

User Authentication System Using Emoji pictures passwords

" نظام مصادقة المستخدم باستخدام الصور التعبيرية "

Prepared by

Raghda Ahmed Malih

Supervised by

Dr. Mohammed Abbas Fadhil Al-Husainy

**A Thesis Submitted in Partial Fulfillment of the Requirements for
the Master Degree in Computer Science**

**Department of Computer Science Faculty of Information Technology
Middle East University Amman – Jordan**

May/2015

AUTHORIZATION STATEMENT

I, am Raghda Ahmed Malih, authorize Middle East University to supply hard and electronic copies of my thesis to libraries, establishments, or bodies and institutions concerned with research and scientific studies upon request, according to the university regulations.

Name: Raghda Ahmed Malih

Date: May 10th, 2015

Signature: 

إقرار تفويض

أنا رغبة احمد مالح أفوض جامعة الشرق الأوسط للدراسات العليا بتزويد نسخ من رسالتي ورقيا أو الكترونيا للمكتبات أو المنظمات أو الهيئات والمؤسسات المعنية بالأبحاث والدراسات العلمية عند طلبها .

الاسم : رغبة أحمد مالح

التاريخ: 2015 / 5 / 10

التوقيع : 

Examination Committee Decision

This is to certify that the thesis entitled "User Authentication System Using Emoji pictures passwords" was successfully defended and approved on May 10th, 2015

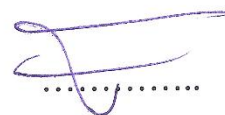
Examination Committee Members Signature

(Head of the Committee)

Prof. Ahmed Kayed

Professor, Dean of Faculty of IT,

Middle East University (MEU)



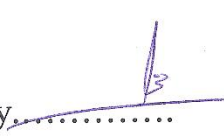
(Supervisor)

Dr. Mohammed Abbas Fadhil Al-Husainy.....

Associate Professor,

Computer Science Department, Faculty of IT

Middle East University (MEU)



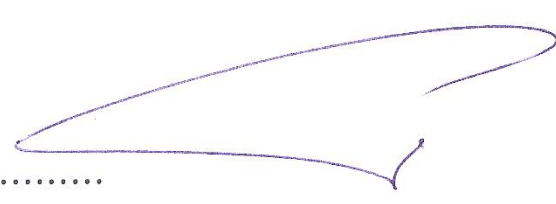
(External Examiner)

Dr. Mohammad Ahmad Alia.....

Associate Professor,

Computer Science Department, Faculty of IT

Al-Zaytoonah University



ACKNOWLEDGMENT

Praise and thanks to God to the completion of this work and After, I would like to specially thank my supervisor Dr. Mohammed A. F. Al-Husainy, who taught me everything that I know about research and the way it should be done. I would like to thank him for his guidance during all stages of this research, for answering endless questions, for his great support, professional advice, and profound understanding. Through this work, Dr. Mohammed A. F. Al-Husainy, has shown me how to attack a problem from different angles, how to approach it, and how to find the most suitable solution.

I also would like to thank all members of staff at Middle East University, in particular, the members of staff at the Graduate College of Computing Studies.

Finally, it would be unthinkable of me not to thank my parents, my husband dear Ammar Al-Izzi, children, brothers and friends for their support and encouragement over the years. I am thankful for anyone who supported me during my master study.

DEDICATION

This thesis is dedicated to my father, who taught me that the best kind of knowledge to have is that which is learned for its own sake. It is also dedicated to my mother, who taught me that even the largest task can be accomplished if it is done one step at a time. To my brothers, and to all friends who they supported me till finish this work. I lovingly dedicate this thesis to my husband dear, who supported me each step of the way.

TABLE OF CONTENTS

AUTHORIZATION STATEMENT.....	II
التفويض	III
EXAMINATION COMMITTEE DECISION.....	IV
ACKNOWLEDGMENT	V
DEDICATION.....	VI
TABLE OF CONTENTS.....	VII
LIST OF TABLES.....	IX
LIST OF FIGURES.....	X
الملخص.....	XII
ABSTRACT.....	XIII
Chapter One: INTRODUCTION.....	1
1.1 Information security.....	1
1.2 System security (user authorization using password)	1
1.3 Human brain remembering capability.....	2
1.3.1 Remember textual password	3
1.3.2 Remember graphical password	3
1.4 Attacks on password.....	4
1.5 Using classical in writing password	5
1.6 Using emoji pictures in writing password	5
1.7 Problem Statement.....	7
1.8 Objectives (contributions of this Work.....	8
1.9 Thesis Outline	10

Chapter Two: LITERATURE SURVEY AND RELATED WORKS	11
2.1 Introduction.....	11
2.2 Remember and save password graphical (Analytical track).....	11
2.3 Immunity of passwords against attackers (Technical track).....	16
Chapter Three: ANALYTICAL TRACK	28
3.1 Proposed model.....	28
3.2 Samples users participants in the analytical track.....	29
3.3 Registration in system.....	30
3.4 Part one: Textual passwords.....	31
3.5 Part two: Expressive emoji password.....	31
3.6 Characteristics of passwords in the system.....	32
3.7 Login to the system.....	33
3.8 The benefits of using emoji pictures in writing password.....	34
3.9 Results, analysis and discussion.....	36
Chapter Four: TECHNICAL TRACK	48
4.1 Proposed model (Authorization System Uses Emoji Pictures).....	48
4.2 Authorization system.....	49
4.2.1 Preparation operations.....	51
4.2.2 Login session.....	52
4.3 Compared the proposed model with previous studies research.....	57
4.3.1 Shoulder Surfing.....	57
4.3.2 Speed and time.....	59
4.3.3 Size of Data Base.....	59
Chapter Five: CONCLUSIONS	60
5.1 Analytical track	60
5.2 <i>Technical</i> track.....	61
REFERENCES	62

LIST OF TABLES

Table 3.1: Number of participants based on the academic achievement	37
Table 3.2: Number of participants based on age.....	37
Table 3.3: Voting for "textual password" based on academic achievement	38
Table 3.4: Voting for "emoji password" based on academic achievement.....	39
Table 3.5: Voting for "textual password" based on ages	40
Table 3.6: Voting for "emoji password" based on age.....	40
Table 3.7: Ratio of voting for "textual Password" based on the series of Login of participants	42
Table 3.8: Ratio of voting for "emoji Password" based on the Series of Login of participants	42
Table 3.9: Ratio of participants who forgot their password based on academic achievement	44
Table 3.10: Ratio of participants who forgot their password based on ages.....	45

LIST OF FIGURES

Figure 1.1: Different categories of emoji pictures	7
Figure 2.1: Login format after use of technique	12
Figure 2.2: Familiar and unfamiliar face.....	14
Figure 2.3: Pass faces based on the brain's innate ability to recognize	14
Figure 2.4: Déjà vu scheme.....	15
Figure 2.5: Click text image with 33 characters	16
Figure 2.6: Click animal images (left) & grid (right).....	16
Figure 2.7: User selection these regions once to produce the password.....	18
Figure 2.8: Choose the user must find 3 of the pass-images and click inside.....	18
Figure 2.9: Choose the face images that belong to password series	19
Figure 2.10: (CARP) five or six click points on an image can produce passwords.....	20
Figure 2.11: Login need that users recognize pictures from their portfolio.....	22
Figure 2.12: ATM system that uses the user signature image as password.....	23
Figure 2.13: Login form using the random character	24
Figure 3.1: Main page of the system.....	29
Figure 3.2: Two types of password accounts	30
Figure 3.3: Textual password.....	31
Figure 3.4: Emoji password	32
Figure 3.5: Level or remembering (Textual password)	33
Figure 3.6: Level or remembering (Emoji password).....	34
Figure 3.7: Example of emoji password with its phrase meaning (in different languages).....	36
Figure 3.8: Percentage of participants based on the academic achievement	37
Figure 3.9: Percentage of participants based on age	38
Figure 3.10: Percentage of voting for "textual Password" based on academic achievement.....	39

Figure 3.11: Percentage of voting for "emoji Password" based on academic achievement 40

Figure 3.12: Percentage of voting for "textual Password" based on Age 41

Figure 3.13: Percentage of voting for "emoji Password" based on Age 41

Figure 3.14: Percentage of voting for "textual Password" based on progress of Time..... 43

Figure 3.15: Percentage of voting for "emoji Password" based on progress of Time 43

Figure 3.16: Participants who forgot their "textual Password" based on academic achievement ... 44

Figure 3.17: Participants who forgot their "emoji Password" based on academic achievement 45

Figure 3.18: Participants who forgot their "textual Password" based age 46

Figure 3.19: Participants who forgot their "emoji Password" based age 46

Figure 3.20: Total percentage of participants who forgot password "textual & emoji password" ... 47

Figure 4.1: Tables (keyboard) of different classes of characters 51

Figure 4.2: Step1 and Step2 of login session 52

Figure 4.3: Step3 and Step4 of login session 53

Figure 4.4: Step5 of login session 54

Figure 4.5: Step6 and Step7 of login session 55

Figure 4.6: Step8 and Step9 of login session 56

" نظام مصادقة المستخدم بأستخدام الصور التعبيرية "

إعداد: رغبة أحمد صالح

إشراف: د. محمد عباس فاضل الحسيني

الملخص

كلمات السر لا تزال واحدة من أكثر الوسائل شيوعاً لتأمين أنظمة الكمبيوتر. كلمات المرور النصية والرسومية هي الوسائل التي تستخدم عادة لمصادقة المستخدمين في معظم نظم المعلومات. كلا كلمات المرور النصية والرسومية تعاني من عدد من السلبيات التي تعتبر من التحديات الكبيرة التي تواجه الباحثين في مجال أمن المعلومات ونظم الحاسوب. تقنية كلمة المرور الحيدة يجب أن تحقق العديد من العوامل: تعطي وسيلة سهلة للتذكر والتعامل مع كلمة المرور من قبل المستخدم، من الصعب سرقة وتخمين كلمة المرور عن طريق المهاجمين، توفير جلسة ادخال آمنة لكلمة المرور الخاصة بالمستخدم والتي تكون تتمتع بمقاومة ضد الأنواع المختلفة من الهجمات لكلمة المرور و لا تأخذ مساحة كبيرة في قاعدة بيانات نظام التوثيق لتخزين كلمات المرور. صور الرموز التعبيرية تستخدم على نطاق واسع وفعال في معظم الهواتف الذكية وأجهزة الكمبيوتر. تركز الدراسة على استخدام الصور تعبيرية، في كتابة كلمة المرور، لإيجاد الحلول والتغلب على المشاكل في كل من كلمات المرور النصية والرسومية وتحقيق كل العوامل اللازمة للحصول على كلمة سر جيدة. شملت الدراسة: المسار التحليلي الذي ركز على إثبات جدوى استخدام الصور الرموز التعبيرية في كتابة كلمة المرور وتسهيل عملية التذكر والتعامل مع كلمة المرور من قبل المستخدمين مجموع من المشاركين الذين نسبت كلمة المرور النصية كلمة المرور الخاصة بهم 74% وتعبيرية عن كلمة 26%. اقترح المسار الفني نموذج مصادقة للمستخدم لإدخال كلمة المرور، والتي تستخدم صور الرموز التعبيرية، من خلال تقديم جلسة ادخال لكلمة المرور بشكل آمن وممتع للمستخدمين. بالإضافة إلى تحقيق هدفين رئيسيين: زيادة قوة كلمة المرور بالمقارنة مع كلمة المرور النصية والحفاظ على حجم مقبول لكلمة المرور في قاعدة بيانات نظام التوثيق مقارنة مع الحجم الكبير المستخدمة في كلمة المرور الرسومية. النتائج المتحصل عليها من كلا المسارين التحليلي والتقني أثبتت نجاح الدراسة في تحقيق أهدافها المرجوة لحل مشاكل كلمات المرور النصية وكلمات المرور الرسومية والتغلب على الصعوبات للحصول على كلمة مرور جيدة. أثبتت هذه الدراسة مقاومة للكثف ركوب الأمواج وسهلة لتذكر كلمة المرور وكذلك إعطاء مساحة التخزين مقبولة في قاعدة البيانات .

الكلمات المفتاحية: الصور التعبيرية، المصادقة، كلمة المرور النصية، كلمة المرور الرسومية.

User Authentication System Using Emoji pictures passwords

Prepared by

Raghda Ahmed Malih

Supervised by

Dr. Mohammed Abbas Fadhil Al-Husainy

Abstract

Passwords are still one of the most common means of securing computer systems. Textual Password and graphical password are the means commonly used to authenticate users in most information systems. Both textual and graphical passwords suffer from a number of drawbacks which are considered as big challenges that face the researchers in the field of systems and information security. Good password technique must achieves many factors: gives an easy to remember and deal with password by user, hard to steal and guess password by attackers, provides safe login session for user that is resisting against different types of password attacks and doesn't take a large space in the authentication system database to store passwords. Emoji pictures are using extensively and effectively in most smart phones and computer devices. The study focuses on the use of Emoji pictures, in writing password, to find solutions and overcome the problems in both textual and graphical passwords and to achieve all the factors needed to get good password.

The study included: Analytical track which focused on demonstrate the feasibility of using Emoji pictures in writing password and facilitate the process of remembering and dealing with password by users. Total of participants who forgot their password textual password 74% and Emoji Password 26%. Technical track proposed a user authentication model for entering password, which is using Emoji pictures, through presenting an enjoyable and safe login session for users. In addition to achieve two main objectives: Increase the strength of password as compared with the textual password and maintain an acceptable size for the password in the authentication system database compared with the large size used in the graphical password. The results obtained from both analytical and technical tracks proved the success of the study in achieving its desired goals to solve the problems of textual and graphical passwords and to overcome the difficulties to get good password. This study proved resistant to shoulder surfing and easy to remember the password as well as give an acceptable storage space in the database.

Key words: Emoji pictures, Authentication, Textual password, Graphical password.

CHAPTER ONE

INTRODUCTION

1.1 Information security

Information security is one of the cornerstones of Information Society. Integrity and privacy of financial transactions, personal information and critical infrastructure data, all depend on the availability of strong and trustworthy security mechanisms. Network and Internet connectivity has provided great benefits to the modern society in terms of sharing and accessing information, one mechanism of information security that has been the subject of much attention in recent years is the security management of the assets of important information crucial challenge. Organizations also provide clients with access everywhere for information systems and the frequency and the evolution of security threats are growing, and the need to provide security assume greater importance. Effective information security management requires security resources, including the prevention of the attack, and reducing vulnerability and threat deterrence (Nazareth, Derek & Choi, 2015)

1.2 System security (user authorization using password)

Authentication predominant technique by which user is securing access to computer systems is realized. One study reports that the average user has approximately 25 online accounts that require passwords (Dunphy ,p,2012) . It must enter an average of eight passwords per day so attacks on the computer infrastructures are becoming an increasingly serious problem nowadays, therefore several information security techniques are available today to protect information systems against unauthorized use, duplication, alteration, destruction and viruses' attacks. (Abraham, Grosan & Chen 2006).

Therefore, information security management has become one of the most pressing issues facing businesses in today's competitive information technology (IT)-driven world. User authentication serves as the first defense against security breaches. As one of the most common authentication methods, passwords help to

secure information by granting access only to authorized parties (Jie, Xin, Somasheker, J 2009).

Password is a secret word or string of characters (numbers, letters and special symbols) that is used for authentication, to prove identity or gain access to a resource (Ari, Ronald, 2013).

In order to serve as an effective authentication method, passwords must be strong, secret, and memorable. 'Strong' passwords are those that are difficult for others to guess; 'secret' passwords are hard for others to locate and obtain; and 'memorable' passwords are those that users can easily remember.

Human factors are often considered the weakest link in a computer security system. (Patrick, long & flinn, 2003) point out that there are three major areas where human computer interaction: authentication, security operations, and developing secure systems focus on the authentication problem. The most common computer authentication method is for a user to submit a user name and a text password. The vulnerabilities of this method have been well known. One of the main problems is the difficulty of remembering passwords. Studies have shown that users tend to pick short passwords or passwords that are easy to remember, these passwords can be easily guessed or broken by the password crackers, passwords that are hard to guess or break are often hard to remember. Studies showed the user can only remember a finite number of passwords; they tend to write them down or will use the similar passwords for various accounts.

1.3 Human brain remembering capability

Human brain can store a tremendous amount of information in a century 21 where people face with the need to remember numbers or personal identification information in everyday tasks and often difficult because of the limitations of human memory. As a knowledge-based authentication mechanism, passwords depend on human memory (Rob J.,Jane L.M. & Karen 2014).

Tests the effects of presentation modality and learning style preference on people's ability to learn and remember unfamiliar melodies and sentences. Also, as expected, meaningful sentences were learned faster and remembered best than less

meaningful ones. Also, musicians learned meaningful melodies faster and remember them better than less meaningful melodies (Korenman, & Peynircioğlu 2007).

What applies to remember melodies applies in the same way to remember passwords of various kinds such as textual passwords and graphical passwords as will be explained in the following paragraphs.

1.3.1 Remember textual password

It was found that 80% of people forget their passwords if the password hard to guess. The underlying reasons behind the forgetfulness or hard to remember password is the incidence of psychological theories, time passing and interventions with other information in long-term memory (Taneski, v, et,al 2014).

