

2015


A Dynamic Behavioral Biometric Approach to Authenticate Users Employing Their Fingers to Interact with Touchscreen Devices

Arturo Ponce

Nova Southeastern University, arturo.ponce@gmail.com

This document is a product of extensive research conducted at the Nova Southeastern University [College of Engineering and Computing](#). For more information on research and degree programs at the NSU College of Engineering and Computing, please click [here](#).

Follow this and additional works at: http://nsuworks.nova.edu/gscis_etd

 Part of the [Bioinformatics Commons](#), and the [Information Security Commons](#)

Share Feedback About This Item

NSUWorks Citation

Arturo Ponce. 2015. *A Dynamic Behavioral Biometric Approach to Authenticate Users Employing Their Fingers to Interact with Touchscreen Devices*. Doctoral dissertation. Nova Southeastern University. Retrieved from NSUWorks, Graduate School of Computer and Information Sciences. (46)
http://nsuworks.nova.edu/gscis_etd/46.

This Dissertation is brought to you by the College of Engineering and Computing at NSUWorks. It has been accepted for inclusion in CEC Theses and Dissertations by an authorized administrator of NSUWorks. For more information, please contact nsuworks@nova.edu.

A Dynamic Behavioral Biometric Approach to Authenticate Users Employing Their
Fingers to Interact with Touchscreen Devices

by

Arturo Ponce

A dissertation submitted in partial fulfillment of the requirements
for the degree of Doctor of Philosophy
in
Computer Information Systems

Graduate School of Computer and Information Sciences
Nova Southeastern University

2015

We hereby certify that this dissertation, submitted by Arturo Ponce, conforms to acceptable standards and is fully adequate in scope and quality to fulfill the dissertation requirements for the degree of Doctor of Philosophy.

Maxine S. Cohen, Ph.D.
Chairperson of Dissertation Committee

Date

Sumitra Mukherjee, Ph.D.
Dissertation Committee Member

Date

Timothy J. Ellis, Ph.D.
Dissertation Committee Member

Date

Approved:

Eric S. Ackerman, Ph.D.
Dean, Graduate School of Computer and Information Sciences

Date

Graduate School of Computer and Information Sciences
Nova Southeastern University

2015

An Abstract of a Dissertation Submitted to Nova Southeastern University in Partial Fulfillment of the Requirements for the degree of Doctor of Philosophy in Computer Information Systems

A Dynamic Behavioral Biometric Approach to Authenticate Users
Employing Their Fingers to Interact with Touchscreen Devices

by
Arturo Ponce
May 2015

The use of mobile devices has extended to all areas of human life and has changed the way people work and socialize. Mobile devices are susceptible to getting lost, stolen, or compromised. Several approaches have been adopted to protect the information stored on these devices. One of these approaches is user authentication. The two most popular methods of user authentication are knowledge based and token based methods but they present different kinds of problems.

Biometric authentication methods have emerged in recent years as a way to deal with these problems. They use an individual's unique characteristics for identification and have proven to be somewhat effective in authenticating users. Biometric authentication methods also present several problems. For example, they aren't 100% effective in identifying users, some of them are not well perceived by users, others require too much computational effort, and others require special equipment or special postures by the user. Ultimately their implementation can result in unauthorized use of the devices or the user being annoyed by the implementation.

New ways of interacting with mobile devices have emerged in recent years. This makes it necessary for authentication methods to adapt to these changes and take advantage of them. For example, the use of touchscreens has become prevalent in mobile devices, which means that biometric authentication methods need to adapt to it. One important aspect to consider when adopting these new methods is their acceptance of these methods by users. The Technology Acceptance Model (TAM) states that system use is a response that can be predicted by user motivation.

This work presents an authentication method that can constantly verify the user's identity which can help prevent unauthorized use of a device or access to sensitive information. The goal was to authenticate people while they used their fingers to interact with their touchscreen mobile devices doing ordinary tasks like vertical and horizontal scrolling. The approach used six biometric traits to do the authentication. The combination of those traits allowed for authentication at the beginning and at the end of a finger stroke. Support Vector Machines were employed and the best results obtained show Equal Error Rate values around 35%. Those results demonstrate the potential of the approach to verify a person's identity.

Additionally, this work tested the acceptance of the approach among participants, which can influence its eventual adoption. An acceptance level of 80% was obtained which compares favorably against other behavioral biometric approaches.

Acknowledgements

A doctoral dissertation requires the help of so many people during a journey that begins with the acceptance to the program. More than six years has passed and during that time a lot of people have helped me one way or another.

First of all, I would like to express my deep gratitude to my advisor Dr. Maxine S. Cohen for her guidance, support, valuable advice, and above all her patience during this journey. Also, many thanks to Dr. Timothy J. Ellis and Dr. Sumitra Mukherjee, the other two members of the dissertation committee, for their time and feedback.

Special thanks to my friend and fellow doctoral student Ricardo Rodríguez for his willingness to share ideas and for his overall support all this time. Also, special thanks to Víctor Díaz and Leo Vélez, two dear friends at UPR – Mayagüez, who helped me with technical issues which made my work easier during portions of this work.

Also, I would like to thank my parents for giving me support and motivation during all these years. Throughout my life, they taught me the value of hard work and the importance of education. They inspire me to every day give the best of my abilities in whatever I do.

Also, I would like to thank all the participants of this study who provide invaluable data for this work. Finally, I would like to thank all of those who gave me direct and indirect support to complete this work.

Table of Contents

Abstract iv
Acknowledgements v
List of Tables viii
List of Figures xiii

Chapters

1. Introduction 1
 Problem Statement 5
 Dissertation Goal 7
 Research Questions 8
 Relevance and Significance 10
 Barriers and Issues 13
 Limitations and Delimitations 14
 Limitations 14
 Delimitations 15
 Definition of Terms 15
 Summary 18

2. Review of the Literature 21
 User Authentication 22
 Biometric Authentication 23
 Biometrics Generic Module 32
 SVMs 39
 One-Class Classification 45
 Testing of Biometric Authentication Systems 47
 Effectiveness of the biometric approach 47
 User's disposition 49
 Resources Searched 52
 Summary 53

3. Methodology 56
 Research Method 59
 Modeling 59
 Implementation 63
 Testing 70
 Recruitment 70
 Tests 72
 Privacy 76
 Summary 76

4. Results 78

About the Sample 79

 How the data was collected 79

 Demographics 80

Biometric Test 82

 Events that affected the biometric tests results 93

Post Test Surveys 95

 User's disposition questionnaire 95

 TAM for biometrics questionnaire 98

Summary 102

 Effectiveness of the biometric approach 102

 Participants' perception of the biometric approach 103

5. Conclusions, Implications, Recommendations, and Summary 105

Conclusions 105

 Effectiveness of the biometric approach in terms of user authentication 107

 Participants' disposition to use the biometric approach 110

Implications 113

Recommendations 113

 Possible implementation 115

Summary 116

Appendices

A. Design Specification for Android and Java Applications 119

B. ARFF Sample File 146

C. Invitation to Participate in Study 147

D. IRB Letters of Approval from UPR-Mayagüez and Nova Southeastern University
148

E. Adult/General Informed Consent 150

F. Demographics Questionnaire 153

G. Biometric Test 156

H. Images Used in the Biometric Test 163

I. Brief Description of Biometrics and the Biometric Traits Captured in this Study 169

J. User's Disposition Questionnaire 171

K. Technology Acceptance Model for Biometrics Questionnaire 174

L. Amount of Time Needed to Complete the Biometric Test and Number of Strokes
Captured for Each Participant 182

M. Biometric Test Results for Different Biometric Traits Combinations 186

N. Comments about Participants during Biometric Tests 198

O. FRR for Participants with Less than 50 Strokes 201

P. FRR for Participants with Changes in their Scrolling Behavior 203

Q. Raw Collected Data for User's Disposition Questionnaire 205

R. Raw Collected Data for Technology Acceptance Model for Biometrics Questionnaire
211

References 215

List of Tables

Tables

1. Comparison of Some Popular Combination Schemes Employed to Fuse Results 38
2. EER for Different Biometric Authentication Approaches 48
3. Descriptive Statistics for Perceived Need for Security 51
4. Descriptive Statistics for Perceived Need for Privacy 52
5. Biometric Traits Captured During Each Motion Event 66
6. Likert Scale Implemented in this Study 75
7. Participants per Program and Year of Studies 81
8. Participant's Age and Gender 81
9. Types of Touchscreen Devices Used by Participants 82
10. Types of Communication Services used by Participants 82
11. Internet usage by Participants 82
12. Best Biometric Traits in Terms of Authentication Accuracy for the Down Motion Event during Horizontal Scrolling 85
13. Best Biometric Traits in Terms of Authentication Accuracy for the Down Motion Event during Vertical Scrolling 85
14. Best Biometric Traits in Terms of Authentication Accuracy for the Up Motion Event during Horizontal Scrolling 85
15. Best Biometric Traits in Terms of Authentication Accuracy for the Up Motion Event during Vertical Scrolling 85

16. Best Biometric Traits in Terms of Authentication Accuracy for the Move Motion Event during Horizontal Scrolling 86
17. Best Biometric Traits in Terms of Authentication Accuracy for the Move Motion Event during Vertical Scrolling 86
18. Number of Participants Correctly Authenticated for Different Levels of Accuracy 87
19. Top Four Biometric Traits in Terms of FRR for the Down Motion Event during Horizontal Scrolling 89
20. Top Four Biometric Traits in Terms of FRR for the Down Motion Event during Vertical Scrolling 89
21. Top Four Biometric Traits in Terms of FRR for the Up Motion Event during Horizontal Scrolling 89
22. Top Four Biometric Traits in Terms of FRR for the Up Motion Event during Vertical Scrolling 89
23. Best FAR Results Obtained for the Top Four Biometric Traits (in Terms of FRR) for the Down Motion Event during Horizontal Scrolling 90
24. Best FAR Results Obtained for the Top Four Biometric Traits (in Terms of FRR) for the Down Motion Event during Vertical Scrolling 90
25. Best FAR Results Obtained for the Top Four Biometric Traits (in Terms of FRR) for the Up Motion Event during Horizontal 91
26. Best FAR Results Obtained for the Top Four Biometric Traits (in Terms of FRR) for the Up Motion Event during Vertical Scrolling 91

27. Best EER Results Obtained for the Top Four Biometric Traits (in Terms of FRR) for the Down Motion Event during Horizontal Scrolling 92
28. Best EER Results Obtained for the Top Four Biometric Traits (in Terms of FRR) for the Down Motion Event during Vertical Scrolling 92
29. Best EER Results Obtained for the Top Four Biometric Traits (in Terms of FRR) for the Up Motion Event during Horizontal Scrolling 92
30. Best EER Results Obtained for the Top Four Biometric Traits (in Terms of FRR) for the Up Motion Event during Vertical Scrolling 92
31. Participants with Less than 50 Strokes Captured during the Biometric Test 93
32. Participants that Changed Hands or Fingers while Scrolling During the Biometric Tests 94
33. Average FRR for the Top Biometric Traits for All Participants, Participants with Less than 50 Strokes Registered, and Participants that Changed their Behavior during the Biometric Tests 94
34. General Perception about Biometric Devices 96
35. Reasonable Amount of Time Needed to Create a Biometric Profile 96
36. Willingness to tolerate errors 97
37. Who do you think should have access to your biometric pattern? 97
38. Beside yourself, who do you think should have access to your biometric pattern? 98
39. The Biometric Application 99
40. Results for TAM for Biometrics Privacy Related Questions 100
41. Results for TAM for Biometrics Security Related Questions 101

A1. Description of Database Table Finger	144
A2. Description of Database Table Person	144
L1. Participants' Times during the Biometric Tests	182
L2. Number of Strokes Captured per Participant during Horizontal and Vertical Scrolling	184
M1. Accuracy and FRR Results from Different Parameter Combinations in the Down Horizontal Motion Event	186
M2. Accuracy and FRR Results from Different Parameter Combinations in the Down Vertical Movement	188
M3. Accuracy and FRR Results from Different Parameter Combinations in the Move Horizontal Movement	190
M4. Accuracy and FRR Results from Different Parameter Combinations in the Move Vertical Movement	192
M5. Accuracy and FRR Results from Different Parameter Combinations in the Up Horizontal Movement	194
M6. Accuracy and FRR Results from Different Parameter Combinations in the Up Vertical Movement	196
N1. General Remarks about Participants during the Biometric Tests	198
N2. Comments on Participants during Horizontal Stroke Portion of the Biometric Tests	199
N3. Comments on Participants during Vertical Stroke Portion of the Biometric Tests	200
O1. Results for Different Parameter Combinations in the Down Horizontal Motion	201
O2. Results for Different Parameter Combinations in the Down Vertical Motion	201
O3. Results for Different Parameter Combinations in the Up Horizontal Motion	201

Q4. Results for Different Parameter Combinations in the Up Vertical Motion	202
P1. Results for Different Parameter Combinations in the Down Horizontal Motion	203
P2. Results for Different Parameter Combinations in the Down Vertical Motion	203
P3. Results for Different Parameter Combinations in the Up Horizontal Motion	203
P4. Results for Different Parameter Combinations in the Up Vertical Motion	204
Q1. Answer to Participants' Level of Agreement of the User's Disposition Questionnaire	205
Q2. Answer to Questions One and Two from Part Two of the User's Disposition Questionnaire	207
Q3. Answer to Question Three (If You Should Use a Biometric Method Like This, Who Do You Think Should Have Access to Your Biometric Pattern?) from Part Two of the User's Disposition Questionnaire	209
R1. Answer for Perceived Need for Security (Questions 1 – 9) and Perceived Need for Privacy (Questions 10 – 18)	211
R2. Answer to Question 1 -5 from the Second Part (The Biometric Application) of the TAM for Biometrics Questionnaire	213

List of Figures

Figures

1. Example of a linearly separable problem in a two dimensional space 40
2. Employing a mapping function Φ , to map the data points x_i of the data space L to the feature space H where a linear separation is possible 42
3. Representation of a finger stroke over the touchscreen 60
4. Finger over a touchscreen 60
5. Cartesian plane 62
6. Behavioral biometric model 63
7. Application diagram 64
8. Representation of a finger stroke over the android application 66
9. Android application used for capturing biometric traits. 83
- A1. System architecture 120
- A2. Welcoming message 121
- A3. Options menu 121
- A4. Credentials for horizontal scroll 122
- A5. Horizontal scroll 122
- A6. Credentials for vertical scroll 123
- A7. Vertical Scroll 123
- A8. Credentials for vertical scroll with tablet in portrait position 124
- A9. Vertical scroll with the tablet in portrait position 125
- A10. Add a new user 126

A11. Class architecture for the android application	127
A12. Entity relationship diagram for android application database	145
H1. Images one to six used in the biometric test	163
H2. Images seven to twelve used in the biometric test	164
H3. Images 13 to 18 used in the biometric test	165
H4. Images 19 to 24 used in the biometric test	166
H5. Images 25 to 30 used in the biometric test	167
H6. Images 31 to 34 used in the biometric test	168

Chapter 1

Introduction

Mobile devices have become ubiquitous in our society and their use has extended to all areas of human life. They have changed the way people work and socialize (Saevanee and Bhatarakosol, 2009). Mobile devices can hold sensitive information from organizations or even personal data from their owners. Moreover, they can connect to global cellular networks and to local Ethernet networks which means that they have the potential to access sensitive information stored on other devices (Nazir, Zubair, and Islam, 2009).

Mobile devices are susceptible to getting lost, getting stolen, or becoming compromised, and to make matters worse, their security mechanisms are constantly breached. IBM X-Force (2011) reported that the first half of 2011 saw an increased level of malware activity targeting the latest generation of smartphones and tablets, as attackers are finally warming to the opportunities these devices represent. They added that the increased number of vulnerability disclosures and exploit releases targeting these platforms shows no sign of slowing down. During the last years this trend has continued and the growth of Android OS devices has captured the attention of malware authors hoping to capitalize on that growth (IBM X-Force, 2013). Attackers have realized the opportu-

nities available to exploit vulnerabilities on these devices. This shows that some kind of authentication is needed in order to provide a secure channel for online applications and to meet the security requirements of users, service providers, and network operators (Alhussain, Drew, and Alfarraj, 2010).

User authentication is an approach that has been used for a long time to prevent unauthorized access to different types of devices including mobile devices. Its main purpose is to guarantee that people share or work with the right person and that only authorized individuals can access the data (Giot, El-Abed, and Rosenberger, 2009). User authentication answers questions like who are the users and if they are who they claim to be. Also, it allows individuals to have access to objects based on their identity and helps to determine who can access certain resources on a device or over a network. User authentication has proven to be extremely important for the security of computers and network systems.

Currently, the most popular approaches employed for user authentication are knowledge based and token based methods. Knowledge based methods rely on something a user knows, like a PIN or a password while token based methods rely on something a user has, like a key or a magnetic card (Niinuma, Park, and Jain, 2010). A more recent approach employed in user authentication is biometrics. Biometrics refers to any physiological and/or behavioral characteristic that can be used to uniquely identify a person. Biometrics takes advantage of an individual's unique characteristics for identification (Matyas and Riha, 2003). This uniqueness makes biometric identifiers essentially more reliable than knowledge-based and token-based methods in differentiating between an authorized user and an impostor (Jain, Hong, and Pankanti, 2000).

Biometric authentication is highly reliable because physical human characteristics are much more difficult to forge than, for example, security codes, passwords, and hardware keys. Biometric authentication has been implemented in areas such as workstation and network access, single sign-on, application logon, data protection, remote access to resources, transaction security, and web security (Bhattacharyya, Ranjan, Das, Kim, and Bandyopadhyay, 2009). Biometric authentication has been mainly used for identity verification and identification. In identity verification mode, the system compares a user's data against the records in a database when it receives an enrollment request. In identification mode, the system matches the user's biometric data against all of its records because the user's identity is unknown.

Biometric authentication systems are divided into two categories: physiological and behavioral. Physiological biometric systems are based on an individual's distinctive characteristics such as fingerprints, iris, retina, facial images, and hand geometry. A more recent approach in physiological biometrics employs cognitive biometrics. Cognitive biometrics measures brain response to odor stimuli, facial perception, and mental performance (Bhattacharyya et al., 2009).

The second category of biometric systems, behavioral biometrics, is based on the way people do things. An example of this category is keystroke dynamics which analyzes keystroke patterns and relies on the fact that each user has a unique way of using the keyboard to enter words (Saevanee and Bhatarakosol, 2009). Another example of this category is mouse dynamics, where mouse actions are monitored while the user is working with graphical user interfaces (GUIs) (Ahmed and Traore, 2007).

Behavioral biometrics' features can be used to positively verify the identity of users that have logged in or positively identify users that are trying to access a mobile device. Some of them are:

- it requires little intervention from users, this contrasts with traditional approaches that usually need to ask users to insert a key or enter a password
- it employs user's own characteristics
- it requires minimal effort from the users, that is, users don't need to remember passwords or carry any special equipment

Today, people make use of touchscreens to interact with their mobile devices. Touchscreen mobile devices are becoming very popular with manufacturers and also with users. Since there is no need for a physical keyboard to take up space on a device, they can have larger screens which can be used more flexibly. The use of touchscreens allows novel forms of text entry and navigation (Hogan, Brewster, and Johnston, 2008). Also, it is often convenient to point and select items in complex environments like computer-assisted design tools or drawing tools because users can avoid learning commands, reduce the chance of typographic errors on a keyboard, and keep their attention on the display (Shneiderman and Plaisant, 2010).

This work presents an approach to dynamically authenticate users interacting with their touchscreen mobile devices. The approach takes advantage of some distinctive features generated when people move their fingers over a touchscreen while doing tasks like browsing the web or skimming through the pages of a document. It uses the following biometric traits: area in contact with the touchscreen, length of the major axis

of an ellipse that describes the touch area at the point of contact, length of the minor axis of an ellipse that describes the touch area at the point of contact, distance traveled, speed, and angle created by the movement. All of them are measured for each finger while making contact with the screen.

The next section presents the problem addressed by this work. It is followed by the goal, the research questions, and the relevance and significance of this work. Then the barriers and issues, limitations and delimitations, and the definition of terms are discussed. Finally a brief summary is presented.

Problem Statement

Security mechanisms in computer devices are constantly breached. The first half of 2011 saw an increased level of malware activity targeting the latest generation of smartphones and tablets (IBM X-Force, 2011). This trend has continued and the growth of Android OS devices has captured the attention of malware authors hoping to capitalize on that growth (IBM X-Force, 2013). Attackers have realized the opportunities they have to exploit vulnerabilities on these devices.

Traditional authentication methods rely on objects to identify users but these objects can get lost, stolen, forgotten, or disclosed (Niinuma, Park, and Jain, 2010). Biometric authentication has been employed as an alternative approach for user authentication since it doesn't rely on objects but on the users' physical characteristics. Current biometric systems cannot guarantee 100% accuracy partly due to the inconsistency of humans (Kanneh and Sakr, 2008).

Several implementations of biometric authentication systems have presented other problems besides accuracy. For example, an implementation that uses keyboard dynamics appears to be less acceptable to users since they report being afraid that their work performance may be monitored in some way (Patrick, Long, and Flinn, 2003). Also, implementations that make use of mouse biometrics usually require an impractical amount of data to be collected before an authentication decision can be made with reasonable accuracy (Ahmed and Traore, 2007; Niinuma, Park, and Jain, 2010).

Other implementations have used physiological biometric traits. One of them, the use of fingerprints, presents the problem that some people consider that its use violates their privacy. Also, researchers have demonstrated that fake gelatin fingers can be easily used to deceive biometric fingerprint devices (Shaikh and Dimitriadis, 2008; Patrick, Long, and Flinn, 2003). Moreover, fingerprints can only be authenticated when the user keeps a finger on the reader embedded in a device. Furthermore, other physiological biometric implementations, like face recognition, aren't considered feasible for many users due to the posture that they have to assume in front of a sensor.

The different authentication implementations present some shortcomings besides not being 100% effective. Some of them are not well perceived by users, others require too much computational effort, and others require special equipment or special postures by the user. Ultimately their implementation can result in unauthorized use of the devices or the user being annoyed by the implementation.

Dissertation Goal

Different ways of human-computer interaction have emerged in recent years with the advent of new mobile devices. This has prompted the need for employing new ways to authenticate users that should be both effective and well received by users. The goal of this work was to test the effectiveness of employing a dynamic behavioral user authentication approach to identify users based on the way they interact with their touchscreen devices. This approach helps authenticate users without the need of user intervention. It is based on the premise that distinctive traits are generated when people move their fingers over a touchscreen mobile device while doing tasks like browsing the web or skimming through the pages of a document. The following biometric traits were captured for each finger in contact with the screen:

1. area in contact with the touchscreen
2. length of the major axis of an ellipse that describes the touch area at the point of contact
3. length of the minor axis of an ellipse that describes the touch area at the point of contact
4. distance traveled
5. speed
6. angle created by the movement

The use of first three traits takes advantage of the fact that everyone's fingers have different shapes and sizes which along with the force applied over the screen can produce distinctive values for each person. The last three: distance traveled, speed, and

angle created by the movement can be influenced by user's abilities, style of browsing, and motor skills which also can produce distinctive values for each person.

A major advantage of using these traits is that they can be collected at any moment without the need of user intervention, they are unique for every person, should remain constant over extended periods of time, and should be hard to forge. The use of the aforementioned biometric traits fulfills the requirements listed by Jain, Ross, and Prabhakar (2004) and Faundez-Zanuy (2005) of universality, distinctiveness, permanence, collectability, performance, acceptability, and circumvention in biometric authentication. This approach complements other authentication methods already in place to positively verify a user's identity.

Summarizing, the biometric traits presented in this study effectively help to verify the identity of users. At the same time these biometric traits are well perceived by those users.

Research Questions

This research focused on the following questions:

RQ1. How effective was this biometric approach in terms of user authentication? – It was very important to determine if these biometric features were effective in user authentication. The effectiveness of the approach was tested calculating false acceptance rate (FAR), false rejection rate (FRR), and equal error rate (EER). They were defined (Sulong, Wahyudi, and Siddiqi, 2009):

$$\text{FRR} = \frac{\text{number of false rejections}}{\text{number of authorized person attempts}} \times 100 \% \quad (1)$$

$$\text{FAR} = \frac{\text{number of false acceptances}}{\text{number of impostor person attempts}} \times 100 \% \quad (2)$$

EER – the error rate when the system's parameters are set such that the FRR and FAR are equal. The lower the EER the more accurate the system is. Usually authentication systems based on user behavior show larger values for EER than those based on physiological characteristics. For example, A haptic system developed by Orozco et al. (2006) in which touch, force, and hand-kinesthetic were continuously measured produced an EER of 22.3%. Also, a study by Schulz (2006) of mouse dynamics for authentication yielded an EER of 24.3%.

Jorgensen and Yu (2011) state that biometric authentication systems are usually evaluated with respect to the above metrics. These metrics have been used in the work by Ahmed and Traore (2007) in their analysis of mouse dynamics and by Kanneh and Sakr (2008) in their study about the use of haptics and fuzzy logic to authenticate users, among others.

RQ2. How was this approach perceived by users? – User acceptance and satisfaction with the implementation was evaluated for this work. El-Abed et al. (2010) point out the importance of user acceptance and satisfaction. They state that their evaluation should include the assessment of the individual's entire interaction with the system, as well as thoughts,

feelings, and outcomes that might result from the interaction that might influence user acceptance.

Also, the Technology Acceptance Model (TAM) states that system use is a response that can be predicted by user motivation, which is directly influenced by the actual system's features and capabilities (Davis, 1993). According to TAM, user motivation can be explained by three factors: perceived ease of use, perceived usefulness, and attitude toward using the system. Besides those factors pointed out by TAM, James, Pirim, Boswell, Reithel, and Barkhi (2008) state that there are other factors that can influence the adoption of a biometric authentication system. Those factors are: perceived need for security, perceived need for privacy, and perceived physical invasiveness. All the six factors determine user motivation, which in turn helps determine user acceptance and satisfaction (James, et al., 2008).

