THE INFLUENCE OF EMOTIONS ON TOUCH BEHAVIOURAL FEATURES FOR BIOMETRIC AUTHENTICATION

BY

RASHA MAHDI ALI ABDULSLALM

A thesis submitted in fulfilment of the requirement for the degree of Doctor of Philosophy in Information Technology

Kulliyyah of Information and Communication Technology
International Islamic University of Malaysia

JULY 2022

ABSTRACT

Touchscreen devices have become increasingly popular recently, mostly due to the affordability and availability of smartphones and tablets. Smartphone security constitutes a necessary requirement due to the functions of smartphones that hold sensitive information and perform essential tasks. Numerous authentication techniques such as passwords, personal identification number codes, number locks, and graphical passwords are presently used to secure smartphones from unauthorised access. However, these techniques remain vulnerable to certain types of security breaches. To overcome the drawbacks of the current authentication techniques, behavioural biometric technology such as touch gesture authentication is being increasingly investigated. The touchscreen is a major source of data input, allowing users to make various movements such as scrolling, tapping, swiping, and so on. Touch gesture biometrics are identified as the process of computing and evaluating user touch gestures on touchscreen devices. When users interact with touchscreen devices, some forms of digital signatures are generated. These signatures may be used as an individual verifier because they are considered to be distinctive and unique for each user. Touch-based data collected from touchscreen sensors has been useful in various applications, such as emotion recognition, automotive vehicles, banking applications, signature verification, health care applications, gaming applications, and others. Recently, a number of studies have focused on using touch gestures as a form of biometric authentication for touchscreen mobile devices. However, these studies have faced several issues when developing touch gesture behavioural biometric approaches, mainly in improving the accuracy of the authentication system. Moreover, several behavioural factors such as emotions and their influences on touch gesture user authentication performance have remained unaddressed. In this research, the effect of emotions on user behaviour in influencing the performance of a touch gesture authentication approach was examined. To achieve this, a touch gesture behavioural biometric authentication approach was developed, and suitable experiment procedures were designed. Furthermore, a controlled experiment was conducted which allowed the collection of touch data in different emotional states (emotional and normal). An Android application was developed in order to collect the 572 touch gestures of 25 participants from touchscreen smartphones. The participants' emotion states were induced using film clips' emotion elicitation method and categorised based on the discrete emotion dimension (amusement, anger, sadness, tenderness, fear, and disgust). Eighteen touch features were extracted from the touch data and five machine learning classifiers were employed. Then, they were compared to evaluate the approach's accuracy. The results of the experiment indicate that the Random Forest technique achieved the best accuracy for the developed touch gesture authentication approach with 95.129% accuracy, 4.8% FRR, 0.22% FAR, and 2.5% EER. Furthermore, the influence of emotions was significant on the accuracy performance of the developed approach due to the accuracy value drop to 82.51%. Only 38.25% of the emotion datasets were correctly classified.