1.3.2 Remember graphical password

Human beings live and interact in an environment wherever the sense of sight is predominant for many activities; our brains are capable of processing and storing massive amounts of graphical data with ease. While may find it difficult to remember a series of fifty characters, easily able to remember the faces of individuals, places we visited, and things we've seen. This graphical information represents immeasurable bytes of data and thus provides a massive password spaces. A graphical password is an authentication system that works by having the user chooses from images (Nithya, 2014). People have been shown to have a remarkable ability to remember particular images in long-term memory, be they everyday scenes, objects and events, or the shapes as most of us would expect (Isola, p, et, al 2011). Hence, visual memory which plays an important role in understanding and generating image description where graphical passwords are an alternative to alphanumeric (textual) passwords as the human brain remembers images better than text where high accuracy is more precise than words (Xinlei Chen, C. Lawrence Zitnick, 2014).

1.4 Attacks on password

Password security is most important in user authentication systems. Different types of passwords like textual password which is the most commonly used for user authentication on different systems. By selecting username and password, one can register their account on system, to successfully login on the system, the user must recall that password. If the selected password is strong, different attacks that reveal password can be avoided. However, if the selected password is weak, it can be vulnerable to various types of attacks. If same password is used across different systems and once that password is revealed, adversary may get access into these different systems. Therefore, different researchers studied various types of passwords, their benefits and drawbacks, how they are vulnerable to different types of attacks (Khairnar & Bhale, 2014). Several studies have appeared in recent years focus on password protection based on authentication of the smart card systems to ensure safe and reliable connection. But these schemes have failed to meet the security attributes desired (Mishra & Dheerendra 2015). Several attacks against the passwords are applied (Mohammed, H., et.al 2015) included the most common attacks:

- Stolen Passwords
- Stolen Password Hashes File
- Poor/Easily Guessable Passwords
- Repeated Password Use

Because of the problems previously mentioned in the techniques that used password in terms of difficulty of keeping and remember password and increase the probability of password theft and unauthorized access by hackers. Many researchers tried to present new types of passwords like: graphical password that focuses of using pictures to determine specific points in the pictures that represent the password, this might leads to make password easy to remember by users and hard to guess by attackers, The biggest drawback for graphical passwords is that the shoulder surfing problem. In spite of graphical passwords are hard to guess, and a person who observes a few login sessions could, depending on the scheme, knows the password. Shoulder surfing is watching over users' shoulders as they process data. Observing the keyboard as users types their password, or views personal information because of

their graphic nature, in general all the graphical password schemes are truly vulnerable to shoulder surfing. Other researchers tried to use Emoji pictures which are a new promising orientation in writing password. In this study, a new scheme of using Emoji pictures in writing password was presented and a model that facilitates users to enter their new Emoji password in an easy and safer manner was built.

1.5 Using textual symbols in writing password

Authentication is process of determining whether someone or something is, in fact who or what to be declared. Authentication mostly textual passwords are used. Passwords are the most commonly used method for identifying users in computer and communication systems. Typically, passwords are strings of letters and digits, they are alpha-numeric. If user chooses a hard password, this makes a password hard to remember. On the other hand, when user chooses passwords that are easy to remember, this will make the password vulnerable to guess easily by attackers. Classical passwords are required to satisfy two contradictory requirements. They have to be easily remembered by a user, while they have to be hard to guess by impostors. Users are known to choose easily guessable and/or short text passwords, which are an easy target of dictionary and brute-forced attacks. Enforcing a strong password policy sometimes leads to an opposite effect, as a user may resort to write his/her difficult-to-remember passwords on sticky notes exposing them to direct theft (Priti Jadhao, Lalit Dole, 2013).

1.6 Using Emoji pictures in writing password

In 1999, users of cellphones in Japan were using picture messages as a way to communicate increasingly. Mobile phone companies spotted this behavior because pictures are much larger than text messages. The size of hundreds if not thousands of text messages may represent the size of a single picture message. The needs of 80 million users forced the mobile operators to struggle for provision a rapidly growing technology to the users. Engineers when asked to fix this problem. The solution is Emoji pictures. Emoji pictures were born in a Japanese research facility.

Users became delighted at having emoticons at their fingertips. Emoji made their text 'come alive'. Emoji is the Japanese term for picture characters. These

"picture characters" are standardized and built into most handsets. Therefore, Emoji pictures can roughly be translated to standardized icons with a meaning. What makes Emoji picture special is that it was developed by scientists? What is the biggest difference between emoji pictures and emoticons?

Emoji: Codes meant to be read and transferred by computers then decoded into Pre-Defined images users can see.

Example: 🙌👩

Emoticons: They are user created images from text so the possible combinations are infinite.

Example: \(^o^)/ (^-^)/

Emoji pictures are used a lot like the way emoticons are used now. They can be used in the same ways but they are largely different. The word Emoji means "picture letter" in Japanese. Emoji pictures are the type of expressions used on iPhone, iPad, Android, Mac OS X and Windows 8: small pictures used in texts to communicate a feeling or an idea. Emoji pictures are classified into many categories such as: People Emoji, Nature Emoji, Objects Emoji, Places Emoji Symbols Emoji, and New Emoji (see figure 1.1). Nowadays, Emoji pictures are used widely in the various applications include Facebook, Google Hangouts, and WhatsApp, message, Snap chat and Instagram.



Figure 1.1: Different categories of Emoji pictures.

Using Emoji pictures gives users highly expressive manner to represent their feelings by pictures in plain text, such as SMS text messages, and e-mail messages. Also used similar techniques (embedded graphics or signs fled set expressions). As in December 2008, there are 110.4 million mobile phone users in Japan (about 87% of the population), and about 90.6% of mobile phones are using the Internet to enable the G3 used widely expressive symbols especially by people under 30 year (Markus S, Mark D& Kat M, Darick T, 2009).

1.7 Problem statement

Textual Password: Choose simple and meaningful password is easy to use and easy to remember by the user, but the problem is that the detection operation of the password by attackers becomes easy and this will lead to penetrate the account by attackers. On the other hand, choosing strong password has no meaning (consists of

random characters) is difficult to detect and penetrate the account by the attackers. But focus on choosing password too complex has the opposite effect. The problem is the difficulty of remembering and conserving it by the user because it consists of random characters and has no meaning. This sometimes leads to a self-destruction of the password security, some users in order to remember their complex password simply they write it down on a small note paper and paste it on the computer screen or on their desk, or using a common password for multiple accounts. Variety surveys about password security widely reported these bad behaviors of users.

The problem of forgetting password can be a big one. Particularly if you work in an environment which involves remembering a large number of new words daily. Terrible calamity indeed! The problem of forgetting passwords.

Graphical Password: A graphical password is simpler than a textual password for many individuals to recollect. The focus here is on the use of the password by selecting sequential images on different screen pages. If there are several pictures on every page, a hacker must try every possible combination at random. Also, there were many other schemes that are suggested by researchers using graphical password. But there are a number of challenges in using graphical password such as: the login session should not takes long time and easy for the use by users, the technique used in entering password must be resistant to shoulder surfing and the storage space needed to store images must be not too large.

1.8 Objectives (contributions) of this work

This study presents a new technique that involves the use of Emoji pictures in writing password. From the above problems which are relate to the difficulties that the user face in selecting and dealing with password emerged the idea of this research which focuses on two tracks: Analytical track and Technical track. The integration between analytical and technical phases helped to find the right solutions to overcome these difficulties. The main objectives in each track of this work are summarized follows:

Analytical track:

1. Keep up with technological development through the use of graphical characters that have become available through mobile phones smart devices.
2. Try to achieve a form of confusion or blackout about the characters used in writing the password.
3. Try to convert the meaning of the password (for the user) from a string of characters without meaning to the phrase of meaningful words.
4. Facilitate the process of selecting, recording and remember the user's password without raising any doubts from attackers about the existence or the nature of the password used.

Technical track:

1. Raise the complexity of the password (i.e., number/range of available symbols used by user in writing password).
2. Improve the immunity of the password against attackers by adding more ambiguity and confusion about the reality of the password.
3. Facilitate the session of enter password by the user and make this session enjoyable and more secure.
4. Provide a new scheme for enter password that achieve a resistance against the shoulder surfing attack.
5. Achieve a balance in the storage space needed to store the new Emoji password. Where the space needed to store the new Emoji password is between the size of textual password and graphical password.

1.9 Thesis outline

This thesis consists of five chapters that organized to give simple and clear presentation for the problem, solution, method of implementation, results and recommendations. The thesis was organized as follows:

Chapter One: *Introduction* - This chapter introduces the motivations and goals of this thesis. Readers are introduced to the problem of password management and the difficulties related.

Chapter Two: *Literature survey and related works* - This chapter provides background information about the various efforts of researchers in this field.

Chapter Three: *Analytical track* - This chapter presents the methodology/model used in the analytical phase of the thesis, its design, how it works, selected samples of users/participants, criteria used for evaluation and the recorded results.

Chapter Four: *Technical track* - This chapter explains the methodology/model used in the technical phase of the thesis, its design, how it works, capabilities that the model provides, how it achieves the desired goals of the thesis.

Chapter Five: *Conclusions* - This chapter provides conclusions that been derived from the thesis and sheds light on the possible future works.

CHAPTER TWO

LITERATURE SURVEY AND RELATED WORK

2.1 Introduction

Usually, users' accounts are affected by the improper selection of passwords and lack of awareness about the correct dealing with passwords. This will result to unauthorized entry to the user's personal account. In order to supply secure and user friendly authentication, the security experts are highly recommending the new graphical passwords, which include clicking or dragging activities on the pictures rather than typing alphanumeric characters which overcomes most of the problems that arise from the textual password system. There are many researchers that have attempted and successfully used graphical characters through different techniques. The majority of efforts are now employed to protect data from theft, but how can make them effective is an important issue.

2.2 Remember and save password graphical (Analytical track)

Prasad, k, & Babu, R, (2013) have been proposed changing authentication technique from textual passwords to graphical authentication technique. For security concerns, passwords have to be protected from the unauthorized users. Authentication and authorization are necessary for primary data, this requires authentication techniques. A main goal of authentication is to give users an easy manner to save and recall their passwords either textual or graphical authentication. A main usability goal for knowledge-based authentication systems is to support users in selecting passwords for higher level security. Textual passwords are higher usability than the graphical authentication technique based on the user perspective in some of the studies. The current graphical password techniques are still in the early stages. Intensive researches and studies about user behaviors are needed in choosing and dealing with graphical password techniques to achieve a higher level of security and protection.

The main aim of Mathur, A, (2011) is to lay stress on the security issues related to password selection and management. The idea is to give the users of web sites an option to choose the password along with their font color. The passwords must not only represent with at least 6 characters scheme, but also with color coded pattern that can be beneficial to improve the security of password. Basic colors including black, red, and white can be adopted to double the password protection to be saved from frauds that happen due to unauthorized access by stealing computer programs. This unauthorized access can be prevented by using colored alphanumeric passwords. The basic colors of red, black and white won't increase the size of the website and would also not slow down the identification process on the web sites but they do not use it for graphical characters (see Figure 2.1).

USERNAME:	abcde
DEFINED PASSWORD:	123abc
COLOR CODING:	
FINAL PASSWORD:	1 2 3abc or 123abc or 123abc

Figure 2.1(Mathur, A): Login format after use of technique

Xiong, Jianwei, Muhammad & Junguo (2013) have been suggested use a smart card for password authentication which is one of the simplest and efficient authentication mechanisms to ensure secure communication in insecure network environments. Lately, Chen et al. proposed a robust smart card based on remote user password authentication scheme to better the security. As per their claims, their scheme is active and can ensure forward secrecy of the session key. However, we find that Chen et al.'s scheme cannot truly ensure forward secrecy, and it cannot detect the wrong password in login phase. In addition, the password change phase of Chen et al.'s scheme is unfriendly and inefficient where the user needs to communicate with the server to update his/her password.

Seděnka ,J, et, al, (2014) present a new technique for biometric key generation (BKG) algorithm suitable for continuous authentication. This is the first technique suitable for the continuous key generation. The approach is based on a scaled parity code, and can be augmented with the use of data to improve security and reduce error. In particular result show that biometric key generation technique has a low error rate (between 3.6% and 5.5%), and presents limited overhead.

Priti & Lalit (2013) presented a little number of graphical password schemes that offer resistance to shoulder surfing. While it is usually possible to ensure that there are no people looking over one's shoulder at the time of login, the value of graphic passwords as an alternative to textual passwords diminishes somewhat if they can be used in authentication password techniques used for security purpose. As authentication techniques generate passwords, but they have to face attacks like dictionary attacks, brute force attacks, shoulder surfing. Authentication needs more powerful authentication techniques which remove all drawback of as mentioned above in authentication password techniques.

Rob,Jane&Karen,(2014), in two studies, tested a knowledge-based authentication system that exploits the psychological contrast between familiar and unfamiliar face recognition. In Study 1 they found that account holders were able to generate target faces that were well known to themselves, but were not well known to other people. Account holders authenticated easily by detecting these familiar targets among other faces (97.5% success rate), and this was the case even after a one-year delay (86.1% success rate). In Study 2 they found that optimal shoulder-surfing attacks by strangers, could be repelled simply by using different photos of the targets in the observed and attacked grids (1.9% success rate). These findings propose that the contrast between familiar and unfamiliar face recognition may be useful for graphical authentication systems (see Figure 2.2).

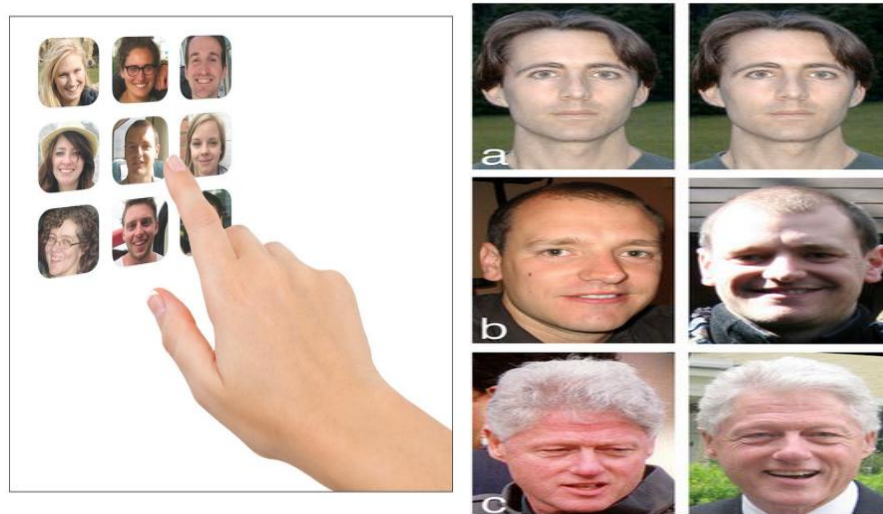


Figure 2.2(Rob, Jane, Karen): Familiar and unfamiliar face matching

Panduranga, P, Lavanya & Srinivasa (2013) several studies have used. Study (1) proposed a graphical password scheme based on “image or image password”. The user chooses and registers a sequence of the chosen thumbnail photos that form password. The user needs to identify the photos and the correct series using a tablet-stylus type of graphical device in order to be authenticated. However, as the numbers of thumbnail photos are limited only to 30, the size of the password space is considered small. This numerical password is shorter than the length of textual password. A user can select one or two thumbnail photos as one single action in order to make and enlarge the size of the password space. However, this will make the understandability of the created password become additional complex and difficult (see Figure 2.3).



Figure 2.3(Panduranga, P, Lavanya & Srinivasa): Pass faces based on the brain's innate ability to recognize faces

Study (2) proposed a scheme using a hash visualization method on the abstract images. The scheme is called “Déjà vu”. According to their studies, the result show that it takes more time to create a graphical password compared to textual password. Besides that, 90% of the authentication using Déjà vu succeeded compared to 70% using the textual password. However, due to the large amount of images stored on the server side, the authentication operation can be tardy due to network traffic delay. Even though the volume of the password area of Déjà vu view is much smaller to compared textual based password, it cannot be concluded that Déjà vu scheme is easy to remember (see Figure 2.4).



Figure 2.4(Panduranga, P, Lavanya & Srinivasa): Déjà vu scheme

Patel M, & Modi N, (2014) proposed a new pictures password scheme. In this Recognition based technique is used with a numerical password which supply more security and easy to remember text and graphical password. Each group contains 25 pictures. The User has to choose at least one image from each group during the registration phase. During login time user has to click on that pictures which is chosen during registration phase. The main wrong is increasing the load on the system. Each other so it is time consuming, sometimes during the login operation. It does not protect from shoulder surfing attack. There is no theoretical sample for this System (see Figure 2.5 and 2.6).



Figure 2.5(Patel M, & Modi N): Click text image with 33 characters

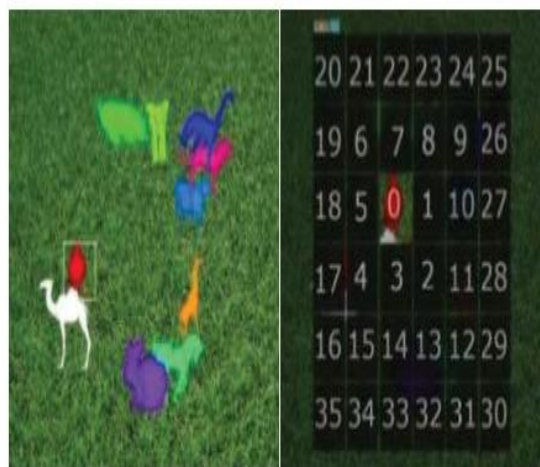


Figure 2.6(Patel M, & Modi N): Click animal images (left) & grid (right)

2.3 Immunity of passwords against attackers (Technical track)

Monroe et al (1999) proposed a technique for improving the security of password-based applications by incorporating biometric information into the password. They recorded each user's keystroke features (keystroke durations and latencies between keystrokes) when typing his password. In this experiment they had 20 users, 481 logins and 1 password. This method of hardening user passwords has some similarities to password salting. A salt is a randomly generated s bit number, which is used to permute some bits during the encryption process this method can also be used to improve salting, by determining some or all of the salt bits using the user's typing features. Also it can be useful against an attacker who knows the password

and is typing to login as that user. Their approach increases the time that it would take an attacker to exhaustively search for this hardened password.

