	user_id	int	□
	login_date	datetime	□
	correct_answers	tinyint	□
	fault_answers	tinyint	□
	trial_number	tinyint	□
	login_time	real	□
	phase1	tinyint	□
	phase2	tinyint	□
	phase3	tinyint	□
	phase4	tinyint	□
▶			□

Figure 3 Login transactions table



	Column Name	Data Type	Allow Nulls
🔑	edu_id	tinyint	□
	edu_level	nvarchar(30)	□
▶			□

Figure 4 Education levels table



	Column Name	Data Type	Allow Nulls
🔑	id	int	□
	user_id	int	□
	pass_image	varchar(100)	□
▶			□

Figure 5 User pass images table

Appendix B

B.1 Survey Frequency tables

- I think that I would like to use this website frequently.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Disagree	1	1.3	1.3	1.3
	neutral	16	20.5	20.5	21.8
	agree	44	56.4	56.4	78.2
	Strongly agree	17	21.8	21.8	100.0
	Total	78	100.0	100.0	

- I found the website unnecessarily complex.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Stongly Disagree	25	32.1	32.1	32.1
	Disagree	37	47.4	47.4	79.5
	neutral	14	17.9	17.9	97.4
	agree	2	2.6	2.6	100.0
	Total	78	100.0	100.0	

- I thought the website was easy to use.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Disagree	3	3.8	3.8	3.8
	neutral	12	15.4	15.4	19.2
	agree	37	47.4	47.4	66.7
	Strongly agree	26	33.3	33.3	100.0
	Total	78	100.0	100.0	

- I think that I would need the support of a technical person to be able to use this website.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Stongly Disagree	19	24.4	24.4	24.4
	Disagree	45	57.7	57.7	82.1
	neutral	11	14.1	14.1	96.2
	agree	3	3.8	3.8	100.0
	Total	78	100.0	100.0	

- I found the various functions in this website were well integrated.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Disagree	2	2.6	2.6	2.6
	neutral	19	24.4	24.4	26.9
	agree	49	62.8	62.8	89.7
	Strongly agree	8	10.3	10.3	100.0
	Total	78	100.0	100.0	

- I thought that there was too much inconsistency in this website.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Stongly Disagree	11	14.1	14.1	14.1
	Disagree	60	76.9	76.9	91.0
	neutral	4	5.1	5.1	96.2
	agree	3	3.8	3.8	100.0
	Total	78	100.0	100.0	

- I would imagine that most people would learn to use this website very quickly.

Q7

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Disagree	1	1.3	1.3	1.3
	neutral	27	34.6	34.6	35.9
	agree	36	46.2	46.2	82.1
	Strongly agree	14	17.9	17.9	100.0
	Total	78	100.0	100.0	

- I found the website very cumbersome to use.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Stongly Disagree	21	26.9	26.9	26.9
	Disagree	53	67.9	67.9	94.9
	neutral	3	3.8	3.8	98.7
	agree	1	1.3	1.3	100.0
	Total	78	100.0	100.0	

- I felt very confident using the website.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Disagree	2	2.6	2.6	2.6
	neutral	17	21.8	21.8	24.4
	agree	42	53.8	53.8	78.2
	Strongly agree	17	21.8	21.8	100.0
	Total	78	100.0	100.0	

- I needed to learn a lot of things before I could get going with this website.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Stongly Disagree	17	21.8	21.8	21.8
	Disagree	47	60.3	60.3	82.1
	neutral	9	11.5	11.5	93.6
	agree	4	5.1	5.1	98.7
	Strongly agree	1	1.3	1.3	100.0
	Total	78	100.0	100.0	