ملخص البحث

يشكل أمن الهواتف الذكية مطلبًا ضروريًا بسبب المعلومات الحساسة التي تحتويها والمهام الضرورية التي تؤديها. تستخدم في الوقت الحالي العديد من تقنيات المصادقة لتأمين الهواتف الذكية من الوصول غير المصرح به مثل كلمة المرور والرمز السري وقفل الرقم وكلمة المرور الرسومية. ومع ذلك، تظل هذه التقنيات عرضة لأنواع معينة من الانتهاكات الأمنية. للتغلب على عيوب تقنيات المصادقة الحالية، يتم التحقيق بشكل متزايد في تقنية القياسات الحيوية السلوكية مثل المصادقة بإيماءات اللمس. تُعرّف المقاييس الحيوية لإيماءات اللمس بعملية حساب وتقييم إيماءات اللمس البشري على الأجهزة التي تعمل باللمس. عندما يتفاعل المستخدمون مع الأجهزة التي تعمل باللمس، يتم إنشاء شكل من أشكال التوقيع الرقمي. ويمكن استخدام هذه التوقيعات كمدقق فردي لأنها تعتبر مميزة وفريدة من نوعها لكل شخص. ركزت العديد من الدراسات مؤخرا على استخدام إيماءات اللمس كمصادقة القياسات الحيوية السلوكية للأجهزة المحمولة التي تعمل باللمس. ومع ذلك، واجهت هذه الدراسات العديد من المخاوف عند تطوير طرق القياسات الحيوية السلوكية بإيماءات اللمس، وخاصة فيما يتعلق بتحسين دقة نظام المصادقة. كذلك ظلت العديد من العوامل السلوكية مثل العواطف وتأثيرها على أداء مصادقة إيماءة لمس المستخدم دون معالجة. في هذا البحث، تم فحص تأثير العواطف على سلوك المستخدم، والذي بدوره يؤثر على أداء تقنية المصادقة بإيماءات اللمس. لتحقيق ذلك، تم تطوير نهج مصادقة القياسات الحيوية السلوكية بإيماءات اللمس، وتم تصميم إجراءات التجربة المناسبة. علاوة على ذلك، تم إجراء تجربة مضبوطة سمحت بجمع بيانات اللمس في حالات عاطفية مختلفة للمشاركين (عاطفية وطبيعية). تم تطوير تطبيق اندرويد من أجل جمع 572 إيماءة لمس لـ 25 مشاركًا من الهواتف الذكية التي تعمل باللمس. تم إثارة حالات عاطفة المشارك باستخدام طريقة استنباط العاطفة بمقاطع الفيلم وتصنيفها بناءً على البُعد العاطفي المنفصل (التسلية، والغضب، والحزن، والحنان، والخوف، والاشمئزاز). تم استنباط ثمانية عشر ميزة تعمل باللمس من بيانات اللمس وتطبيق خمس مصنّفات للتعلم الآلي. ثم تمت مقارنتهم لتقييم دقة النهج. تشير نتيجة التجربة إلى أن تقنية Random Forest حققت أفضل دقة لنهج المصادقة بإيماءات اللمس المطور بدقة 95.129٪. وقد حققت 4.8٪ لمعدل الرفض الخاطئ (FRR) و0.22٪ لمعدل القبول الخاطئ (FAR) و2.5٪ معدل الخطأ المتساوي (EER). علاوة على ذلك، كان تأثير الحالات العاطفية مهمًا على دقة أداء النهج المطور من خلال الانخفاض إلى 82.51٪. تم تصنيف 38.25٪ فقط من مجموعة بيانات المشاعر بشكل صحيح.

APPROVAL PAGE

The thesis of Rasha Mahdi Ali Abdulsalam has been approved by the following:

Akram MZM Khedhe
Supervisor

Normaziah bt Abdul Aziz
Internal Examiner

Ali Selamat
External Examiner

Adel Al-Jumaily
External Examiner

Meftah Hrairi
Chairman

DECLARATION

I hereby declare that this thesis is the result of my own investigations, except where otherwise stated. I also declare that it has not been previously or concurrently submitted as a whole for any other degrees at IIUM or other institutions.

Rasha Mahdi Ali Abdulsalam

Signature .... Date ....

INTERNATIONAL ISLAMIC UNIVERSITY MALAYSIA

DECLARATION OF COPYRIGHT AND AFFIRMATION OF FAIR USE OF UNPUBLISHED RESEARCH

THE INFLUENCE OF EMOTIONS ON TOUCH BEHAVIOURAL FEATURES FOR BIOMETRIC AUTHENTICATION

I declare that the copyright holders of this thesis are jointly owned by the student and IIUM.

No part of this unpublished research may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise without prior written permission of the copyright holder except as provided below

1. Any material contained in or derived from this unpublished research may be used by others in their writing with due acknowledgement.

2. IIUM or its library will have the right to make and transmit copies (print or electronic) for institutional and academic purposes.

3. The IIUM library will have the right to make, store in a retrieved system and supply copies of this unpublished research if requested by other universities and research libraries.

By signing this form, I acknowledged that I have read and understand the IIUM Intellectual Property Right and Commercialisation policy.

Affirmed by Rasha Mahdi Ali Abdulsalam

……..…………………….. ………………………..
Signature Date

I dedicate this work to Omi Hussen. I miss you, and we will meet in Jannah InshAllah.

ACKNOWLEDGEMENTS

In the Name of Allah, the Most Merciful, the Most Beneficent. Praise be to the Lord of all worlds. Prayers and peace be upon our Prophet, Mohammad. I humbly express my appreciation and thanks to my creator Allah subhanahu wa ta'ala for his blessings and guidance.