Charoen, d et al (2008) investigated problems from the end users' point of view in terms of password utilization. They found that users are not unanimous about the necessity of having a strong password. Some agreed that a strong password is necessary to protect the systems. However, some users disagreed with the password policy. They believed that a strong password is not necessary for the system.

Current proactive password checkers are based on a dictionary attack. Yan ,j(2000) check the user-chosen password against a dictionary and if it matches a dictionary item, then that password is unacceptable and therefore rejected. But this approach sometimes fails to filter some weak passwords with low entropy. They suggested a method to dig out effective patterns of weak passwords with low entropy.

Nithya (2014) was highlighted on many studies. In study (1), a new password technicality of the type graphical that deals with authentication through pictures. The user selects these regions once he/she to produce the password. The user can decide the places of the four regions which he/she finds simple to remember. The user can introduce his/her own images for creating the graphical passwords and also for make stronger security, more than four clicked points could be chosen. Perhaps the biggest obstacle for current graphical passwords is that the shoulder surfing problem (see figure 2.7).



Figure 2.7(Nithya): User selection these regions once to produce the password

In study (2), authentication system in this password technique randomly spread a set of images on the screen. The number could be some hundred or some thousand, and the images should be various enough so that the user can make distinction them. At login the system will randomly select a placement of the images. However, the system will randomly choose a patch that covers half the screen, the and randomly places the chosen images in that patch. To the login, the user must find 3 of the pass-images and click inside the invisible triangle formed by those 3 pictures (see Figure 2.8).

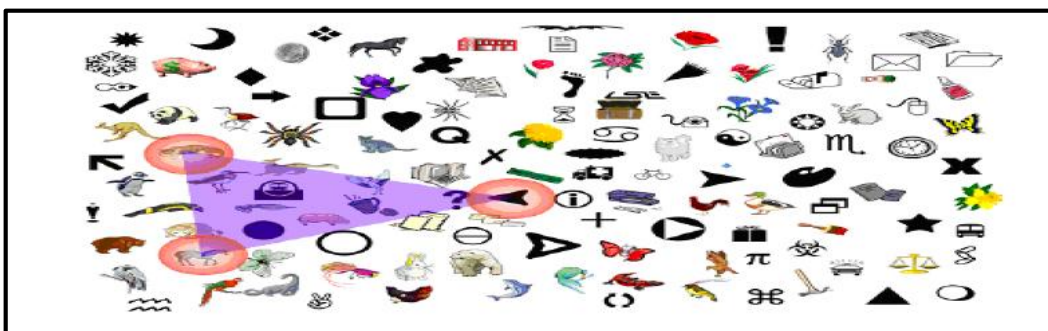


Figure 2.8(Nithya): Choose the user must find 3 of the pass-images and click inside

Study (3) presented a technology that uses faces instead of pictures, takes advantage of the brain's innate capability to recognize and recall faces. Based on the "never forget a face" capability of people, this advantage is skillfully employed in creation of authentication through face-based entry pass. Here the pass phrase is not a series of alphanumeric characters, however a string of face image. You can select images groups and whenever you are attempting to arrival a service based on authentication technique, the system will display you a set of faces from which you need to choose the ones that belong to your password series (see Figure 2.9).

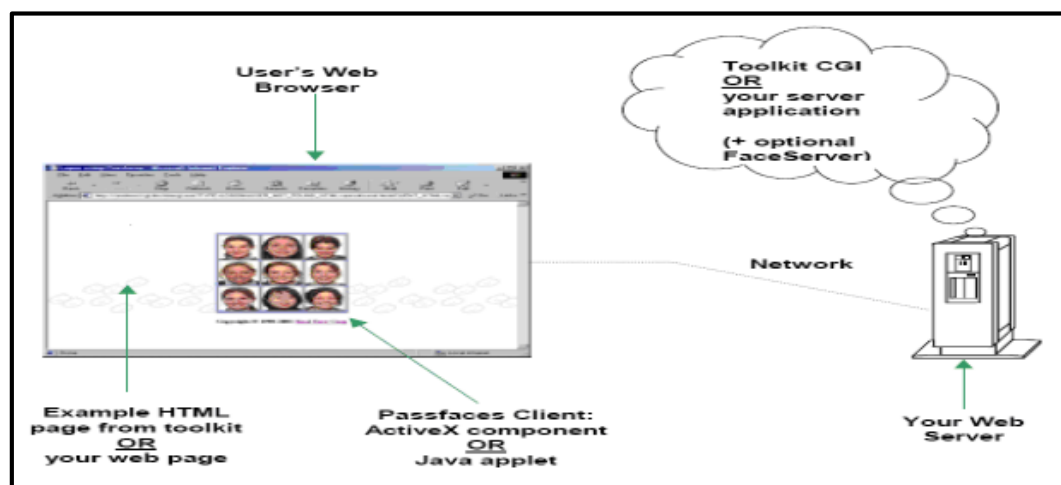


Figure 2.9(Nithya): Choose the face images that belong to password series

Sayli N Kokate, et. al. (2014) presented a new password technique CAGP (Captcha as Graphical Passwords) is click-based graphical passwords, where a sequence of clicks on an image is used to infer a password. Unlike other click-based graphical passwords, a new CARP image is created for every login try. CAGP offers defense against online dictionary attacks on passwords, which is for long time a major security threat for different online services. Graphical-based password techniques have been proposed as a probable alternative to text-based, supported partially by the fact that people can remember images best than text. CAGP is not resolution, but it offers acceptable security and usability and appears to fit well with some applications for improving online security (see Figure 2.10).

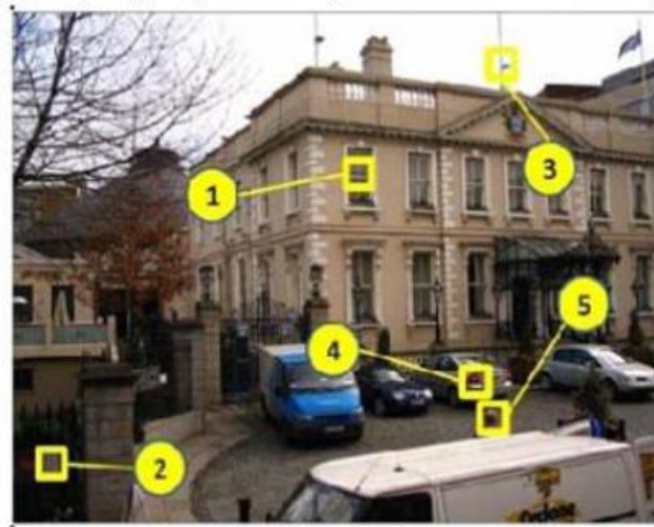


Figure 2.10(Sayli N Kokate, et. Al): (CARP) five or six click points on an image can produce passwords

Lokhande K. & Gajbhiye V. (2014) proposed a system based on employing both text and color during password entry session to extend password security against shoulder surfing and spyware by providing color combination with each character. Password that is provided to authenticate the user for a session and it will send via text message to his/her registered mobile number. The session password includes two items, user text password and its color collection code. Passwords are used only once. Every time the users enter a session, he/she has to input dissimilar password.

Balaji, et. al., (2012) gave a study about the shoulder surfing that is watching over people's shoulders by observing the keyboard during a person typing his/her password, input a PIN number, or watching personal information. Because of their graphic kind, nearly all graphical password schemes are very vulnerable to shoulder surfing. Most of the existing schemes simply circumvent the issue by stating that graphical passwords should only be used with hand-held devices or workstations set up in such a way that only one person can view the screen at the time of login and ensure that there are no human looking over one's shoulder at the time of login.

Barate ,A,K,& Shinde,S ,S(2014) used Cued Click Points (CCP) graphical password, Persuasive Cued Click-Points (PCCP). Where a password consists of string of clicks on predefined regions of pictures. Cued Click Points (CCP) are a proposed to alternate Pass Points. In CCP, users click one point on each of the pictures rather than five points on one pictures. Alert valid users if they have made a mistake when enter their latest click point (at which point they can cancel their attempt and retry from the beginning). It also makes attack based on hotspot analysis widely challenging. If a user enters an incorrect, then the string of pictures from that point onwards will be and erroneous thus the login attempt will fail. For an attacker who does not know the true string of pictures, this braid will not be of use.

Majumder, S, Chakraborty,S, &Das,S, (2014) presented a study new & unique way of user authentication & data confidentiality. Authentication is done through two factor authentication system. First factor is graphical user name. Second factor is voice password. Data confidentiality is well done through public key cryptography. Two keys are used in different phase of plain text to cipher text & cipher text to plain text conversion process. Two layer keys make the data more secure & confidential. It suggest a new user authentication and data confidentiality service, which results much better service in terms of security than the traditional services.

Ayannuga (2012) proposed a graphical password scheme where login need that users recognize images from their portfolio. The login task involves computing track through a panel of pictures based on whether particular pictures belong to the user's portfolio. Present dissimilar panel each time. After each round, the system computes the cumulative probability that the true answer was not input entered by chance. Then the user is authenticated. This allows for some user error, but if the threshold is not passed within a certain number of round, the user is unacceptable. The keyboard is used for input, rather than a mouse, to support decrease shoulder-surfing. Users receive system assigned portfolios of pictures and receive extensive directing to initially memorize their portfolio since it includes a great number of pictures approximately 100. Login takes from 1.5 to 3 minutes. On average, 95% login success rate was achieved (see Figure 2.11).



Figure 2.11(Ayannuga): Login need that users recognize pictures from their portfolio.

Gagan Dua , et,al , (2013) present a new technique, the Ticket Granting Server (TGS), an improved method which prevents attacks by using the triple password scheme. Three passwords are stored on Authentication Server and Authentication Server sends two passwords to the Ticket Granting Server (one for Application Server) by encrypting with the secret key be shared between Authentication server and Ticket Granting server TGS sends it by encrypting it with the user password that is familiar only to the user. So, if this ticket was created from the attacker, he will not be able to use the service from the Application Server or will not be able to relay messages to the Application Server because the attacker does not know the user password.

Khalil ,M, A (2013) implemented an Auto Teller Machine (ATM) system that uses the user signature image as password beside user's PIN information, to realize more secure verification and authentication of ATM bank users, and to strength the ATM security to prevent theft and to combat ATM crime. The ATM system will implement Inquiry, Deposit, and Withdrawal transactions for users ATM has gradually become a target of crimes due to providing direct access to safe and cash, deposit or withdrawal fraud, software and network attack and thieves try to infect the

machines or hack into the ATM's internal data networks to steal the account information (see Figure 2.12).

Auto Teller Machine (Main Screen)			
ID number:	4	address:	mansour quarter
accnam:	Tara	balance:	12000
signature:		deposit type:	
PIN:	1235	the sum:	
signature PassWord:	14		
gender:	female		

Figure 2.12(Khalil ,M, A): ATM system that uses the user signature image as password

Maitra,., T, (2015) has been used Karuppiah and Saravanan's Scheme in try to use the same notations as offered. Their scheme consists of five stages, namely, initialization, registration phase, login phase, authentication and password change phase. Maitra shown that Karuppiah and Saravanan's scheme has a fatal fault in login phase, so that their scheme is impractical for real world application.

Lonkar V., Raut, S. & Mesakar S. (2014) proposed a new algorithm using water marking technique as the solution by using the random character set generated for each image for resistance the attack to provide best system security. All the information, images in the registration phase will be processed by copyright protection of watermarking where the login page will check this information for security objective. Some researchers have developed authentication techniques that use pictures as passwords. Graphical Password is based on the fact that people tend to remember images better than watermark which depends on the use case in which it is applied. A digital watermark has to be rather robust against modifications that can be applied to the carrier signal (see Figure 2.13).

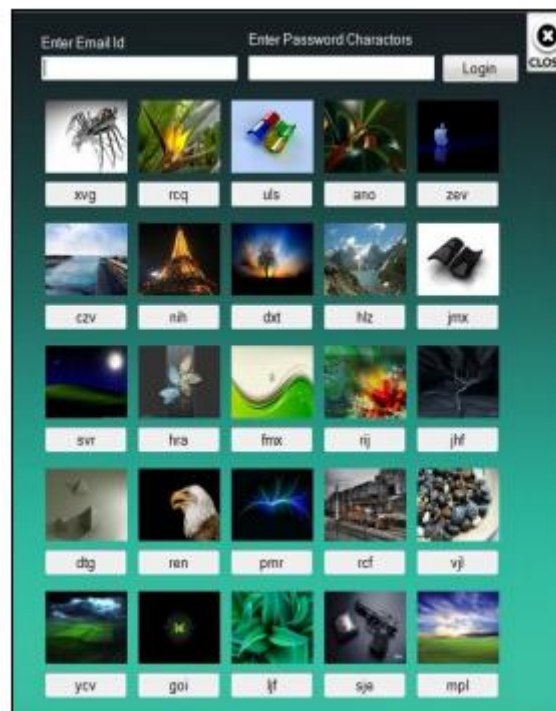


Figure 2.13(Lonkar V., Raut, S. & Mesakar S.): Login form using the random character.

Markus S, Mark D& Kat M, Darick T,(2009).aimed to use of special characters encodes of expressive core group interoperable with existing data that has been generated by the number of users of Japanese mobile phones in 2007. Survey of 13,000 users - 80% of whom are 30 years or more - and found that even among this older group, and 78% "often" or "Sometimes," the use of emoticons in mails. According to respondents using a wide range of expressions, including expressions of faces, weather, emotions, vehicles and buildings, drink and food, animals, etc., especially among younger users, and e-mail is mostly or exclusively used on mobile phones instead of computers. Between cell phone users, 90% use e-mail in the first place on mobile phones, and 60% use e-mail exclusively on cell phones. Expressive symbols have been applied on Japanese cell phones for 10 years.

Shannon R (2006) .did a study on users' behaviors toward selecting their password. Of 315 Participants, the average number of character per password was found to be 6.84. Almost 75% of them reported that they have a set of predetermined passwords that they use frequently. Almost 60% reported that they don't change the complexity of their password depending on the nature of the site. A recent poll by Sophos (2009) reported that almost one third of users use the same password for all their accounts on different websites.

These results also have been backed up by another study by Stone Grass et al (2009) who took over the botnet for ten days and collected around 298 thousands username and passwords. They found that almost 28% of users reused their passwords for accessing different websites and they managed to crack over 40% of the passwords in less than 75 minutes. These results show that having strong passwords for less important websites such as social networking websites is as necessary as for the higher value websites like online banking.

These studies show that having an effective password creation policy does not always mean having strong passwords and a secure system, since users are forced to create passwords that may not be easy to memorize, most users tend not to change their passwords often or have different passwords for different websites.

(Nur Haryani Zakaria et al) Use technology DAS (Draw A-Secret) is the resistance to surf the Internet it was clear the protection, but most of the time remain visible on the screen where hidden is the favorite of the users, but it is prone to attacks. Graphical passwords are still far from being perfect. A password supplied for authentication by a user in a public place, if not properly protected, can be stolen by a bystander who observes over the user" s shoulder. This is known as a shoulder surfing attack and commonly regarded as a drawback to various graphical password systems Alpha-numeric passwords are defended against this by substituting asterisks for the password characters in the display as the user logs in. To make graphical passwords reliable in the real world, it is essential to arm them with good shoulder surfing defence mechanisms. The easy-to-use of terms to remember but the average time of login errors. The humans ability to remember pictures better than text has been well documented in numerous cognitive and

psychological studies .Possible schemes take more space on the one hand storage DAS is a representative graphical password scheme and worthy of extensive study for the following reasons, theoretical password space can be larger than that of text passwords. Second, unlike many other graphical password systems, DAS can be used for not only user authentication, but also for key generation.

Fabian Monrose et al.(2002) It was suggested to incorporate information biometric in the password, and Image Generation randomly this creates a non-comfortable to the user in identifying the password. User login process will take time to write the Password. This is useful against the attackers who know the password. Not take much space in the database.

Kenneth R.(2006) Use Technology (TO) Technical operation the password is complex and has many negative points. Obtaining a new password or having one reset is normally straightforward, Take more time because the process remember a complex password needed time. Human factors issues include cognitive issues, such as the number and complexity of passwords that employees must remember. Not surprisingly, the literature shows that people have difficulty remembering many usernames and passwords, especially when they are complex and change frequently. Other human factors issues such as the perceived consequences for breaking information security policies. Because nearly all of the existing human factors research in user identification has been conducted in corporate and academic environments, we also analyzed differences between those environments and FAA TO. Provided general recommendations for improving the human factors of user identification technologies and policies. Our recommendations included reducing the number of logins that must remember and providing with techniques, such as using mnemonics that would help them remember their logins more easily. Storage process be balanced in terms of size because it uses digital chains.

Kemal Bicakci (2011) suggested that the use of grid Word a hybrid system that combines elements of the texts and graphs passwords is by selecting words from lists words, but entering the password be Visual. Vantages to using words corresponding to “concrete "objects for which visual images are easily formed, studies show their retrieval from memory is far better than abstract words takes a long time on the network are stored passwords.

