Republic of Iraq
Ministry of Higher Education
and Scientific Research
University of Diyala
College of Science

Smartphone Authentication Based on Iris Recognition

A Research
Submitted to the Department of Computer Science\ College of Sciences\ University of Diyala in a Partial Fulfillment of the Requirements for the Degree of Master in Computer Science

By

Rana Jassim Mohammed

Supervised By

Dr. Taha M. Hassan
Assistant Professor

Naji M. Sahib
Assistant Professor

2018 A.D. **1439A.H.**

بِسمِ ٱللَّهِ ٱلرَّحمنِ ٱلرَّحِيمِ

﴿قُلْ هُوَ الَّذِي أَنشَأَكُمْ وَجَعَلَ لَكُمُ السَّمْعَ وَالْأَبْصَارَ وَالْأَفْئِدَةَ قَلِيلاً مَا تَشْكُرُونَ 23 قُلْ هُوَ الَّذِي ذَرَأَكُمْ فِي الْأَرْضِ وَإِلَيْهِ تُحْشَرُونَ 24﴾

صَدقَ ٱللَّهُ العَظيم

سورة الملك

آيات (23-24)

Dedication

To...

My family

My dear parents

My dear husband

My children Safa & Abdallah

All our distinguished teachers those who paved the way for our science and knowledge

Rana Jassim Mohammed

Acknowledgment

*First of all, praise is to **GOD**, the lord of the whole creation, on all the blessing was the help in achieving this research to its end.*

*I wish to express my thanks to my supervisors, **Asst. Prof. Dr. Taha Mohammad Hassan** and **Asst. prof. Naji Mutar Sahib** for supervising this research and for the generosity, patience and continuous guidance throughout the work. It has been my good fortune to have the advice and guidance from them. My thanks to the academic and administrative staff at the Department of the computer sciences.*

*I would like to express my gratitude to **my father**, **my mother**, **my sister** and **my brothers** who were unlimited support and patience.*

*Finally, there are no words enough to thank **my dear husband** for being supportive and believing in me all the time and his encouragement during the period of my study. Praise be to God Who helped me and gave me the ability and power to perform and complete my thesis.*

I wish to express my thanks to MICHE (Mobile Iris Challenge Evolution) Group.

RANA -JASSIM

Linguistic Certification

I certify that this research entitled ***"Smartphone Authentication Based on Iris Recognition"*** *was prepared by* ***Rana Jassim Mohammed*** *and was reviewed linguistically. Its language was amended to meet the style of English language.*

Signature : Sarab

Name : Assist.Prof. Dr. Sarab Kadir Mugair

Date : 20/1/ 2019

Supervisor's Certification

We certify that this research entitled ***"Smartphone Authentication Based on Iris Recognition"*** *was prepared by* ***Rana Jassim Mohammed*** *under our supervisions at the University of Diyala Faculty of Science Department of Computer Science, as a partial fulfillment of the requirements needed to award the degree of* ***Master of Science in Computer Science.***

(Supervisor)

Signature :

Name:Assist. Prof. Dr.Taha M. Hassan

Date :20/ 1 / 2019

(Supervisor)

Signature :

Name : Assist. Prof. Naji M. Sahib

Date :20/ 1 /2019

Approved by University of a Diyala Faculty of Science Department of Computer Science.

Signature:

Name : Assist. Prof. Dr. Taha M. Hassan

Date :20/ 1 / 2019

(Head of Computer Science Department)

Examination Committee Certification

We certify that we have read this research entitled ***" Smartphone Authentication Based on Iris Recognition"****, and as an examining committee, examined the student* ***"Rana Jassim Mohammed"*** *in its contents and that in our opinion, it is adequate as fulfill the requirements for the Degree of Master in Computer Science at the Computer Science Department, University of Diyala.*

(Chairman)

Signature: Ayad Al Ani
Name: Prof. Dr. Ayad A. Al-Ani
Date:22/ 1/2019

(Member)

Signature:
Name: Assist. Prof. Dr. Salam A. Noaman
Date: 21/1/2019

(Member)

Signature:
Name: Dr. Jumana W. Saleh
Date: : 21/1/2019

(Member / Supervisor)

Signature:
Name:Assist. Prof. Dr. Taha M. Hassan
Date:21/1/2019

(Member/ Supervisor)

Signature:
Name: Assist. Prof. Naji M. Sahib
Date:21/1/2019

Approved by the Dean of College of Science, University of Diyala.