Relevance and Significance

Mobile devices have extended to all areas of human life and have changed the way people work and socialize (Saevanee and Bhatarakosol, 2009). These devices sometimes hold sensitive information from organizations or even personal data from their owners. Also, they can connect to global cellular networks and local networks which mean that they have the potential to access sensitive information (Nazir, Zubair, and Islam, 2009). The increase in the use of mobile devices to store large amounts of data carries the risk of data loss or theft which can compromise the security of the information

(Alhussain, Drew, and Alfarraj, 2010). Since mobile devices are prone to get lost, stolen, or compromised and their security mechanisms are breached constantly, it is important to have effective security mechanisms in place.

It has been argued that sometimes security mechanisms are not effective in authenticating users and are seen by some users as an invasion of privacy. Also, it has been argued that sometimes they create overhead for users and require unworkable user behavior. To make matters worse, users are not completely aware of security issues and perceive many of the security mechanisms as laborious and unnecessary which also contributes to the difficulty of keeping these devices secure (Chen and Ku, 2009).

The positive identification of people is crucial in instances like access to buildings, computer systems, laptops, cellular phones, ATMs, and internet commerce (Jain, Ross, and Prabhakar, 2004). The increase in credit card fraud and identity theft in recent years is one instance that demonstrates the need for effective user authentication (Bhattacharyya et al., 2009). The level of security of traditional password based authentication systems is limited to relatively weak human memory and therefore, it is not a preferred method for systems which require high level of security (Sutcu, Sencar, and Memon, 2005). Hence, a high level of authentication has become crucial to provide a secure channel to meet the security requirements of users, service providers, and network operators (Alhussain, Drew, and Alfarraj, 2010). An alternative approach is to use biometrics instead of passwords for authentication. Higher entropy and uniqueness of biometrics make them favorable in many applications that require high level of security (Sutcu, Sencar, and Memon, 2005).

The approach, presented in this work without the need of constant user intervention, dynamically verifies the identity of users while they are using their touchscreen mobile devices. It uses behavioral data from users such as area in contact with the touchscreen at different points, length of the major axis of an ellipse that describes the touch area at the point of contact, length of the minor axis of an ellipse that describes the touch area at the point of contact, distance travelled, speed, and angle created by the movement. The first three traits are measured directly using Android OS functions and the last three are calculated using the (x, y) coordinates at the point of contact, and the time of contact. Each finger in contact with the touchscreen is analyzed since sometimes more than one finger is in contact with the screen during a task. Also the difference between using the left hand or the right hand was examined.

The use of finger traits for authentication relies mainly on the user's motor-skills. According to Yampolskiy and Govindaraju (2008), behavioral biometric systems can be classified into five categories: authorship based events, HCI based events, events that can be obtained by monitoring user's HCI behavior indirectly, motor-skills based events, and purely behavioral based events. The motor-skills based category includes other biometric approaches like keystroke dynamics, mouse dynamics, and haptics.

The approach presented does not use any physiological data that users have traditionally rejected because of privacy concerns. User overload is minimal since there is no need for constant user intervention. Also, it positively authenticates users and assists them in maintaining the security of their touchscreen mobile devices. This approach is more effective than other dynamic behavioral authentication mechanisms because the finger as an input device has many traits inherent to the user. Some traits inherent to the

finger include the fingerprints, the size, and the form of the finger. Also, the pressure exerted over a surface, the speed and direction of the finger moving throughout the surface, and the area in contact with the surface can be considered part of these traits.

Barriers and Issues

As mentioned before, a practical biometric system doesn't make perfect match decisions (Jain et al., 2004). To be of practical use, a security system should detect a substantial percentage of imposters while keeping the FRR at an acceptable level (Kanneh and Sakr, 2008). The biometric traits help to achieve this. One problem encountered was the amount of computational resources needed because of the number of traits that were employed. This problem has occurred in the past, neural networks have been effective in detecting impostors while keeping the FRR at low levels but a problem with them is that they often need a large amount of training for effective classifying as demonstrated in the work of Ngugi, Kahn, and Tremaine (2011). In recent years, support vector machines (SVMs) have generated more interest because they often require fewer parameters to achieve similar or better accuracy levels than neural networks (Witten, Frank, and Hall, 2011).

Environmental factors can influence the results of evaluations, as was the case in some experiments involving keyboard and mouse dynamics. Stress, general health, working and environmental conditions, and time pressure all effectively conspire to make humans inconsistent. These variables if not properly controlled from one test subject to the next can have a consequence in the results. It is difficult to determine whether the results of the evaluations actually reflect detectable differences in behavior among test

subjects, or differences among their computing environments (Jorgensen and Yu, 2011). Another problem is that some users do not perform well in terms of false match rates and false non-match rates. Yager and Dunstone (2010) described some characteristics of different types of users. These characteristics need to be identified to avoid any negative effect on the results. Also, the use of biometric systems has raised the issue of privacy since biometrics measures our personal traits (Yampolskiy, 2007).

Finally, sometimes the acceptance of an application depends on undetected factors. El-Abed et al. (2010) recommend the evaluation of the individual's entire interaction with the system, as well as thoughts, feelings, and outcomes that might result from the interaction.

Limitations and Delimitations

Limitations

A limitation of this research is that not every mobile device can handle functions that detect attributes like area in contact with the touchscreen, length of the major axis of an ellipse that describes the touch area at the point of contact, and length of the minor axis of an ellipse that describes the touch area at the point of contact. A Lenovo ThinkPad 10.1" Tablet, running the Android 4.1 OS, was used for testing. The Lenovo ThinkPad Tablet can handle these functions.

Another limitation is the fact that lab-based experiments may not be a good representation of users' typical interaction behavior. It has been reported that participants may behave differently in lab based experiments due to the stress of being observed, the

different environment, or the rewards offered for participation. This phenomenon is called the “Hawthorne effect” (Lazar, Feng, and Hochheiser, 2010).

Delimitations

For this research, it was expected that participants had some experience using mobile devices. Also, participants could not be color blind since some test questions made reference to color on the images. Furthermore, this research examined the captured biometric traits while the participants scrolled to a preset image. The scrolling that participants did was either horizontal or vertical and each type was examined separately. No other type of scrolling was studied.

Definition of Terms

- Behavioral biometric systems – Biometric systems that are based on the way people do things (Matyas and Riha, 2003).
- Biometrics – It refers to any physiological and/or behavioral characteristic that can be used to uniquely identify a person. Biometrics takes advantage of an individual’s unique characteristics for identification (Matyas and Riha, 2003).
- Down motion event – It means that a pressed gesture has started (Android Developers, n.d.a).
- Dynamic authentication – This type of authentication is applied after the start of a session, and monitors if the current user is the same as the user who performed the initial static authentication. It is also called continuous authentication (Bours and Barghouthi, 2009).

- Entropy – It is defined as lack of order or predictability ("Definition of entropy", 2013).
- Equal error rate (EER) – The error rate when the system's parameters are set such that the FRR and FAR are equal (Sulong, Wahyudi, and Siddiqi, 2009).
- Failure to enroll (FTE) rate – FTE rate is the percentage of the population which fails to complete enrollment for a biometric solution or application. It can be caused by physical differences, lack of training, environmental conditions or ergonomics (Jain, Ross, and Prabhakar, 2004).
- False acceptance rate (FAR) – The ratio of the number of false acceptances divided by the number of impostor person attempts (Sulong, Wahyudi, and Siddiqi, 2009).
- False rejection rate (FRR) – The ratio of the number of false rejections divided by the number of authorized person attempts It is defined (Sulong, Wahyudi, and Siddiqi, 2009).
- Finger Stroke – A stroke made using the finger (see Stroke).
- Hyperplane – In SVMs, it is a decision boundary that separates the tuples of one class from another (Han, Kamber, and Pei, 2006).
- Move motion event – It means that a change has happened during a press gesture between down and up motion events (Android Developers, n.d.a).
- Multimodal biometric systems – They can consist of multiple sensors for the same biometric, multiple biometric characteristics, multiple units of the same biometric, multiple snapshots of the same biometric, or multiple representations and

matching algorithms for the same biometric (Jain, Nandakumar, and Ross, 2005; Puente-Rodriguez, Garcia-Crespo, Poza-Lara, and Ruiz-Mezcua, 2008).

- Overfitting – Occurs when a model begins to memorize training data rather than learning to generalize from trend (Han, Kamber, and Pei, 2006).
- Physiological biometric systems – Biometric systems that are based on an individual’s distinctive characteristics such as fingerprints, iris, retina, facial images, and hand geometry (Matyas and Riha, 2003).
- Static authentication – This type of authentication is done when accessing a service by providing an identity and proof of that identity. It is valid throughout a full session until the user logs off. A common example of this type of authentication is the well-known username/password combination for access to computers or websites (Bours and Barghouthi, 2009).
- Stroke – A single unbroken movement; especially: one of a series of repeated or to-and-fro movements (“Stroke”, 2014).
- Support Vector Machines (SVMs) – A method used for the classification of both linear and nonlinear data. A SVM uses a nonlinear mapping to transform the original training data into a higher dimension. Within this new dimension, it searches for the linear optimal separating hyperplane. Data from two classes can always be separated by a hyperplane with an appropriate nonlinear mapping to a sufficiently high dimension,. SVMs find this hyperplane using support vectors and margins (Han, Kamber, and Pei, 2006).
- Touchmajor – It refers to the length of the major axis of an ellipse that describes the touch area at the point of contact (Android Developers, n.d.a).

- Touchminor – It refers to the length of the minor axis of an ellipse that describes the touch area at the point of contact (Android Developers, n.d.a).
- Touchscreen – An electronic visual display that can detect the presence and location of a touch within the display area. It enables users to interact directly with what is displayed, rather than indirectly with a cursor controlled by a mouse or touchpad (Bhalla and Bhalla, 2010).
- Up motion event – It means that a pressed gesture has finished (Android Developers, n.d.a).
- User authentication – An approach that has been used for a long time to prevent unauthorized access to different types of devices including mobile devices. Its main purpose is to guarantee that people share or work with the right person and that only authorized individuals can access the data. User authentication answers questions like who are the users and if they are who they claim to be (Giot, El-Abed, and Rosenberger, 2009).

Summary

The use of mobile devices has extended to all areas of human life and has changed the way people work and socialize. Mobile devices are susceptible to getting lost, stolen, or compromised. Authentication systems have been implemented to protect the information stored on them. Unfortunately, the authentication implementations present some shortcomings besides not being 100% effective. Some of them are not well perceived by users, others require too much computational effort, and others require special equipment or special postures by the user. Ultimately their implementation can

result in unauthorized use of the devices or the user being annoyed by the implementation.

The goal of this work was to test how effective a dynamic behavioral user authentication approach can be in identifying users. The approach was based on the way people interact with their touchscreen devices assuming that distinctive traits are generated when people move their fingers over a touchscreen mobile device. The following biometric traits were captured for each finger in contact with the screen: area in contact with the touchscreen, length of the major axis of an ellipse that describes the touch area at the point of contact, length of the minor axis of an ellipse that describes the touch area at the point of contact, distance traveled, speed, and angle created by the movement.

This work focused on answering the following questions:

- How effective was the biometric approach in terms of user authentication?
- How was the approach perceived by users?

To be of practical use, biometric traits should help to detect a substantial percentage of imposters while keeping the FRR at an acceptable level, a requirement for any security system although the intended use of the application determines the ideal values (Bours and Barghouthi, 2009). SVMs have generated interest recently because they often require fewer parameters to achieve similar or better accuracy levels than neural networks (Witten, Frank, and Hall, 2011). In the past, neural networks have been effective detecting impostors but they have not been effective in keeping the amount of computational resources needed at low levels (Ngugi, Kahn, and Tremaine, 2011). Also, the success of biometric systems rely on how well they are perceived by users (El-Abed, Giot, Hemery, and Rosenberger , 2012).

The next chapter presents a review of different types of biometric authentication systems, how effective they have been authenticating users, and how that effectiveness is measured. In addition, the chapter discusses the importance of people's perception of biometric systems and how it can be measured. Chapter 3 discusses the methodology employed to answer the two research questions and the rationale behind it. Chapter 4 shows the results obtained from testing the effectiveness of the approach presented and its acceptance by users. Finally, Chapter 5 presents the conclusions of this study, followed by the implications, and the recommendations for future research.

Chapter 2

Review of the Literature

User authentication has been employed for years to prevent unauthorized access to many devices. It guarantees that people share or work with the right person and that only authorized individuals can access the data (Giot, El-Abed, and Rosenberger, 2009). The following section describes what user authentication is and the different methods that are employed for authentication. One of these methods, biometric authentication, and its two types are examined in more detail. After that, the general biometric model, which divides the authentication process in different levels, is discussed. The data obtained in any of these levels can be fused using different schemes. One of them, SVMs and the One-Class implementation, which defines a classification boundary around a target class with the objective of accepting as many objects as possible from the positive class while minimizing the chance of accepting outlier objects (Khan & Madden, 2010), is presented in detail. Afterwards the testing of biometric authentications systems is discussed and the resources employed for doing the literature review are presented. The chapter ends with a brief summary.

User Authentication

User authentication answers questions like who are the users and also if they are who they claim to be (Giot et al., 2009). It allows individuals to have access to objects based on their identity and also helps to determine who can access certain resources on a particular device or over a network.

There are two types of user authentication mechanisms: static and dynamic (Niinuma, Park, and Jain, 2010). Static authentication verifies identity on just one occasion. A major disadvantage of static authentication systems is that anyone can access the system resources if the authorized user doesn't properly logout or leaves a device unattended. Dynamic authentication validates users at any moment during their interaction with a device. An authentication mechanism that constantly requests users to enter a password or a card can be irritating.

The majority of static and dynamic authentication systems are knowledge based methods or token based methods and both methods are currently the most popular approaches for user authentication. Knowledge based methods rely on something the user knows like a PIN or a password while token based methods rely on something a user owns, like a key or a magnetic card (Niinuma, Park, and Jain, 2010). Both of these methods have many security flaws, for example, passwords can be shared, stolen, or forgotten and smart cards can be shared, stolen, lost, or duplicated.

Biometric authentication is another method that has been employed recently. Biometrics is the science of identifying people using physiological features (De Luis-Garcia, Alberola-López, Aghzout, and Ruiz-Alzola, 2003). It takes advantage of the individual's unique characteristics. It is considered to be highly reliable because physical

human characteristics are much more difficult to forge than security codes, passwords, or hardware keys (Matyas and Riha, 2003). Biometric authentication has been implemented in areas such as workstation and network access, single sign-on, application logon, data protection, remote access to resources, transaction security, and web security (Bhattacharyya et al., 2009).

Biometric Authentication

Biometric authentication has been mainly used for identity verification and for identification. Identity verification compares a user's data against the records in a database when the system receives an enrollment request. Identification matches the user's biometric data against all its records because the user's identity is unknown.

Different biometric features have been studied for authentication, but any biometric feature needs to comply with the following guidelines (Jain, Ross, and Prabhakar, 2004; Faundez-Zanuy, 2005):

- Universality – Everyone should have the selected biometric identifier.
- Distinctiveness – Two individuals should not have the same biometric characteristic.
- Permanence – The characteristic should remain the same for long periods of time.
- Collectability – The biometric characteristic can be measured quantitatively.
- Performance – The system should be able to make the analysis accurately and fast.

- Acceptability – People should be willing to use the particular biometric characteristic.
- Circumvention – The characteristic should not be easy to imitate using fraudulent methods.

All biometric systems are divided into two categories: physiological and behavioral. Physiological biometric systems are based on an individual's distinctive characteristics and include, among others, fingerprints, iris, retina, facial images, and hand geometry (Shaikh and Dimitriadis, 2008; Patrick, Long, and Flinn, 2003). A more recent method employed in physiological biometrics has made use of cognitive biometrics which employs, among other things, brain response to odor stimuli and facial perception, and mental performance to authenticate users (Bhattacharyya et al., 2009). The following list presents a brief description of these and other physiological biometrics that have been studied:

- Body odor – The body odor biometrics is based on the fact that virtually each human smell is unique. The smell is captured by sensors that are capable to obtain the odor from nonintrusive parts of the body such as the back of the hand (Jain, Ross, and Prabhakar, 2004).
- Capacitive fingerprinting – It uses Swept Frequency Capacitive Sensing, which measures the impedance of a user to the ground across a range of AC frequencies. It is based on the fact that different people have different bone densities and muscle mass, wear different footwear, and so on. This produces different impedance profiles which can be used to authenticate users (Harrison, Sato, and Poupyrev, 2012)

- Ear shape – Identifying individuals by the ear shape is used in law enforcement applications where ear markings are found at crime scenes (Jain, Ross, and Prabhakar, 2004).
- Face recognition – Facial recognition analyzes features that include position, size, and shape of the eyes; nose; cheekbones; and jaw line. Initially, this process was known as a two dimensional facial recognition because two dimensional images were typically taken from security cameras that had integrated facial recognition technology.

A more recent approach is three dimensional biometric facial recognition which is an updated version of the two dimensional process. Images are captured with a real-time 3D camera or by digitally scanning a 2D photo. Detailed information like the contour of the eye sockets, nose and cheekbones help make identification easier (Bhattacharyya, Ranjan, Das, Kim, & Bandyopadhyay, 2009)

- Finger geometry – This approach is similar to hand geometry and includes length and width of the fingers. (Kumar, Wong, Shen, and Jain, 2003)
- Fingernail bed – The fingernail is made up of nearly parallel rows of vascular rich skin. The distance between the narrow channels that exist between these parallel dermal structures is measured (Bhattacharyya, Ranjan, Farkhod-Alisherov, & Choi, 2009).
- Fingerprint – A fingerprint is an impression of the friction ridges of all or any part of the finger. A friction ridge is a raised portion of the finger. This technology analyzes the ridges and valleys patterns on the fingertip for differ-

ences. The fingerprint patterns include the arch, loop, and whorl (Jain, Ross, and Prabhakar, 2004; Bhattacharyya, Ranjan, Farkhod-Alisherov, & Choi, 2009).

- Hand geometry – This approach is based on the fact that nearly every person's hand is shaped differently and that the shape of a person's hand does not change after certain age. It includes the estimation of length, width, thickness, and surface area of the hand (Bhattacharyya, Ranjan, Das, Kim, & Bandyopadhyay, 2009).
- Hand vein – Hand vein geometry is based on the fact that the vein pattern is different for everyone. Images taken with an infrared camera show darker patterns of the veins under the skin, which absorb the infrared light (Jain, Ross, and Prabhakar, 2004).
- Iris – It takes advantage of the colored area that surrounds the pupil to authenticate users. This technology employs a combination of specific characteristics known as corona, crypts, filaments, freckles, pits, furrows, striations, and rings (Bhattacharyya, Ranjan, Das, Kim, & Bandyopadhyay, 2009)
- Palmprint – Palmprint verification is a slightly different implementation of the fingerprint technology. Palmprint features are composed of the principal lines, wrinkles, details, delta points, etc. that can describe the palm of the hand (Kumar, Wong, Shen, and Jain, 2003).
- Retina geometry – It is based on the blood vessel pattern in the retina of the eye. It analyzes the blood vessels at the back of the eye which produce a

unique pattern, from eye to eye and person to person. (Bhattacharyya, Ranjan, Farkhod-Alisherov, & Choi, 2009)

- Speaker recognition – Speaker verification focuses on the vocal characteristics that produce speech and not on the sound or the pronunciation of speech itself. The vocal characteristics depend on the dimensions of the vocal tract, mouth, nasal cavities and the other speech processing mechanism of the human body. It doesn't require any special and expensive hardware. Speaker recognition uses the acoustic features of speech that have been found to differ between individuals. These acoustic patterns reflect both anatomy (e.g. size and shape of the throat and mouth) and learned behavioral patterns. Speaker identification and recognition is used to discover an unknown speaker's identity based on patterns of voice pitch and speech style. Behavioral patterns of a voice differ with every individual (Bhattacharyya, Ranjan, Farkhod-Alisherov, & Choi, 2009).

Behavioral biometric systems are based on the way people do things. Behavioral biometric systems can be classified into five categories (Yampolskiy and Govindaraju, 2008):

- Authorship based – It relies on examining a piece of text or a drawing produced by a person.
- HCI based– It examines the different strategies, styles, and unique abilities and knowledge employed by users. It can be subdivided into interaction with

input devices and into haptics which can register inherent, distinctive, and consistent muscle actions.

- Events that can be obtained by monitoring user's HCI behavior indirectly via observable low level actions of computer software
- Motor-skills of users – It measures innate, unique, and stable muscle actions of users performing a particular task.
- Purely behavioral – It measures the strategies, skills, and knowledge during performance of mentally demanding tasks.

One implementation of behavioral biometric systems has been the use of keystroke dynamics which analyzes keystroke patterns and relies on the fact that each user has a unique way of using the keyboard to enter words. Another implementation has been the use of mouse dynamics where mouse actions are monitored while the user is working with graphical user interfaces (GUIs). Some of the features of mouse dynamics produce a series of values that are used to build a mouse dynamic signature (MDS) (Ahmed and Traore, 2007). Other behavioral biometric systems have made use of haptic technology to authenticate users. Haptic systems involve the sense of touch, force, and hand-kinesthetic in human-computer interaction (Orozco, Asfaw, Adler, Shirmohammadi, and El Saddik, 2005; Kanneh and Sakr, 2008). It is important to notice that none of these implementations have used finger biometric traits; like pressure over the touchscreen, area of the finger touching the screen, and speed and direction of the finger while moving over the touchscreen; as a way to authenticate users. The following list presents a brief description of these and other behavioral biometrics that have been studied:

- Biometric sketch – A sketch is a set of structurally variable and statistically correlated drawing primitives of different complexity. A sketch contains rich information in how the shapes relate to each other, which differentiates sketches from handwritten signatures and symbols (Brömme and Al-Zubi, 2003).
- Haptic – Haptic systems provide a sensory channel to the human-computer interaction scenarios through tactile and kinesthetic. It measures 3D world location of the pen, its average speed, mean velocity, mean standard deviation, navigation style, angular turns, and rounded turns. These personal features are analyzed and compared with a reference or against others models in order to provide a level of authenticity (Trujillo, Shakra, and El Saddik, 2005)
- Keystroke dynamics – Keystroke dynamics is based on verifying the identity of individuals by their typing rhythm. Some features include time durations between the keystrokes; inter-key strokes and dwell times, which is the time a key is pressed down; overall typing speed; frequency of errors; use of numpad; and order in which user presses shift key to get capital letters. Its effectiveness depends on an individual using the same keyboard as different types may create a variance in the keystroke pattern measured (Saevanee and Bhatarakosol, 2009).
- Mouse dynamics – Mouse dynamics biometrics involves a signature that is based on selected mouse movement characteristics, which are computed using statistical techniques such as neural networks. These movement characteristics include: x and y coordinates of the mouse, horizontal velocity, vertical

velocity, tangential velocity, tangential acceleration, tangential jerk, and angular velocity (Ahmed and Traore, 2007).

- Speaker recognition – Speaker verification focuses on the vocal characteristics that produce speech and not on the sound or the pronunciation of speech itself. The vocal characteristics depend on the dimensions of the vocal tract, mouth, nasal cavities, and other speech processing mechanisms of the human body. It doesn't require any special and expensive hardware. Speaker recognition uses the acoustic features of speech that have been found to differ between individuals. These acoustic patterns reflect both anatomy (e.g. size and shape of the throat and mouth) and learned behavioral patterns. Speaker identification and recognition is used to discover an unknown speaker's identity based on patterns of voice pitch and speech style. Behavioral patterns of a voice differ with every individual (Jain, Ross, and Prabhakar, 2004)
- Signature verification – The signature dynamics recognition is based on the dynamics of making the signature, rather than a direct comparison of the signature itself afterwards. The dynamics is measured as a means of the pressure, direction, acceleration and the length of the strokes, and dynamics of number of strokes and their duration (Yampolskiy and Govindaraju, 2008).
- Speaker or voice authentication – Speaker or voice authentication is the analysis of vocal behavior by matching it to a voice model template that was previously recorded (Yampolskiy and Govindaraju, 2008).
- Dynamic facial features – Human faces contain abundant information of human facial behaviors. This approach takes advantage of the fact that facial

expressions can be described by the movements of points that belong to the facial features such as eye brows, eyes, nose, mouth, and chin. The experiments showed that facial behaviors may provide information about individual differences that may be used as another behavioral biometric. (Pohsiang, Hintz, and Jan, 2007).

- Eye-movement – The measured data includes pupil sizes and their dynamics, gaze velocities, and distances of infrared reflections of the eyes. (Bednarik, Kinnunen, Mihaila and Fränti, 2005)
- Finger touch gestures – It is based upon classifying movement characteristics of the center of the palm and fingertips. It employs pattern recognition techniques to identify biometric gesture characteristics of individuals (Sae-Bae, Ahmed, Isbister, and Memon, 2012)
- Signature/handwriting – Depending on the signature capturing device used the following traits might be captured: coordinates of the signature, pressure at pen tip, acceleration and pen-tilt, signing speed, and signature bounding box (Jain, Griess, and Connell, 2002).
- Webbiometrics – Webbiometrics is based on the mouse movement while the user inserts the PIN number. This biometric method aims to provide a non-intrusive soft behavioral biometric add-on to enhance on-line security (Gamboa, Fred, and Jain, 2007).

Biometrics Generic Module

Usually, generic biometric systems consist of five modules (Puate-Rodriguez, et al., 2008):

1. The sensor module which captures the biometric data.
2. The feature extraction module which processes the biometric data and extracts a set of discriminatory features.
3. The matching module which extracts the features and compares them against the stored templates to generate matching scores. Computational intelligence has been used to enhance the robustness, adaptivity, and recognition performance of the matching module. Some computational intelligence based biometric matching methods include (Zhang and Zuo, 2007):
 - radial basis function neural networks (RBFNN) which are computationally simple and robustly generalizable
 - SVMs which are tools for classification and regression
 - fuzzy technology which has been successfully applied to face, fingerprint, and multimodal biometrics.
4. The decision module is where a user's claimed identity is confirmed or a user's identity is established based on a matching score.
5. The system database module is used to store the biometric templates of the enrolled users.