CHAPTER THREE

ANALYTICAL TRACK

3.1 Proposed model

The analytical track of this study involves building an online authentication system. The system consists of two parts: In first part, users can use textual password (text, numbers and special symbols). In second part, users have been given a new proposed password that is employing Emoji pictures in addition to (text, numbers and special symbols) that previously used in textual password.

Necessary keyboards for each part of the system have been built to facilitate for users writing their password of each type. The goal of building this system is to make an analytical comparison between using textual password and Emoji password through using the two parts of the system by users. The comparison is made based on ease of keeping and remembering the password by users in the two cases. PHP Programming Language has been used in building this system. PHP is the latest programming languages used in building web sites. PHP provides an ability to build an effective web sites, PHP also supports using databases in programming environment for algorithm development, data analysis, visualization, and numerical computation. Figure 3.1 shows the main page of the system.



Figure 3.1: Main page of the system

In this system, several factors have been used to make the analytical study more objective. These factors include:

1. Age group of participants.
2. Educational attainment of participants.
3. The password length not less than eight characters.
4. The period of time between successive login operations is around 7 days.
5. Password chosen must not be very simple.

3.2 Samples users participants in the analytical track

We have been keen to choose the appropriate number of participants of different ages and educational backgrounds (academic achievements). In our study, we chose more than 100 participants to test the authentication system.

Age distribution of participants has been chosen based on the following classes:

1. Less than 15
2. 15-25
3. 25-35

4. 35-45
5. 45-70
6. Older than 70

Also, the educational backgrounds (academic achievement) of participants have been chosen based on the following classes, these classes have been determined by International Standard Classification of Education (ISCED 2011):

1. Less than primary education
2. Primary education
3. Lower secondary education
4. Upper secondary education
5. Post-secondary non-tertiary education
6. Short-cycle tertiary education
7. Bachelor's or equivalent level
8. Master's or equivalent level
9. Doctoral or equivalent level
10. Not elsewhere classified

3.3 Registration in system

To register in the authentication system, each user must firstly create two accounts in the system: One for Textual password and another for Emoji password as shown in figure 3.2.

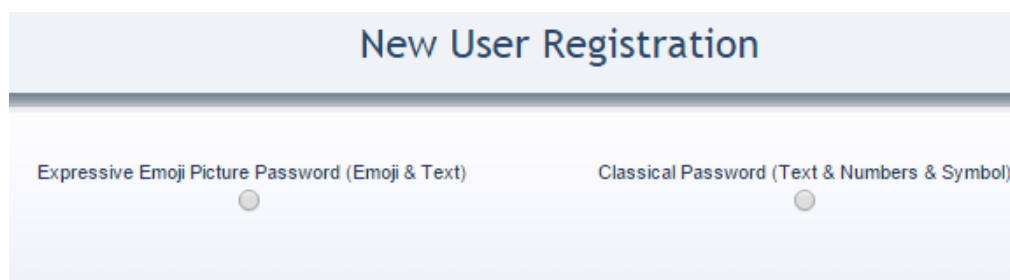


Figure 3.2: Two types of password accounts

After the user selects the desired type of password account, the system asks the user to enter some mandatory information that will use later by this study to conduct the analysis. This information involves: Username, Password, Full name, Age group, and Academic achievement (see figure 3.3 and 3.4). After creating two

accounts (Textual and Emoji) through the registration stage, user became one of the participants in the system.

3.4 Part one: Textual passwords

Textual password is a string of characters, consists of numbers (0, 1, 2, ..., 9), alphabetic English letters ('a', 'b', ...'z') and ('A', 'B', ...'Z') and Arabic letters (أ, ب, ...ي) and most common used special symbols ('%', '#', '\$', '!', '@',) that are used in writing password (see figure 3.3):

Figure 3.3: Textual password

3.5 Part two: Expressive Emoji password

Emoji pictures are used increasingly in picture messages as a way to communicate such as Whats App, Viber, etc.. Emoji pictures are categorized in various types like People, Places, Nature, Objects, and Symbols. The proposed demo system constructs the groups from: 168 people images, 111 nature images, 227 object images, 190 symbol images and 84 place images. The Emoji pictures in each group has been arranged and displayed as keyboard to allow users use in writing their Emoji passwords (see figure 3.4).

Figure 3.4: Emoji password

3.6 Characteristics of passwords in the system

In order to achieve an effective authentication system that can evaluate later and make an identical comparison between textual and Emoji password, passwords entered by users in each part must satisfy the certain conditions. The system enforces on users write their passwords with the following constraints:

1. The password length should be minimum eight characters.
2. The password should be complex enough, therefore the password entered by user must contains at least one character from each type (i.e., numbers, upper and lower alphabet letters and special symbols in textual password and one Emoji picture from each group in Emoji password as illustrated in section 3.5).
3. User should not write their password on sticky note or store their password in file on the computer storage.
4. Users who participate in the system must use (in login session) their brain's ability only to remember their passwords that have been chosen during the registration session.

3.7 Login to the system

To achieve a realism and objectivity in login operation by users into their accounts in the system, we asked from users login to their accounts one time weekly (both textual and Emoji accounts). This will give the user's brain an enough period of time to forget and remember his/her. This makes the login operation seems as natural as possible. The total period for evaluation of the system spanned about two months.

At each successful login operation by user, the system does the following actions:

1. The system asks users to determine the level of remember of their password and records their choice in the system's database. The levels of remembering password have already been defined by the system as (Too Easy, Easy, Medium, Difficult and Too Difficult). Figure 3.5 and 3.6 for examples.
2. The system records the actual period (in days) between the previous and current login by the user.

Username: raghda 1			
Full Name: raghda 1			
Age Group: 25-35			
Academic Achievement: Bachelor or equivalent level			
Login Date	Emoji Picture Password	Text Password	Date
1 ->(2015-01-30)		Medium	2015-01-30
2 ->(2015-02-05)		Difficult	2015-02-05
3 ->(2015-02-10)		Easy	2015-02-10
4 ->(2015-02-15)		Medium	2015-02-15

Figure 3.5: Level or remembering (Textual password)

Username: yasin
 Full Name: yasin khalid
 Age Group: 15-25
 Academic Achievement: Post-Secondary non-tertiary education

Login Date	Emoji Picture Password	Text Password	Date
1 ->(2015-01-23)	Too Easy		2015-01-23
2 ->(2015-01-28)	Easy		2015-01-28
3 ->(2015-02-02)	Easy		2015-02-02
4 ->(2015-02-07)	Too Easy		2015-02-07

Figure 3.6: Level or remembering (Emoji password)

3.8 The benefits of using Emoji pictures in writing password

The use of Emoji pictures in writing password raises the password security and gives users good facility to deal with their password:

1. By increase the range of symbols that used in writing password after adding the Emoji pictures to the characters that already used in the textual password. This will add more difficulties against attackers through making the password more complex than textual password. Therefore, Emoji password is stronger and very difficult than textual password to guess by unauthorized users attackers. To give more clarification about this point, we will cite some examples below:

Example (1): If the range of characters used in writing password is the uppercase alphabet English letters 'A'...'Z' only (which is weak password), this means that each character in the password can be one of 26 cases, and the number of necessary cases for testing to guess password is 26.

Example (2): If the range of characters used in writing password is the uppercase and lowercase alphabet English letters "A"..."Z" and "a"..."z", digits "0"..."9", alphabetic Arabic letters "أ"..."ي" with (about 30) selected popular used special symbols "@"..."#". This means that each character in the password can be one of $(26+26+10+28+30) = 120$ cases, and the number of necessary cases for testing to guess password is 120. This obviously makes this password stronger and more difficult than the password in Example (1).

Example (3): Adding Emoji pictures to list of characters that users can be used in writing password will widen the range of characters used to create any password. Since there are a huge number (thousands) of Emoji pictures recently used in computer systems, therefore add these Emoji pictures to the characters that already used in the textual password will raise high the number of cases for each character used in password to be in thousands. Certainly this increases the immunity of password against attackers through adding more difficulties to guess the password by the attackers. Certainly, this will maximize the strength of the Emoji password and make the Emoji password very hard to guess by attackers.

2. Using Emoji pictures in writing password will facilitate remember the password by users. Where most recent studies by researchers proved that the human brain has an ability to remember images more than random texts. The meaning of Emoji picture is word or set of words. Although there is default meaning for each Emoji picture but each user might have his/her own meanings that refer to Emoji pictures used in writing password. The list of words, that represents the Emoji pictures in password, can keep in mind to describe the whole password. We should note here that remember meanings for Emoji pictures that are selected in private manner by user is easier than remember the default meanings for these Emoji pictures and even the traditional password. In addition, remember meaningful words (or phrase) are easier for the user from remember a set of random characters have no meaning (see figure 3.7).
3. Users will have a lot of freedom in writing any set of words (or sentence that contains a set of words) that describes the expressive images (Emoji pictures) used in the password on any book, paper or store these words in file on the computer storage unit even if they are written clearly. This will add more confusion about knowing what is the password and exclude any doubt by the attackers about the actual Emoji pictures used in writing password.
4. Using Emoji pictures in writing passwords adds more security to the password and makes it hard for others to locate it and obtained by make it easy for users.

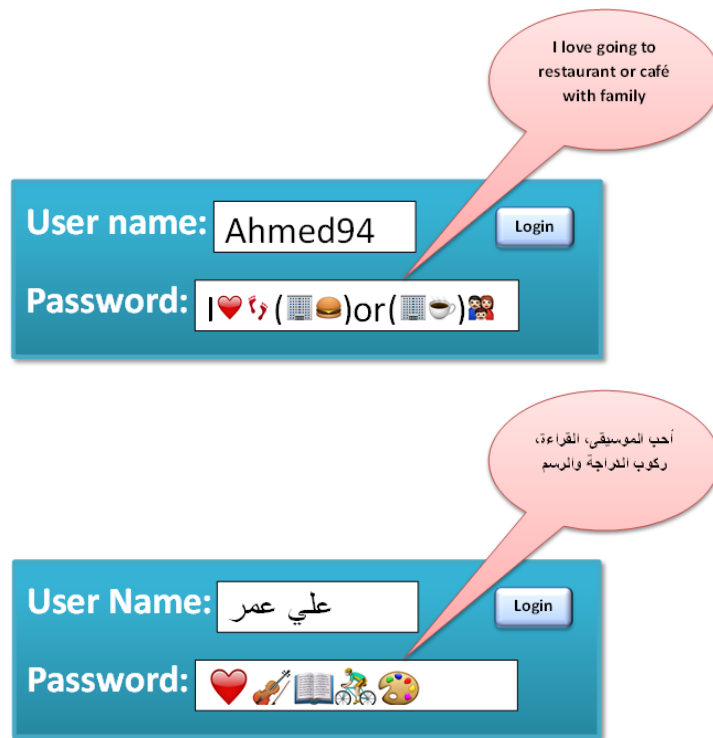


Figure 3.7: Example of Emoji password with its phrase meaning (in different languages)

3.9 Results, analysis and discussion

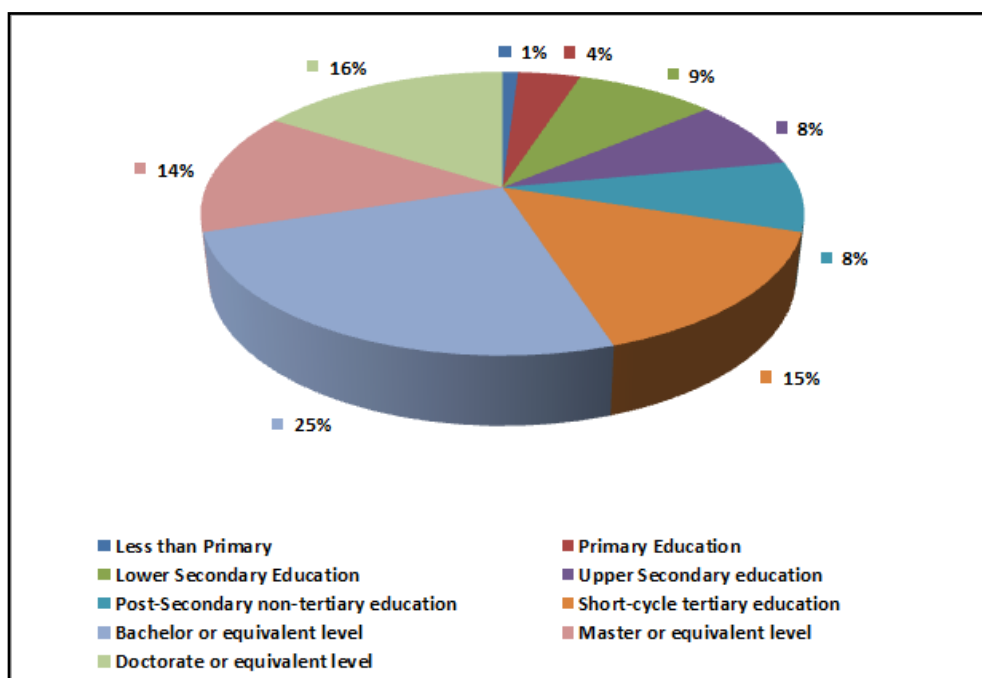
The analytical results of the capability levels of remembering for each type of passwords (textual and Emoji) have been recorded by users through the login operation during the period of the analytical study will presented in the following paragraphs.

Number and percentage of participants in the analytical study distributed:

1. Based on the educational backgrounds (academic achievement) classes, that are mentioned before, is shown in table 3.1 and figure 3.8.

Table 3.1: Number of participants based on the academic achievement

Educational Attainment	Number of Participants
Less than Primary	1
Primary Education	4
Lower Secondary Education	9
Upper Secondary education	8
Post-Secondary non-tertiary education	8
Short-cycle tertiary education	15
Bachelor or equivalent level	25
Master or equivalent level	14
Doctorate or equivalent level	16
Total	100

**Figure 3.8: Percentage of participants based on the academic achievement**

2. Based on the age classes, that are mentioned before, is shown in table 3.2 and figure 3.9.

Table 3.2: Number of participants based on age

Age	Number of Participants
Less than 15	10
15-25	31
25-35	35
35-45	16
45-70	7
Older than 70	1
Total	100

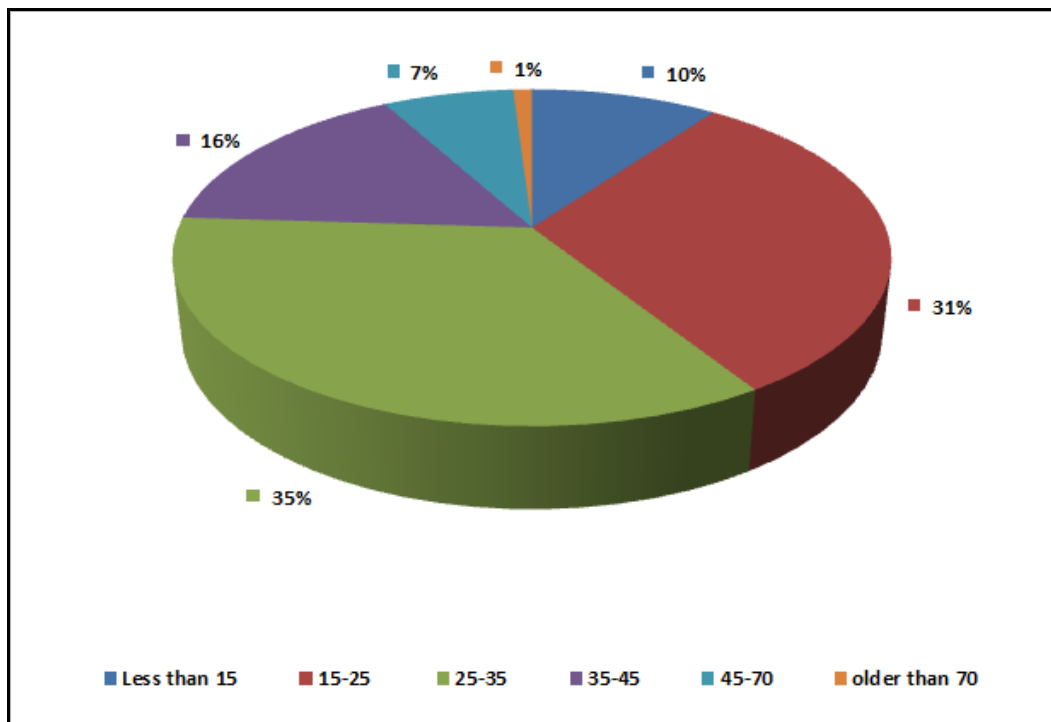


Figure 3.9: Percentage of participants based on age

After completion the analytical study and collecting the recorded results in the database of the authentication system, the levels of remembering password by users, as mentioned before, (both textual and Emoji) and their percentages have been recorded in the following tables and depicted graphically (as charts) in the following figures.

1. Based on the educational backgrounds (academic achievement) classes, see table 3.3, table 3.4, figure 3.10 and figure 3.11.