To my parents, Dr Mahdi and Qiblah. Thank you for the support and everything you gave me in my life. You believe in me more than I believe in myself. Forgive me for any shortcomings. I also express my appreciation to my family and friends; thank you for helping me and stay by my side during this time.

I am incredibly thankful to my supervisor Prof. Dr Akram MZM Khedhe for his continuous encouragement, support, and patient. Moreover, a special gratitude to Assoc. Prof. Dr Normaziah bt Abdul Aziz, Prof. Dr Ali Selamat, and Prof. Dr Adel Al-Jumaily for their guidance and comments that helped me to enhance my work.

My heartfelt gratitude goes to IIUM and this country for accepting me and for the opportunities they gave me. Finally, I like to express my appreciation to Aden University and my country Yemen for funding my study. GG

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATION

2-D	Two Dimensional
3-D	Three Dimensional
AUC	Area Under the ROC Curve
AC	Accuracy
API	Application Programming Interface
ARFF	Attribute-Relation File Format
ATM	Automated Teller Machine
CPU	Central Processing Unit
CSV	Comma Separated Values
DES	Differential Emotions Scale
DTW	Dynamic Time Wrap
ECG	Electrocardiography
EEG	Electroencephalography
EER	Equal Error Rate
EMUI	Emotion User Interface
FAR	False Accepted Rate
FP	False Positive
FRR	False Rejected Rate
GMM	Gaussian Mixture Model
GNU	General Public License
GUI	Graphical User Interface
HRV	Heart Rate Variability
IAPS	International Affective Picture System
IBK	Instance Based Learner

ID	Identity document
IIUM	International Islamic University of Malaysia
ISO	International Organization for Standardization
JDK	Java Development Kit
JRE	Java Runtime Environment
KBA	Knowledge-Based Authentication
KICT	Kulliyyah of Information and Communication Technology
KNN	K-Nearest Neighbours
MATLAB	Matrix Laboratory
MCMC	Markov Chain Monte Carlo
MLP	Multi-Layer Perceptron
MSO	Microsoft office
OS	Operating System
PIN	Personal Identification Number
PSO-RBFN	Particle Swarm Optimization-Radial Basis Function Networks
PUK	Pearson VII Universal kernel
RBFN	Radial Basis Function networks
ROC Curve	Receiver Operating Characteristic Curve
SAM	Self-Assessment Manikin
SMO	Sequential Minimal Optimization
SVD	Singular Value Decomposition
SVDE	Support Vector Distribution Estimation
SVM	Support Vector Machine
TER	Total Error Rate
TP	True Positive
UM	University of Malaysia
WEKA	Waikato Environment for Knowledge Analysis

WkNN	Weighted k-Nearest Neighbour
XML	Extensible Mark-up Language

CHAPTER ONE

INTRODUCTION

1.1 RESEARCH OVERVIEW

Over the years, mobile technology has improved remarkably. Through essential inventions in hardware design, wireless technology, networking, human-computer interaction, and power-efficient computing, mobile devices offer access to information and computation processes everywhere and anywhere. The latest growth in mobile technology has provided a new type of programmable mobile device, the smartphone. Smartphones present modern mobile operating systems, location-aware services, large application stores, and massive social networks that reach millions of users globally, thus impacting their lives (Laffaye, 2014). According to Statista (2019), 45.12% of the population has a smartphone, with 3.5 billion smartphone users in 2020.

Today, more and more people use smartphones to manage their lives. Smartphones are being used to perform significant tasks, such as transferring money, and storing private and sensitive information, such as financial details, pictures, emails, password list, and location history. However, the availability of these services and private information poses multiple security risks and attacks. Data security is as essential for smartphones as it is for laptops, tablets, or any electronic devices. Thus, it is an important priority to protect their integrity, confidentiality, and availability. Numerous authentication schemes are presently used to secure smartphones from unauthorised access. However, these techniques remain vulnerable to certain types of security breaches (Shafique et al., 2017).

Authentication is an essential stage to protect the confidentiality and integrity of mobile devices that can only be sustained by identifying the end users. Numerous authentication schemes such as password, PIN code, number lock, and graphical password are presently used to secure smartphones from unauthorised access. However, these techniques remain vulnerable to certain types of security breaches such as shoulder surfing, Brute Force, smudge, and dictionary attack (Shafique et al., 2017).