This model has been extensively used for unimodal biometric systems. The majority of biometric systems belong to the unimodal category, which relies on a single source for authentication (Ross and Jain, 2004). These biometric systems are often

affected by problems such as noise in the data, which can result from defective or improperly maintained sensors or unfavorable ambient conditions; non-universality; intraclass variations, which are caused by incorrect interaction with a sensor or when the characteristics of the sensor are modified during authentication; interclass similarities, which consist of overlaps in the feature space of multiple users; unacceptable error rates; and spoof attacks, which occur when users try to imitate characteristics of other users (Faundez-Zanuy, 2005).

People seek ways to improve performance since no single modality can help to accomplish the task analysis perfectly. The use of multimodal biometric systems helps to reduce some of the problems present in unimodal systems. Multimodal data usually contains complimentary, correlated, and redundant information. Also, multimodal data is useful for tasks like detection, recognition, identification, tracking, and decision making (Wang and Kankahalli, 2010). Multimodal biometric systems consolidate the data obtained from different sources and provide some benefits such as: a decrease in FARs and in FRRs, a more robust authentication against individual sensor or subsystem failures, and a reduction in the number of cases where the system is not able to achieve a result. The more common examples of the use of multimodal biometric data include iris and retina of the eye; fingerprints, geometry and palm print of the hand; and face and ears (Wang and Yanushkevich, 2007).

Moreover, multimodal biometric systems can consist of multiple sensors for the same biometric, multiple biometric characteristics, multiple units of the same biometric, multiple snapshots of the same biometric, or multiple representations and matching algorithms for the same biometric (Jain, Nandakumar, and Ross, 2005; Puente-Rodriguez et

al., 2008). Also, they can operate in three modes: serial, parallel or hierarchical. In serial mode, the output for one trait is used to narrow down the number of possible identities before the next trait is used. In parallel mode, information from multiple traits is used simultaneously. In hierarchical mode, individual classifiers are combined in a tree-like structure.

To integrate the different results, multimodal biometric systems add a fusion module to the generic biometric model. This module is used to consolidate the data from different modules. The consolidation of the data can occur at different levels (Snelick, Indovina, Yen, and Mink, 2003; Jain, Ross, and Prabhakar, 2004; Monwar and Gavrilova, 2009):

- Sensor level – The raw data extracted from multiple sensors can be processed and integrated to produce new data from which features are extracted.
 - Feature level - Different features are extracted over a single biometric signal and these features are then combined.
 - Match score level - It consists of the combination of the scores provided by each matcher. The matcher provides a distance measure or a similarity measure between the input features and the models stored in a database.
- Score level fusion is preferred when consistent data is being fused (De Marsico, Nappi, Riccio, and Tortora, 2011). Match score level fusion can be approached in two different ways. One approach sees it as a classification problem while the other sees it as a combination problem. In the classification approach, a feature vector is built using the individual matching scores which is then classified in one of two classes: “accept” or “reject”. In the

combination approach, the individual matching scores are combined to generate a single scalar score which is then used to make the final decision (Jain, Nandakumar, and Ross, 2005).

- Rank Level – It consolidates the multiple ranks associated with each enrolled identity and determines a new rank that would aid in establishing the final decision. It is preferred when dealing with inconsistent data (De Marsico et al., 2011).
- Decision level - Each classifier provides a decision.

Sometimes the output provided by a level may contain numeric values resulting from measuring different features using different scales. A direct combination of these values can give incorrect results because scores need to be comparable (De Marsico et al., 2011). Normalization techniques can be used to prevent this from happening. Some of these are (Snelick et al., 2003):

- Min-max – It is the simplest one and is best suited for cases where the maximum and minimum values are known. Given a set of matching scores $\{s_k\}$, $k = 1, 2, \dots, n$, the normalized scores are given by:

$$s'_k = \frac{s_k - \min}{\max - \min} \quad (3)$$

- Decimal scaling – It can be applied when the scores of different matchers are on a logarithmic scale. Given a set of matching scores $\{s_k\}$, $k=1, 2, \dots, n$, the normalized scores are given by:

$$s'_k = \frac{s_k}{10^n} \quad (4)$$

where $n = \log_{10} \max(s_i)$.

- Z-score – It is the most commonly used and employs the arithmetic mean and standard deviation of the given data. Given a set of matching scores $\{s_k\}$, $k=1, 2, \dots, n$, the normalized scores are given by

$$s'_k = \frac{s_k - \mu}{\sigma} \quad (5)$$

where μ is the arithmetic mean and σ is the standard deviation of the given data.

- Median – median absolute deviation (MAD) – It is insensitive to outliers and points in the extreme tails of the distribution. Given a set of matching scores $\{s_k\}$, $k=1, 2, \dots, n$, the normalized scores are given by

$$s'_k = \frac{s_k - \text{median}}{\text{MAD}} \quad (6)$$

where $\text{MAD} = \text{median}(|s_k - \text{median}|)$.

- Tanh – Given a set of matching scores $\{s_k\}$, $k=1, 2, \dots, n$, the normalized scores are given by

$$s'_k = \frac{1}{2} \left\{ \tanh \left[0.01 \left(\frac{s_k - \mu_{GH}}{\sigma_{GH}} \right) \right] + 1 \right\} \quad (7)$$

where μ_{GH} and σ_{GH} are the mean and standard deviation estimates, respectively, of the genuine score distribution.

It was found that min-max, z-score, and tanh normalization techniques followed by a simple sum of scores fusion method result in superior genuine acceptance rate (GAR) than all other normalization and fusion techniques (Jain et al., 2005).

Once the outputs from the different levels are ready to be combined, several combination schemes can be applied to fuse them. The most popular ones are (Puentes-Rodriguez, 2008):

- Weighted sums – A very simple algorithm that combines the input scores using a weighted sum to obtain a final score. The decision is calculated by comparing this final score against a threshold. Its best characteristic is its low computational cost as it only needs to carry out sums and multiplications.
- Weighted products – A combined score is obtained by weighted multiplication of unimodal scores. The decision is also calculated by comparing this score against a threshold.
- Neural networks – The most standard ones consist of several layers of neurons: an input layer, hidden layers, and output layers. Input layers take the input and distribute it to the hidden layers, which do all the necessary computation and output the results to the output layer. This output layer is the one that takes the final decision.
- SVMs – SVMs are considered intuitive, theoretically well founded and also have shown to be successful in practice. According to Witten, Frank, and Hall (2011), SVMs often require fewer parameters to achieve similar or better accuracy levels than neural networks.

All of the schemes employed to fuse results present some advantages and disadvantages (Table 1). The use of the correct scheme for a work depends on the type of data but probably one may never know if the best scheme was applied (Triantaphyllou, 2000). It can be inferred from the data in Table 1 that using SVMs is the better choice for this

research since its main advantage is that it protects against overfitting while computational complexity is avoided by the use of kernels.

Table 1

Comparison of Some Popular Combination Schemes Employed to Fuse Results

Scheme	Advantages	Disadvantages
Weighted sums	It is a straightforward method, especially used in single dimensional problems. Its best characteristic is its low computational cost as it only needs to carry out sums and multiplications (Triantaphyllou, 2000).	It present problems when is applied to multi-dimensional decision making problems. The combination of different dimensions, and consequently different units, provokes the violation of the additive utility assumption (Triantaphyllou, 2000).
Weighted products	It is sometimes called dimensionless analysis because its structure eliminates any units of measure. It can be used in single and multidimensional analysis. (Triantaphyllou, 2000).	It is more expensive in terms of computational requirements than weighted sums because of the implementation of the scores raised to the power of the attribute importance weight (Triantaphyllou, 2000).
Neural Networks	They require less formal statistical training, ability to implicitly detect complex nonlinear relationships between dependent and independent variables, ability to detect all possible interactions between predictor variables, and the availability of multiple training algorithms (Tu, 1996).	Its black box nature, greater computational load, proneness to overfitting, and the empirical nature of model development (Tu, 1996).
SVMs	It can implicitly detect complex nonlinear relationships between dependent and independent variables, detect all possible interactions between predictor variables (Tu, 1996). Overfitting, a problem often found in other approaches, is unlikely to occur with SVMs (Puente-Rodríguez, et al., 2008)	Computational complexity can occur but it can be solved with the use of kernels (Puente-Rodríguez, et al., 2008).

SVMs

SVMs are algorithms that use linear models to implement nonlinear class boundaries (Luts, Ojeda, Van de Plas, De Moor, Van Huffel, and Suykens, 2010; Witten, Frank, and Hall, 2011). In practical terms, SVMs assigns each input value to a positive or negative class. A key issue with SVMs is that they have to be trained on data points whose labels are known, called training data. The training data can be represented as a set:

$$X = \{(x_1, y_1), \dots, (x_l, y_l) : x_i \in \mathbb{R}^n, y_i \in \{-1, +1\}\} \quad (8)$$

, where x_i are the data points and y_i their label and can be either -1 or $+1$.

$$\text{The decision function } f: \mathbb{R}^n \rightarrow \{-1, +1\} \quad (9)$$

maps the input vectors x_i to the negative or positive class.

SVMs select a small number of critical boundary instances called support vectors from each class and build a linear discriminant function that separates them as widely as possible. This instance-based approach goes beyond the limitations of linear boundaries by making it practical to include extra nonlinear terms in the function, making it possible to form quadratic, cubic, and higher-order decision boundaries (Witten, Frank, and Hall, 2011). That discriminant function is called the maximum-margin hyperplane. This hyperplane is just a linear model that gives the greatest separation between the classes and it comes no closer to either class than it has to (Figure 1).

The hyperplane is defined by its normal vector w and its offset b , defined as the distance by which the plane is displaced from the origin of the coordinate system (Hearst, Dumais, Osman, Platt, and Scholkopf, 1998):

$$\text{Hyperplane (H)} = \{x \mid (w, x) + b = 0\} \quad (10)$$

, with $w \in \mathbb{R}^n$, $b \in \mathbb{R}$ and (\cdot, \cdot) denoting the dot product or scalar product.

The decision function:

$$f(x) = \text{sign}((w, x) + b), \quad (11)$$

will return +1 for points lying on the positive side of the hyperplane and -1 for points on the negative side.

A training set $X = \{(x_1, y_1), \dots, (x_n, y_n) : x_i \in \mathbb{R}^n, y_i \in \{-1, +1\}\}$ is separable by a hyperplane $(w, x) + b = 0$ if both a unit vector w ($\|w\| = 1$) and a constant b exists so that :

$$(w, x_i) + b > 0 \text{ if } y_i = +1 \quad (12)$$

$$(w, x_i) + b < 0 \text{ if } y_i = -1 \quad (13)$$

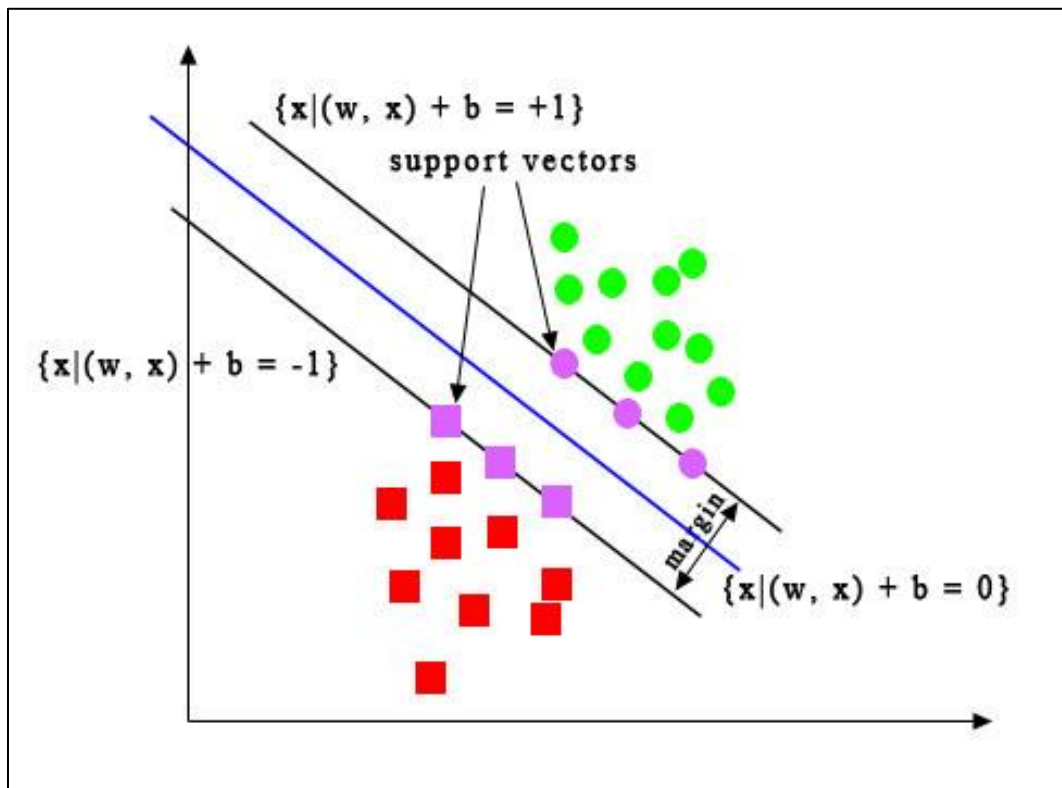


Figure 1. Example of a linearly separable problem in a two dimensional space. Adapted from "Support-vector networks" by C. Cortes and V. Vapnik, 1995, Machine learning, 20(3), p. 275.

There are many possible ways to place a hyperplane that will separate the two classes. Therefore, an optimal separating hyperplane (OSH) can be determined. The optimal hyperplane is defined as the one with the maximal margin of separation between the two classes. A basic assumption of learning from examples is that new data points are believed to lie close to or in-between the known training data. Therefore, the OSH should allow small deviations in the data and be in the middle of the structures of the positive and negative data clouds. Any implementation needs to determine the unit vector w and the constant b that maximize the margin of the training set $X(w, b)$ need to be determined.

Sometimes data cannot be separated linearly in a reasonable way. In most cases, the process by which the data were generated simply cannot be approximated by a linear function. One solution is to employ a function Φ , the feature map, which pairs the data points x_i of the data space L to the feature space H where a linear separation is possible (Figure 2) (Hearst et al., 1998):

$$\Phi : \mathbb{R}^n \rightarrow H \quad (14)$$

$$x_i \in L \rightarrow \Phi(x_i) \in H \quad (15)$$

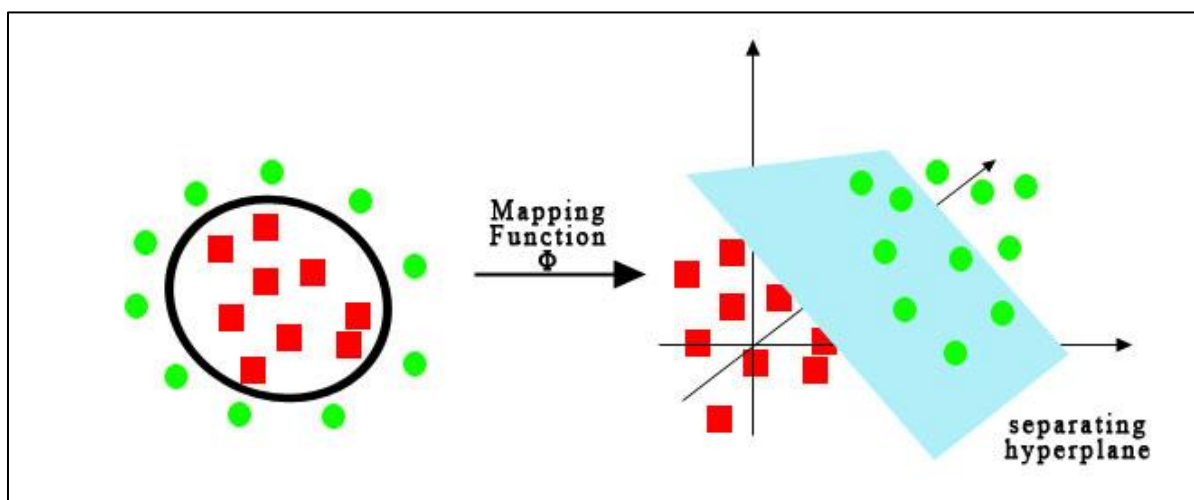


Figure 2. Employing a mapping function Φ , to map the data points x_i of the data space L to the feature space H where a linear separation is possible. Adapted from “A tutorial on support vector machine-based methods for classification problems in chemometrics” by J. Luts et al., 2010, *Analytica Chimica Acta*, 665(2), p.131.

Supposing that an appropriate mapping function Φ that allows for a linear separation in the feature space H is found. It has been observed that all formulas depend only on the data through dot products in H , i.e. on functions of the form $\Phi(x_i) \cdot \Phi(x_j)$ when solving the equations for the optimal separating hyperplane in the hyperspace.

If H is high-dimensional, $\Phi(x_i) \cdot \Phi(x_j)$ will be very expensive to compute (Hearst et al., 1998). In some cases, a simple kernel k can be used to evaluate it efficiently:

$$k(x_i, x_j) = \Phi(x_i) \cdot \Phi(x_j) \quad (16)$$

Equation 16 can be used as a similarity measure for x_i and x_j without explicitly knowing Φ nor the dimension of H . The kernel function should return a measure of similarity. All computations can be done directly in H , which keeps the possibility of a geometric interpretation of SVMs by the optimal separating hyperplane.

Kernel functions calculate the dot product before the nonlinear mapping is performed on the original attribute set. They are based on the dot product and some of them are (Burges, 1998; Müller, Mika, Rätsch, Tsuda, and Schölkopf, 2001):

- linear kernel – It computes the dot product of two vectors x_i and x_j :

$$k(x_i, x_j) = \langle x_i, x_j \rangle \quad (17)$$

- polynomial kernel – It computes the dot product of two vectors x_i and x_j and raises the result to the power d :

$$k(x_i, x_j) = (s\langle x_i, x_j \rangle + c)^d \quad (18)$$

, where s , c , and d are kernel specific parameters.

A common way of choosing the value of d is to start with 1 (a linear model) and increment it until the estimated error ceases to improve. Usually, quite small values suffice. To include lower-order terms, a kernel $(x_i \cdot x_j + 1)^d$ can be used.

- radial basis function (RBF) kernel – A support vector machine with the RBF kernel is simply a type of neural network called an RBF network.

$$k(x_i, x_j) = \exp\left(-\frac{\|x_i - x_j\|^2}{2\sigma_0^2}\right), \text{ where } 2\sigma_0^2 = \text{mean } \|x_i - x_j\|^2 \quad (19)$$

- sigmoid kernel – It implements another type of neural network, a multilayer perceptron with one hidden layer :

$$k(x_i, x_j) = \tanh(s\langle x_i, x_j \rangle + c) \quad (20)$$

where s and c are kernel specific parameters.

The radial basis function (RBF) kernel and the sigmoid kernel are often suggested and both produce good results. Usually, the best results depend on the application, although the differences are rarely large in practice (Hsu, Chang, and Lin, 2003).

A major advantage of using SVMs is the fact that overfitting, a problem often found in other approaches, is unlikely to occur. Overfitting is caused by too much flexibility in the decision boundary. The reason is that the maximum-margin hyperplane is relatively stable, i.e., it only moves if training instances that are support vectors are added or deleted. The support vectors are global representatives of the whole set of training points, and there are usually few of them, which gives little flexibility.

A problem that can be found in SVMs is computational complexity. For example, if the transformed space is a high-dimensional one then the transformed support vectors and test instances have many components. This means that every time an instance is classified its dot product with all support vectors must be calculated. In the high-dimensional space produced by the nonlinear mapping this is rather expensive in terms of computational resources. Obtaining the dot product involves one multiplication and one addition for each attribute, which means that the number of attributes in the new space can be enormous. This problem can occur not only during classification but also during training because the optimization algorithms have to calculate the same dot products very frequently. This problem is solved by using kernel functions (Luts et al., 2010).

SVMs have been used in conventional multiclass classification problems where data from two or more classes is available and the decision boundary is supported by the presence of samples from each class. In some classification problems this is not the case, sometimes negative data is either absent or limited in its distribution, which means that

only one side of the classification boundary can be determined. These problems are known as One-Class Classification problems.

One-Class Classification

One-Class Classification (OCC) problems are usually harder than problems of conventional multiclass / binary classification. Moreover, the drawbacks that are encountered in multiclass classification problems; such as estimation of error rates, measuring the complexity of a solution, curse of dimensionality, and generalization of the method; also appear in OCC, and sometimes become even more prominent. The task in OCC is to define a classification boundary around the target class, such that it accepts as many objects as possible from the positive class, while it minimizes the chance of accepting outlier objects (Khan & Madden, 2010).

Several approaches have been implemented to face the OCC problems:

- Support Vector Data Description (Tax and Duin, 2002). This method seeks to solve the problem of OCC by distinguishing the positive class from all other possible patterns by building a hyper-sphere around the positive class data instead of using a hyper-plane to distinguish between two classes. This hyper-sphere encompasses almost all points in the data set with the minimum radius. A drawback of this technique is that it often requires a large data set. Additional problems may arise when large differences in density exist, that is, objects in low-density areas will be rejected although they are legitimate objects (Khan & Madden, 2010).

- Scholkopf, Williamson, Smola, Shawe-Taylor, and Platt (1999) suggested a method of adapting the SVM methodology to the OCC problem by using a separating hyper-plane. They try to separate the surface region containing data from the region containing no data. This is achieved by constructing a hyper-plane which is maximally distant from origin, with all data points lying on the opposite side from the origin and such that the margin is positive. After transforming the feature via a kernel, they treat the origin as the only member of the second class and separate the image of the one-class from the origin. Then standard two-class SVM techniques are employed. One-Class SVMs have the same advantages as SVM, such as efficient handling of high dimensional spaces and systematic nonlinear classification using advanced kernel functions (Yu, H. (2003).
- Manevitz and Yousef (2002) proposed a different version of the one-class SVM. Their idea was to work first in the feature space, and assume that not only is the origin the second class, but also that all data points close enough to the origin are considered as noise or outliers. Also, they treated vectors lying on standard sub-spaces of small dimension as outliers. Their results, evaluated using Reuters Data set 1, were worse than the results obtained with the One-Class SVM algorithm presented by Scholkopf et al (Khan and Madden, 2010).

Testing of Biometric Authentication Systems

Practical biometric systems don't make perfect match decisions (Jain et al., 2004). A biometric system cannot guarantee 100% accuracy partly due to the inconsistency of humans. Stress, general health, working and environmental conditions, and time pressures all effectively conspire to make humans inconsistent. This accentuates the need for an evaluation of acceptability and user satisfaction (El-Abed, Giot, Hemery, and Rosenberger, 2010).

Obviously, the effectiveness of these approaches needs to be tested and experimental research has been employed to do so. Experimental research helps to make judgments with systematically measured confidence and reliability. The control of potential influential factors is challenging in experimental research but their impact can be reduced to acceptable levels through well-designed and conducted experiments (Lazar, Feng, and Hochheiser, 2010).

Two aspects usually need to be tested in biometric systems: system effectiveness and user acceptance. These aspects were covered by the research questions of this work:

- How effective was this biometric approach in terms of user authentication?
- How was this approach perceived by users?

Effectiveness of the biometric approach

In terms of effectiveness, different metrics are used to evaluate performance. For example, Jorgensen and Yu (2011) suggest that biometric authentication systems, like those based on mouse dynamics, are typically evaluated with respect to the following metrics: FAR, the probability that the system will incorrectly label an active user as the same user that produced the enrollment signature; FRR, the probability that the system

will incorrectly label the active user as an impostor; EER, the error rate when the system's parameters are set such that the FRR and FAR are equal; and Verification Time, the time required by the system to collect sufficient behavioral data to make an authentication decision.

Usually, biometric systems based on physiological traits (DNA, physiological signals) have lower EER values than those based on behavioral traits (keystroke dynamics, mouse dynamics) or morphological traits (fingerprint, face) (Table 2). Most of all, biometric systems cannot guarantee 100% accuracy due to the inconsistency of humans, the systems and the environment (Kanneh and Sakr, 2008).

Table 2

EER for Different Biometric Authentication Approaches

Type	EER
brain signal	16% to 28%
heart sound signals	4%
fingerprint	2%
face recognition	5% to 10%
haptics devices	10% to 22%
gait	19% to 37%
voice verification	near 5%
keystroke authentication for mobile phones	15%
keystroke authentication for computer keyboard	near 5%
online signature verification	near 5%
mouse dynamics	24%

Note. Adapted from Mahier, J., Pasquet, M., Rosenberger, C., & Cuzzo, F. (2008). Biometric authentication. *Encyclopedia of Information Science and Technology*, 13.

FAR and FRR reflect the system's ability to allow limited entry to authorized users. Both measures can vary significantly depending on how the sensitivity of the mechanism that matches the biometric trait is adjusted. For example, a tighter match

between the measurements and the template employed will probably decrease the false-acceptance rate but at the same time can increase the false-rejection rate (Liu and Silverman, 2001).

Sulong, Wahyudi, and Siddiqi (2009) used FRR of legitimate users and FAR of impostors to determine effectiveness in their approach to identify users based on keystroke pressure. A security system should detect a substantial percentage of imposters while keeping FRR at an acceptable level. The threshold or match scores should be chosen to give a low FAR if security is the most important criterion for the biometric device (Kanneh and Sakr, 2008).

Others like El-Abed et al. (2010) recommend the use of metrics such as failure to enroll (FTE) to evaluate performance. FTE rate denotes the percentage of times users are not able to enroll in a recognition system. It can be caused by physical differences, lack of training, environmental conditions or ergonomics. For this work, the implementation required an activity very familiar to those using touchscreen devices which means that biometric traits were easily captured and this type of evaluation was not implemented.