Table 3.3: Voting for "textual Password" based on academic achievement

Educational Attainment	Too Easy	Easy	Medium	Difficult	Too Difficult
Less than Primary	0	0	2	2	0
Primary Education	0	2	4	7	0
Lower Secondary Education	0	8	14	10	4
Upper Secondary education	1	6	11	12	2
Post-Secondary non-tertiary education	1	7	12	10	2
Short-cycle tertiary education	1	13	19	25	2
Bachelor or equivalent level	13	25	9	25	7
Master or equivalent level	4	18	25	9	0
Doctorate or equivalent level	2	20	30	4	2
Total	22	99	126	104	19

Table 3.4: Voting for "Emoji Password" based on academic achievement

Educational Attainment	Too Easy	Easy	Medium	Difficult	Too Difficult
Less than Primary	0	1	0	2	0
Primary Education	5	7	1	3	0
Lower Secondary Education	11	14	4	7	0
Upper Secondary education	11	11	5	5	0
Post-Secondary non-tertiary education	10	7	7	7	1
Short-cycle tertiary education	16	24	11	8	2
Bachelor or equivalent level	48	41	12	10	1
Master or equivalent level	25	23	4	4	0
Doctorate or equivalent level	23	28	7	5	1
Total	150	156	51	51	5

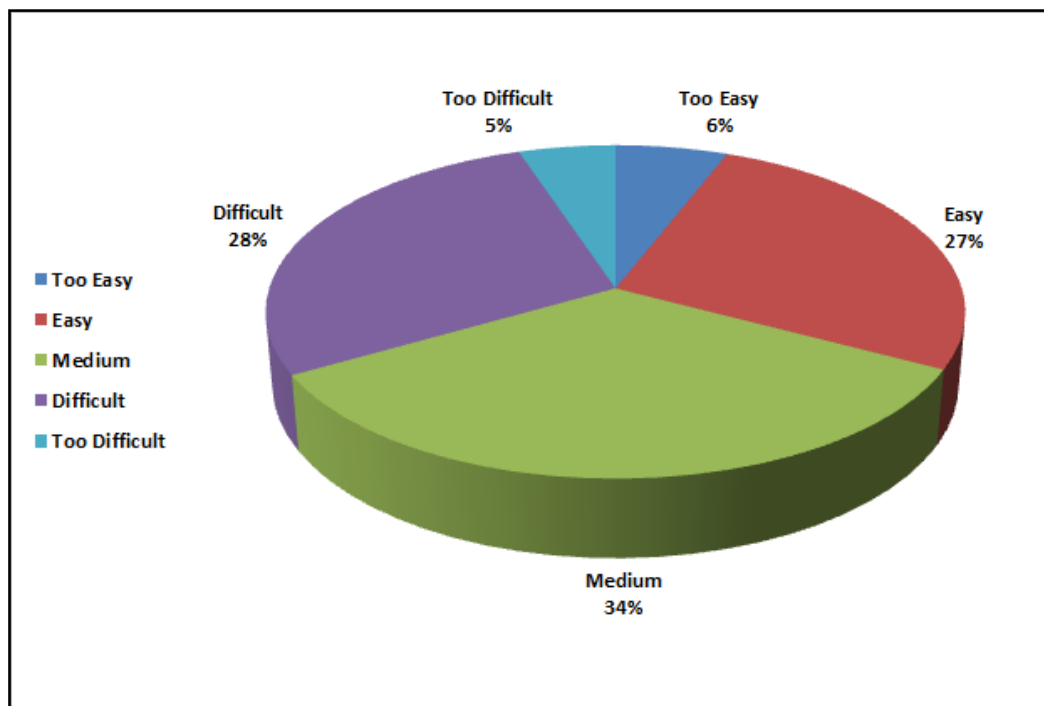


Figure 3.10: Percentage of voting for "textual Password" based on academic achievement

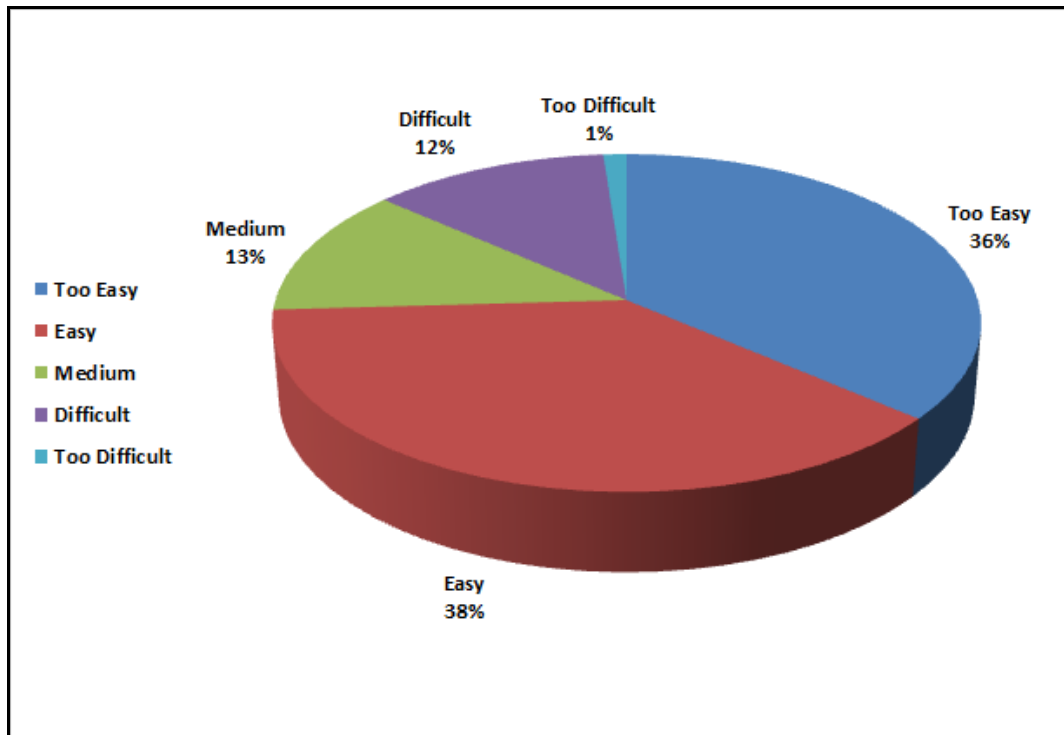


Figure 3.11: Percentage of voting for "Emoji Password" based on academic achievement

2. Based on the educational backgrounds (academic achievement) classes, see table 3.5, table 3.6, figure 3.12 and figure 3.13.

Table 3.5: Voting for "textual Password" based on ages

Age	Too Easy	Easy	Medium	Difficult	Too Difficult
Less than 15	0	8	14	21	1
15-25	3	25	26	33	13
25-35	3	18	28	16	3
35-45	6	21	36	25	1
45-70	8	25	47	23	1
Older than 70	0	0	3	1	0
Total	20	97	154	119	19

Table 3.6: Voting for "Emoji Password" based on age

Age	Too Easy	Easy	Medium	Difficult	Too Difficult
Less than 15	13	16	5	10	0
15-25	30	39	14	15	2
25-35	28	24	8	8	0
35-45	35	31	13	8	1
45-70	37	50	10	6	0
Older than 70	2	2	0	0	0
Total	145	162	50	47	4

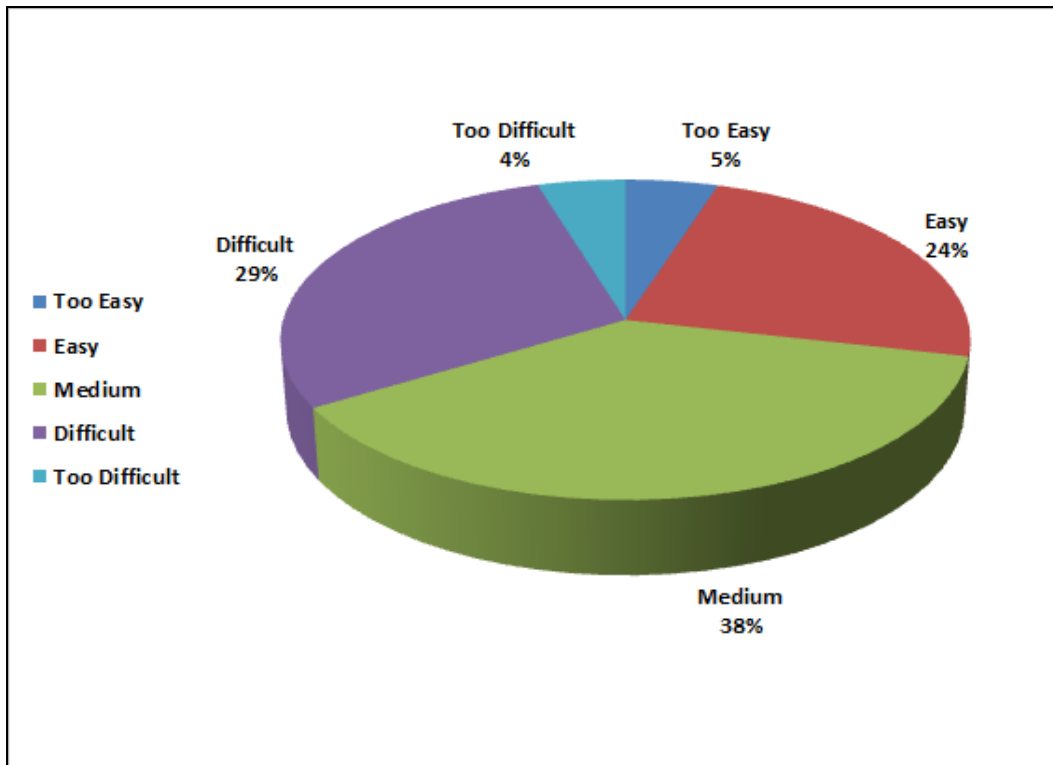


Figure 3.12: Percentage of voting for "textual Password" based on age

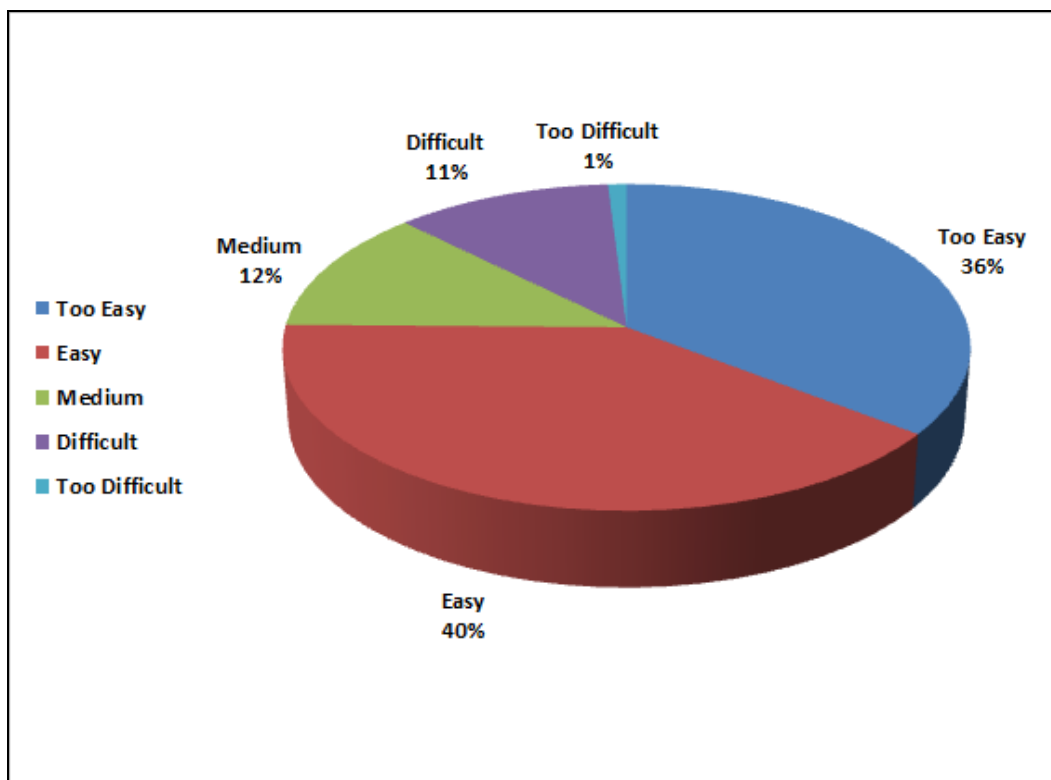


Figure 3.13: Percentage of voting for "Emoji Password" based on age

3. Based on the progress of time, see table 3.7, table 3.8, figure 3.14 and figure 3.15.

Table 3.7: Ratio of Voting for "textual Password" Based on the Series of Login of Participants

Educational Attainment	Too Easy	Easy	Medium	Difficult	Too Difficult
Login 1	20	55	15	11	2
Login 2	4	10	23	63	4
Login 3	1	4	52	32	5
Login 4	1	21	54	14	12
Total	26	90	144	120	23

Table 3.8: Ratio of Voting for "Emoji Password" Based on the Series of Login of Participants

Educational Attainment	Too Easy	Easy	Medium	Difficult	Too Difficult
Login 1	56	31	11	8	1
Login 2	2	56	12	32	3
Login 3	19	50	30	10	1
Login 4	66	23	11	1	0
Total	143	160	64	51	5

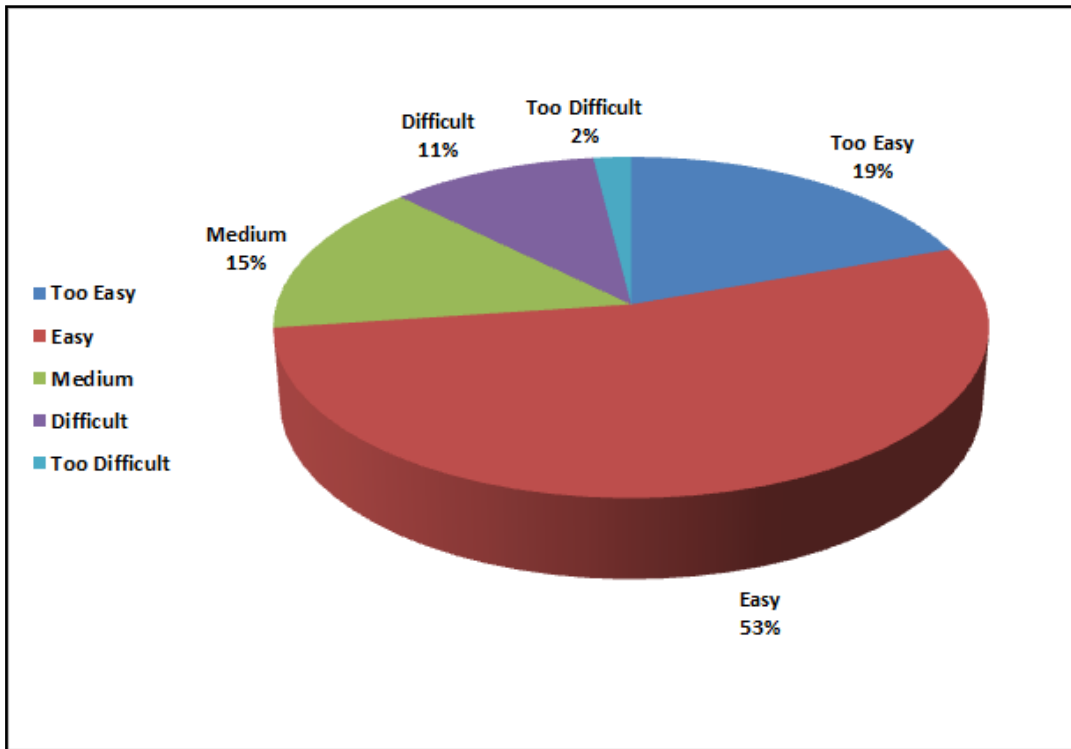


Figure 3.14: Percentage of voting for "textual Password" based on progress of time

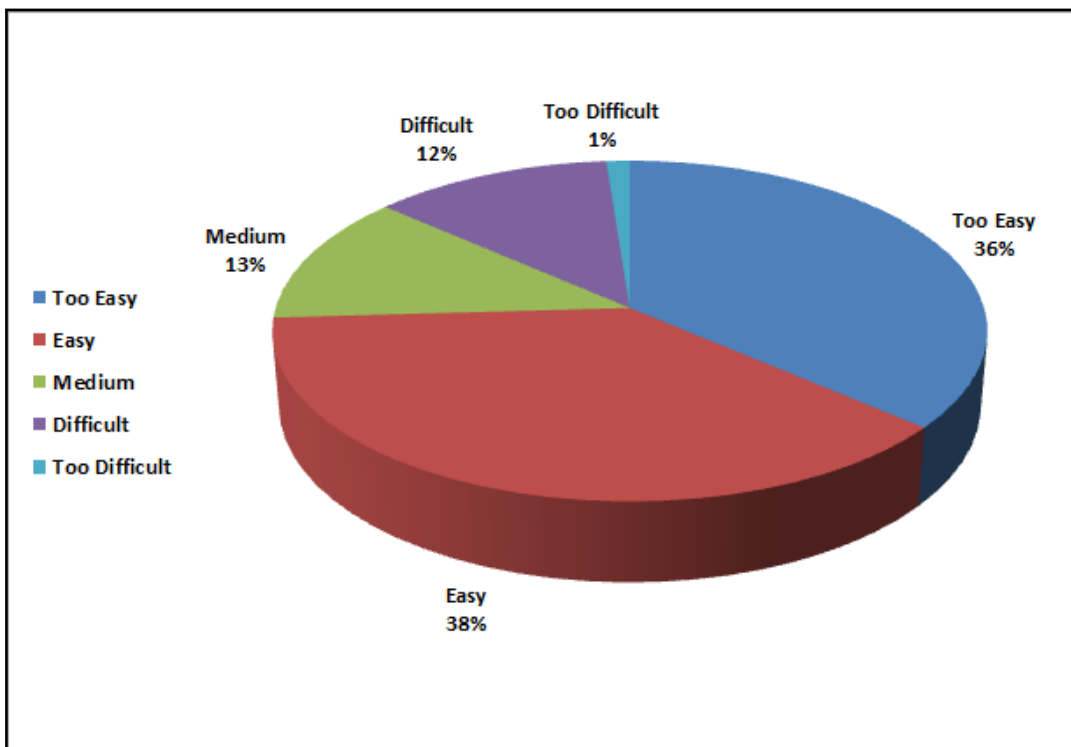


Figure 3.15: Percentage of voting for "Emoji Password" based on progress of time

4. Based on the percentage of users who completely forgot their password; see table 3.9, figure 3.16, and figure 3.17.

Table 3.9: Ratio of Participants who forgot their Password Based on academic achievement of Participants