(The Dean)

Signature:
Name: Prof.Dr. Tahseen Hussein Mubarak
Date: 4/2/2019

Abstract

The widespread use of smartphones with internet connectivity has resulted in the storage of sensitive data. This has heightened the need to perform reliable user authentication on smartphones in order to prevent an adversary from accessing such data.

Biometric systems are getting further attention in the field of mobiles Security. Iris recognition is one of the fast, accurate, reliable and secure biometric techniques for human identification and verification. It provides automatic authentication of an individual based on characteristics and unique features in iris structure.

In this thesis, we build an efficient iris recognition system (IRS) in smartphones environment in order to decrease the error rate in the identification and verification process and obtain high recognition rate. This system consists of five main stages aiming to build an efficient IRS , the stages of the system are: (1) Picking up the iris patterns, (2) Locating the iris boundaries, (3)Transforming the iris boundaries to the polar coordinate system, (4) Features extraction, and (5) Pattern matching.

The proposed system uses a new method of circular histogram to find initial center of the iris in noisy images . In iris segmentation stage uses circular distribution of angles to segmented iris, for feature extraction uses three methods: (1)Color Histogram (CH), (2) Hu moments (HMs) and (3) Zernike moments (ZMs) to extract features and represent those features as numeric vectors stored in database so that they can be used in pattern matching stage and achieve high matching rate. Pattern matching stage uses (K Nearest Neighbor (KNN)) to find the similarity degree between the two irises, one is the tested iris template and the other stored in the database.

The proposed system has been tested by using MICHE -I (Galaxy S4) dataset has been registered 85% segmentation accuracy. The results indicate that the proposed system has high average accuracy rate compared to other existing methods where it (80%) average accuracy rate using (MICHE GS4) with ZMs, (78.6%) average accuracy rate with Color Histogram feature , and (50.5%) average accuracy rate with HMs.

Contents

List of Figures

List of Tables

List of Pseudo codes

List of Abbreviations

Abbreviations	Meaning
IRS	Iris Recognition System
BMP	Bitmap Image
C#	C sharp
MICHE	Mobile Iris Challenge Evaluation
CD	Circular Distribution
Avg	Average
DB	Data Base
EER	Equal Error Rate
FA	False Accepts
TA	True Accepts
ROC	Receiver Operating Characteristic
FAR	False Acceptance Rate
FRR	False Rejection Rate
T	Threshold
2D	Two Dimension
NMs	Normal Moments
ZMs	Zernike Moments
μ	Mean Value
σ	Standard Deviation
A_{nm}	Moment Based Operators
R_{pq}	Radial Polynomials
V'_{pq}	Complex polynomial

List of Symbols Table

Symbol	Meaning
*	Multiplication operation
+	Addition operation
/	Division operation
-	Subtraction operation
=	Equality sign
Θ	Theta
∑	Summation - sum of all values in range of series
|X|	The absolute value bars
Log	Logarithm
Δ	Delta
Σ	Sigma
%	Percent sign
Sin	Sin function
Cos	Cos function
⊕	Circled plus / oplus – xor
⊖	Circled minus /ominus
√	Square root
(*a*,*b*)	Ordered pair, collection of 2 elements
( )	Parentheses, calculate expression inside first
º	Degree, 1 turn = 360º

Chapter One

General Introduction

Chapter one
General Introduction

1.1 Introduction

A ‘Smartphone’ is defined as a mobile phone that can be used as a small computer and that connects to the internet, in spite of the first smartphone - IBM Simon - was introduced more than two decades ago, the world witnessed an immense evolution of smartphones after the introduction of the first iPhone in 2007, the world noticed a great growth for smartphones, the present smartphones are not only a computer, a camera, a database, a phone, a locator and contain all the information in the world at our fingertips, but a personal companion that can be considered part of our daily life , It is speculated that the smartphone’s role as a constant companion, helper, coach and guardian has only just begun[1].

"In less than two year, a smartphones could be your only computer", wrote Christina Bonnington on wried.com in 2015[2], referring to the rapid takeover of the consumer computing market by smartphones and tablet computers .

Modern phones and tablet computers provide unparalleled convenience to users, allow them to browse the social network, check emails, take photographs, bank and shop online on the go. Many modern mobile devices are provided with high resolution cameras, GPS, radio, accelerometer, and other sensors that enable novel application, such as instant video calls, navigation, fitness, and support for many other applications not practical with traditional laptop and desktop computers[3].