User's disposition

The evaluation of acceptance and user satisfaction involves various factors. The acceptance of a biometric system depends on its operational, technical, manufacturing, and financial possibilities. El-Abed et al. (2010) recommend the evaluation of the individual's entire interaction with the system, as well as thoughts, feelings, and outcomes that might result from the interaction. They added that several factors influence how a biometric system is perceived. These factors are: reliability; ease of use; user acceptance which is mainly determined by the perceived obstructiveness and intrusiveness; ease of

implementation; and the cost of equipment, installation, training, software, and system maintenance. All of these issues need to be carefully examined before adopting a new authentication biometric mechanism.

Also, as previously mentioned, TAM states that system use is a response that can be predicted by user motivation and it is directly influenced by the actual system's features and capabilities (Davis, 1993). According to the model, user motivation can be explained by: perceived ease of use, perceived usefulness, and attitude toward using the system. Attitude is a function of perceived usefulness and, in a less degree, perceived ease of use. Perceived usefulness is defined as the degree to which an individual believes that using a particular system will enhance his or her job performance. Perceived ease of use is defined as the degree to which an individual believes that using a particular system would be free of physical and mental effort.

James, Pirim, Boswell, Reithel, and Barkhi (2008) state that there are other factors that can influence the adoption of a biometric authentication system besides the factors pointed out by TAM. Those additional factors are: perceived need for security, perceived need for privacy, and perceived physical invasiveness. Perceived need for security is defined as one's perceived need for the safekeeping of physical or informational assets. Perceived need for privacy is defined as the importance to an individual of being able to control the acquisition and usage of personal information. Finally, perceived physical invasiveness is defined as one's perception of the invasiveness of the technology to their person. In their study, they asked several questions about user's perceptions about security and privacy. They found that users are

concerned about security and privacy (Table 3, Table 4) and that both factors have an effect on perceived physical invasiveness which affects intention to use.

Table 3

Descriptive Statistics for Perceived Need for Security

Statement	Mean	S.D.
S1 I feel that the safeguarding from potential external threats of my physical being is important to me.	1.56	0.76
S2. I feel that my personal security at my home or in my vehicle is important to me.	1.39	0.67
S3. I feel that my personal security at my place of work or other work related places is important to me.	1.51	0.71
S4. My security at places of public access, such as a mall or airport, or special public events, such as the Olympics or the Super Bowl, is important to me.	1.48	0.64
S5. I feel that the security of my tangible assets (such as my home, vehicle, etc.) is important to me.	1.53	0.70
S6. I feel that keeping my personal possessions, such as jewelry, money, electronics, etc. safe is important to me.	1.66	0.74
S7. I feel that the safekeeping of my informational assets contained in digital or paper format is important to me (such as financial records, medical records, etc.)	1.53	0.72
S8. I feel that the security of my personal information, such as my PC files or personal records (financial, medical, etc.) is important to me.	1.56	0.72
S9. I feel that the safekeeping of information I have provided to a corporation or other entity is important to me.	1.66	0.78
Average	1.54	0.72

Note. S. D. = Standard Deviation. Adapted from “An extension of the technology acceptance model to determine the intention to use biometric devices,” by T. James, T. Pirim, K. Boswell, B. Reithel, and R. Barkhi, 2008, In S. Clarke, (Ed.), *End User Computing Challenges and Technologies: Emerging Tools and Applications* (pp. 67), Hershey, PA: IGI Global.

Table 4

Descriptive Statistics for Perceived Need for Privacy

Statement	Mean	S.D.
P1. I feel my privacy is very important to me.	1.47	0.68
P2. I feel that my control over my personal information is very important to me.	1.51	0.69
P3. I feel that it is important not to release sensitive information to any entity.	1.92	0.97
P4. I feel it is important to avoid having personal information released that I think could be financially damaging.	1.48	0.70
P5. I feel it is important to avoid having personal information released that I think could be socially damaging to me.	1.65	0.76
P6. I feel it is important to avoid having personal information about me released that may go against social morals and attitudes.	1.80	0.86
P7. I feel that the release of personal information to individuals with whom I have a high comfort level is unacceptable.	2.62	1.19
P8. I feel that the release of personal information to entities where I feel as though I am anonymously providing the information is unacceptable.	2.27	1.11
P9. I feel that the use of personal information that has been released by me but is used in a manner not intended by me is unacceptable.	1.61	0.86
Average	1.81	0.89

Note. S. D. = Standard Deviation. Adapted from “An extension of the technology acceptance model to determine the intention to use biometric devices,” by T. James, T. Pirim, K. Boswell, B. Reithel, and R. Barkhi, 2008, In S. Clarke, (Ed.), *End User Computing Challenges and Technologies: Emerging Tools and Applications* (pp. 67), Hershey, PA: IGI Global.

Resources Searched

The literature review was completed using the online databases available to the author at NSU and UPR – Mayagüez, where the researcher works. The online databases employed were:

- Academic OneFile – Gale Cengage Learning
- Academic Search Complete – EBSCOhost
- ACM Digital Library – Association for Computing Machinery
- IEEE Xplore – IEEE
- ProQuest Science Journals - ProQuest

- ScienceDirect – Elsevier
- SpringerLink Online Journals – Springer
- Google Scholar

Summary

User authentication has been implemented for many years as a way to ensure that the authorized person has access to certain resources (Giot et al., 2009). There are two types of user authentication mechanisms: static and dynamic (Niinuma, Park, and Jain, 2010). Static authentication verifies identity on just one occasion while dynamic authentication validates users at any moment during their interaction with a device. The majority of static and dynamic authentication systems are knowledge based methods or token based methods, i. e., they depend on something a user knows or something a user has.

Biometric authentication is another method that has been used recently. It employs physiological features to authenticate users (De Luis-Garcia et al., 2003). Biometric authentication is considered to be highly reliable because physical human characteristics are much more difficult to forge than security codes, passwords, or hardware keys (Matyas and Riha, 2003).

Biometric systems are divided into two categories: physiological and behavioral. Physiological biometric systems are based on an individual's distinctive characteristics like fingerprints, iris, retina, facial images, and hand geometry (Shaikh and Dimitriadis, 2008; Patrick, Long, and Flinn, 2003). Behavioral biometric systems are based on the way people do things. Implementations of behavioral biometrics include: keystroke dynamics and mouse dynamics.

The implementation of a biometric system usually consists of five modules: sensor module, feature extraction module, matching module, decision module, and system database module (Puente-Rodriguez, et al., 2008). Computational intelligence has been used to enhance the robustness, adaptivity, and recognition performance of the matching module. Some computational intelligence based biometric matching methods include: radial basis function neural networks (RBFNN), SVMs, and fuzzy technology (Zhang and Zuo, 2007).

This generic behavioral biometric model has been extensively used for unimodal biometric systems but people seek ways to improve performance since no single modality can help to accomplish the task analysis perfectly. Multimodal biometric systems employ data obtained from different sources which usually contains complimentary, correlated, and redundant information.

Multimodal biometric systems add a fusion module to the biometric model to integrate the different results. This fusion module is used to consolidate the data from different modules. The consolidation of the data can occur at different levels: sensor level, feature extraction level, match score level, rank level, or decision level (Snelick et al., 2003; Jain, Ross, and Prabhakar, 2004; Monwar and Gavrilova, 2009).

Once the outputs from the different levels are ready to be combined, several combination schemes can be applied to fuse them. The most popular ones are: weighted sums, weighted products, neural networks, and SVMs (Puente-Rodriguez et al., 2008). SVMs are discriminative classifiers that perform a nonlinear mapping from an input space to an SVM feature space. Linear classification techniques are then applied in this potentially high-dimensional space. Its inputs are the unimodal matching scores, and the

output is the final decision about the user claimed identity. SVMs are considered intuitive, theoretically well founded and also have shown to be successful in practice. They often require fewer parameters to achieve similar or better accuracy levels than neural networks (Witten, Frank, and Hall, 2011).

Obviously, the efficacy of these approaches needs to be tested and experimental research has been employed to do so. Experimental research helps to make judgments with systematically measured confidence and reliability. Two aspects usually need to be tested in biometric systems: system effectiveness and user acceptance. In terms of effectiveness, Jorgensen and Yu (2011) suggest the use of the following metrics: FAR, FRR, and EER. One important issue regarding practical biometric systems is that they don't make perfect match decisions (Jain et al., 2004). A biometric system cannot guarantee 100% accuracy partly due to the inconsistency of humans. This fact accentuates the need for an evaluation of acceptability and user satisfaction (El-Abed et al., 2010).

Chapter 3

Methodology

Scholarly research can follow two tracks: quantitative research or qualitative research. The selection of the path depends on the nature of the research problem and the questions that will be asked. Quantitative research identifies a research problem based on trends in the field or on the need to explain why something occurs. Describing a trend means that the research problem can be best answered by a study in which the researcher seeks to establish the overall tendency of responses from individuals. Qualitative research addresses a research problem where the variables and need to explore are not known. The literature might yield little information about the phenomenon of study, and there is a need to learn more from participants through exploration (Creswell, 2012).

The type of data needed along with the nature of the problem being addressed by the research help to determine the method to be employed. Several methods have been commonly employed in information systems research (Ellis and Levy, 2009):

- Experimental – This type of research determines if a cause and effect relationship exists between different factors or set of factors. In this type of experiment, the researcher manipulates the independent variables, assigning participants randomly to different groups that receive different treatments or imple-

mentations of the independent variable. The performance of the participants on the dependent variable is measured to determine if changes in the independent variables affect the dependent variable.

- Causal Comparative – It also determines if a cause and effect relationship exists between different factors or set of factors. This method differs from experimental research in the fact that the researcher does not have control of the independent variable and cannot manipulate it. The researcher observes, measures, and compares the performance on the dependent variable or variables of subjects in naturally-occurring groupings based on the independent variable.
- Case Study – A case study investigates a contemporary phenomenon within its real life context using multiple sources of evidence. The data collected in a case study is typically qualitative. It focuses on developing an in-depth understanding.
- Historical – It explains the causes of change through time by interpretation of qualitative data. It is based upon the recognition of a historical problem or the identification of a need for certain historical knowledge. It generally collects as much information about the problem or topic as possible.
- Correlational – It determines the presence and degree of a relationship between two factors. Similarly to causal-comparative research, it focuses on analyzing quantitative data to determine if a relationship exists between two variables. Contrary to causal-comparative research, it does not attempt to determine if a cause-effect relationship exists. The goal for correlational

studies is to determine if a predictive relationship exists. There is no distinction between independent and dependent variables in correlational research.

- **Developmental** – It is employed when there is not a suitable solution to test for efficacy in addressing a problem. It assumes that researchers don't even know how to go about building a solution that can be tested. Developmental research attempts to answer the question: How can researchers build something to address the problem?
- **Grounded Theory** – Grounded Theory is a qualitative procedure used to generate theory that explains a process, an action, or interaction about a topic. It is used when available theories cannot adequately explain the phenomena observed.
- **Ethnography** – Ethnography deals with an in-depth qualitative investigation of a group that shares a common culture.
- **Action Research** – Action research focuses on finding a solution to a local problem in a local setting. In this type of research, the researcher himself or herself are part of the practitioners group that face the actual problem the research is trying to address. The aim of action research is to investigate a localized and practical problem.

The decision of which approach to employ is determined by the type of questions that the research will answer and the type of data needed (Ellis and Levy, 2009). The next section discusses the research method employed in this study and the rationale behind that decision. It is followed by the model employed and how it was implemented.

Afterwards the testing procedure employed and the resources used are discussed. The chapter ends with a brief summary.

Research Method

This research answered, as already mentioned, two questions:

- How effective was this biometric approach in terms of user authentication?
- How was this approach perceived by users?

As can be seen, these questions have a confirmatory and predictive nature. Ellis and Levy (2009) state that studies driven by this type of questions are generally based on quantitative data. Additionally, the cause and effect nature of these research questions confirm that experimental research had to be employed as research method.

Experimental research allows making judgments with systematically measured confidence and reliability. This method has been used in previous biometric research. Lazar, Feng, and Hochheiser (2010) state that the control of potential influential factors in this type of research is challenging but the impact of these factors can be reduced to acceptable levels through well-designed and conducted experiments.

Modeling

A multimodal behavioral biometric model was constructed to test the effectiveness of the proposed approach. The model captures and processes biometric traits that are generated while a person's finger moves over a touchscreen (Figure 3).

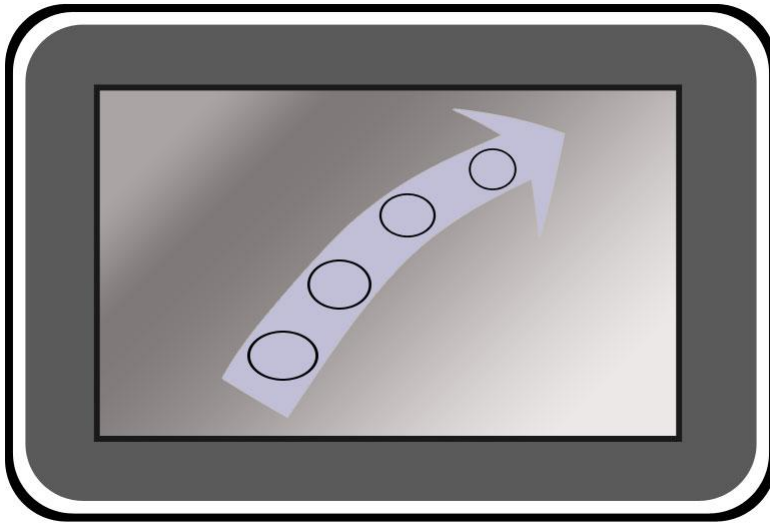


Figure 3. Representation of a finger stroke over the touchscreen.

The following biometric traits were captured:

1. area in contact with the touchscreen (Figure 4)
2. length of the major axis of an ellipse that describes the touch area at the point of contact (Figure 4)
3. length of the minor axis of an ellipse that describes the touch area at the point of contact (Figure 4)

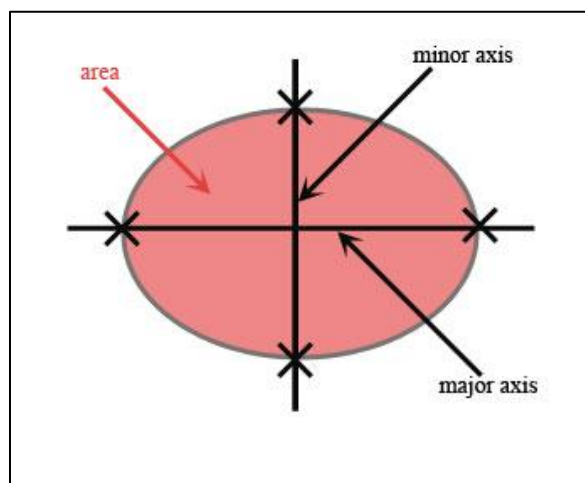


Figure 4. Finger over a touchscreen.

4. distance traveled, given by

$$d = \sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2} \quad (21)$$

where (x_1, y_1) and (x_2, y_2) are the coordinates at point u and point v respectively (Figure 5) (Beecher, Penna, and Bittinger, 2011).

5. speed, given by

$$s = \frac{\sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2}}{t_2 - t_1} \quad (22)$$

where (x_1, y_1, t_1) and (x_2, y_2, t_2) are the coordinates and times of contact measured at point u and point v respectively (Figure 5) (Beecher, Penna, and Bittinger, 2011).

6. angle created by the movement, which is the angle (θ) between the vectors passing through each point with origin at $(0,0)$ in a Cartesian Plane (Figure 5). The angle between two vectors with origin at $(0,0)$ is defined as (Beecher, Penna, and Bittinger, 2011):

$$\theta = \cos^{-1} \left(\frac{\vec{U} \cdot \vec{V}}{|\vec{U}| |\vec{V}|} \right) \quad (23)$$

where,

\vec{U} is a vector that passes through point $u(x_1, y_1)$

\vec{V} is a vector that passes through point $v(x_2, y_2)$

$\vec{U} \cdot \vec{V}$ is the dot product and is defined as by $x_1 \cdot x_2 + y_1 \cdot y_2$ (24)

$|\vec{U}|$ is the magnitude and is defined by $\sqrt{x_1^2 + y_1^2}$ (25)

$|\vec{V}|$ is the magnitude and is defined by $\sqrt{x_2^2 + y_2^2}$ (26)

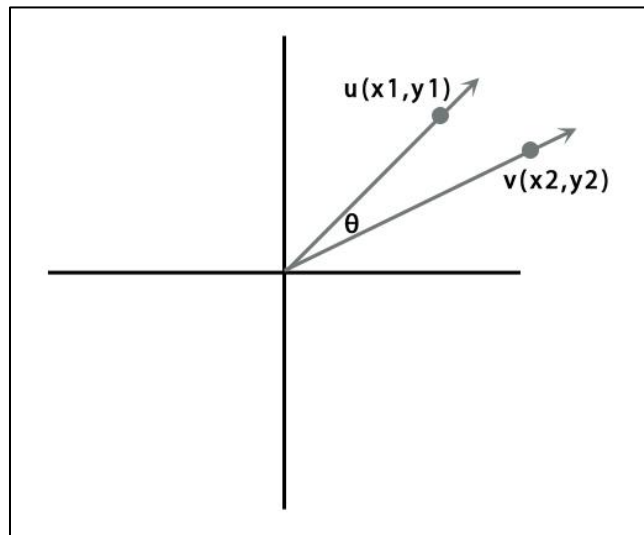


Figure 5. Cartesian plane.

Area in contact with the touchscreen, length of the major axis of an ellipse that describes the touch area, length of the minor axis of an ellipse that describes the touch area, (x, y) coordinates, and time of contact were captured directly using an application. The scanning of these traits began as soon as the user made contact with the screen surface. This approach makes this a multimodal biometric system since different traits were captured at different points during the interaction (Jain, Nandakumar, and Ross, 2005; Puente-Rodriguez et al., 2008). These traits were stored in a database which allowed the raw data to be preprocessed and analyzed at other stages.

The model used followed the generic biometric model presented by Wayman (1999) (Figure 6). At the sensor level, the raw data was acquired. Then it moved to the feature extraction level where traits like distance, speed, and the angle created by the movement were calculated. After that, the resulting data was moved to the matching score level where it was decided if the user is who he or she claims to be. The outputs of the classifiers from each multimodal data were combined to develop a final classifier.

The integration at the matching score level is easier in accessing and combining scores (Monwar and Gavrilova, 2009). It offers the best tradeoff in terms of the information content and the ease in fusion (Nandakumar, Chen, Dass, and Jain, 2008).

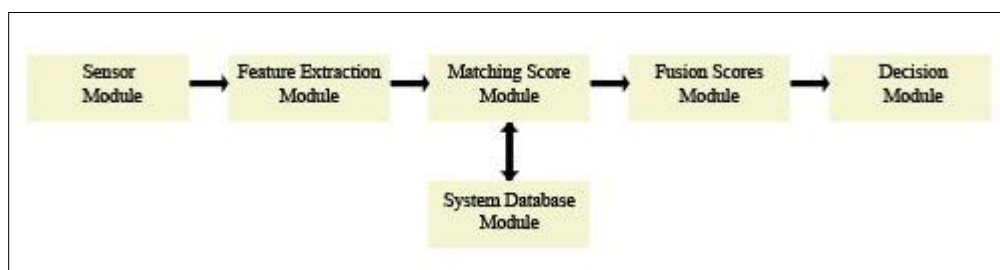


Figure 6. Behavioral biometric model. Adapted from “Technical testing and evaluation of biometric identification devices” by J. L. Wayman. 1999, In Jain, Anil K., Bolle, Ruud, & Pankanti, Sharath (Eds.), *Biometrics: Personal Identification in Networked Society*, p. 4.

Implementation

Three applications were constructed to verify the effectiveness of the proposed approach (Appendix A). One of the applications was built to capture the biometric traits. The other two applications built the SVM models and assess their effectiveness.

The three applications encompass the behavioral biometric model consisting of five processing modules and a database module (Figure 7). The Android application was built using the Eclipse Environment and it was designed to work in a 10 inch Lenovo ThinkPad Tablet using Android OS 4.0.3. Android OS provides developers full access to device features and services. Also, it does not charge any licensing, royalty, membership, or certification fees to develop applications (Cinar, 2012).

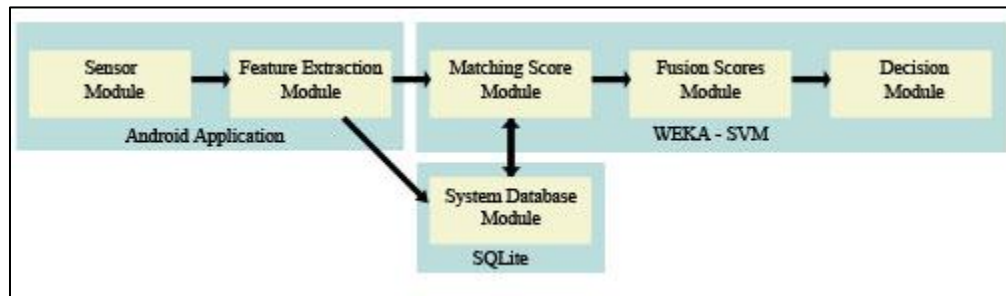


Figure 7. Application Diagram.

The design of the Android application followed Ben Shneiderman's Eight Golden Rules of Interface Design (Shneiderman and Plaisant, 2010):

1. strive for consistency
2. cater to universal usability
3. offer informative feedback
4. design dialogs to yield closure
5. prevent errors
6. permit easy reversal of actions
7. support internal locus of control
8. reduce short-term memory load

The raw biometric data from the contact of the fingers with the touchscreen was captured using the Android class `MotionEvent`. Also, the application calculated speed, distance, and angle created by the movement of the finger. The computation was done after all the raw data from a user had been captured. The scanning rate was implemented in milliseconds (ms). This was considered sufficient since the time it takes human beings to do things is measured in seconds or even minutes (Pusara and Brodley, 2004). Several studies have used scanning rates employing a similar range. For example, Hashia,

Pollett, and Stamp (2005) on their study about the effectiveness of using mouse movements as a biometric recorded data every 50 ms. In another study, Pusara and Brodley (2004) examined whether the mouse has moved every 100 ms.

That data for each user was grouped into strokes. A stroke was defined as a single unbroken movement (“Stroke”, 2014). It included the events occurring since the user pressed against the screen until he or she was no longer in contact with it. For this work, the objective was to capture 50 strokes of data for vertical scrolling and also 50 strokes for horizontal scrolling. Assuming one second per stroke, it would yield 50 seconds of data. A similar approach was employed by Gamboa and Fred (2003) who used 50 strokes in their study about mouse dynamics. They defined a stroke as the movement occurring between two clicks. They obtained an EER of 2%. In another study involving mouse dynamics, Schulz (2006) grouped his data in terms of curves and used 60 curves in his analysis that yielded an EER of 24.3%.

Each stroke was subdivided into three types of events and captured using the `getAction` method from the `MotionEvent` Class(Figure 8):

- down motion event – when contact with the touchscreen is initiated
- move motion event – when the finger is moving through the touchscreen
- up motion event – before the finger leaves the screen.



Figure 8. Representation of a finger stroke over the Android application.

Each stroke was composed of one down event and one up event but could contain several move events. The number of move events depended on the length of the stroke and the speed of the movement by the user. The down event captured: size (area), touchmajor, and touchminor. The move event captured: size (area), touchmajor, and touchminor, distance, speed, and angle which were defined with respect to a previous move event. The up event captured the same traits as the move event but distance, speed, and angle were calculated with respect to the previous down event (Table 5).

Table 5

Biometric Traits Captured During Each Motion Event

action	Biometric trait					
	size (area)	touchmajor	touchminor	distance	speed	angle
down	x	x	x			
move	x	x	x	x	x	x
up	x	x	x	x	x	x

The division of strokes into three types of events allows user authentication at three different points. Although events are part of the same stroke, they are independent events. The data obtained from the down event do not affect the data obtained from the up event.

The captured biometric traits were preprocessed using a java application (Appendix A). The preprocessing consisted of dividing the data captured for each participant into six data files (Appendix B). The data files were created according to the event captured while the finger was in contact with the touchscreen. Six files were created according to:

- down event during horizontal scrolling,
- move event during horizontal scrolling,
- up event during horizontal scrolling,
- down event during vertical scrolling,
- move event during vertical scrolling,
- up event during vertical scrolling.

Those files were used by another Java application to create and test six models for each participant using SVMs (Appendix A). The SVM model creation and analysis was made using the Waikato Environment for Knowledge Analysis (WEKA). WEKA was implemented through library functions from the java application created. WEKA is a collection of machine learning algorithms and data preprocessing tools. It was developed by the University of Waikato in New Zealand. It is written in Java and distributed under the terms of the GNU General Public License (Han, Kamber, and Pei, 2006).

As mentioned before, a model was created for each participant type of event (Appendix A). One-Class SVMs were used for classification purposes. The type of authentication problem presented in this work fits the type of problem addressed by One-Class classification. In cases like this one, sometimes negative data is either absent or limited in its distribution, which means that only one side of the classification boundary can be determined.

Based on the previous premises, this work implemented One-Class SVMs. The implementation was done employing LIBSVM. LIBSVM a library for SVMs commonly used in SVMs (Chang and Lin, 2011). The following parameter values were employed:

- ν – It is an upper bound on the ratio of training points on the wrong side of the hyperplane, and therefore, ν is also an upper bound on the training error rate. The ν parameter is a value between 0 and 1. It was set to 0.5.
- Normalization – Large margin classifiers are known to be sensitive to the way features are scaled. Therefore it is essential to normalize either the data or the kernel itself. This observation carries over to kernel based classifiers that use non-linear kernel functions: The accuracy of an SVM can severely degrade if the data is not normalized (Ben-Hur and Weston, 2010). Normalization of parameters was employed.
- Kernel – The kernel employed was the RBF kernel. It offers many advantages (Hsu, Chang, and Lin, 2003):
 - it nonlinearly maps samples into a higher dimensional space, that is, it can handle the case when the relation between class labels and attributes is nonlinear, contrary to the linear kernel which cannot,

- the linear kernel is a special case of RBF since the linear kernel with a penalty parameter C has the same performance as the RBF kernel with some combinations of parameters cost and gamma (C, γ),
- the sigmoid kernel behaves like RBF for certain parameters,
- the number of hyper parameters which influences the complexity of model selection is less when compared to the polynomial kernel,
- the RBF kernel has fewer numerical difficulties

The parameters used for the RBF kernel were selected using the grid search algorithm. The grid search algorithm consists of training SVMs with all the desired RBF combinations of cost (C) and gamma (γ) parameters and screening them according to the training accuracy. Hsu, Chang, and Lin (2003) recommend using various pairs of (C, γ), and select the one with the best cross-validation accuracy. The values used were those recommended by Hsu, Chang, and Lin (2003): $C = 2^{-5}; 2^{-3}, \dots, 2^{15}$ and $\gamma = 2^{-15}, 2^{-13}, \dots, 2^3$.