Educational Attainment	Classical Password	Emoji Password
Less than Primary	1	1
Primary Education	2	0
Lower Secondary Education	4	1
Upper Secondary education	7	1
Post-Secondary non-tertiary education	4	1
Short-cycle tertiary education	5	2
Bachelor or equivalent level	9	5
Master or equivalent level	6	1
Doctorate or equivalent level	2	2
Total	40	14

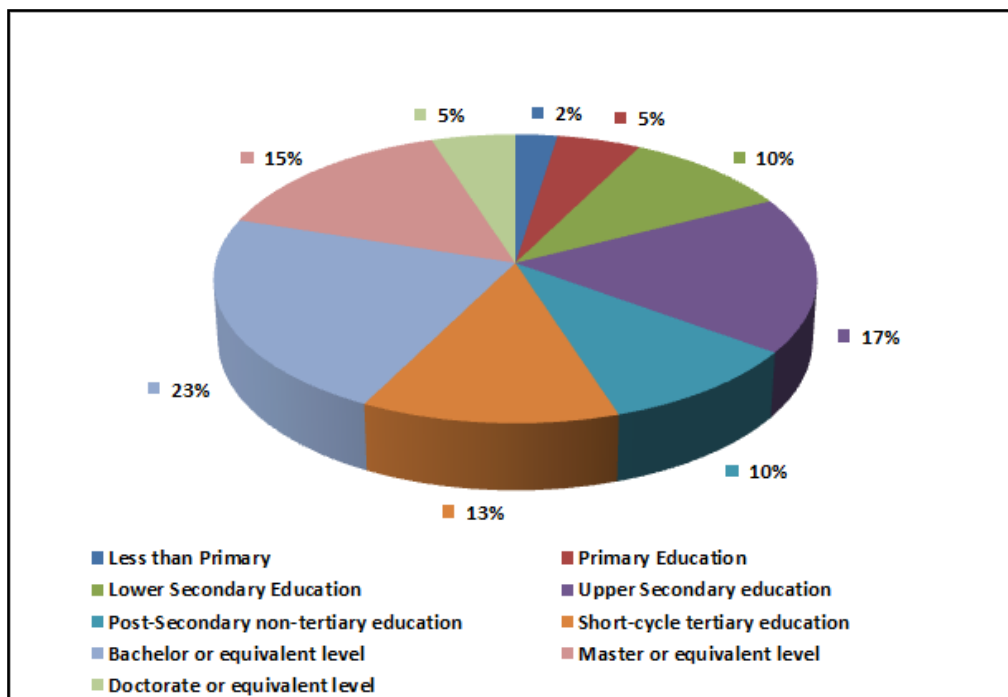


Figure 3.16: Percentage of participants who forgot their "textual Password" based on academic achievement

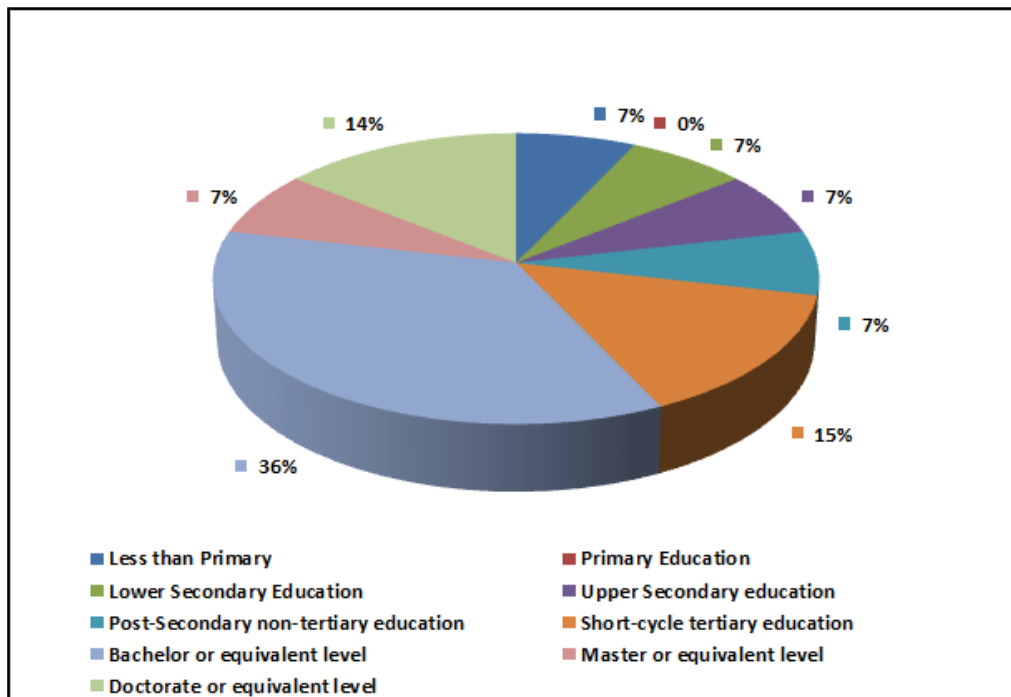


Figure 3.17: Percentage of participants who forgot their "Emoji Password" based on academic achievement

5. Based on the percentage of users who completely forgot their password, see table 3.10, figure 3.18, figure 3.19 and figure 3.20.

Table 3.10: Ratio of Participants who forgot their Password Based on Ages of Participants

Educational Attainment	Classical Password	Emoji Password
Less than 15	1	0
15-25	5	2
25-35	11	1
35-45	17	8
45-70	6	3
Older than 70	0	0
Total	40	14

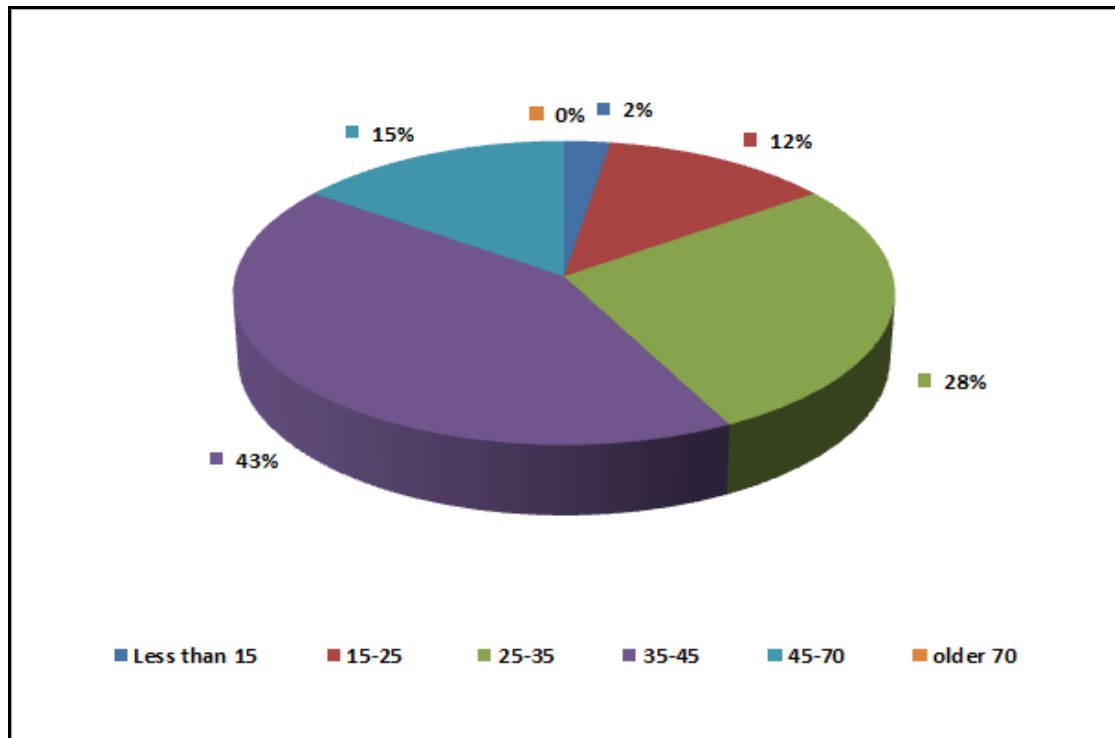


Figure 3.18: Percentage of participants who forgot their "textual Password" based age

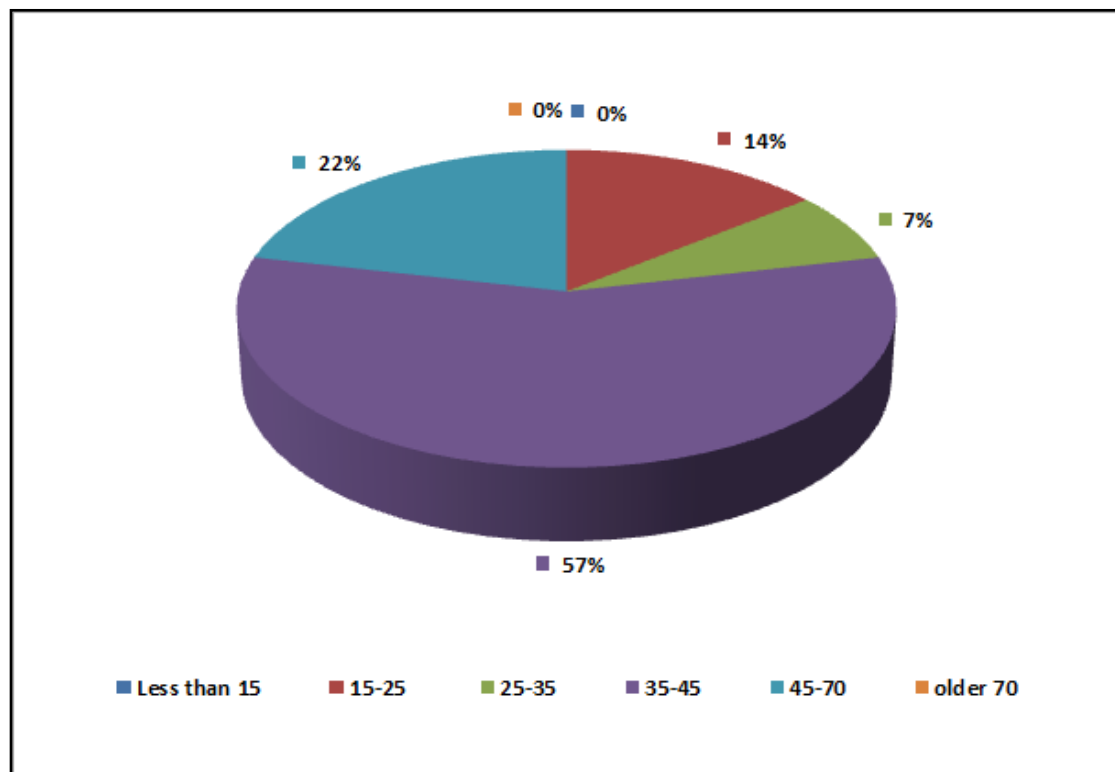


Figure 3.19: Percentage of participants who forgot their "Emoji Password" based age

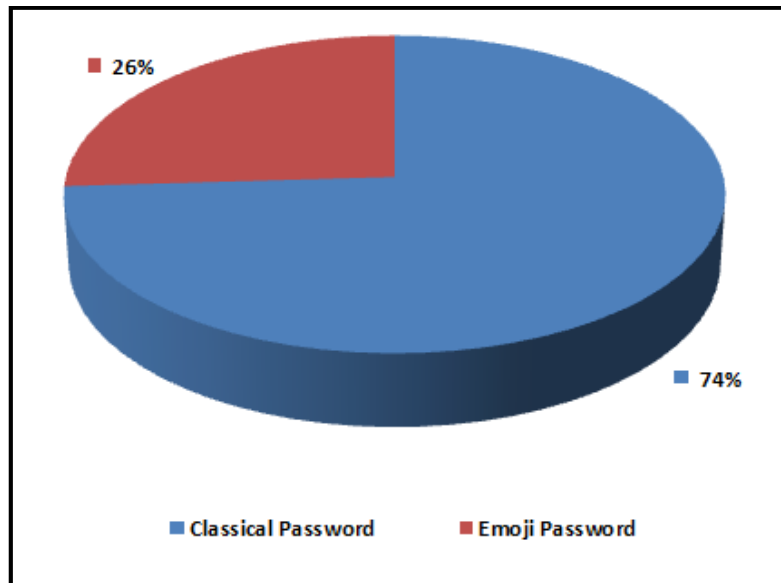


Figure 3.20: Total percentage of participants who forgot their password "both textual and Emoji Password"

The exhaustive results extracted from the above analytical track of this study shows statistically that the using Emoji pictures in writing password really facilitate to users remember and deal with their password in addition to raise the immunity of password against attackers.

From the above actual analytical study that proved the powerful points of using Emoji pictures in writing password. This study went ahead to the technical part which focuses on building a user authentication model that actually use Emoji pictures in writing password and tries to achieve more and more facilities for users to enter their password in safe and enjoyable session.

CHAPTER FOUR

TECHNICAL TRACK

4.1 Proposed model (Authorization System Uses Emoji Pictures)

From the promising results that have been obtained from the analytical track of the study, started the idea of building an experimental user authentication system that is using Emoji pictures. C# Programming Language has been used in building this system. C# is one of the latest programming languages used in building the effective GUI applications. C# supported by many utilities that facilitates the programmers to build their applications in an easy and effective way. Figure 4.2 shows the main page of the system.

4.2 Authorization system

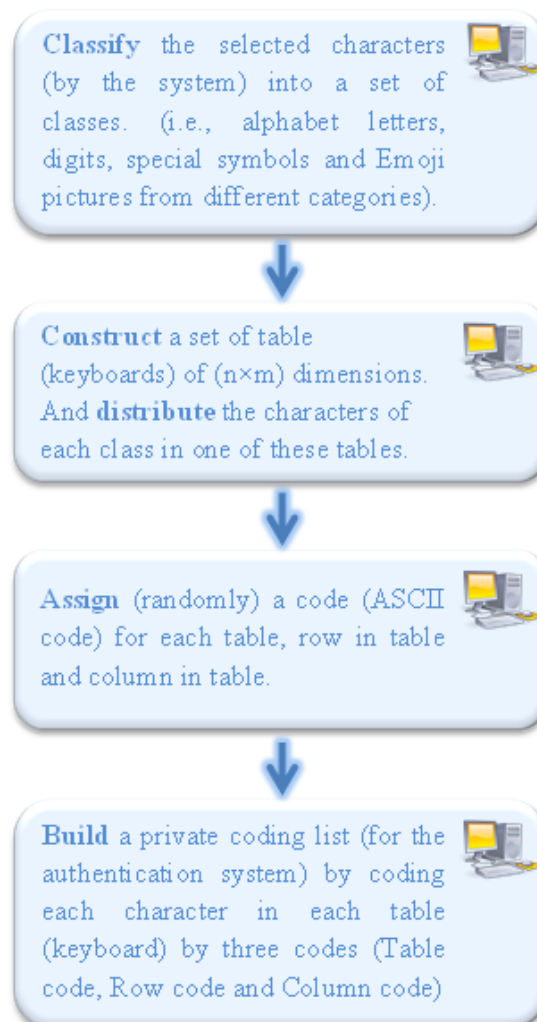
The user authentication system has been built carefully to achieve the above goals. The system's operations consist of two parts: Preparation operations and Login session. The following two diagrams depict the sequence of operations in each part of the system. Where:



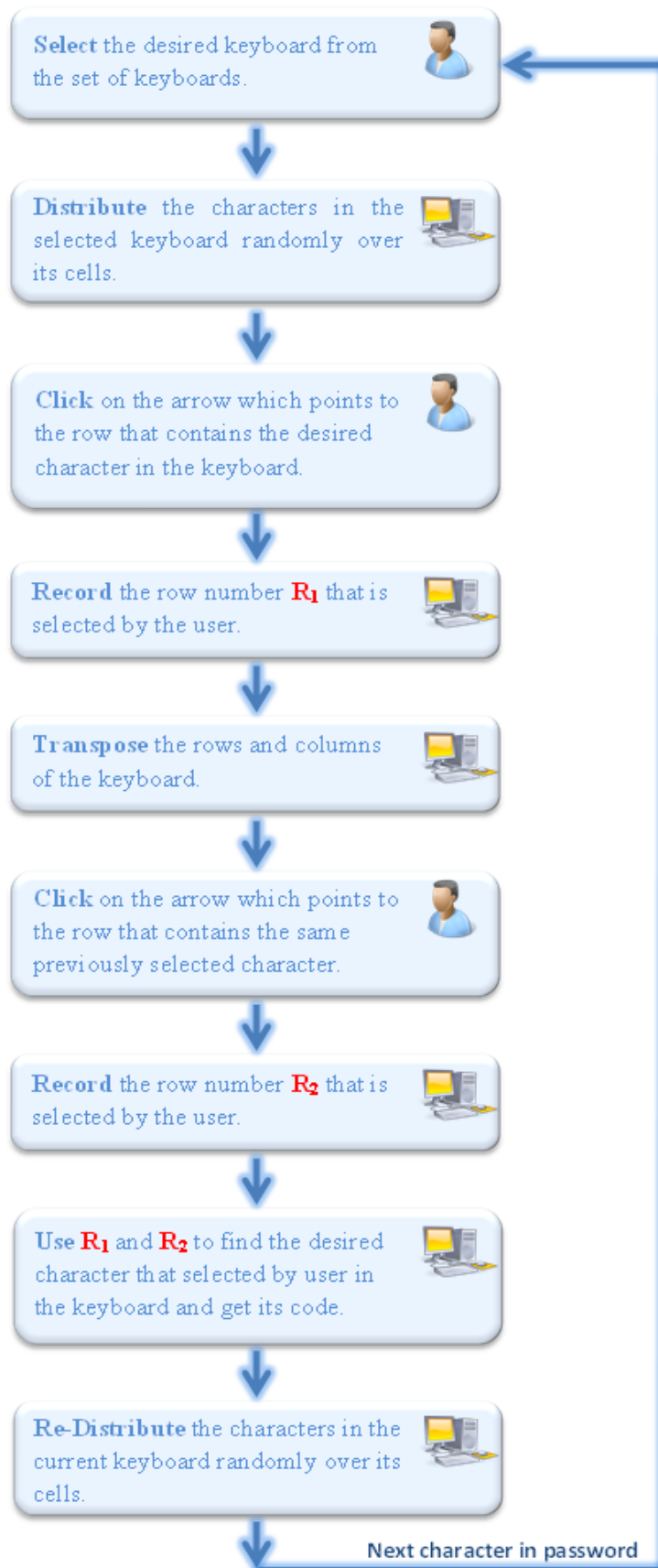
Represents operation performed by *User Authentication System*



Represents operation performed by *User*



Preparation operations



Login session

The following sections will give readers more explanation about the operations in *Preparation* and *Login session*.