To overcome the drawbacks of password, PIN code, number lock, and graphical password authentication, biometric-based methods have been investigated in smartphone authentication (Meng et al., 2015). Within a wide variety of security systems, biometrics technology is now progressively adopted. These systems verify users using their human assessable traits, such as keystroke dynamics, speech, gait, fingerprint, signature, and hand geometry (Bokor, Antal, & Aszl, 2014).

Based on the biometric characteristics used to identify the users, biometric methods consist of two categories: behavioural and physical. Physical biometrics have been employed in mobile phone authentication, as each human's physical biometric characteristics are unique and not transferable or duplicable (Meng et al., 2015). However, physical biometrics can be expensive, hard for collect, and require special purpose hardware. Moreover, physical biometric systems are complex, can be challenging to implement, and have low user acceptability (Alariki & Manaf, 2014; Shafique et al., 2017).

Behavioural biometrics are another potential solution to verify and identify users by measuring their unique behavioural characteristics. The most common behavioural characteristics include gait, voice, signature, keystroke dynamics, mouse dynamics, and touch dynamics. The behavioural biometric system provides a transparent security layer that is easy to execute, as it only requires a software implementation (Yampolskiy & Govindaraju, 2010). Additionally, collecting data in most behavioural biometric systems can be cost effective without the need for special hardware (Yampolskiy & Govindaraju, 2008).

Currently, different behavioural biometric techniques have been considered in mobile device authentication such as gait recognition, voice recognition, signature recognition, keystroke dynamics, mouse dynamics, and touch dynamics. With the arrival of touchscreen smartphones, touch gesture biometrics have become important to both industry and academia (Meng et al., 2015).

Touch gesture biometrics are identified as the process of computing and evaluating human touch strokes on touchscreen devices. When humans interact with touchscreen devices, some form of a digital signature is generated. These signatures may be used as an individual verifier, where they are considered to be distinctive and unique for each person (Teh et al., 2016).

Because practically all smartphones utilize the touch screen as the primary input method, touch gesture behaviour is becoming more relevant compared to its counterpart, keyboard behaviour, as the popularity of touchscreen mobile phones grows (Meng et al. 2013). Even if a shoulder surfer witnesses the full motion, a gesture-based authentication system would make it more difficult to repeat the password. Subtleties such as speed, pressure, force, flexibility, and individual anatomical variances would hinder the casual viewer of the password from mimicking the password (Niu and Chen 2012).

Extensive research has been conducted to use touch-based data collected from touchscreen sensors for a variety of applications, including automotive applications (Pitts et al. 2014), authentication in banking applications (Basar et al. 2019), Signature verification (Ren et al. 2020), health care applications (Farhana et al. 2019; Siek et al. 2011), emotion recognition applications (Meng et al. 2021; Shah, Teja, and Bhattacharya 2015), touch recognition systems (Park et al. 2019), gaming applications (A. Lee et al. 2015), Free-hand-Sketching application (Yi Li et al. 2015), and others.

A growing number of research have recently focused on the use of touch gestures behavioural biometric as an authentication method for touchscreen mobile devices. The studies reported that touch gesture could identify user behaviour and can be used as an authentication scheme to secure touchscreen mobile devices by authenticating legitimate users and detecting imposters (Alariki & Manaf, 2014; De Luca et al., 2012; Beton, Marie, & Rosenberger, 2013; Shahzad, Liu, & Samuel, 2013; Cai et al., 2013; Lin, Chang, & Liang, 2013; Alpar, 2015; Li et al., 2015; Antal & Szabó, 2016). However, while developing touch gesture behavioural biometric methods, these research ran into number of challenges, the most significant of which was enhancing the accuracy of the authentication systems (De Luca et al., 2012; Beton et al., 2013; Alariki & Manaf, 2014; Burgbacher, Prätorius, & Hinrichs, 2014; Alpar, 2015).