The resulting SVMs were used during the verification mode. To estimate FRR, the resulting SVMs were verified using ten-fold cross validation against the data employed to create the models. In ten-fold cross validation, the dataset D is randomly split into ten mutually exclusive subsets (the folds) D_1, D_2, \dots, D_{10} of approximately equal size. The inducer is trained and tested k times; each time $t \in \{1, 2, \dots, 10\}$, it is trained on $D \setminus D_t$ and tested on D_t . The cross validation estimate of accuracy is the overall number of correct classifications divided by the number of instances in the dataset. The advantage of this method is that all the examples in the dataset are eventually used in

testing (Kohavi, 1995). The best model for each user event was selected based on the accuracy obtained.

The estimation of FAR was done building a data set with the data from all participants in the study. The data set for each participant was built using all participants' data except the one being evaluated. For example, the data set used to calculate FAR for participant number one was the data obtained from participants number two to number 40, the data set used for participant number two was the data obtained from participant number one and participants number three to number 40, and so forth.

Testing

Recruitment

Testing was divided in two parts: pilot testing and the actual tests. Pilot testing helps refine research protocols, identifying questions that may have been initially omitted while potentially exposing flaws in the analysis plan (Lazar, Feng, and Hochheiser, 2010).

The success of a biometric authentication system in terms of usage depends on its success authenticating people and also on the perception users have about them as stated by El-Abed, Giot, Hemery, and Rosenberger (2012). Their study presents a comparison between a keystroke and a face recognition authentication system. In their study, respondents perceived a keystroke authentication system, with an EER around 18%, better in terms of performance than a face authentication one with an EER around 9%. Also, they felt more satisfied with the keystroke authentication system with results around 90% than with the face recognition system with a result around 76%.

For this work a 90% acceptance rate was used based on the assumption that a keystroke dynamic authentication system is similar, in terms of invasiveness, to the system presented in this work in terms of perceived invasiveness. Confidence level was given a 0.95 value. Confidence can be any value between 0 and 1. Usually, it is set equal to a number such as 0.90, 0.95, or 0.99 (Brase and Brase, 2007). Finally, the margin of error was set at 10%. This means that there is a 95% confidence that the acceptance rate will range from 80 to 100% for this biometric system.

The number of participants needed was calculated using the formula for calculating sample for proportion on a single population (Brase and Brase, 2007):

$$n \geq \left(\frac{z}{e}\right)^2 p(1-p) \quad (27)$$

where n equals the number of participants, e equals the margin of error (10%), p equals the population distribution (90%), and z equals the area of a standard normal distribution, which is obtained from the confidence level (95%).

Substituting in the formula gives:

$$n \geq \left(\frac{1.96}{0.01}\right)^2 0.9(1 - 0.9) = 34.57 \approx 35$$

According to the formula, the actual test required a minimum of 35 participants. This calculation agrees with a statement by Lazar, Feng, and Hochheiser (2010). They stated that, for an HCI experiment, results from studies with 20 or more participants are more convincing and that smaller studies may miss potentially interesting results. Also, the value is similar to the number of participants used by Sulong, Wahyudi, and Siddiqi (2009) in their biometric authentication study which was 30. Other studies, like the one

by Ahmed and Traore (2007) using mouse dynamics, also have employed 20 or more participants.

This test includes the data obtained from 40 participants divided between three participants in the pilot tests and 37 participants in the actual tests. Participants were selected among University of Puerto Rico – Mayagüez students and staff. These participants were readily available since University of Puerto Rico – Mayagüez is the author's workplace. Recruitment was done by posting messages on bulletin boards across the campus (Appendix C). Recruitment of participants was simple since there was no need of any special training or abilities. Also, there were no restrictions about education, gender, age, or beliefs. The only requirement were that participants needed to be familiar with touchscreen devices and were not color blind since some questions of the biometric test made reference to the colors in the images.

Tests

The tests began on October 30, 2013 and ended on December 12, 2013. They began once the dissertation proposal was approved by the dissertation committee and the proposed methodology for testing with human subjects was approved by Nova Southeastern University Institutional Review Board. Also, approval from University of Puerto Rico – Mayagüez Institutional Review Board was needed since participants were selected from there (Appendix D). During the tests, each participant received a consent form that explained, among other things, the purpose of the study and how their personal data was going be protected (Appendix E). Participants read and signed it before taking the test. The consent form was based on a template provided by Nova Southeastern University Institutional Review Board (Nova Southeastern University, 2011).

Each test took approximately 30 minutes to complete. It consisted of three paper based parts: a pre-test, a biometric test, and a post-test. The pre-test consisted of several demographic questions to assess the level of expertise of participants in using touchscreen mobile devices (Appendix F). El-Abed, Giot, Hemery, and Rosenberger (2010) used similar type of questions in their study about user acceptance of biometric systems and assess the importance of knowing the type of participant in a study.

After the participant answered the demographic questions, the biometric part of the test began. It consisted of asking participants to describe some images (Appendix G). Agriculture related images were selected because almost anyone can relate to them and there is almost no possibility that the images will offend someone. Participants had to browse through different images to answer questions about them. To make it easier for participants, images were labeled and ordered alphabetically (Appendix H). The questions were relatively simple but they forced participants to use the scroll utility which, in turn, allowed the proposed biometrics to be captured. This part of the test was subdivided in two parts: the first one captured the biometric traits while participants were doing horizontal scrolling and the second part captured the traits while the participants were doing vertical scrolling. Each one of these parts consisted of 16 questions. The assumption made was that for each image an average of three strokes were going to be made, that would give approximately 50 strokes of data for each part.

While doing the biometric part of the test, participants did not know that the proposed metrics were been captured. The rationale behind this was that it is possible that knowing the exact purpose of the test would affect the results. Although concealing the true nature of a study can present some concerns regarding the validity of informed

consent, this practice is often necessary, particularly in situations where full disclosure might compromise the realism of the study (Lazar, Feng, and Hochheiser, 2010).

Athanassoulis and Wilson (2009) argue that there are certain kinds of research that cannot be done without deception: in some instances providing certain kinds of information about the study will invalidate the results, as it may lead to the participants modifying their behavior in light of this knowledge. They state that the operative moral principle should not be whether or not a given piece of research involves deception, but whether it involves deception that is obviously wrong. At the end of the biometric part of the test, each participant received a description of the goals of the study and the biometric traits that were captured (Appendix I). The idea behind this was to inform participants of what biometric traits were captured which was not explained at the beginning of the test. This way they were better equipped to answer the questions about the biometric system proposed.

The post-test asked participants some questions about their experience during the test and it was divided into two parts (Appendix J, Appendix K). Paper questionnaires were given to participants, which helped analyze perceived ease of use, perceived usefulness, and attitude toward using the proposed biometric system. The questions in the first part were based on the work of Furnell, Dowland, Illingworth, and Reynolds (2000) and also the UKPS biometric enrollment trial (2005). The questions in the second part were based on the Technology Acceptance Model for Biometrics Questionnaire by James, et al. (2008), which derives from the Technology Acceptance Model (TAM) by Davis (1993).

Participants reported their level of agreement with some issues related to the proposed biometric approach using Likert Scales for some questions in the first part and for all questions in the second part. Likert Scales is one of the classical methods for efficiently capturing participants' perceptions (Tullis and Albert, 2008). A five point Likert scale was used to report data (Table 6):

Table 6

Likert Scale Implemented in this Study

Answer	Points
Strongly agree	1
Agree	2
Nor agree neither disagree	3
Disagree	4
Strongly disagree	5

Neither part of this test introduced risks to participants beyond those inherent to using mobile devices. After the tests were finished, data was analyzed, and the results were discussed. The approvals were secured and granted by Nova Southeastern University Institutional Review Board and the University of Puerto Rico – Mayagüez Institutional Review Board.

Privacy

Photographs, videos, or audio recording were not taken during the tests. Also, the identity of participants was not disclosed in any form. To achieve this, the name of participants and their demographic data was kept in separate files from the test results. Moreover, the personal data of participants was kept locked in a different place from the test results. Only the personnel listed on the IRB application form had access to the data. The data will be retained for 36 months after the study is completed, afterwards it will be destroyed. This procedure was explained in the consent form given to participants (Appendix E).

Summary

A quantitative experimental research was employed to test the effectiveness of a multimodal authentication biometric approach. An application was built to capture the proposed biometric traits while users interacted with a touchscreen device. The application captured: area in contact with the touchscreen at different points, length of the major axis of an ellipse that describes the touch area at the point of contact, and length of the minor axis of an ellipse that describes the touch area at the point of contact. Also, it captured the (x, y) coordinates at the point of contact and time of contact, which was used to calculate: distance travelled, speed, and angle created by the movement.

SVMs were used for authentication purposes. They were implemented using One-Class Classification. The SVM analysis was made using the Waikato Environment for Knowledge Analysis (WEKA), which is a collection of machine learning algorithms

and data preprocessing tools developed by the University of Waikato in New Zealand (Han, Kamber, and Pei, 2006).

Testing involved 40 participants. The tests consisted of asking users to describe some images. Participants did not know that their scrolling behavior was being monitored. Different metrics were used to verify the proposed approach: FAR, FRR, and EER. Additionally, an evaluation of acceptability and user satisfaction was performed. Paper questionnaires were given to participants, which helped analyze perceived ease of use, perceived usefulness, and attitude toward using the system.

Chapter 4

Results

This study was divided in two parts, the first one consisted of the construction of an application to capture the biometric traits employed for user authentication (Appendix A). An Android application was built and installed in a Lenovo Thinkpad Tablet running Android OS 4.0.3. The application presented a series of images to participants and captured their finger biometric traits while they scrolled through some images (Appendix H). Also, the application helped participants familiarize with how a biometric authentication system might look and feel. The second part consisted of testing the effectiveness of the approach in authenticating users and determining user acceptance of this kind of authentication approach.

The next section presents a description of the sample population of the tests. It is followed by the results obtained from the biometric tests. Afterwards, the results obtained from the user's perception questionnaire and the results obtained from the Technology Acceptance Model (TAM) for biometrics questionnaire are presented. The chapter ends with a brief summary of the results obtained.

About the Sample

How the data was collected

The testing process with people began on October 30th, 2013 and ended on December 12th, 2013 after the Institutional Review Boards (IRBs) of UPR-Mayagüez and Nova Southeastern University had approved the testing plan for this work (Appendix D). The data presented in this study was collected from a total of 40 participants. The testing process was divided between pilot and the actual testing.

The pilot testing consisted of three participants. Once the pilot testing ended, the methodology employed was analyzed. It was decided to include the results obtained from the pilot testing in the final analysis since there were no significant changes made to the testing procedures.

During the actual tests, 37 participants were employed. The plan for the actual tests was to use at least 35 participants, which is the minimum number of participants required according to the formula for calculating sample for proportion on a single population (Brase and Brase, 2007). This formula is commonly used to select a subset of individuals from within a population to estimate characteristics of the whole population. The values obtained from the formula implied that a sample of 35 participants was needed to obtain results where 90% of the population would accept this type of authentication method with a 10% margin of error and a 95% confidence level. During the recruitment process, it was assumed that some people would not show up for testing after being scheduled. At the end, as previously stated, 40 participants took part in the study which is more than the minimum required.

Demographics

This study did not require participants to have any special training or abilities. There were no restrictions about education, gender, age, or beliefs. Participants only needed to be familiar with touchscreen devices. The only requirement was that participants could not be color blind because some of the questions in the biometric test made reference to colors in the images.

Participants received a demographics questionnaire (Appendix F) before beginning the biometric portion of the test. This helped to assess the type of participant in this study. Among other things, participants were mostly engineering students from UPR-Mayagüez Campus. The vast majority of them, an 85% (n=35), were from electrical and computer engineering majors (Table 7). Probably the fact that a lot of flyers were placed on the electrical and computer engineering building bulletin boards or an interest by the students in the subject matter caused this type of response, although this does not represent any problem or concern. Also, the majority of participants were males representing 77.5% (n=31) of the population which can be attributed to the fact that electrical and computer engineering majors have been historically dominated by men (Yorden, 2013). Participant's age ranged from 18 to 35 years, an average of 19.95, which can be explained by the fact that the majority of them were second and third year students (Table 8).

Table 7

Participants per Program and Year of Studies

Year	BA	CpE	EE	Blank	Total
First	0	0	1	0	1
Second	0	11	9	4	24
Third	1	3	6	0	10
Fourth	0	2	0	0	2
Fifth	0	2	0	0	2
Sixth or more	0	0	1	0	1
Total	1	18	17	4	40

Note. BA = Business Administration, CpE = Computer Engineering, EE = Electrical Engineering.

Table 8

Participants per Age and Gender

Gender	Number of Participants	Average Age	Standard Deviation
Female	9	19.44	1.50
Male	31	20.10	2.98
Total	40	19.95	2.76

There were some interesting facts about mobile devices use among participants. One of them is the intense use of touchscreen devices among participants. They reported an average daily use of 7.36 hours which might be explained by the fact that the majority of them were students from technology related majors. The most used touchscreen device was the smartphone which participants reported employed frequently for regular telephony, text messaging, and Internet navigation (Table 9, Table 10). Finally, participants reported spending their time on the Internet mostly sending and receiving emails, searching for information, and doing social networking (Table 11).

Table 9

Types of Touchscreen Devices Used by Participants

Type	Number	Percentage
Smartphone	37	92.5%
Tablet	26	65.0%
Other	6	12.5%

Note. The 40 participants could select more than one option.

Table 10

Types of Communication Services used by Participants

Type	Number	Percentage
Regular Telephony	33	82.5%
Text messaging	37	92.5%
Internet	40	100%
Other	4	10%

Note. The 40 participants could select more than one option.

Table 11

Internet usage by Participants

Type	Number	Percentage
read/send email	40	100.0%
search for information	38	95.0%
shopping	14	35.0%
listen to music	31	77.5%
play games	29	72.5%
social networking (Facebook, Twitter, etc.)	38	95.0%
other	5	12.5%

Note. The 40 participants could select more than one option

Biometric Test

As already discussed, the biometric portion of the test consisted of participants browsing through different images and answering questions about them. It was divided

in two parts: one designed to capture the biometric traits while participants were doing horizontal scrolling and the other one designed to capture the biometric traits while participants were doing vertical scrolling. The biometric traits were captured using an Android application built for that purpose (Figure 9) (Appendix A). A total of 80 data sets were captured during the tests (two for each participant). A data set was comprised of the data collected from the finger strokes.

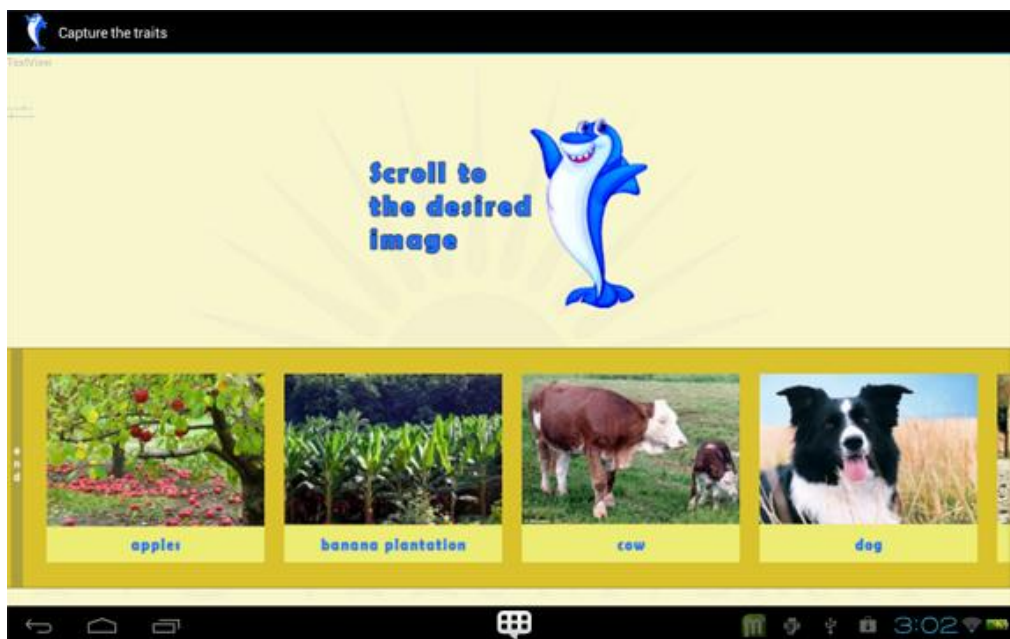


Figure 9. Android application used for capturing biometric traits.

Participants spent an average of 15.82 minutes browsing through the different images and answering questions about them (Appendix L). During that period an average of 88.45 strokes per participant was captured during horizontal scrolling and an average of 151.35 strokes during the vertical scrolling. The standard deviations were 43.11 and 85.78 respectively (Table L2). The goal was to capture at least 50 strokes for each type of scrolling for each participant. This goal was based on the approach followed

by Gamboa and Fred (2003) and also the approach by Schulz (2006). This goal was not reached for 10 of the 80 sets (Appendix L).

Each stroke was divided into three events: down, move, and up. This means that for each participant, six types of events were registered and six files were created. Those strokes contained the different traits that were used directly to authenticate users using the SVM models. This work implemented One-Class SVM and emphasized on the verification of users. The best model for each user action event was selected based on the accuracy in correctly verifying the identity of people.

Thirty four different combinations of biometric traits were tested for each one of the six types of movement captured. This was done for each participant (Appendix M). Tables 12 through Table 17 show the results for the best four biometric traits of the 34 combinations tested in terms of the authentication accuracy. Those results were obtained for each type of motion event during horizontal and vertical scrolling.

The data shows that the best results in terms of authentication accuracy were obtained during the down motion event for both types of scrolling. Table 12 and Table 13 show accuracy results around 80% for both scrolling types. The up motion event, for both horizontal and vertical scrolling, follows in terms of accuracy. Table 14 and Table 15 show accuracy results around 70% for both types of scrolling. Also, the results in Table 16 and Table 17 show that the move motion-event during horizontal or vertical scrolling was accurate around 50% of the time, which is similar to what can be obtained with a coin toss.

Table 12

Best Biometric Traits in Terms of Authentication Accuracy for the Down Motion Event during Horizontal Scrolling

Biometric Traits	Accuracy
touchmajor	86.75%
size (area), touchmajor	84.99%
touchminor	84.99%
size (area)	84.96%

Table 13

Best Biometric Traits in Terms of Authentication Accuracy for the Down Motion Event during Vertical Scrolling

Biometric Traits	Accuracy
size (area)	80.05%
touchmajor	79.50%
size (area), touchmajor	79.10%
touchmajor, touchminor	76.74%

Table 14

Best Biometric Traits in Terms of Authentication Accuracy for the Up Motion Event during Horizontal Scrolling

Biometric Traits	Accuracy
angle	72.13%
distance	71.56%
touchminor	71.06%
speed	70.21%

Table 15

Best Biometric Traits in Terms of Authentication Accuracy for the Up Motion Event during Vertical Scrolling

Biometric Traits	Accuracy
touchmajor	71.58%
size (area)	70.09%
size (area), touchmajor	68.87%
angle	68.58%

Table 16

Best Biometric Traits in Terms of Authentication Accuracy for the Move Motion Event during Horizontal Scrolling

Biometric Traits	Accuracy
touchmajor	57.29%
touchminor	56.53%
size (area)	52.66%
distance	51.23%

Table 17

Best Biometric Traits in Terms of Authentication Accuracy for the Move Motion Event during Vertical Scrolling

Biometric Traits	Accuracy
touchminor	56.35%
touchmajor	52.65%
size (area)	52.16%
distance	51.48%

The results show that biometric traits like touchmajor, touchminor, and size are effective in authenticating people at the beginning of a finger stroke (Table 12, Table 13). Additionally, those traits are effective at the end of a stroke although the angle and distance traits proved to be slightly better at the end of the horizontal stroke (Table 14, Table 15). Furthermore, the results show that the distance parameter is somewhat effective in authenticating people after a finger stroke has initiated and the angle parameter is effective at the end of a stroke (Table 16, Table 17). The speed parameter, which belongs to the same type of parameter as angle and speed, shows its best accuracy only at the end of the horizontal scroll movement (Table 14).

A closer look at the effectiveness of the biometric traits authenticating people individually shows that those traits were effective in authenticating some of the 40

participants more than 90% of the time (Table 18). Also, the majority of those traits were capable of authenticating the participants more than 66% of the time (Table 18).

Table 18

Number of Participants Correctly Authenticated for Different Levels of Accuracy

Biometric Traits	Accuracy	Event				Total
		Down		Up		
		Horizontal	Vertical	Horizontal	Vertical	
Size (area)	90%	10	12	1	6	29
	80%	17	11	10	5	43
	75%	11	5	5	4	25
	66%	2	9	7	8	26
Touchmajor	90%	18	15	1	5	39
	80%	13	14	8	7	42
	75%	6	5	7	4	22
	66%	1	3	7	7	18
Touchminor	90%	8	9	1	2	20
	80%	13	17	10	8	48
	75%	9	3	5	2	19
	66%	2	4	9	8	23
Distance	90%	0	0	3	3	6
	80%	0	0	12	8	20
	75%	0	0	3	2	5
	66%	0	0	9	8	17
Speed	90%	0	0	4	1	5
	80%	0	0	9	10	19
	75%	0	0	3	3	6
	66%	0	0	7	5	12
Angle	90%	0	0	4	3	7
	80%	0	0	9	6	15
	75%	0	0	3	5	8
	66%	0	0	10	6	16
Size (area) and Touchmajor	90%	8	9	0	2	19
	80%	19	10	9	8	46
	75%	8	10	4	4	26
	66%	5	7	7	8	27
Touchmajor and Touchminor	90%	5	7	0	2	14
	80%	15	10	7	6	38
	75%	13	7	8	3	31
	66%	4	12	7	9	32

Note: For each event n = 40.

The best results, in terms of verifying the identity of users, were obtained during the down motion event and the up motion event. The results show that the data obtained from the move action events was not effective in verifying the identity of users.

The computation of the FRR was based on the previous results. Since the One-Class SVM application divided the results between correctly classified and unclassified. The cases labeled as not classified by the One-Class SVM were defined as FRR cases. The FRR results were calculated taking the best FRR results for each participant and averaging them. The biometric data used to determine FAR values was the biometric data obtained from the remaining participants that had not been evaluated at a particular moment. For example, if participant number one was being evaluated, the biometric data from participants number two to number forty was used to calculate FAR. The FAR value was calculated using the parameters that gave the best FRR results for each participant.

The use of the application determines the FAR and FRR values being used. For example, it might be desirable to have a low FAR to access high security areas and a low FRR to keep customers happy for access in places like an internet cafe (Bours and Barghouthi, 2009). The EER value represents the point where both FAR and FRR values are equal.

The best FRR results were obtained from the down motion event (Table 19, Table 20). The FRR results for the down horizontal motion event were around 15% and for the down vertical motion event they were around 20%. In both cases the results for FAR were around 60%. For the up motion event, the FRR results were around 30% and the FAR results were in the range of 47% to 60% (Table 21, Table 22).

Table 19

Top Four Biometric Traits in Terms of FRR for the Down Motion Event during Horizontal Scrolling

Biometric Traits	FRR		FAR	
	Average	95% CI	Average	95% CI
touchmajor	13.25%	[6.88%, 21.96%]	67.59%	[59.03%, 76.14%]
size (area), touchmajor	15.01%	[12.92%, 17.78%]	60.62%	[54.40%, 66.84%]
touchminor	15.01%	[10.91%, 32.72%]	54.47%	[43.11%, 65.83%]
size (area)	15.34%	[13.09%, 17.61%]	55.76%	[49.19%, 62.33%]

Note. CI = Confidence Interval.

Table 20

Top Four Biometric Traits in Terms of FRR for the Down Motion Event during Vertical Scrolling

Biometric Traits	FRR		FAR	
	Average	95% CI	Average	95% CI
size (area)	19.95%	[15.34%, 28.20%]	58.52%	[51.23%, 65.81%]
touchmajor	20.50%	[12.98%, 28.03%]	59.50%	[50.86%, 68.13%]
size (area), touchmajor	20.90%	[16.42%, 28.96%]	58.24%	[50.61%, 65.87%]
touchmajor, touchminor	24.77%	[18.68%, 30.86%]	58.08%	[50.43%, 65.72%]

Note. CI = Confidence Interval.

Table 21

Top Four Biometric Traits in Terms of FRR for the Up Motion Event during Horizontal Scrolling

Biometric Traits	FRR		FAR	
	Average	95% CI	Average	95% CI
angle	27.87%	[23.65%, 32.28%]	50.69%	[41.21%, 60.16%]
distance	28.42%	[23.90%, 32.94%]	48.87%	[39.46%, 58.29%]
touchminor	28.94%	[25.22%, 32.66%]	58.91%	[51.21%, 66.61%]
speed	29.79%	[25.19%, 34.57%]	57.16%	[47.77%, 66.54%]

Note. CI = Confidence Interval.