4.2.1 Preparation operations

There are a number of preparation operations that must be done by any authentication system that uses the proposed idea in the technical track of the study. These operations are: (See Figure 4.1) below.

- 1) **Classify** the selected characters (by the system) into a set of classes. (i.e., alphabet letters, digits, special symbols and Emoji pictures from different categories).
- 2) **Construct** a set of table (keyboards) of ($n \times m$) dimensions. And **distribute** the characters of each class in one of these tables.
- 3) **Assign** (randomly) a code (ASCII code) for each **table**, **row** in table and **column** in table.
- 4) **Build** a private coding list (for the authentication system) by coding each character in each table (keyboard) by three codes (**Table code**, **Row code** and **Column code**) For example: Code of: 🚚 is @8V

E	%	+	U	d	3	;	@	V	0	>	T	5	W
F	😊	😄	😁	😂	😃	😄	?	🏠	🏡	🏢	🏣	🏤	🏥
[😞	😟	😠	😡	😢	😣	}	🏠	🏡	🏢	🏣	🏤	🏥
^	😞	😟	😠	😡	😢	😣	:	🌅	🌆	🌇	🌈	🌉	🌊
j	😞	😟	😠	😡	😢	😣	*	📈	🚢	🚣	🚤	🚥	🚦
z	😞	😟	😠	😡	😢	😣	s	🚗	🚘	🚙	🚌	🚎	🚏
6	💙	💜	💖	💚	❤️	💔	8	🚚	🚛	🚜	🚝	🚞	🚟

#	s	^	7	z	,	}	3	K	}	B	a	5	<
?	1	2	3	4	5	6	R	A	B	C	D	E	F
}	7	8	9	0	!	@	6	G	H	I	J	K	L
K	[]	{	}	()	+	M	N	O	P	Q	R
t	%	&	*	-	+	=	#	S	T	U	V	W	X
w	^	#	\$	/	?	~	f	Y	Z	.	,	;	:
7	<	>	"	'		_	4	()	{	}	[]

Figure 4.1: Tables (keyboard) of different classes of characters.

Adding Emoji pictures to the characters, which are already used in textual password, will increase the range of available characters that are used by users in writing their password. Also, coding each character using three codes (bytes) will increase the complexity of each character through increase the number of cases that are needed to be tested by attackers to guess each character.

4.2.2 Login session

After the authentication system complete the preparation operations, the registration/login session for the users to enter their passwords become ready. To enter each character in the user's Emoji password, the authentication system and user will cooperate to complete this task. The following steps demonstrate this task.

Step 1: the user **selects** the desired keyboard from the set of keyboards in the right panel by clicking on the radio button. See figure 4.2

Step 2: the authentication system **distributes** the characters in the selected keyboard randomly over its cells. See figure 4.2

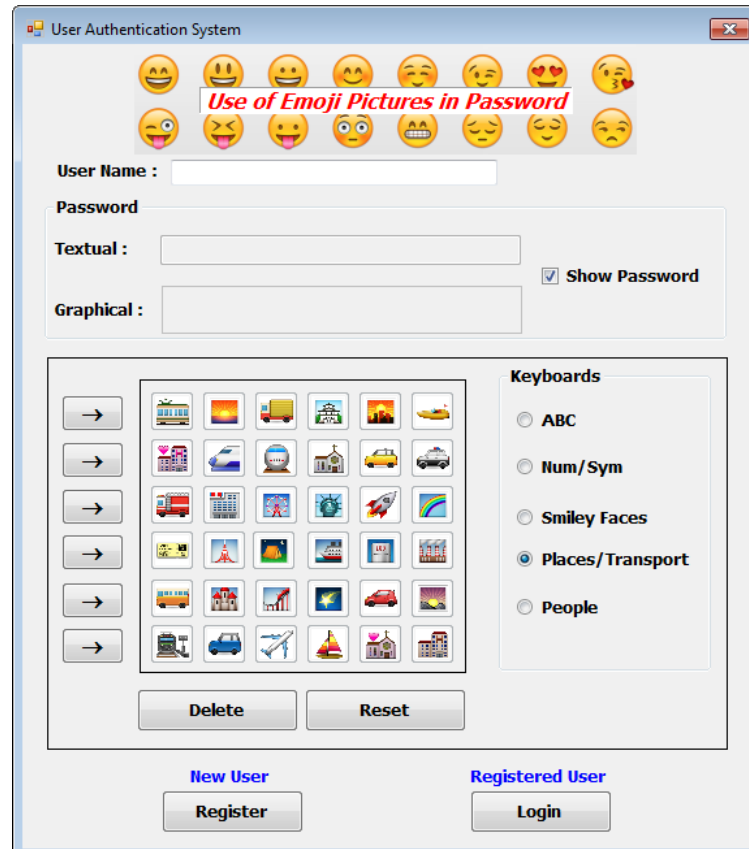
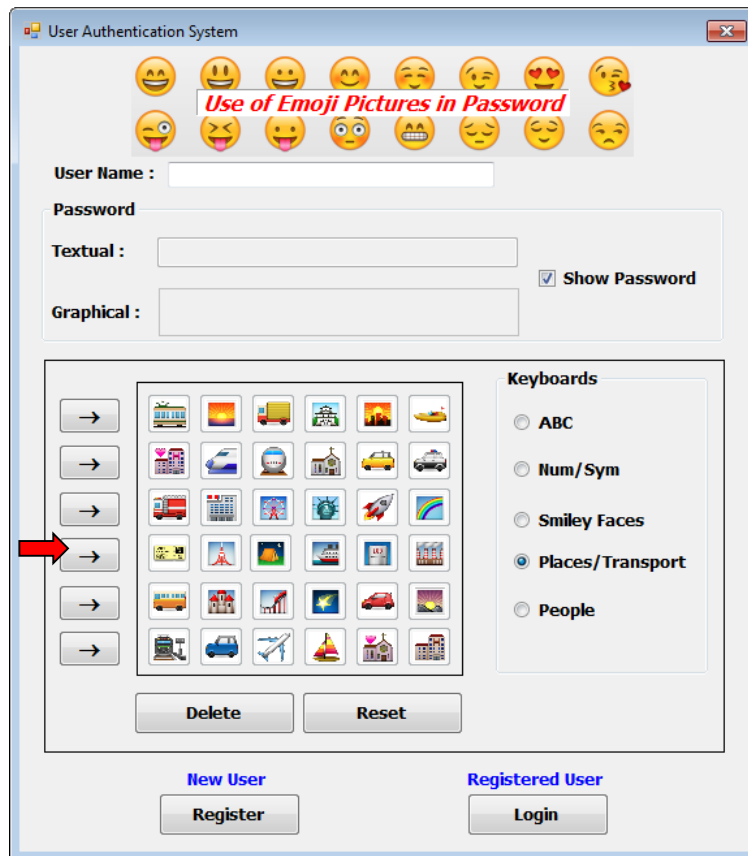


Figure 4.2: Step1 and Step2 of login session

Step 3: the user clicks on the arrow that points to the row that contains the desired character in the keyboard. See figure 4.3.

Step 4: the authentication system records the row number that is selected by the user (row number 2 in the figure 4.3).



Step 5: the authentication system transposes the rows and columns of the keyboard. This is done by exchange the elements in each row with the elements in each column. For example the character in row 2 and column 5 becomes in row 5 and column 2. See figure 4.4

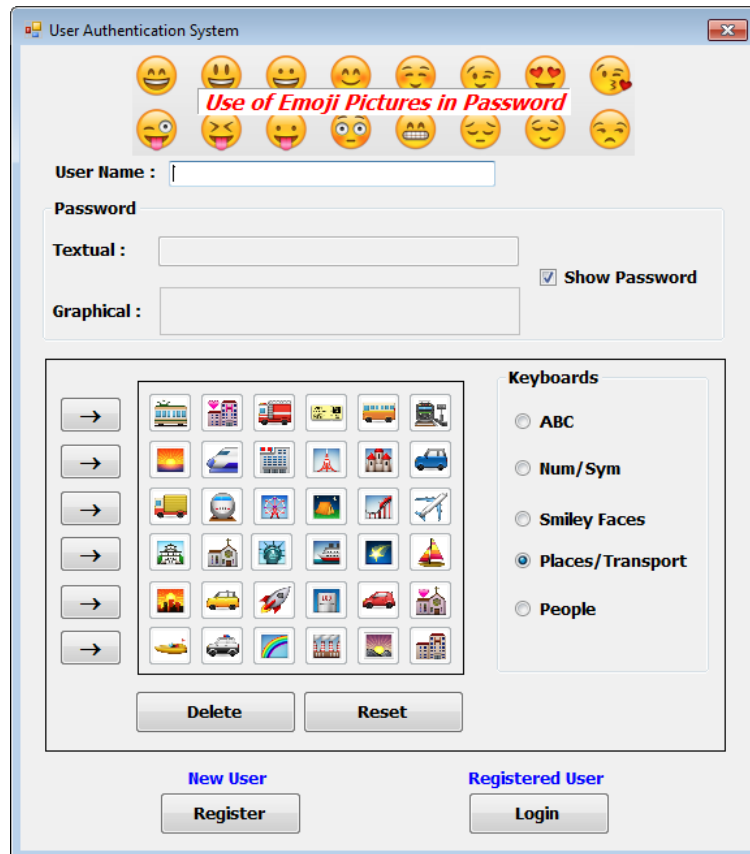


Figure 4.4: Step5 of login session

Step 6: the user clicks on the arrow that points to the row that contains the same selected character in step 3. See figure 4.5.

Step 7: the authentication system records the row number that is selected by the user (row number 5 in the figure 4.5).

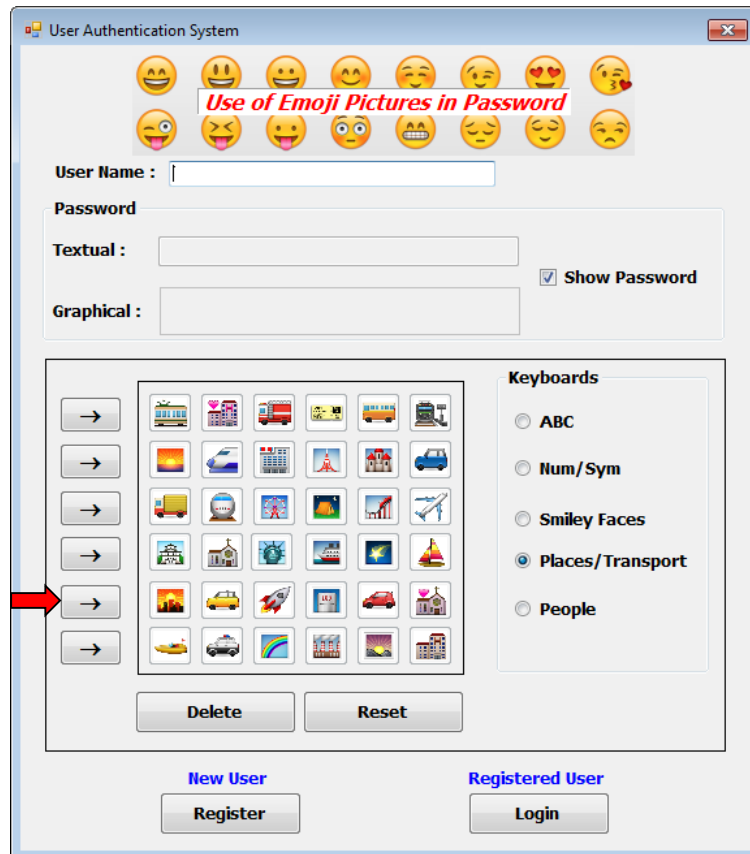


Figure 4.5: Step6 and Step7 of login session

Step 8: the authentication system uses the rows numbers in Step 4 and Step 7 (Numbers 2 and 5 above). The authentication system determines the selected character by the user and its code which assigned to it previously by the authentication system in preparation operation. This is done through getting the character at row 2 and column 5 from the keyboard in figure 4.3 (the keyboard used in Step 3). Certainly, only the authentication system can see (access) the mentioned keyboard, because the current keyboard that is now displayed to user (and attacker if he/she exists and monitors the login session) is completely different than the keyboard displayed in Step 3. This will gives the authentication system a high immunity against the shoulder surfing attacks.

Step 9: Authentication system, immediately, re-distributes randomly all the characters in the current keyboard. (See figure 4.6).

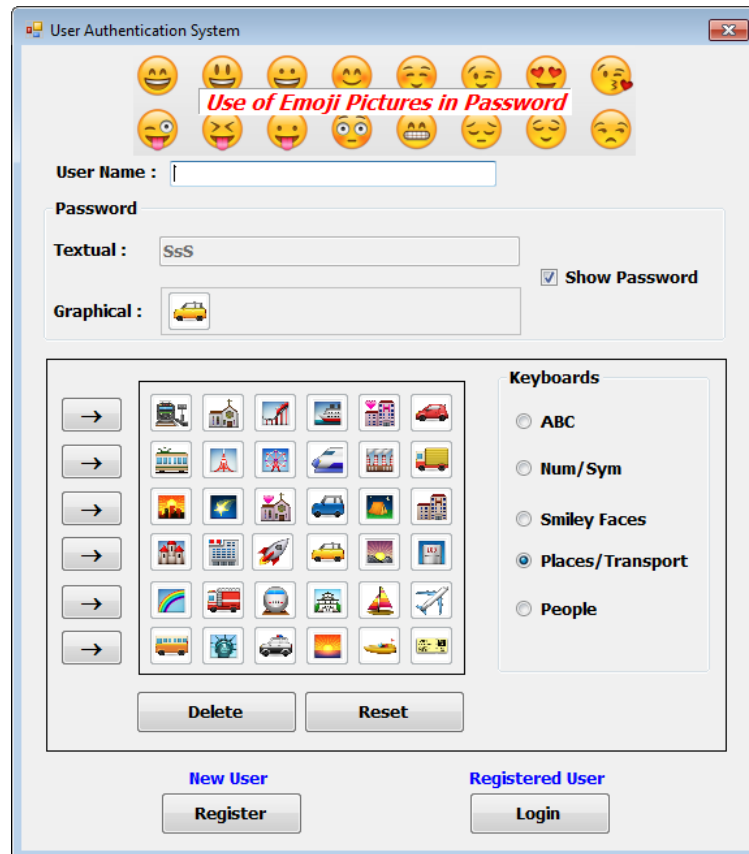


Figure 4.6: Step8 and Step9 of login session

As we see in the above figure, each Emoji picture (character) in the new password will be represented in three bytes (i.e., three ASCII codes). These codes represent Table code, Row code and Column code for the selected Emoji picture by user, as mentioned in the preparation operation above. The authentication system stores all the three bytes (codes) of all characters of the password in its database. The

selected character by the user in the above steps is 🚗, and its code (the three bytes of it), that have been determined previously by the authentication system in the preparation operation, are **SsS**. This code is set randomly and it has different code in other authentication systems.

This will keep the space required to store passwords in small size in comparison with the space used in most graphical password schemes. The same nine steps above will be used to enter each character in the new Emoji password.

It is necessary here to state that the authentication system may use any technique to encrypt the passwords in its database. This will add more difficulties against the attackers.

4.3 Compared the proposed model with previous studies based on the research mentioned in Chapter two

In this part we will work with the proposed model compared with existing models in previous studies in the chapter two, and be by comparison points mentioned in the model in terms of Shoulder Surfing, and time and, the size of authentication in the database.