Some studies reported that the gesture length and type affects the accuracy performance of the authentication system (De Luca et al., 2012; Bokor et al., 2014; Alpar, 2015; Li et al., 2015; Matsubara et al., 2016). If the length of the gesture is too short, the accuracy of the system is low, but if it is too long it affects the usability of the authentication system (Teh et al., 2016). Moreover, one of the challenges in previous studies is the feature selection and extraction (De Luca et al., 2012; Alariki & Manaf, 2014; Burgbacher et al., 2014). Selecting and extracting the appropriate set of touch gesture features have a huge impact on the system performance (Mahfouz, Mahmoud, & Eldin, 2017).

Another issue is the selection of the appropriate machine learning classifier for the authentication system. Using the appropriate machine learning technique, to be compared to other techniques, affects the performance of the authentication system (Beton et al., 2013; De Luca et al., 2012; Matsubara et al., 2016). Other issues faced by previous studies in the development of touch gesture authentication systems included user body posture (Lin et al., 2013; Burgbacher et al., 2014), subject size (Beton et al., 2013; Alariki & Manaf, 2014; Gong et al., 2016), and the number of training sample (Shahzad et al., 2013; Burgbacher et al., 2014; Alpar, 2015; Martinez-Diaz, Fierrez, & Galbally, 2016).

Individual behaviour is not totally repeatable, which is one of the issues with behavioural biometrics. Rather, it is heavily influenced by a variety of external factors, including mood, emotion, exhaustion, health, drugs, conflicts, prior experiences, and the surrounding environment (Yampolskiy & Govindaraju, 2010; Abdulkader, Atia, & Mostafa, 2015; Cherifi et al., 2010; Revett, 2010). Some behavioural recognition systems are very sensitive to all these factors, depending on the sensor being used (keystroke dynamics, mouse dynamics, touch dynamics, etc.) (Cherifi et al., 2010).

Additionally, emotions impact a person's behavioural touch gestures, with a simple finger movement on a touchscreen providing a profound emotional experience (Zhu & Li, 2014). A biometric system's robustness must be validated against all of these causes of variation before it can be used in a real-world setting (Cherifi et al., 2010). Given that the major goal of touch gesture biometric system design has been to improve accuracy (Sayed et al., 2013), the impact of an individual's emotional state on touch gesture biometric system needs to be investigated (Alariki, Manaf, and Mousavi 2016; Teh et al. 2016).

1.2 PROBLEM STATEMENT

Behavioural biometrics can be used as an alternative authentication method for mobile devices to overcome the drawback of current authentication methods. Touch gesture is gaining popularity as a behavioural biometric authentication method. Touch gesture can identify user behaviour and be used as an authentication scheme to secure mobile devices by authenticating legitimate users and detecting imposters.

Recently, an increasing number of studies have focused on developing touch gesture authentication schemes (De Luca et al., 2012; Bokor et al., 2014; Alpar, 2015; Li et al., 2015; Matsubara et al., 2016; Beton et al., 2013; Alariki & Manaf, 2014; Burgbacher et al., 2014; (De Luca et al. 2012)Lin et al., 2013; Gong et al., 2016; Shahzad et al., 2013; Martinez-Diaz et al., 2016). These studies faced several concerns when developing touch gesture behavioural biometric schemes, mainly in enhancing the accuracy of the authentication schemes. Based on the previous studies, several issues affected the performance of the authentication systems namely, gesture length and type, feature extraction, selection of the machine learning classifier, subject size, and training sample number.

Moreover, one of the problems with behavioural biometrics is that individual behaviour itself is not perfectly repetitive. Instead, it is highly dependent on many factors such as mood, emotion, tiredness, health, drugs, conflict, previous events, and surrounding environment (Yampolskiy & Govindaraju, 2010; Abdulkader et al., 2015; Cherifi et al., 2010; Revett, 2010).

In addition, emotions have an influence on an individual behaviour's touch gesture where a simple finger movement on a device touchscreen can carry rich emotional experience (Zhu & Li, 2014). In order to be used in real-world context, the performance of a biometric system needs to be tested against these variations (Cherifi et al., 2010). Although the primary focus in the design of touch gesture biometric systems has been on improving their accuracy (Sayed et al., 2013), the influence of individual emotions on the behaviour of touch gesture biometric systems requires additional investigation (Alariki et al. 2016; Teh et al. 2016).

From the literature review, it can be observed that when developing a touch gesture authentication system, different aspects need to be considered. Furthermore,