The number of mobile phone users worldwide is expected to pass the five billion mark by 2019 [4], and by 2018, the number of tablet computer users is projected to reach 1.34 billion [5].

This proliferation of smartphones and tablets raises concerns about the security and privacy of data stored on mobile devices if there are lost, stolen, or hacked. An attacker with physical accesses to a mobile device can potentially steal a user's banking information, read his/her emails, look at private photos, and perform other criminal actions. The scale of the problem is vast, according to the consumer Reports.org, 2.1 million mobile phones were stolen and 3.1 million phones were lost in 2013 in United states alone [6].

The initial countermeasures for restricting unauthorized access of mobile devices were password (e.g Google Android-based device) and four digit PIN codes (e.g iPhone smartphones and iPad tablets). However, this approach has proven ineffective, for the sake of conveniences, many users choice easily guessable passwords and PINs. For example ,according to TIME magazine, the most widely iPhones PIN numbers in 2011 were are follows :

1. “1234” 2. “0000” 3. “2580” 4. “1111”
5. “5555” 6. “2683” 7. “0852” 8. “2222”
9. “1212” 10. “1998”

Similar problems still exist in 2016 [7,8].

Unlike PCs and laptops, users store their personal data on the smartphone, health information, passwords, daily calendars, and much more[10]. Hence, secure authentication of a smartphone user’s identity is crucial.

There must be a mechanism to authenticate users and it is difficult to be imitated or stolen which is unique to each user to achieve security balancing for smartphones. ‘Biometrics’ could be ideal for this

purpose[1]. Some devices that have the ability to capture biometric data are shown in Figure (1.1).

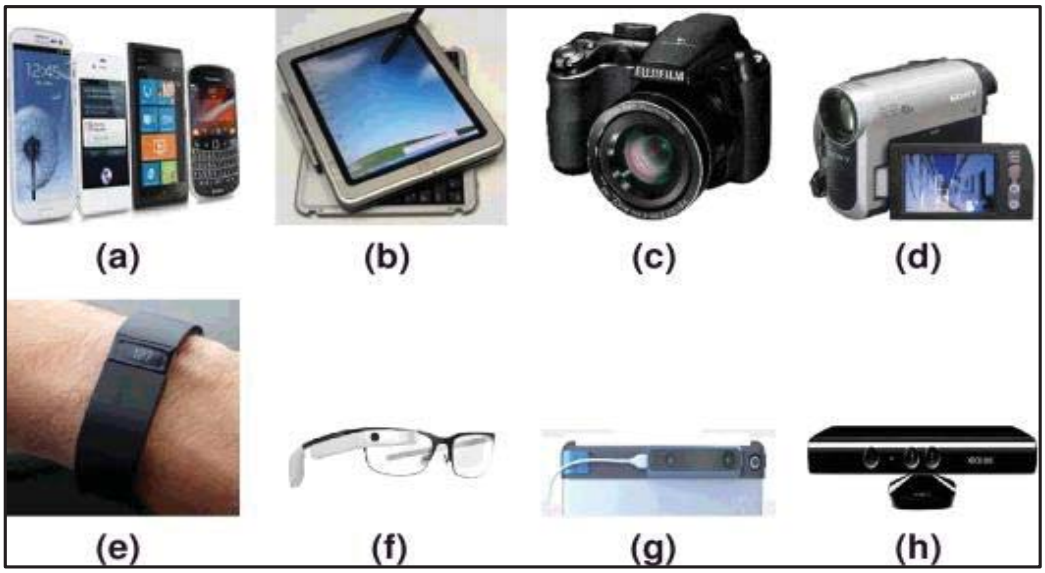

Figure (1.1) : Examples of mobile devices capable of capturing biometric data: (a) smartphones, (b) tablet computers, (c) digital cameras, (d) digital video recorders, (e) wearable activity trackers (e.g., Fitbit), (f) wearable head-mount displays (e.g., Google Glass), (g) 3D sensors [e.g., STRUCTURE (2014)], and (h) portable game consoles (e.g., XBOX Kinect)[1].

1.2 Biometrics

Biometrics is the science of recognizing individuals depend on their physical or behavioral traits, there are more physical characteristics that may be used for identification such us fingerprints, hand geometry, palm prints, iris patterns and retinal patterns, behavioral characteristics include signature, keystroke dynamics and voice pattern[11].