4.3.1 Shoulder Surfing

Panduranga, P, Lavanya & Srinivasa (2013) The user chooses and registers a sequence of the chosen thumbnail photos that form password. This will make the understandability of the created password become additional complex and difficult, but it makes the images vulnerable to shoulder surfing because it is visible on the screen.

The proposed model in the letter if you type your password is pressure on the rows, which is determined not to be a visual images on the screen.

Patel M, & Modi N, (2014) proposed a new pictures password scheme. In this Recognition based technique is used with a numerical password which supply more security and easy to remember text and graphical password. Each group contains 25 pictures. The main wrong is increasing the load on the system. . It does not protect from shoulder surfing attack.

The proposed model in the thesis protects against shoulder surfing. Because the images are not clear the attacker.

Nithya (2014) the user can decide the places of the four regions which he/she finds simple to remember. The user can introduce his/her own images for creating the graphical passwords and also for make stronger security, Perhaps the biggest obstacle for current graphical passwords is that the shoulder surfing problem.

The proposed model in the thesis. Are not taken to identify the image, but we define rows by which to choose photos in writing password..

Ayannuga (2012) proposed a graphical password scheme where login need that users recognize images from their portfolio. But enter the password from the keyboard, not the mouse.

The proposed model is the process of determining of the rows that define the images in writing the password be, through any kind of inclusion of operations writing password, the as for in keyboard, or the mouse there are no fixed insert process..

Khalil ,M, A (2013) implemented an Auto Teller Machine (ATM) system that uses the user signature image as password beside user's PIN information, to realize more secure verification and authentication of ATM bank users, But it became vulnerable to theft.

The proposed model not use the image of the user's personal signature. Where there is a large number of images makes the admission process more convenient for the user, while in the case of the introduction of the signing of user, be one image or a static .image.

Lonkar V., Raut, S. & Mesakar S. (2014) proposed a new algorithm using water marking technique as the solution by using the random character set generated for each image to provide best system security.

In the proposed model not use the random letters. Uses photos in writing password.

4.3.2 Speed and time

Mathur, A, (2011) used the basic colors of red, black and white to double password protection but been slow during the logon process password. Take more time.

The proposed model enter the password be a quick process and not take a lot of time in the process of writing the password.

Sayli N Kokate, et. al. (2014) use CARP image is created for every login try but in this technique for each login steps of the new take more time.

The proposed model in the process of writing password. Not need to re-register new in each entry password process.

4.3.3 Size of Data Base

Rob,Jane&Karen,(2014) use faces the contrast between familiar and unfamiliar face recognition may be useful for graphical authentication systems. But they take up much space in the database.

In the proposed model is storage space in database, be balanced not be the great as in graphical password and, the small as textual password.

CHAPTER FIVE

CONCLUSIONS

After complete the study, which is focused on using Emoji pictures in writing password to overcome the drawbacks of textual passwords and graphical passwords, and presenting solid justifications about the feasibility of using Emoji pictures to achieve a good security for the information systems. Through seeing the successes that can be recorded in this study, we can summarize the conclusions obtained from the study as follows:

5.1 Analytical track

Use Emoji pictures in writing password helps users to use the recent and common technology used in most mobile phones and computed devices. The high feasibility for using Emoji pictures in writing password in user authentication systems. This makes the new password stronger and very difficult to guess by attackers through increasing the range of symbols that used in writing each character of the password.

Use Emoji pictures in writing passwords makes passwords easier to remember by users than before and facilitates for users to deal with the new password in more safe way. Through the comparison between password uses Emoji pictures and textual password, the recorded results (in tables and charts) showed that the password uses Emoji pictures is easy to remember by users with the passage of time. And easy to remember in spite of the differences in educational attainment and age groups for users. The results demonstrate, as in the tables and figures. Total of participants who forgot their password textual password 74% and Emoji Password 26%. Allow users choose and deal with a set of words or (sentence) that refers to the meanings of the Emoji pictures used in password instead of using the same characters (Emoji pictures) used. This will give the users an ability to deal with their password in a more safe way. Even if the user wrote the sentence that refers to the password, but not the password itself, on the note book or storing it in file on the computer storage unit, this doesn't give the attackers

any useful information that can be used to guess the password and removes any doubts about the truth of the characters being used in the password.

5.2 Technical track

Using Emoji pictures in writing password raises the complexity of the password (i.e., raises the number/range of available symbols used by user in writing password). Using Emoji pictures in writing password improves the immunity of the password against attackers by adding more ambiguity and confusion about the truth of the password. From the proposed user authentication system, we can facilitate the session of entering password for the user and make this session enjoyable and more secure. In addition to achieve a resistance against the shoulder surfing attacks. The proposed user authentication system uses not large storage space to store the new Emoji password compared with most graphical passwords used.

REFERENCES

1. Ari J., Ronald L. R. (2013). Honeywords: making password-cracking detectable, CCS'13, Berlin, Germany.
<http://www.arijuels.com/wp-content/uploads/2013/09/JR13.pdf>
2. A. S. Patrick, A. C. Long, and S. Flinn,(2003) "HCI and Security Systems," presented at CHI, Extended Abstracts (Workshops). Ft. Lauderdale, Florida, USA.,
<http://www.andrewpatrick.ca/CHI2003/HCISEC/w10-patrick.pdf>
3. Abraham, A, Grosan, C, & Chen, Y. (2006). Evolution of Intrusion detection Systems. Retrieved October 18, 2011, from
<http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.161.5620>
4. Ambarish Karole, Nitesh Saxena, and Nicolas Christin , A Comparative Usability Evaluation of Traditional Password Managers
<https://www.cis.uab.edu/saxena/docs/ksc-icisc10.pdf>
5. Ayannuga (2012) a Review of the Security and Usability Features of Different Graphical Password Authentication Schemes. African Journal of Computing & ICT, Vol 5. No. 5.
<http://www.ajocict.net/uploads/P14- Ayanuga - AJOCICT - Vol 5 Sep 2012.pdf>
6. Balaji, Lakshmi. A, .Revanth, .Saragini, Venkateswara Reddy(2012). AUTHENTICATION TECHNIQUES FOR ENGENDERING SESSION PASSWORDS WITH COLORS AND TEXT Advances in Information Technology and Management 71 Vol. 1, No. 2,
[https://www.google.jo/webhp?sourceid=chromeinstant&ion=1&espv=2&ie=UTF-8#q=Reddy-Authentication%20Techniques%20for%20Engendering%20Session%](https://www.google.jo/webhp?sourceid=chromeinstant&ion=1&espv=2&ie=UTF-8#q=Reddy-Authentication%20Techniques%20for%20Engendering%20Session%20)

7. Barate ,A,K, and Shinde,S ,S (2014) Graphical Password System using Different Techniques–A Review . International Journal of Engineering Trends and Technology (IJETT) – Volume 9 Number 11.

<http://www.ijettjournal.org/volume9/number-11/IJETT-V9P303.pdf>

8. Chin-Ling Chen ,Yu-Fan Lin , Fang-Yie Leu(2011) . An Improvement of Chen Et al.'s Scheme for Mobile Pay-TV. International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, Pages: 555-560, DOI: 10.1109/IMIS.2011.54.

http://www.researchgate.net/publication/224251743_An_Improvement_of_Cheng_Et_al.'s_Scheme_for_Mobile_Pay-TV

9. Charoen, D., Raman, M., & Olfman, L. (2008). Improving End User Behaviour in Password Utilization: An Action Research Initiative. Systemic Practice and Action Research, 21(1), 55. Retrieved January 6, 2010.

<http://link.springer.com/article/10.1007%2Fs11213-007-9082-4#page-1>

10. Dunphy ,p (2012) usable , secure and deployable graphical password

<https://openlab.ncl.ac.uk/publications/Dunphy-Thesis.pdf>

11. Gagan Dua , Nitin Gautam , Dharmendar Sharma , Ankit Arora(2013) REPLAY ATTACK PREVENTION IN KERBEROS AUTHENTICATION PROTOCOL USING TRIPLE PASSWORD . International Journal of Computer Networks & Communications (IJCNC) Vol.5, No.2.

<http://arxiv.org/ftp/arxiv/papers/1304/1304.3550.pdf>

12. ISCED(2011) International Standard Classification of Education (ISCED) UNESCO Institute for Statistics .

<http://www.uis.unesco.org/Education/Documents/isced-2011-en.pdf>

13. Jie Z., Xin L., Somasheker A. and Jennifer Z.. (2009). improving multiple password recall: an empirical study. European Journal of Information Systems
<http://www.unm.edu/~xinluo/papers/EJIS2009.pdf>
14. Kenneth R.(2006) Human Factors Considerations for Passwords and Other User Identification Techniques Part 2: Field Study, Results and Analysis
<http://www.tc.faa.gov/its/worldpac/techrpt/tc06-9.pdf>
15. Kemal Bicakci , (2011) A Multi-Word Password Proposal (gridWord) and Exploring Questions about Science in Security Research and Usable Security Evaluation
<http://www.nspw.org/papers/2011/nspw2011-bicakci.pdf>
16. Khairnar , Bhale (2014) A Survey on Password Security Systems . International Journal of Electronics and Computer Science Engineering, ISSN-2277-1956.
<http://citeseerx.ist.psu.edu/viewdoc/download;jsessionid=4FAC91434C9B681D27EF748C6F6CEBAA?doi=10.1.1.300.7626&rep=rep1&type=pdf>
17. Khalil, M, A (2013) Auto Teller Machine (ATM) System Security with User Signature Image as Password. Eng. &Tech. Journal .Vol31, Part (B), No. 4, 2013. <http://www.iasj.net/iasj?uiLanguage=ar>
18. Korenman, L. M., & Peynircioğlu, Z. P. (2007). Individual Differences in Learning and Remembering Music: Auditory versus Visual Presentation. Journal of Research in Music Education, 55(1), 48-64.
<http://jrm.sagepub.com/content/55/1/48.short>
19. Lokhande K. and Gajbhiye V. (2014) Extended Text and Color Based Session Password Security against Shoulder Surfing and Spyware, (Volume 1 Issue 7). <http://www.jetir.org/papers/JETIR1407015>

20. Lonkar,V, Raut,S, Mesakar, S, (2014) Graphical Password by Watermarking for security, Journal of Engineering Research and Applications Vol. 4, Issue 11. <http://www.slideshare.net/ijeraeditor/o0411058187>
21. Maitra, T, (2015) Cryptanalysis of a Secure Remote User Authentication Scheme Using Smart Cards rXiv: 1502.04820v1 [cs.CR] 17 Feb 2015. <http://arxiv.org/abs/1502.04820>
22. Matt Weir, Sudhir Aggarwal, Michael Collins, Henry Stern , Testing Metrics for Password Creation Policies by Attacking Large Sets of Revealed Passwords <http://dl.acm.org/citation.cfm?id=1866327>
23. Majumder, S, Chakraborty,S,& Das,S, (2014) A New Advanced User Authentication and Confidentiality Security Service. International Journal of Computer Applications. Volume 93 – No.11. <http://arxiv.org/ftp/arxiv/papers/1406/1406.4748.pdf>
24. Markus Scherer, Mark Davis, Kat Momoi, Darick Tong (2009) Proposal for Encoding Emoji Symbols,N3582,L2/09-025R2. <http://unicode.org/L2/L2007/07257-emoji-wd.html>
25. Mathur, A, (2011). Improved password selection method to prevent data thefts, International Journal of Scientific & Engineering Research. 2(6). <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.301.8248&rep=rep1&type=pdf>
26. Mishra, Dheerendra (2015) On the Security Flaws in ID-based Password Authentication Schemes for Telecare Medical Information Systems, Journal of Medical Systems, :39Issue:1Pages:1-16Provider:Springer,DOI <http://link.springer.com/article/10.1007%2Fs10916-014-0154-6#page-1>

27. Monroe, F., Reiter, M., and Wetzel, S.(1999) Password hardening based on keystroke dynamics ACM Conference on Computer and Communications Security, <http://cs.unc.edu/~fabian/papers/acm.ccs6.pdf>
28. Mohammed H, Almeshekah, Mikhail J. Atallah and Eugene H, Spafford (2015) "Defending against Password Exposure using Deceptive Covert Communication ". IN 47907-2086.
http://www.meshekah.com/research/publications_files/password_exposure_tr.pdf
29. Nazareth, Derek L. and Choi, J. (2015). A system dynamics model for information security management. Information & Management Vol. 52 Issue: 1. Pages: 123-134.Elsevier,DOI:10.1016/j.im.2014.10.009
<http://www.sciencedirect.com/science/article/pii/S0378720614001335>
30. Nithya (2014) GRAPHICAL PASSWORD , International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online) Vol. 2, Issue 3, pp: (57-63), Month: July - September 2014, Available at:
<https://www.google.jo/webhp?sourceid=chrome-instant&ion=1&espv=2&ie=UTF-8#q=graphical+password+r.+nithya+1+>
31. Nur Haryani Zakaria, David Griffiths, Sacha Brostoff, Jeff Yan , Shoulder Surfing Defence for Recall-based Graphical Passwords
https://cups.cs.cmu.edu/soups/2011/proceedings/a6_Zakaria.pdf
32. Patel M, & Modi N, ,(2014) Authentication Using Graphical Password . International Journal of Computational Engineering Research (IJCER). ISSN (e): Vol, 04 Issue, 11. <http://dl.acm.org/citation.cfm?id=1073002>
33. Pavan Gujjar Panduranga, G.Lavanya Devi, P.Srinivasa.(2013) A Study of Various Graphical Passwords Authentication Schemes Using Ai Hans Peter Wickelgren Approach. Journal of Computer Engineering (IOSR-JCE) Volume 10, Issue 6.
<http://www.iosrjournals.org/iosr-jce/papers/Vol10-issue6/C01061420.pdf>

34. Phillip Isola, Devi Parikh, Antonio Torralba, Aude Oliva (2011). Understanding the Intrinsic Memorability of Images.. Understanding the intrinsic memorability of images.NIPS,2011,preprint.
<http://web.mit.edu/phillipi/www/publications/UnderstandingMemorability.pdf>
35. Prasad, k, & Babu, R, (2013) Evolution of Authentication Mechanisms. International Journal of Computer Science and Mobile Computing. IJCSMC, Vol. 2, Issue. 11. <http://www.ijcsmc.com/docs/papers/November2013/V2I11201351>
36. Priti J. and Lalit D. (2013). Survey on authentication password techniques. International Journal of Soft Computing and Engineering (IJSCE), 3(2).
<http://www.ijscce.org/attachments/File/v3i2/B1430053213.pdf>
37. Rob J., Jane L. M. and Karen R. (2014). Face lock: familiarity-based graphical authentication. PeerJ 2:e444.LAST VISITED AT 22- 8- 2014.
<https://peerj.com/articles/444/>
38. Sayli N Kokate, Manasi P Khade, Priyanka D Patil, Ashwini B Gawali, Archana C Lomte (2014) CARP: AN IMAGE BASED SECURITY USING I-PAS , International Journal of Technical Research and Applications ,Volume 2, Issue 6.
<http://www.ijtra.com/view/carp-an-image-based-security-using-i-pas>.
39. Sed'enka, J, Balagani,K,S , Phoha ,V, Gasti, P, (2014). Privacy-preserving population-enhanced biometric key generation from free-text keystroke dynamics extended version. International Joint Conference on Biometrics.
<http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.301.8248&rep=rep1&type=pdf>

40. Shannon R(2006). Password Security: What Users Know and What They Actually Do. Usability News, 8(1),.

<http://psychology.wichita.edu/surl/usabilitynews/81/pdf/Usability%20News%2081%20-%20Riley.pdf>

41. Sophos (2009) "Security at risk as one third of surfers admit they use the same password for all

[http://www.sophos.com/pressoffice/news/articles/2009/03/password security.](http://www.sophos.com/pressoffice/news/articles/2009/03/password%20security)

42. Soumyadeb Chowdhury, Ron Poet, Lewis Mackenzie, A Comprehensive Study of the Usability of Multiple Graphical Passwords, School of Computing Science, University of Glasgow

<http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.397.6603&rep=rep1&type=pdf>

43. Suganya G, Kargavalli S, Christina V (2010) Proactive Password Strength Analyzer Using Filters and Machine Learning Techniques , International Journal of Computer Applications . Volume 7– No.14,

<http://ijcaonline.net/volume7/number14/pxc3871788.pdf>

44. Stone-Gross, M. Cova, L. Cavallaro, B. Gilbert, M. Szydowski, R. , C. Kruegel, and G. Vigna,(2009) "Your botnet is my botnet: Analysis of a botnet takeover," Tech. Rep.,

<https://seclab.cs.ucsb.edu/media/uploads/papers/torpig.pdf>

45. Xinlei Chen., C. Lawrence Zitnick(2014) Learning a Recurrent Visual Representation for Image Caption Generation. arXiv:1411.5654v1 [cs.CV] 20 Nov.

<http://arxiv.org/abs/1411.5654>

46. Xiong L., Jianwei N., Muhammad K. K. and Junguo L. (2013). An enhanced smart card based remote user password authentication scheme. Journal of Network and Computer Applications, 36(5).

<http://www.sciencedirect.com/science/article/pii/S1084804513000726>

47. Yan, J., Blackwell, A., Anderson, R. and Grant, A., (2000)“The Memorability and Security of Passwords -- Some Empirical Results”, Technical Report No. 500 (September 2000) Computer Laboratory, University of Cambridge.

<https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-500.pdf>