Table 22

Top Four Biometric Traits in Terms of FRR for the Up Motion Event during Vertical Scrolling

Biometric Traits	FRR		FAR	
	Average	95% CI	Average	95% CI
touchmajor	28.42%	[24.10%, 32.74%]	60.07%	[52.94%,67.19%]
size (area)	29.91%	[25.42%, 34.36%]	57.42%	[49.28%,65.57%]
size (area), touchmajor	31.13%	[26.78%, 35.45%]	54.64%	[47.43%,61.84%]
angle	31.42%	[27.08%, 35.58%]	47.17%	[38.07%,56.26%]

Note. CI = Confidence Interval.

The top biometric traits combinations in terms of FRR were also evaluated to find best FAR results that could be obtained with them. A similar procedure to the one employed with FFR was implemented. The best FAR results obtained for each instance were averaged. The Table 23 and Table 24 show that the best FAR values were around 10% for the down motion event but the FRR values obtained were around 79%. Table 25 and Table 26 show FAR values from 20% to 30% during the up motion event and FRR values around 50%.

Table 23

Best FAR Results Obtained for the Top Four Biometric Traits (in Terms of FRR) for the Down Motion Event during Horizontal Scrolling

Biometric Traits	FAR		FRR	
	Average	95% CI	Average	95% CI
touchmajor	8.22%	[5.73%, 10.71%]	78.08%	[71.02%, 85.13%]
size (area), touchmajor	9.91%	[5.73%, 14.09%]	69.85%	[63.46%, 76.24%]
touchminor	4.18%	[2.21%, 6.15%]	78.69%	[71.05%, 86.34%]
size (area)	10.19%	[6.52%, 13.87%]	66.08%	[58.53%, 73.63%]

Note. CI = Confidence Interval.

Table 24

Best FAR Results Obtained for the Top Four Biometric Traits (in Terms of FRR) for the Down Motion Event during Vertical Scrolling

Biometric Traits	FAR		FRR	
	Average	95% CI	Average	95% CI
size (area)	13.03%	[9.06%, 17.01%]	68.40%	[61.88%, 74.92%]
touchmajor	8.87%	[5.84%, 11.90%]	78.07%	[71.57%, 84.56%]
size (area), touchmajor	12.65%	[8.92%, 16.38%]	69.94%	[63.83%, 76.05%]
touchmajor, touchminor	10.84%	[7.42%, 14.26%]	68.17%	[60.97%, 75.37%]

Note. CI = Confidence Interval.

Table 25

Best FAR Results Obtained for the Top Four Biometric Traits (in Terms of FRR) for the Up Motion Event during Horizontal

Biometric Traits	FAR		FRR	
	Average	95% CI	Average	95% CI
angle	20.09%	[15.70%, 24.48%]	56.18%	[52.57%, 59.59]
distance	22.80%	[18.44%, 27.16%]	53.50%	[49.56%, 57.44]
touchminor	23.63%	[20.32%, 26.95%]	53.86%	[50.79%, 56.94]
speed	25.81%	[20.63%, 30.99%]	55.40%	[51.41%, 59.38]

Note. CI = Confidence Interval.

Table 26

Best FAR Results Obtained for the Top Four Biometric Traits (in Terms of FRR) for the Up Motion Event during Vertical Scrolling

Biometric Traits	FAR		FRR	
	Average	95% CI	Average	95% CI
touchmajor	24.65%	[20.67%, 28.82%]	59.47%	[56.12%, 62.82]
size (area)	27.45%	[23.26%, 31.65%]	56.69%	[52.99%, 60.39]
size (area), touchmajor	28.26%	[24.89%, 31.63%]	52.12%	[48.71%, 55.53]
angle	19.86%	[15.46%, 24.25%]	56.57%	[49.47%, 63.68]

Note. CI = Confidence Interval.

These results show the importance of obtaining the EER values. EER values for the Best Configurations in Terms of FRR Results were around 40% (Table 27 - Table

30). The best EER result obtained was 34.27% and it was obtained using the size biometric trait during down horizontal motion event. The worst EER obtained was 48.20% using the touchminor biometric trait during the down horizontal motion event.

The EER values are higher than other behavioral biometric approaches like mouse dynamics that reported values around 24% and keystroke dynamics authentication in mobile phones with 15% (Table 2). Obviously, the values are much higher than other approaches like the use of fingerprints that traditionally have been associated to crime scenes.

Table 27

Best EER Results Obtained for the Top Four Biometric Traits (in Terms of FRR) for the Down Motion Event during Horizontal Scrolling

Biometric Traits	EER	
	Average	95% CI
touchmajor	43.23%	[38.25%, 48.21]
size (area), touchmajor	35.21%	[32.54%, 37.87]
touchminor	48.20%	[39.54%, 56.86]
size (area)	34.27%	[31.72%, 36.83]

Note. CI = Confidence Interval.

Table 28

Best EER Results Obtained for the Top Four Biometric Traits (in Terms of FRR) for the Down Motion Event during Vertical Scrolling

Biometric Traits	EER	
	Average	95% CI
size (area)	40.82%	[35.64%, 45.99%]
touchmajor	46.08%	[40.41%, 51.75%]
size (area), touchmajor	40.86%	[35.67%, 46.06%]
touchmajor, touchminor	40.29%	[35.17%, 45.40%]

Note. CI = Confidence Interval.

Table 29

Best EER Results Obtained for the Top Four Biometric Traits (in Terms of FRR) for the Up Motion Event during Horizontal Scrolling

Biometric Traits	EER	
	Average	95% CI
angle	40.33%	[37.66%, 43.00%]
distance	40.11%	[36.85%, 43.37%]
touchminor	40.66%	[38.27%, 43.06%]
speed	43.22%	[40.31%, 46.13%]

Note. CI = Confidence Interval.

Table 30

Best EER Results Obtained for the Top Four Biometric Traits (in Terms of FRR) for the Up Motion Event during Vertical Scrolling

Biometric Traits	EER	
	Average	95% CI
touchmajor	44.31%	[41.95%, 46.68%]
size (area)	43.83%	[41.45%, 46.21%]
size (area), touchmajor	43.87%	[41.65%, 46.10%]
angle	39.63%	[36.37%, 42.88%]

Note. CI = Confidence Interval.

One important advantage that the results show is that individuals can be authenticated at different event points. This aspect can make the authentication process more dynamic and fast. People can be authenticated after the down motion and after the up motion since both action events showed satisfactory authentication values.

Events that affected the biometric tests results

Two independent events occurred during the biometric tests that could affect the results. First, in 10 instances the minimum number of 50 strokes per participant was not reached (Table 31, Appendix L). As mentioned earlier, this goal was based on the approach followed by Gamboa and Fred (2003) and also the approach by Schulz (2006).

Table 31

Participants with Less than 50 Strokes Captured During the Biometric Test

Participant	Horizontal	Vertical
6	45	45
15	45	88
21	49	151
28	46	70
29	49	76
35	49	71
37	25	44
38	37	82

Second, some people changed their behavior while scrolling during the biometric tests (Appendix N). Specifically, some participants changed hands and fingers used during their interaction with the Android Application (Table 32).

Table 32

Participants that Changed Hands or Fingers while Scrolling During the Biometric Tests

Scrolling Type	Participants	Total
Horizontal	15, 16, 21, 23, 24, 29, 30, 31, 32, 34, 35, 37, 40	13
Vertical	20, 21, 25, 26, 29, 30, 32, 34, 35, 36, 40	11

The FRR values for those two cases (Appendix O, Appendix P) were calculated. It was found that changes in hand and finger used have a negative effect on the FRR results. That effect can be seen in the down motion event results (Table 33). The up motion event demonstrated being less susceptible to those changes. Finally, the fact that the minimum number of strokes was not reached showed mixed results in terms of FRR. The down vertical motion event results were better in those participants with less than 50 strokes recorded but the down horizontal motion event and up vertical motion event results worsen.

Table 33

Average FRR for the Top Biometric Traits for All Participants, Participants with Less than 50 Strokes Registered, and Participants that Changed their Behavior during the Biometric Tests

Event	Participants		
	All	Less than 50 Strokes	Changes in Behavior
Down Horizontal Motion	14.58%	25.43%	22.68%
Down Vertical Motion	21.15%	10.90%	26.90%
Up Horizontal Motion	28.76%	28.32%	26.30%
Up Vertical Motion	30.22%	42.40%	26.84%

Post-Test Surveys

The success of a biometric authentication system in terms of usage depends on its success authenticating people and also on the perception users have about them (El-Abed, et al., 2012). Two survey questionnaires were given to participants to investigate their willingness to adopt this type of authentication approach. The first one was a user's disposition questionnaire based on the work by Furnell, et al. (2000) and the UKPS biometric enrollment trial (2005). The second one was the TAM for biometrics questionnaire by James et al. (2008). They developed a model of technology acceptance for biometric devices based on the TAM developed by Fred Davis (1993).

User's disposition questionnaire

Several questions were asked to assess the disposition of people to accept this kind of technology as a mean of authentication (Appendix J). A five point Likert scale was employed for the first three question of the questionnaire, the scale used assigned a value of 1 to the strongly agree option and a value of 5 to the strongly disagree option

(Table 6). The questions used in the questionnaire were based on the work by Furnell, Dowland, Illingworth, and Reynolds (2000) and also the UKPS biometric enrollment trial (2005).

The results from the questionnaire (Appendix Q) show that participants are willing to accept biometrics as a way of authentication with a Likert Scale average score of 1.78 (Table 34). Also, the results show that participants would feel comfortable with a system like the one tested, with an average response score of 2.05. One important finding is the need of participants to know if they are being monitored, with an average score of 1.73.

Table 34

General Perception about Biometric Devices

Statement	Average	SD	95% CI
I would be in favor of biometrics being adopted as a mean of verifying identity	1.78	0.58	[1.60, 1.95]
I feel comfortable with a system, like the one tested, that continuously captures biometric data	2.05	0.78	[1.81, 2.29]
I should be aware if biometric data is being captured while using a device.	1.73	0.88	[1.45, 2.00]

Note. SD = Standard Deviation, CI = Confidence Interval. Range: 1-strongly agree, 2-agree, 3-nor agree neither disagree, 4-disagree, and 5- strongly disagree. N = 40.

Another interesting finding is that the majority of participants (57%) are willing to spend from 3 to 10 minutes creating a biometric profile (Table 35). Also, it is worth noticing that 75% of participants are willing to tolerate false rejection from a monitoring system if it is just less than 10% of the time (Table 36). This shows that users required precise systems but do not want to spend time creating biometric profiles.

Table 35

Reasonable Amount of Time Needed to Create a Biometric Profile

Option	Number	Percentage
no time	1	2.5
less than 1 minute	3	7.5
1 to 3 minutes	4	10.0
3 to 5 minutes	12	30.0
up to 10 minutes	11	27.5
up to 30 minutes	3	7.5
up to 60 minutes	2	5.0
beyond 60 minutes	4	10.0

Table 36

Willingness to Tolerate Errors

Option	Number	Percentage
I don't consider it a problem	2	5.0
less than 20% of the time	4	10.0
less than 15% of the time	4	10.0
less than 10% of the time	9	22.5
less than 5% of the time	15	37.5
0 % (Never)	6	15.0

In terms of sharing their biometric data, participants are almost divided in half between those who are willing to share their biometric information with other people and those who doesn't, 55% to 45% (Table 37). Those who are willing to share their biometric profile would do it mainly with their bank, the government, and their telephone/internet provider (Table 38).

Table 37

Who do you think should have access to your biometric pattern?

Time	Number	Percentage
only yourself	22	55%
yourself and	18	45%

Table 38

Beside yourself, who do you think should have access to your biometric pattern?

Options	Number
your telephone/Internet provider	5
your employer/school	4
your bank office	6
the government (county, state, federal)	5
whoever you buy something from	1
other	3

Note. Participants who answered yourself and ... to the question could select more than one option.

TAM for biometrics questionnaire

The analysis of TAM for this study was done using as reference the work by James, et al. (2008) who developed a model of technology acceptance for biometric devices. They state that the need for privacy and security, along with the perceived invasiveness of the device and the original TAM constructs of perceived usefulness and ease of use, will impact the decision to use biometric devices. They use a five point Likert scale for their questionnaire, ranging from one point given to strongly agree answers to five points given to strongly disagree (Table 6).

The results from the TAM for biometrics survey (Appendix R) show that participants are open to the possibility of using a biometric system like the one tested. The question related to their willingness to use a biometric system like the one presented in this study received an average Likert score of 2.00 (Table 39), which means that on average they agree with the statement. The disposition of participants to use this biometric approach is supported by their reported perceived ease of use of the proposed

biometric with a Likert score of 1.58 of and a perceived usefulness score of 1.70 both values between the strongly agree and agree answers to those questions.

Table 39

The Biometric Application

Statement	Mean	SD	95% CI
1. I think this biometric device is useful.	1.70	0.56	[1.53, 1.87]
2. I think this biometric device is easy to use.	1.58	0.59	[1.4, 1.76]
3. I think one of the reasons this device is useful is because of its ease of use.	1.83	0.81	[1.58, 2.08]
4. I think that this device would be physically invasive.	2.80	1.03	[2.45, 3.15]
5. I think I would use this device.	2.00	0.82	[1.75, 2.25]

Note. SD = Standard Deviation, CI = Confidence Interval. N = 40.

Also, the disposition of participants to use this biometric approach is supported by their reported need for privacy. Participants need for privacy is reflected by the results from Statements P1 – P9 from the TAM for Biometrics Questionnaire (Appendix K). The average obtained for this group of statements was 1.47 (Table 40). Also, the results show participants need for security with a Likert score average of 1.21 in questions pertaining security issues (Table 41).

Table 40

Results for TAM for Biometrics Privacy Related Questions

Statement	Mean	SD	95% CI
P1. I feel my privacy is very important to me.	1.15	0.36	[1.04, 1.26]
P2. I feel that my control over my personal information is very important to me.	1.10	0.30	[1.01, 1.19]
P3. I feel that it is important not to release sensitive information to any entity.	1.38	0.63	[1.19, 1.57]
P4. I feel it is important to avoid having personal information released that I think could be financially damaging.	1.23	0.53	[1.07, 1.39]
P5. I feel it is important to avoid having personal information released that I think could be socially damaging to me.	1.43	0.64	[1.23, 1.63]
P6. I feel it is important to avoid having personal information about me released that may go against social morals and attitudes.	1.63	0.87	[1.36, 1.90]
P7. I feel that the release of personal information to individuals with whom I have a high comfort level is unacceptable.	2.13	0.99	[1.82, 2.44]
P8. I feel that the release of personal information to entities where I feel as though I am anonymously providing the information is unacceptable.	1.67	0.93	[1.32, 2.02]
P9. I feel that the use of personal information that has been released by me but is used in a manner not intended by me is unacceptable.	1.43	0.87	[1.16, 1.70]
Average	1.47	0.72	[1.00,1.94]

Note. SD = Standard Deviation, CI = Confidence Interval. N = 40.

Table 41

Results for TAM for Biometrics Security Related Questions

Statement	Mean	SD	95% CI
S1. I feel that the safeguarding from potential external threats of my physical being is important to me.	1.38	0.54	[1.21, 1.55]
S2. I feel that my personal security at my home or in my vehicle is important to me.	1.10	0.30	[1.01, 1.19]
S3. I feel that my personal security at my place of work or other work related places is important to me.	1.10	0.30	[1.01, 1.19]
S4. My security at places of public access, such as a mall or airport, or special public events, such as the Olympics or the Super Bowl, is important to me.	1.18	0.38	[1.06, 1.30]
S5. I feel that the security of my tangible assets (such as my home, vehicle, etc.) is important to me.	1.30	0.52	[1.14, 1.46]
S6. I feel that keeping my personal possessions, such as jewelry, money, electronics, etc. safe is important to me.	1.60	0.96	[1.30, 1.90]
S7. I feel that the safekeeping of my informational assets contained in digital or paper format is important to me (such as financial records, medical records, etc.).	1.00	0.00	[1.00, 1.00]
S8. I feel that the security of my personal information, such as my PC files or personal records (financial, medical, etc.) is important to me.	1.10	0.30	[1.01, 1.19]
S9. I feel that the safekeeping of information I have provided to a corporation or other entity is important to me.	1.15	0.42	[1.02, 1.28]
Average	1.21	0.48	[0.90,1.52]

Note. SD = Standard Deviation, CI = Confidence Interval. N = 40.

An issue that appears to be inconclusive is the perception of physical invasiveness. The question related to that issue obtained an average Likert score of 2.80 with a standard deviation of 1.03 (Table 39). That is almost in the middle of the Likert scale employed, which means neither agree nor disagree.

Summary

The testing process for this study lasted more than a month and each participant spent around half hour doing the test. Participants were mostly second and third year engineering students from the University of Puerto Rico-Mayagüez Campus. One important characteristic of the participants is their reported intense usage of touchscreen devices and also internet applications.

Effectiveness of the biometric approach

The approach presented in this study proved to be effective in authenticating participants. A look at the effectiveness of the biometric traits authenticating people individually shows that the traits used were effective authenticating some participants more than 90% of the time. Also, it is important to mention that the majority of the traits were capable of authenticating the participants more than 66% of the time (Table 18).

The effectiveness of the approach was tested calculating FAR, FRR, and EER values. These metrics are usually used when evaluating biometric approaches (Sulong, Wahyudi, and Siddiqi, 2009). For the most part, the use of the application determines the ideal FAR and FRR values being used in an application. For example, it might be desirable to have a low FAR to access high security areas and a low FRR to keep customers happy for access in places like an internet cafe (Bours and Barghouthi, 2009). The EER value represents the point where both FAR and FRR values are equal.

The best results, in terms of verifying the identity of users, were obtained during the down motion event and the up motion event. The best EER result obtained was 34.27% and it was obtained using the size biometric trait during the down horizontal

motion event. For this study, EER average results were around 40% (Table 27 - Table 30).

The EER values obtained in this study are higher than the values reported for other behavioral biometric approaches. For example, mouse dynamics reported an EER value around 24% (Schulz, 2006) and a haptic system developed by Orozco et al. (2006) reported an EER of 22.3%. An advantage of the authentication approach presented is that individuals can be authenticated at different event points during a finger stroke over the touchscreen device. People can be authenticated after the down motion event and after the up motion event since both action events showed satisfactory authentication values. Both events can be considered independent events since the data obtained from the down event do not affect the data obtained from the up event. The results obtained can be lowered if the two points are combined. The probability multiplication rule for independent events says that the probability of two events occurring at the same time is the probability of one event occurring times the other event occurring (Brase and Brase, 2007). For example, the best result from the down horizontal event can be combined with the best one from the up horizontal event for better authentication results. The same concept can be applied to the vertical scrolling motion which means that lower results could be obtained.

Participants' perception of the biometric approach

As already mentioned, the success of a biometric authentication system in terms of usage depends on its success authenticating people and on user's perception have about them (El-Abed, et al., 2012). Two survey questionnaires were given to participants to investigate their willingness to adopt this type of authentication approach. The

first one was based on the work by Furnell, et al. (2000) and the UKPS biometric enrollment trial (2005). The second one was the TAM for biometrics questionnaire by James et al. (2008). A five point Likert scale was employed for most of both surveys' questions, the scale used assigned a value of 1 to the strongly agree option and a value of 5 to the strongly disagree option (Table 6).

The results from the user's disposition questionnaire show that participants are willing to accept biometrics as a way of authentication with an average Likert Scale score of 1.78 (Table 34). Also, participants reported that they would feel comfortable with a system like the one tested, with an average response score of 2.05. Additionally, participants reported a need to know if they are being monitored, with an average score of 1.73.

The results from the TAM for biometrics survey show that participants are open to the possibility of using a biometric system like the one tested. They reported an average Likert score of 2.00 (Table 39). The disposition of participants to use this biometric approach is supported by their reported need for privacy and security. The average obtained from questions pertaining to privacy issues in the TAM for Biometrics Questionnaire was 1.47 (Table 40). The average score obtained from questions pertaining to security issues was 1.21 (Table 41).

Chapter 5

Conclusions, Implications, Recommendations, and Summary

This work tested the effectiveness of employing a dynamic behavioral user authentication approach to identify people and its acceptance among participants, which can affect an eventual adoption. The approach was based on the way people interact with their touchscreen devices using their fingers. Additionally, it relied on the premise that distinctive traits are generated when people move their fingers over a touchscreen mobile device while doing tasks like browsing the web or skimming through the pages of a document. The next section presents the conclusions of this study. It is followed by the implications, the recommendations for future research, and ends with a summary.

Conclusions

This study focused on two questions that were discussed throughout this work:

- How effective was this biometric approach in terms of user authentication?

This aspect was tested calculating false acceptance rate (FAR), false rejection rate (FRR), and equal error rate (EER).

- How did users perceive this approach? This aspect was tested surveying participants about their acceptance and satisfaction with the approach presented.

Forty participants were selected among students and staff of UPR-Mayagüez. The majority of them were from engineering related fields. The testing phase was divided in three parts: a pre-test, a biometric test, and a post-test where participants answered questions about their experience and their perception of biometric authentication.

During the pre-test, participants answered several demographic questions. For the biometric test, participants answered questions about pictures while doing horizontal or vertical scrolling. An android application was built to capture six biometric traits for each finger in contact with the screen:

1. area in contact with the touchscreen
2. touchmajor
3. touchminor
4. distance traveled
5. speed
6. angle created by the movement

The use of first three traits took advantage of the fact that everyone's fingers have different shapes and sizes which along with the force applied over the screen produce distinctive values for each person. An advantage of using these three traits is that they can be captured immediately after the user touches the screen, giving an additional point of authentication that other approaches like mouse authentication cannot provide. The

last three traits: speed, distance traveled, and angle created by the movement can be influenced by user's abilities, style of browsing, and motor skills which produce distinctive values for each person.

The aforementioned traits can be collected without the need of user intervention, they are unique for every person, should remain constant over extended periods of time, and should be hard to forge. The use of these biometric traits fulfills the requirements listed by Jain, Ross, and Prabhakar (2004) and Faundez-Zanuy (2005) of universality, distinctiveness, permanence, collectability, performance, acceptability, and circumvention in biometric authentication. This approach could be used to complement other authentication methods to positively verify a user's identity.

The Android application divided each finger stroke into three actions:

- down motion event
- move motion event
- up motion event

This application used the biometric traits to authenticate people at those three independent events. Participants could be authenticated at the beginning of a finger stroke using the biometric traits: area in contact with the touchscreen, touchmajor, and touchminor. All the six aforementioned biometric traits could be used to authenticate people while moving the finger over the screen and also when the finger leaves the screen.

Effectiveness of the biometric approach in terms of user authentication

This work implemented One-Class SVM and emphasized on the verification of users. The best model for each user action event was selected based on the accuracy in

correctly verifying the identity of people. From the results, it can be implied that the best moment to authenticate a user is at the beginning of a finger stroke. The best authentication results showed accuracy of 86% during the horizontal down motion event (Table 12) and accuracy of 80% during the vertical down motion event (Table 13). The results even showed accuracies of 90% or better for several participants (Table 18). The results also show the best numbers were achieved using only one biometric trait to authenticate.

The previous results demonstrate that the proposed traits can be used to authenticate people but biometric authentication systems are usually evaluated with respect to EER, FRR, and FAR (Jorgensen and Yu, 2011). Those metrics have been used in several biometric studies, for example in the work by Ahmed and Traore (2007) where they analyzed mouse dynamics and also by Kanneh and Sakr (2008) in their study about the use of haptics and fuzzy logic to authenticate users. Those biometric traits that gave the best results in terms of authentication effectiveness were used to calculate the metrics:

- EER – The best results, in terms of EER, were obtained during horizontal scrolling. During the down motion event an EER of 34.27% was obtained using the size (area) parameter. During the up motion event an EER of 40.11% was obtained with distance as parameter. The EER results during vertical scrolling were similar to those obtained during horizontal scrolling. An EER of 40.29% for the down motion while using a combination of touchmajor and touchminor as parameters and an EER of 39.63% for the up motion while using angle as parameter.

- FRR – In terms of FRR, the best results were obtained during the down motion while doing horizontal scrolling. A FRR of 13.25% was obtained using touchmajor as a parameter. During the up motion the best FRR results were 27.87% obtained using angle as a parameter.

The best FRR results for the down motion while doing vertical scrolling were 19.95% while using size (area) as a parameter. During the up motion the best FRR results were 28.42% while using touchmajor as a parameter.

- FAR – The FAR obtained, while using the parameter that gave the best FRR result, was 67.59%. It was obtained with touchmajor as a parameter during the down event while doing horizontal scrolling. During the up motion the FAR results were 50.69% with angle as a parameter.

The FAR result obtained in the down motion while doing vertical scrolling was 58.52% with size (area) as a parameter. During the up motion the best results were 60.07% with touchmajor as a parameter.

As can be seen the best EER value obtained was 34.27%, which is higher than values obtained by other authentication methods. It was expected to have this type of high values, although higher than similar authentication methods based on behavioral traits, since usually authentication systems based on user behavior show larger values for EER than those based on physiological characteristics. For example, a haptic system developed by Orozco et al. (2006) in which touch, force, and hand-kinesthetic were continuously measured produced an EER of 22.3%. Also, a study by Schulz (2006) of mouse dynamics for authentication yielded an EER of 24.3%.

It is important to emphasize that the biometric approach presented offers the advantage that for each stroke two independent events can be used to authenticate a person: the first one is when the finger first makes contact with the touch screen and the second one is at the end of a stroke before the finger leaves the touchscreen. These events can be considered independent from one another since the data obtained from one event do not affect the data obtained from the other event. This means that the results obtained can be lowered if the two points are combined. The probability multiplication rule for independent events says that the probability of two events occurring at the same time is the probability of one event occurring times the other event occurring (Brase and Brase, 2007). For example, the best result from the down horizontal event can be combined with the best one from the up horizontal event for better authentication results. The same concept can be applied to the vertical scrolling motion.

Participants' disposition to use the biometric approach

As mentioned before, the success of a biometric authentication system in terms of usage depends on its success authenticating people and also on the perception users have about them (El-Abed, Giot, Hemery, and Rosenberger , 2012).