Traits of individuals that can be used for identification or verification purposes. refer to the technology of identifying a person or verifying a person identity based on these unique biometric traits. Such technology is widely deployed in several applications today, from immigration and border control to access control in online banking, ATM, laptops, and mobile phones[12,13]. Passwords and PINs are susceptible to loss, theft, and guessing attacks. Similarly, magnetic cards

are subject to loss, theft , forgery, and duplication. Biometric-based techniques, on the other hand, are resilient to such threats: people's biological traits cannot be misplaced or forgotten, and are difficult to steal or forge[12]. Biometric techniques are categorized as either **st□tic** or **□□□□mic**. Static biometrics examine physiological traits of the individual such as face, fingerprints, iris, and hand geometry. Dynamic biometrics examine behavioral characteristics such as keystroke dynamics and voiceprints. Some biometric types are shown in Figure (1.2).

Any physiological or behavioral traits which satisfy a number of requirements such as universality, permanence, distinctiveness, performance, collectability, acceptability, and circumvention can be classified as a practical biometric trait, out of all the multiple physical characteristics available, for physiological characteristics the iris is consider a common examples that can be used [1]. A brief comparison of these modalities is shown in Figure (1.3).

A good biometric is described by using of a feature that is highly unique so that the chance having of any two people will be minimal with the same characteristics, stable so that the feature doesn't change over time, and be easily captured in order to provide convenience to the user, and prevent misrepresentation of the feature[13].

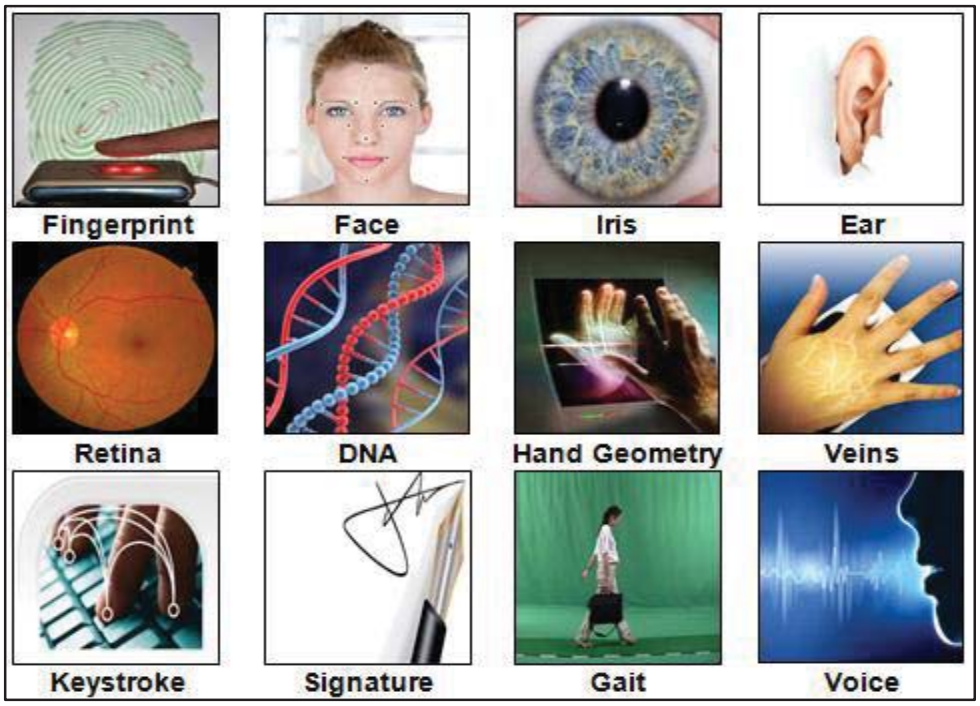

Figure (1.2) Examples of different biometric types[13].

BIOMETRIC	FINGERPRINT	FACE	HAND GEOMETRY	IRIS	VOICE
					
Barriers to universality	Worn ridges; hand or finger impairment	None	Hand impairment	Visual impairment	Speech impairment
Distinctiveness	High	Low	Medium	High	Low
Permanence	High	Medium	Medium	High	Low
Collectibility	Medium	High	High	Medium	Medium
Performance	High	Low	Medium	High	Low
Acceptability	Medium	High	Medium	Low	High
Potential for circumvention	Low	High	Medium	Low	High

Figure (1.) Comparison of various biometric modalities[11].

1. Iris Recognition

Iris recognition is the method of recognizing individuals depend on their iris pattern. As in Figure (1.4), the annular area within the eye