User acceptance and satisfaction with the authentication approach was evaluated for this work. El-Abed et al. (2010) state that the evaluation of user acceptance and satisfaction of authentication methods should include the assessment of the individual's entire interaction with the system, as well as thoughts, feelings, and outcomes that might result from the interaction that might influence user acceptance.

The first part of this test evaluated the participant's disposition to adopt this type of biometric authentication approach. One important aspect found was 98% of

participants would be in favor of the adoption of some kind of biometric to verify identity. Another important aspect was that 80% people reported feeling comfortable with the system (Appendix Q) which coincides with the original expectations reported on Chapter 3 of an 80 – 100% acceptance from participants. That value lies between a keystroke authentication system with satisfaction around 90% and a face recognition system with a satisfaction around 76% (El-Abed et al., 2012). Additionally, for this work the same percentage of people expressed that they should be aware of biometric data being recorded.

In terms of the time needed to create a biometric profile, the vast majority of users are not willing to spend more than 15 minutes creating a biometric profile (Table 35) which coincides with the results by Furnell et al. (2000). Also, users don't want to be falsely rejected by authentication systems to make mistakes as demonstrated by the results from Table 36 and Furnell et al. (2000) study. The combination of these results represent a big challenge to any biometric authentication system since, as already discussed, behavioral biometric authentication systems present higher levels of mistakes than other methods. An advantage of the approach presented in this work is that the biometric traits can be captured at any moment and a profile can be created without user knowledge.

The second part of the post-test, TAM for biometrics, evaluated users willingness to use this kind of biometric system. TAM states that system use is a response that can be predicted by user motivation, which is directly influenced by the actual system's features and capabilities (Davis, 1993). According to TAM (1993), user motivation can be explained by three factors: perceived ease of use, perceived usefulness, and attitude

toward using the system. Besides the factors pointed out by TAM, James, et al. (2008) state that there are other factors that can influence the adoption of a biometric authentication system. Those factors are: perceived need for security, perceived need for privacy, and perceived physical invasiveness. All six factors determine user motivation, which in turn helps determine user acceptance and satisfaction (James, et al., 2008).

The most important finding in terms of user acceptance was that participants reported that they would agree to use this device. The answers from participants to this question averaged a 2.0 in the Likert scale. This result is supported by the results obtained in other TAM for biometrics questions. The results from questions P1 – P9 and S1 – S9 show that people place security over privacy although not by a large margin. The results from questions P1 – P9 reflect participants need for privacy with a 1.47 average and a 0.72 standard deviation (Table 38). Also, the results from questions S1 – S9 from the TAM for biometrics questionnaire show participant's need for security with an average of 1.21 and a 0.48 standard deviation (Table 39). Those numbers are similar to those obtained by James et al. (2008) in their study. They found an average of 1.54 for security related questions with a standard deviation of 0.72 and a 1.81 average for the privacy related ones with a standard deviation of 0.89.

One issue that appears to be inconclusive, and can affect the adoption of this type of authentication, is the perception of physical invasiveness. The question related to that issue obtained an average Likert score of 2.80 with a standard deviation of 1.03.

Implications

The results of this study show that the biometric traits presented can be used to authenticate a user. Two events during a finger stroke are best suited for that, the down motion event (when the screen is touch for the first time) and the up motion event (when the finger leaves the screen). Above all, the results show that people are willing to use this approach as an authentication method.

This type of authentication can be used as a compliment to other methods of authentication like passwords with the advantage that it can be done at any moment and without user intervention. Obviously, it can help prevent unauthorized access to sensitive information of any kind. Also, it can be used to authenticate users on a local machine or even in remote locations as the use of remote systems become more prevalent. Also, it can help to authenticate people doing e-commerce.

Recommendations

This study demonstrated that the biometric approach presented can effectively authenticate users. Obviously, as in any work, there are many aspects that can be further studied:

- This study involved the participation of 40 participants. Those participants were mostly men from engineering majors which tend to embrace new technologies. It would be interesting to study other types of users to see how they would react to this kind of technology in terms of acceptance,
- what authentication results would be obtained in a more open environment than the one used in this study or even in a more restrictive environment,

- the effect of stress on participants,
- how time affects the biometric traits stored for each user,
- how the participant's posture in front of the equipment affects the results.
- how the context affects browsing behavior, it is possible that informal browsing on media like sports or entertainment have completely different results when compared to reading a book or answering a test,
- determine the ideal amount of time needed to create a biometric profile for finger stroke authentication.

Probably some of these questions can be answered by building a complete application. It would help to test the approach in a more real scenario that authenticates users in real time.

Possible implementation

The results show that it is possible to authenticate someone while that person is using the fingers to browse through different images. Also, the results show that it can be done with minimum intervention from the user. Obviously, the implementation of this type of authentication where security is critical needs improvement. The data collected shows that people are not willing to tolerate errors in authentication.

An authentication application can be implemented by using an approach similar to the one suggested by Bours and Barghouthi (2009) in their work about keystroke dynamic authentication. They suggested the use of confidence levels. The approach consists of determining the level of confidence that a user has not changed at certain points in time, based upon previous browsing behavior. At any point in time this confidence can increase or decrease, but once the confidence becomes below a certain level, actions must be taken, e.g. the user needs to provide a password in order to prove that he has not changed. They suggest implementing confidence levels by using a penalty and reward function. When a session starts, a value C is initialized as 0. For each stroke made by the user, the C value is adjusted, based upon the information in the template. If the information is correct, then the user is rewarded by reducing the value of C . In case the information is not correct, meaning it does not match the information stored in the template, then the user is punished by increasing the value of C . If the C value stays below a predetermined threshold, it means that the user has not changed and no action will be undertaken. If however the C value becomes too high, then the system will need to take action to re-confirm the identity of the user.

The previous concept can be applied to the finger stroke approach presented. A finger stroke can be comprised of two points. This means that people could be authenticated after the down motion and after the up motion since both action events showed satisfactory authentication values. Although they are part of the same stroke, they can be considered independent events since the data obtained from the down event do not affect the data obtained from the up event. This lowers the possibility of a wrong identification and the probability multiplication rule for independent events can be applied (Brase and Brase, 2007):

$$P(A \text{ and } B) = P(A) \times P(B) \quad (28)$$

For example, the top result from the down horizontal event can be combined with the up horizontal event for better authentication results. The same concept can be applied to the vertical scrolling motion.

Obviously, the parameters used for authentication need to be adjusted according to the use of the application. The use of the application should determine the FAR and FRR values being used. For example, it might be desirable to have a low FAR to access high security areas and a low FRR to keep customers happy for access in an internet cafe (Bours and Barghouthi, 2009)..

Summary

Biometric authentication has been employed as an alternative approach for user authentication since it doesn't rely on objects but on the users' physical characteristics.

Current biometric systems cannot guarantee 100% accuracy partly due to the inconsistency of humans (Kanneh and Sakr, 2008).

Several implementations of biometric authentication systems have presented other problems besides accuracy. Some approaches appear to be less acceptable to users since they report being afraid that their work performance may be monitored in some way (Patrick, Long, and Flinn, 2003). Other implementations have used physiological biometric traits that people have shown resistance to their use. For example, some people consider that the use of fingerprints violates their privacy. Also, researchers have demonstrated that fake gelatin fingers can be easily used to deceive biometric fingerprint devices (Shaikh and Dimitriadis, 2008; Patrick, Long, and Flinn, 2003). Moreover, fingerprints can only be authenticated when the user keeps a finger on the reader embedded in a device. Furthermore, other physiological biometric implementations, like face recognition, aren't considered feasible for many users due to the posture that they have to assume in front of a sensor.

Different authentication implementations present some shortcomings besides not being 100% effective. Some of them are not well perceived by users, others require too much computational effort, and others require special equipment or special postures by the user. Ultimately their implementation can result in unauthorized use of the devices or the user being annoyed by the implementation.

This study presented an authentication method that can constantly verify the user's identity which can help prevent unauthorized use of a device or access to sensitive information. The approach presented in this study was well perceived by users and the

authentication results, although not a100% effective, compare favorably against some behavioral biometric approaches.

Appendix A

Design Specifications for Android and Java Application

Introduction

This document is designed to be a reference for any person wanting to implement a biometric authentication system based on the finger movement over a touchscreen device. Three applications were developed to capture and analyze the data obtained. This document describes the applications' architecture, the associated interfaces, and the motivation behind the chosen designs.

Scope of the development project

The project was divided into three applications: one that captures of the biometric traits using an android application, another which pre-process of the data, and the third one that does the SVMs training and evaluates the results obtained. The android application was designed to run on a Lenovo Thinkpad tablet running the Android 4.1 OS. The pre-processing of the data and the SVM application were developed as separate java applications mainly for computation capacity issues respecting Android Tablets.

System architecture description

The biometric authentication was divided into three applications: an android application to capture some biometric traits over a touchscreen device, a data pre-processing application, and an authentication application that employed SVMs (Figure A1).

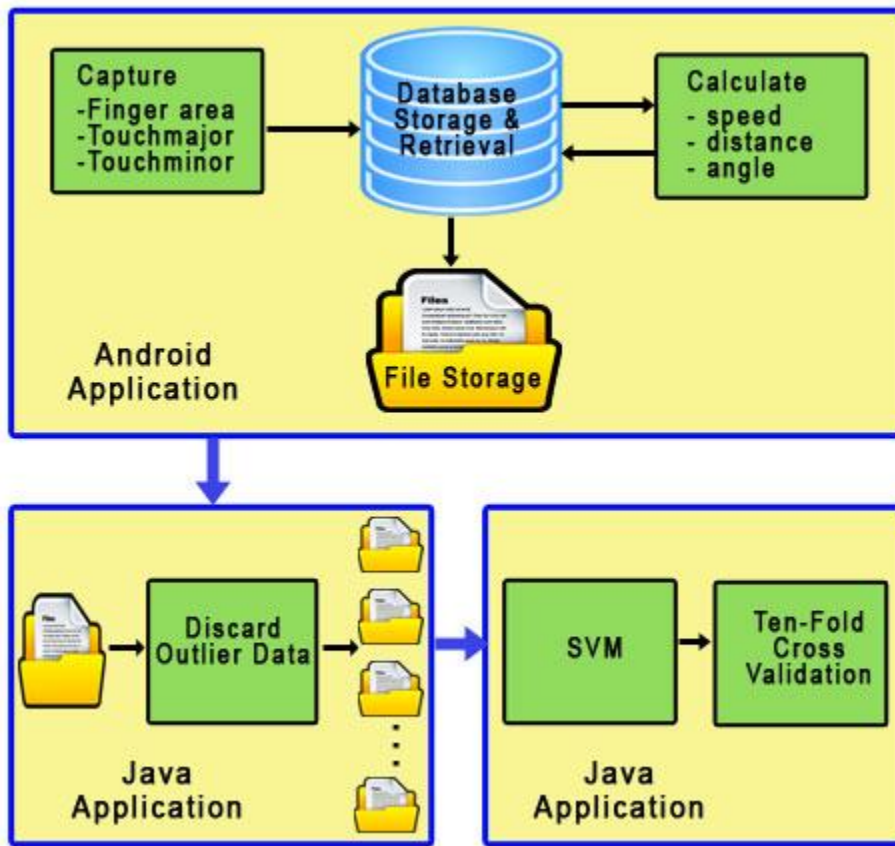


Figure A1. System Architecture

Overview of modules / components

Android Application

The android application captures some finger biometric traits while people are doing horizontal or vertical scrolling. This application was developed using Eclipse IDE for Java Developers Version: Indigo Service Release 2 with the Android Development Toolkit Version: 20.0.3 on a Dell Studio 1535 running Windows Vista with 4 GB of RAM.

The resulting application runs on a Lenovo Thinkpad Tablet with the Android OS 4.0.3. It was implemented through a series of classes that interact with the Android

MotionEvent Class. The application captures biometric traits directly and uses some of them to calculate other traits. Finally, the application stores the results to a database and has the capability of transferring those results to a text file.

User Interface

The android application greets the user at the beginning (Figure A2), after the user presses the Ok button a series of options are presented (Figure A3):



Figure A2. Welcoming Message



Figure A3. Options Menu

The Menu options are:

- Horizontal Screen Capture – This option asks for the user credentials (Figure A4) and then the application goes to the section where the data is captured (Figure A5).



Figure A4. Credentials for horizontal scroll



Figure A5. Horizontal scroll

- Vertical Screen Capture – First, it asks for the user credentials (Figure A6) and then the application goes to the section where the data is captured (Figure A7).



Figure A6. Credentials for vertical scroll



Figure A7. Vertical Scroll

- Vertical Screen Capture (Portrait) – First, it asks for the user credentials (Figure A8) and then the application goes to the section where the data is captured (Figure A9).



Figure A8. Credentials for vertical scroll with tablet in portrait position

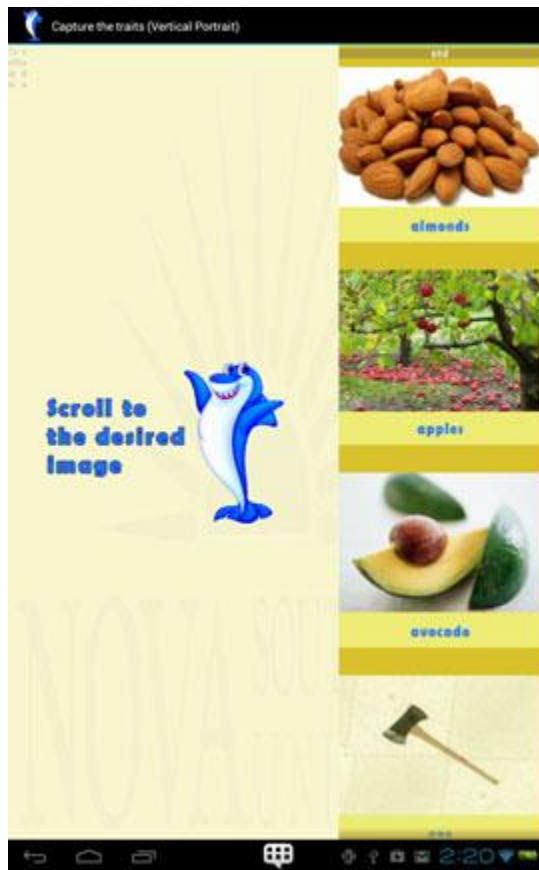


Figure A9. Vertical Scroll with the tablet in portrait position

- Pre-Process Data – It checks the data and calculates distance, speed, and angle for each stroke.
- Store Data – Transfer the data from the database to a text file.
- Add User – It adds a user to the database (Figure A10).



Figure A10. Add a new user

Classes' structure and relationships

As previously mentioned, the application consists of 10 classes that capture the data, do an initial processing of the data, and store results to a database and also to a file (Figure A11).

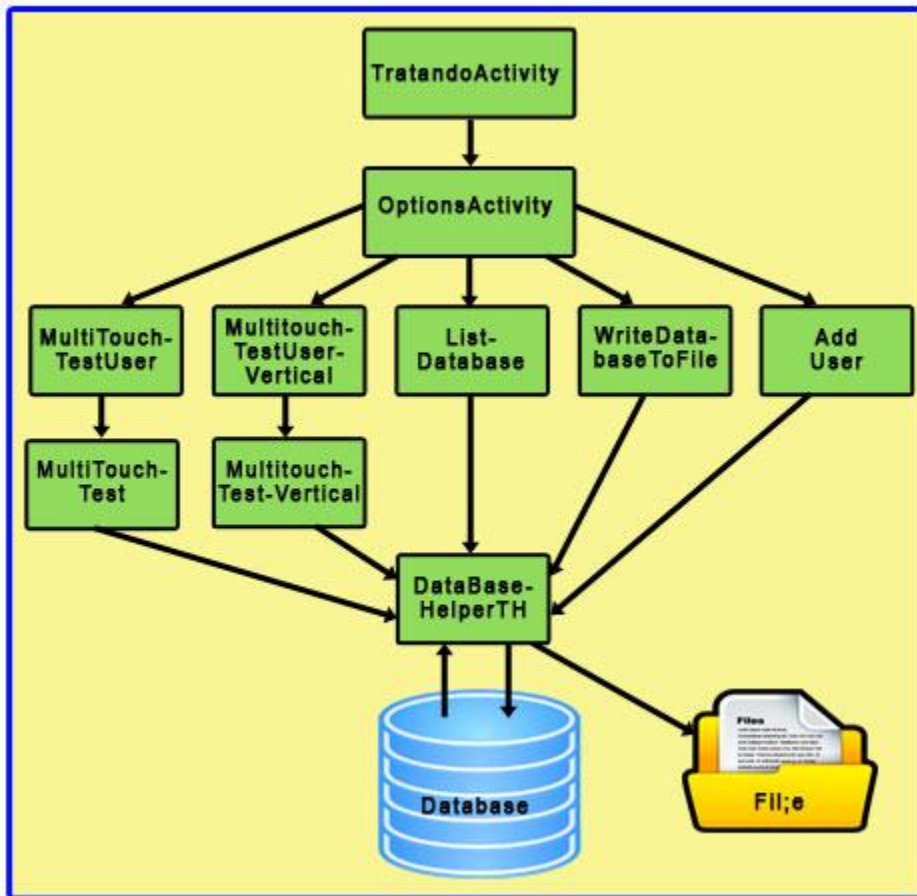


Figure A11. Class architecture for the android application

Classes Description

- Class TratandoActivity

Description:

```
public class TratandoActivity extends Activity
```

It shows the application's welcoming message.

Called by:

none

Calls:

Local Class:

OptionsActivity()

Android and Java Classes:

android.app.Activity;
 android.content.Intent;
 android.os.Bundle;
 android.view.View;

Constructor:

```
public TratandoActivity()
```

Methods:

```
public void onCreate(Bundle savedInstanceState)
public void calculateClickHandler(View view)
```

- Class OptionsActivity

Description:

```
public class OptionsActivity extends Activity
```

It shows the different options available .

Called by:

Class TratandoActivity

Calls:

Local Classes:

MultiTouchTestUser
 MultiTouchTestUserVertical
 MultiTouchTestUserVerticalLong
 ListDatabase

WriteDatabaseToFile

AddUser

Android and Java Classes:

android.os.Bundle

android.app.Activity

android.content.Intent

android.view.View

android.widget.AdapterView

android.widget.AdapterView.OnItemClickListener

android.widget.ListView

Constructor:

```
public OptionsActivity()
```

Methods:

```
public void onCreate(Bundle savedInstanceState)
```

- Class MultiTouchTestUser

Description:

```
public class MultiTouchTestUser extends Activity
```

Shows the window to enter user credentials.

Called by:

TratandoActivity

Calls:

Local Class:

MultiTouchTest

Android and Java Classes:

```
android.app.Activity  
android.app.AlertDialog  
android.content.DialogInterface  
android.content.Intent  
android.database.SQLException  
android.os.Bundle  
android.widget.EditText  
android.view.View
```

Constructor:

```
public MultiTouchTestUser()
```

Methods:

```
public void onCreate(Bundle savedInstanceState)  
public void calculateClickHandler(View view)
```

- Class MultiTouchTest

Description:

```
public class MultiTouchTest extends Activity
```

It captures the biometric traits while doing horizontal scrolling.

Called by:

```
MultiTouchTestUser
```

Calls:

Local Class:

```
DatabaseHelperTH
```


Android and Java Classes:

```
android.app.Activity
android.content.Intent
android.database.SQLException
android.net.Uri
android.os.Bundle
android.os.Environment
android.widget.ImageView
android.widget.LinearLayout
android.widget.TextView
android.util.Log
android.view.MotionEvent
android.view.View
android.view.View.OnClickListener
android.view.View.OnTouchListener
java.io.File
```

Constructor:

```
public MultiTouchTest()
```

Methods:

```
public void onCreate(Bundle savedInstanceState)
```

```
public void onClick(View arg0)
```

- Class MultiTouchTestUserVertical

Description:

```
public class MultiTouchTestUserVertical extends Activity
```

It shows the window to enter user credentials.

Called by:

OptionsActivity

Calls:

Local Class:

MultiTouchTestVertical

Android and Java Classes:

android.app.Activity

android.app.AlertDialog

android.content.DialogInterface

android.content.Intent

android.database.SQLException

android.os.Bundle

android.widget.EditText

android.view.View

Constructor:

```
public MultiTouchTestUserVertical()
```

Methods:

```
public void onCreate(Bundle savedInstanceState)
```

```
public void calculateClickHandler(View view)
```

- Class MultiTouchTestVertical

Description:

```
public class MultiTouchTestVertical extends Activity
```

Captures the biometric traits while doing vertical scrolling.

Called by:

```
MultiTouchTestUserVertical
```

Calls:

Local Class:

```
DatabaseHelperTH
```

Android and Java Classes:

```
android.app.Activity;
```

```
android.database.SQLException
```

```
android.os.Bundle
```

```
android.widget.ImageView
```

```
android.widget.LinearLayout
```

```
android.widget.TextView
```

```
android.view.MotionEvent
```

```
android.view.View
```

```
android.view.View.OnClickListener
```

```
android.view.View.OnTouchListener
```

Constructor:

```
public MultiTouchTestVertical()
```

Methods:

```
public void onCreate(Bundle savedInstanceState)
```

```
public void onClick(View arg0)
```

- Class MultiTouchTestUserVerticalLong

Description:

```
public class MultiTouchTestUserVerticalLong extends Activity
```

Called by:

```
OptionsActivity
```

Calls:

Local Class:

```
MultiTouchTestVerticalLong
```

Android and Java Classes:

```
android.app.Activity
```

```
android.app.AlertDialog
```

```
android.content.DialogInterface
```

```
android.content.Intent
```

```
android.database.SQLException
```

```
android.os.Bundle
```

```
android.widget.EditText
```

```
android.view.View
```

Constructor:

```
public MultiTouchTestUserVerticalLong()
```

Methods:

```
public void onCreate(Bundle savedInstanceState)
```

```
public void calculateClickHandler(View view)
```

- Class MultiTouchTestVerticalLong

Description:

```
public class MultiTouchTestVerticalLong extends Activity
```

Captures the biometric traits while doing vertical scrolling.

Called by:

```
MultiTouchTestUserVerticalLong
```

Calls:**Local Class:**

```
DatabaseHelperTH
```

Android and Java Classes:

```
android.app.Activity
```

```
android.database.SQLException
```

```
android.os.Bundle
```

```
android.widget.ImageView
```

```
android.widget.LinearLayout
```

```
android.widget.TextView
```

```
android.view.MotionEvent
```

```
android.view.View
```

```
android.view.View.OnClickListener
```

```
android.view.View.OnTouchListener
```

Constructor:

```
public MultiTouchTestVerticalLong()
```

Methods:

```
public void onCreate(Bundle savedInstanceState)
```

```
public void onClick(View arg0)
```

- Class ListDatabase

Description:

```
public class ListDatabase extends Activity
```

Process all the data that hasn't been processed.

Called by:

OptionsActivity

Calls:

Local Class:

```
DatabaseHelperTH
```

Android and Java Classes:

```
java.io.IOException
```

```
android.app.Activity
```

```
android.database.SQLException
```

```
android.os.Bundle
```

```
android.os.Environment
```

```
android.widget.ImageView
```

Constructor:

```
public ListDatabase()
```

Methods:

```
protected void onCreate(Bundle savedInstanceState)
```

- Class WriteDatabaseToFile

Description:

```
public class WriteDatabaseToFile extends Activity
```

Writes the data to the file.

Called by:

OptionsActivity

Calls:

Local Class:

DatabaseHelperTH

Android and Java Classes

java.io.IOException

android.app.Activity

android.database.SQLException

android.os.Bundle

android.os.Environment

android.widget.ImageView

Constructor:

```
public WriteDatabaseToFile()
```

Methods:

```
protected void onCreate(Bundle savedInstanceState)
```

- Class AddUser

Description:

```
public class AddUser extends Activity
```

Add users.

Called by:

OptionsActivity

Calls:

Local Class:

DatabaseHelperTH

Android and Java Classes:

android.app.Activity

android.app.AlertDialog

android.content.DialogInterface

android.database.SQLException

android.os.Bundle

android.widget.EditText

android.view.View

Constructor:

```
public AddUser()
```

Methods:

```
public void onCreate(Bundle savedInstanceState)
```

```
public void calculateClickHandler(View view)
```

- Class DataBaseHelperTH

Description:

```
public class DataBaseHelperTH extends SQLiteOpenHelper
```

Handles all the operations related to the database input/output.

Called by:

Class MultiTouchTestUser, MultiTouchTestUserVertical,
MultiTouchTestUserVerticalLong, ListDatabase, WriteDatabaseToFile,
AddUser

Calls:

Android and Java Classes:

android.content.ContentValues
android.content.Context
android.database.Cursor
android.database.SQLException
android.database.sqlite.SQLiteDatabase
android.database.sqlite.SQLiteException
android.database.sqlite.SQLiteOpenHelper
android.os.Environment
java.io.File
java.io.FileOutputStream
java.io.FileWriter
java.io.IOException
java.io.InputStream
java.io.OutputStream
java.io.OutputStreamWriter

Constructor:

```
public DataBaseHelperTH(Context context)
```

Methods:

```
public void createDataBase()

public void openDataBase()

public void close()

public void onCreate(SQLiteDatabase db)

public void onUpgrade(SQLiteDatabase db,int oldVersion,int
newVersion)

public void createEntry(int id,int finger_number,java.lang.Boolean
touched,float xpoint,float ypoint,float size,float time,float touchmajor,float
touchminor,float distance,float speed,float angle,int count,int
person_fk,java.lang.Boolean processed,java.lang.String
action,java.lang.String direction)

public void createEntryUser(java.lang.String theusername,java.lang.String
thepassword)

public java.lang.String getData()

public void newwritefromDBtoFile(Context context)

public void processDataDB(Context context)

public int SearchUser(java.lang.String theusername,java.lang.String
thepassword)
```

Data Transformation (Java Application)

This application was developed using Eclipse IDE for Java Developers Version: Indigo Service Release 2 on a Dell Studio 1535 running Windows Vista with 4 GB of RAM. The application implements a class that divides the resulting file into six different files according to the type and direction of the finger movement.

- Class transfor

Description:

```
public class transfor extends java.lang.Object
```

Creates six files (.arff) for each user based on direction and type of movement. Also, it eliminates outliers using the quarterly method.

Called by:

None

Calls:

Android and Java Classes:

```
java.io.BufferedReader
```

```
java.io.FileReader
```

```
java.util.Scanner
```

```
java.io.BufferedWriter
```

```
java.io.File
```

```
java.io.FileWriter
```

Constructor:

```
public transfor()
```

Method:

```
public static void main(java.lang.String[] args)
```

Test Data (Java Application)

This application was developed using Eclipse Standard/SDK Kepler Version Service Release 1 on a virtual machine running a 64 bit Windows 7 Professional OS with 8 GB of RAM. The application implements a class that trains a SVM and evaluates the training results using ten-fold cross validation.

- Class Test

Description:

```
public class Test extends java.lang.Object
```

Performs the SVM training and uses tenfold cross validation to evaluate the results, it implements WEKA libraries

Called by:

None

Calls:

Android and Java Classes:

```
java.io.BufferedReader
```

```
java.io.FileReader
```

```
java.util.Random
```

```
java.io.BufferedWriter
```

```
java.io.File
```

```
java.io.FileWriter
```

```
weka.classifiers.Evaluation
```

```
weka.classifiers.functions.LibSVM
```

```

weka.classifiers.evaluation.EER
weka.core.Instances
weka.core.SelectedTag
weka.classifiers.evaluation.ThresholdCurve
weka.filters.Filter
weka.filters.unsupervised.attribute.Discretize
weka.filters.unsupervised.attribute.Remove

```

Constructor:

```
public Test()
```

Methods:

```

public static void main(java.lang.String[] args)
public static void analysis(java.lang.String myfile)
public static void analysis_removed_attributes(java.lang.String myfile)

```

Database

The database stores the biometric traits for each registered user. The database was created and edited using SQLite Database Browser version 2.0b1. SQLite Database Browser is an open source, public domain, freeware visual tool used to create, design, edit SQLite 3.x database files. SQLite is a software library that implements a self-contained, serverless, zero-configuration, transactional SQL database engine.

Two tables were created, one named Person and another named Finger. Person stores username and password of participants. Finger stores the biometric data for each stroke while scrolling (Table A1, Table A2). The data for each user is associated via the person_fk field (Figure A12)

Table A1

Description of Database Table Finger

Field	Type	Description
_id	integer primary key	Primary key
direction	varchar2	Movement direction. Possible values: h (horizontal) or v (vertical)
action	varchar2	Type of action being registered by the application. Possible values: down, move, and up
processed	varchar2	Indicates if the values for distance, speed, and angle have been calculated.
finger_number	numeric	Finger being registered. Possible values: 0 – 9.
touched	varchar2	Registered if the screen was touched.
xpoint	numeric	X coordinate of the finger over the screen
ypoint	numeric	Y coordinate of the finger over the screen
size	numeric	Area of the finger in contact with the touchscreen
time	numeric	Time when the contact was made.
touchmajor	numeric	Length of the major axis over the screen
touchminor	numeric	Length of the major axis over the screen
distance	numeric	Distance between the coordinates of a previous record and the actual record
speed	numeric	Speed of the movement c
angle	numeric	Angle of the movement
count	integer	Internal count of the instance number for a stroke
person_fk	integer	Foreign key to table person

Table A2

Description of Database Table Person

Field	Type	Description
_id	integer primary key	Primary key
username	varchar2	Username
password	varchar2	Password

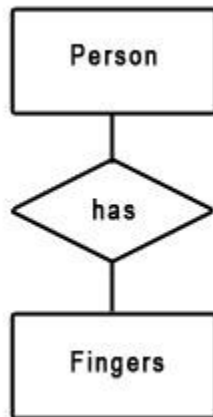


Figure A12. Entity Relationship Diagram for Android Application Database

Appendix B

ARFF Sample File

```

@relation finger

@attribute orientation {v,h}
@attribute action {down,move,up}
@attribute finger_number {0,1,2,3,4,5,6,7,8,9}
@attribute size real
@attribute touchmajor real
@attribute touchminor real
@attribute distance real
@attribute speed real
@attribute angle real
@attribute count real
@attribute person_fk
{1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31,32,33,34,35,36,37,38,39,40,41,42,43,44,45,46,47,48,49,50}

@data
h,down,0,40.555557,77.60181,65.136635,0.0,0.0,0.0,0.0,2
h,down,0,26.736113,51.6938,42.406025,0.0,0.0,0.0,0.0,2
h,down,0,27.013891,51.6938,43.383686,0.0,0.0,0.0,0.0,2
h,down,0,27.013891,51.6938,43.383686,0.0,0.0,0.0,0.0,2
h,down,0,27.013891,51.6938,43.383686,0.0,0.0,0.0,0.0,2
h,down,0,19.652779,46.095165,24.268986,0.0,0.0,0.0,0.0,2
h,down,0,27.013891,51.6938,43.383686,0.0,0.0,0.0,0.0,2
h,down,0,27.013891,51.6938,43.383686,0.0,0.0,0.0,0.0,2
h,down,0,27.013891,51.6938,43.383686,0.0,0.0,0.0,0.0,2
h,down,0,34.375,77.60181,43.383686,0.0,0.0,0.0,0.0,2
h,down,0,27.013891,51.6938,43.383686,0.0,0.0,0.0,0.0,2
h,down,0,27.013891,51.6938,43.383686,0.0,0.0,0.0,0.0,2
h,down,0,33.194447,69.20767,48.65299,0.0,0.0,0.0,0.0,2
h,down,0,20.833334,51.6938,21.63074,0.0,0.0,0.0,0.0,2
h,down,0,34.375,77.60181,43.383686,0.0,0.0,0.0,0.0,2
h,down,0,27.013891,51.6938,43.383686,0.0,0.0,0.0,0.0,2
h,down,0,27.013891,51.6938,43.383686,0.0,0.0,0.0,0.0,2
h,down,0,32.98611,68.428604,48.65299,0.0,0.0,0.0,0.0,2
h,down,0,27.013891,51.6938,43.383686,0.0,0.0,0.0,0.0,2
h,down,0,40.555557,77.60181,65.136635,0.0,0.0,0.0,0.0,2
h,down,0,33.854168,75.76869,43.383686,0.0,0.0,0.0,0.0,2

```


Appendix D

IRB Letters of Approval from UPR-Mayagüez and Nova Southeastern University



Institutional Review Board
CPSHI/IRB 00002053
University of Puerto Rico – Mayagüez Campus
Dean of Academic Affairs
Call Box 9000
Mayagüez, PR 00681-9000



September 16, 2013

Prof. Arturo Ponce-Román
PO Box 365
San Antonio, PR 00690

Dear Prof. Ponce-Román,

The IRB has received and reviewed the revised Informed Consent form for the research project titled *A Dynamic Behavioral Biometric Approach to Authenticate Users Employing their Fingers to Interact with Touchscreen Devices*.

In view of the fact that your project qualifies for an expedited approval process and you have incorporated our recommendations, the IRB gladly grants its approval for one year, as requested, from October 1, 2013 thru September 30, 2014. Please remember that you should submit to the IRB an annual report with a summary of the results of your study, including any adverse effects that human subjects have suffered or are suffering as a result of this research.

Modifications and amendments to the approved protocol must be reviewed and approved by the IRB before they are implemented. The IRB must be immediately notified of any adverse effects or unanticipated problems involving risks to subjects or others if any undue harms result from the study. The IRB must be notified as well if any complaints, either from the subjects or the study staff, are made regarding the research study or any breach of confidentiality occurs.

We appreciate your commitment to uphold the highest standards of protections for human subjects in research and remain,

Sincerely,

Rosa F. Martínez Cruzado
Rosa F. Martínez Cruzado, Ph.D.
President
CPSHI/IRB
UPR-RUM

NOVA SOUTHEASTERN UNIVERSITY
Office of Grants and Contracts
Institutional Review Board



MEMORANDUM

To: Arturo Ponce
From: Ling Wang, Ph.D.
Institutional Review Board

Date: Oct. 9, 2013

Re: *A Dynamic Behavioral Biometric Approach to Authenticate Users Employing Their Fingers to Interact with Touchscreen Devices*

IRB Approval Number: wang08151303

I have reviewed the above-referenced research protocol at the center level. Based on the information provided, I have determined that this study is exempt from further IRB review. You may proceed with your study as described to the IRB. As principal investigator, you must adhere to the following requirements:

- 1) **CONSENT:** If recruitment procedures include consent forms these must be obtained in such a manner that they are clearly understood by the subjects and the process affords subjects the opportunity to ask questions, obtain detailed answers from those directly involved in the research, and have sufficient time to consider their participation after they have been provided this information. The subjects must be given a copy of the signed consent document, and a copy must be placed in a secure file separate from de-identified participant information. Record of informed consent must be retained for a minimum of three years from the conclusion of the study.
- 2) **ADVERSE REACTIONS:** The principal investigator is required to notify the IRB chair and me (954-262-5369 and 954-262-2020 respectively) of any adverse reactions or unanticipated events that may develop as a result of this study. Reactions or events may include, but are not limited to, injury, depression as a result of participation in the study, life-threatening situation, death, or loss of confidentiality/anonymity of subject. Approval may be withdrawn if the problem is serious.
- 3) **AMENDMENTS:** Any changes in the study (e.g., procedures, number or types of subjects, consent forms, investigators, etc.) must be approved by the IRB prior to implementation. Please be advised that changes in a study may require further review depending on the nature of the change. Please contact me with any questions regarding amendments or changes to your study.

The NSU IRB is in compliance with the requirements for the protection of human subjects prescribed in Part 46 of Title 45 of the Code of Federal Regulations (45 CFR 46) revised June 18, 1991.

Cc: Protocol File

Appendix E



Adult/General Informed Consent

Consent Form for Participation in the Research Study Entitled
 “A Dynamic Behavioral Biometric Approach to Authenticate Users Employing Their
 Fingers to Interact with Touchscreen Devices”

Funding Source: None.

IRB protocol #:

Principal investigator(s)
 Arturo Ponce, MS Electrical Engineering
 PO Box 365, San Antonio, PR 00690
 (787)598-8438
 arturo.ponce@upr.edu

Co-investigator(s)
 Maxine Cohen, PhD
 Graduate School of Computer and Infor-
 mation Sciences, Nova Southeastern Univer-
 sity, 3301 College Avenue, Ft. Lauderdale,
 FL 33314-7796
 954 262-2072
 cohenm@nova.edu

For questions/concerns about your research rights, contact:
 Human Research Oversight Board (Institutional Review Board or IRB)
 Nova Southeastern University
 (954) 262-5369/Toll Free: 866-499-0790
IRB@nsu.nova.edu
 or

Initials: _____

Date: _____

Page 1 of 3

Committee for the Protection of Human Beings in Research
Office of the Dean of Academic Affairs University of Puerto Rico-Mayagüez Campus
(787) 832-4040 x.6277
cpshe@uprm.edu

What is the study about?

The goal of this project is to study how people browse through different images while using their touchscreen devices. This study will collect data that will be later analyzed.

Why are you asking me?

You were selected because of your experience with touchscreen mobile devices. Approximately 30 participants like you will be part of this study.

What will I be doing if I agree to be in the study?

Your participation will take approximately 30 minutes.

This study consists of three parts: a pre-test, a biometric test, and a post-test. The pre-test consists of answering several demographic questions. The biometric test consists of browsing through different images and answering questions about them. The post-test consists of answering some questions related to your experience during the test.

Is there any audio or video recording?

There is no audio or video recording.

What are the dangers to me?

All research carries risk. The standard for minimal risk is that which is found in everyday life. With the research team's efforts to maintain confidentiality, risk of your identification is unlikely; however there is risk of breach of confidentiality. Safeguards are in place to minimize the risk of breach of confidentiality, as outlined in the confidentiality section. Risks greater than those encountered in everyday life are not anticipated.

If you have any questions about the research, your research rights, or have a research-related injury, please contact Arturo Ponce (ap911@nova.edu). You may also contact the IRB at the numbers indicated above if you have any complaint about this research.

Are there any benefits for taking part in this research study?

There are no direct benefits for taking part in this research study.

Will I get paid for being in the study? Will it cost me anything?

There are no costs to you or payments made for participating in this study.

Initials: _____

Date: _____

How will you keep my information private?

Confidentiality regarding your participation will be maintained. Any notes associated with this test materials will be used without reference to your name. All data will be stored on a designated computer with login and password protection. Data will be kept locked in the PI's office and retained for 36 months after the study is complete. Only those personnel who are listed on this IRB application form will have access to the data. The project's research records may be reviewed by departments at Nova Southeastern University responsible for regulatory and research oversight and at the University of Puerto Rico – Mayagüez.

What if I do not want to participate or I want to leave the study?

You have the right to leave this study at any time or refuse to participate. If you do decide to leave or you decide not to participate, you will not experience any penalty or loss of services you have a right to receive.

Other Considerations:

If significant new information relating to the study becomes available, which may relate to your willingness to continue to participate, this information will be provided to you by the investigators.

Voluntary Consent by Participant:

By signing below, you indicate that

- this study has been explained to you
- you have read this document or it has been read to you
- your questions about this research study have been answered
- you have been told that you may ask the researchers any study related questions in the future or contact them in the event of a research-related injury
- you have been told that you may ask Institutional Review Board (IRB) personnel questions about your study rights
- you will receive a copy of this form after you have read and signed it
- you voluntarily agree to participate in the study entitled "A Dynamic Behavioral Biometric Approach to Authenticate Users Employing their Fingers to Interact with Touchscreen Devices"

Participant's Signature: _____ Date: _____

Participant's Name: _____ Date: _____

Signature of Person Obtaining Consent: _____

Date: _____

Initials: _____ Date: _____

Appendix F
Demographics Questionnaire

Participant # _____

Date _____

Please answer the following questions:

1. Age: _____

2. Gender:

_____ Male

_____ Female

3. Program of Studies: _____

4. Year of Studies:

_____ First

_____ Fourth

_____ Masters

_____ Second

_____ Fifth

_____ PhD

_____ Third

_____ Sixth or more

5. Are you color blind?

_____ Yes

_____ No

_____ Not sure

6. Do you own or use touchscreen devices?

_____ Yes (go to 7)

_____ No (Stop)

7. Which of the following touchscreen devices do you use or own? (you can select more than one)

_____ smartphone

_____ tablet

_____ other _____

8. Approximately, how many hours a day do you spend using all your touchscreen devices (smartphones, tablets, etc.)

9. Which services do you use on your touchscreen devices? (you can select more than one)

_____ regular telephony

_____ text messaging

_____ Internet

_____ other _____

10. If you use Internet on your touchscreen devices, what do you use it for? (you can select more than one)

_____ read/send email

_____ search for information

_____ shopping

_____ listen to music

_____ play games

_____ social networking (Facebook, Twitter, etc.)

_____ other_____

Appendix G

Biometric Test

First Part (Horizontal Scrolling)

Participant # _____

Date _____

Instructions: Please, go to the indicated image and answer the corresponding question. Answer the questions in the order that they are presented.

1. Please, go to the banana plantation image.

How many banana plants can you count?

2. Please, go to the farmers market image.

How many products on the table can you count?

3. Please, go to the goat image.

What color are the spots on the goat?

4. Please, go to the cow image.

What color are the spots on the cow's calf?

5. Please, go to the flowers image.

Name two colors of the flowers.

6. Please, go to the hens image.

How many hens are in the image?

7. Please, go to the pick image.

What is the color of the handle?

8. Please, go to the fork image.

What color is the fork?

9. Please, go to the dog image.

What color are the spots on the dog?

10. Please, go to the harvesting image.

What is the color of the machine?

11. Please, go to the pigs image.

How many pigs can you count?

12. Please, go to the horses image.

What color are the horses?

13. Please, go to the starfruit image.

What color is the starfruit inside?

14. Please, go to the rooster image.

What color is the rooster's tail?

15. Please, go to the mangos image.

What color are the mangos?

16. Please, go to the almonds image.

How many almonds can you see?

Stop.

The first part of the biometric test has ended. Please, wait for further instructions.

Second Part (Vertical Scrolling)

Participant # _____

Date _____

Instructions: Please, go to the indicated image and answer the corresponding question.

Answer the questions in the order that they are presented.

1. Please, go to the breadfruit image.

What color is the inside of the breadfruit?

2. Please, go to the farm barn image.

What color are the buildings to the right of the barn?

3. Please, go to the cow image.

What color are the spots on the cow?

4. Please, go to the geese image.

How many geese are in the image?

5. Please, go to the rake image.

What is the color of the rake's handle?

6. Please, go to the mangos image.

What color is the background?

7. Please, go to the goat image.

What color is the goat?

8. Please, go to the papaya image.

What color is the inside of the papaya?

9. Please, go to the soybean plantation image.

What color is the soybean plantation?

10. Please, go to the tractor image.

What color is the tractor?

11. Please, go to the summer bounty image.

Name one item on the image.

12. Please, go to the sheep image.

What color are the sheep?

13. Please, go to the horses image.

What color is the mane of the first horse from the left?

14. Please, go to the farmers market image.

How many people can you count?

15. Please, go to the wind farm image.

How many wind mills can you count?

16. Please, go to the sugar cane field image.

What color is the top of the sugar cane field?

Stop.

The biometric test has ended. Please, wait for further instructions.

Appendix H

Images Used in the Biometric Test



Figure H1. Images one to six used in the biometric test. Adapted from: 1. Authentic Self Wellness, <http://authenticselfwellness.com/2011/09/23/the-health-benefits-of-almonds/>; 2. Austin Public Library, <http://library.austintexas.gov/blog-entry/apples>; 3. The Examiner.com, <http://www.examiner.com/article/super-food-of-the-month-avocado>; 4. Ray's House Help, <http://www.rayshousehelp.com/axe-types-styles-and-best-uses/>; 5. Wikimedia Commons, http://commons.wikimedia.org/wiki/File:Banana_Farm_-_Kerala.jpg; 6. The PaleoFood Recipe Collection, <http://paleofood.com/recipes/veggies-breadfruitboiled.htm>



Figure H2. Images seven to twelve used in the biometric test. Adapted from: 7. Daily Mail, <http://www.dailymail.co.uk/sciencetech/article-1360166/New-Zealand-abandons-cloning-farm-animals-90-PER-CENT-died-trials.html>; 8. Wallcoo.net, <http://old.wallcoo.net/animal/farm-animal/html/image13.html>; 9. Fanpop, <http://www.fanpop.com/clubs/domestic-animals/images/5356758/title/farm-animals-collection-wallpaper>; 10. Countryfarm Lifestyles, <http://www.countryfarm-lifestyles.com/Canadian-Farms.html>; 11. Grafton Farmers Market, <http://graftonfarmersmarket.com/>; 12. Special Farms[Online], <http://www.kidcyber.com.au/topics/farmspecial.htm>

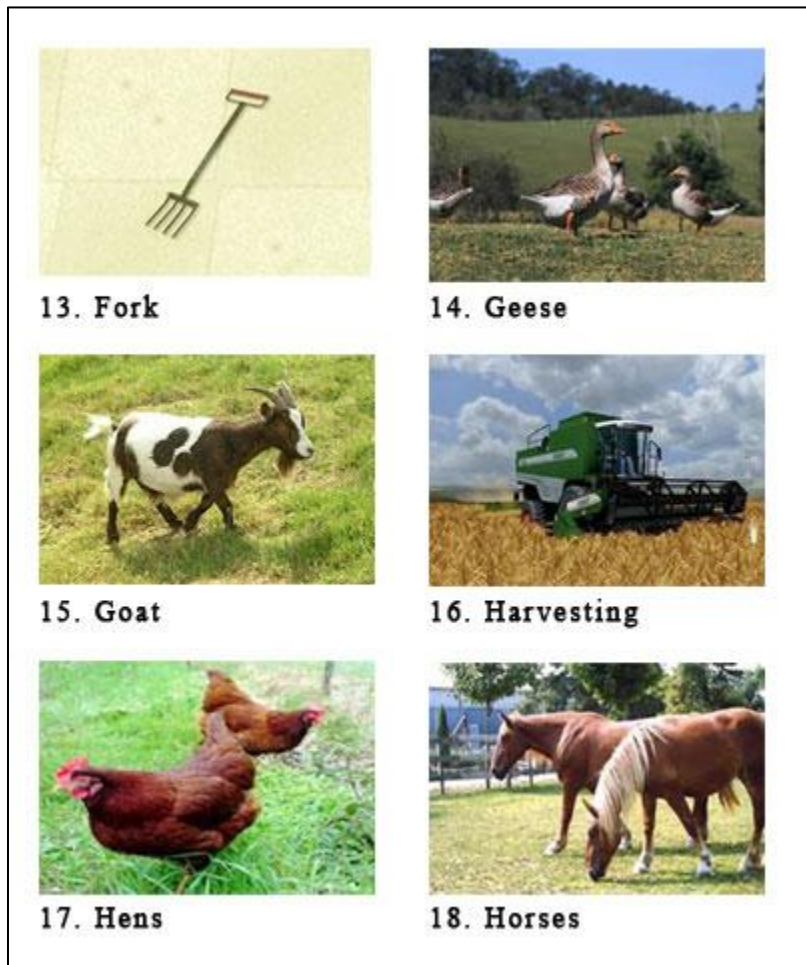


Figure H3. Images 13 to 18 used in the biometric test. Adapted from: 13. http://www.agway.com/catalog/rural/farm_tools_and_equipment/forks/10501007_bully_tools_super_spading_fork_with_steel_d-grip_handle_4-tines_45_6in.html; 14. Animal World USA, <http://www.kentuckyanimals.org/information.html>; 15. Images-for-schools.org.uk, <http://www.visualeducationforall.com/farm-animals/02-goat.htm>; 16. Gamercast, <http://www.gamercast.net/farming-simulator-gold-review>; 17. Hudson Valley Humane Society, <http://www.hvhumane.org/pets-for-adoption/?command=nav&catid=5&page=2>; 18. Associated Humane Societies and Popcorn Park Zoo, <http://www.ahscares.org/page2.asp?page=farmanimals&style=2>

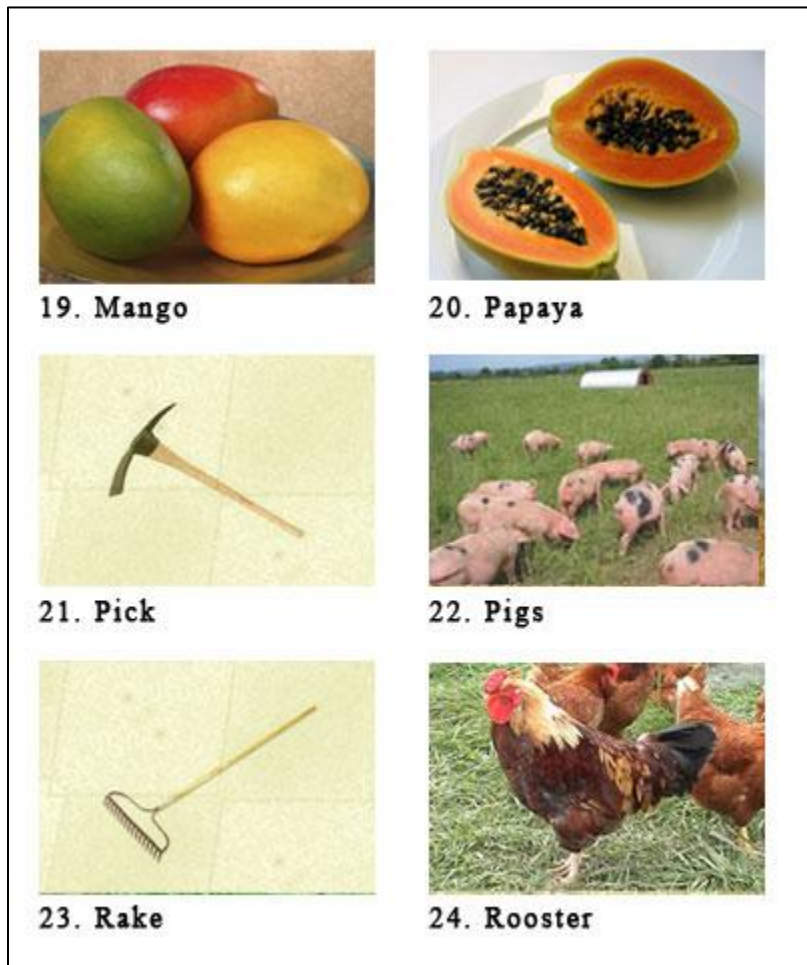


Figure H4. Images 19 to 24 used in the biometric test. Adapted from: 19. Mango.org, <http://www.mango.org/taxonomy/term/10>; 20. EU Jacksonville, <http://www.eujacksonville.com/story2.php?storyid=518>; 21. Agway, http://www.agway.com/catalog/rural/farm_tools_and_equipment.html; 22. Moonbeams Land, http://www.moonbeamsland.co.uk/shop/our-gloucester-old-spots/i_3.html; 23. The Interpretation of Dreams, <http://eofdreams.com/rake.html>; 24. Oracle ThinkQuest, <http://library.thinkquest.org/06aug/01220/basic4.htm>



Figure H5. Images 25 to 30 used in the biometric test. Adapted from: 25. Sheep101, <http://www.sheep101.info/>; 26. West Seattle Tools Library, <http://wstoollibrary.org/2011/09/shovels/>; 27. Soybean plantation. Yeso Agrícola Malargüe, <http://www.yesoyam.com.ar/>; 28. Grow your own Fruit, <http://growfruit.tripod.com/starfruit.htm>; 29. Royalty Free Stock Photos, http://www.123rf.com/photo_15223190_sugar-cane-plantation-in-northeastern-of-thailand.html; 30. Live Earth Farm (Com) Post, <http://www.writerguy.com/deb/compost/2007/Nws16-2007.html>

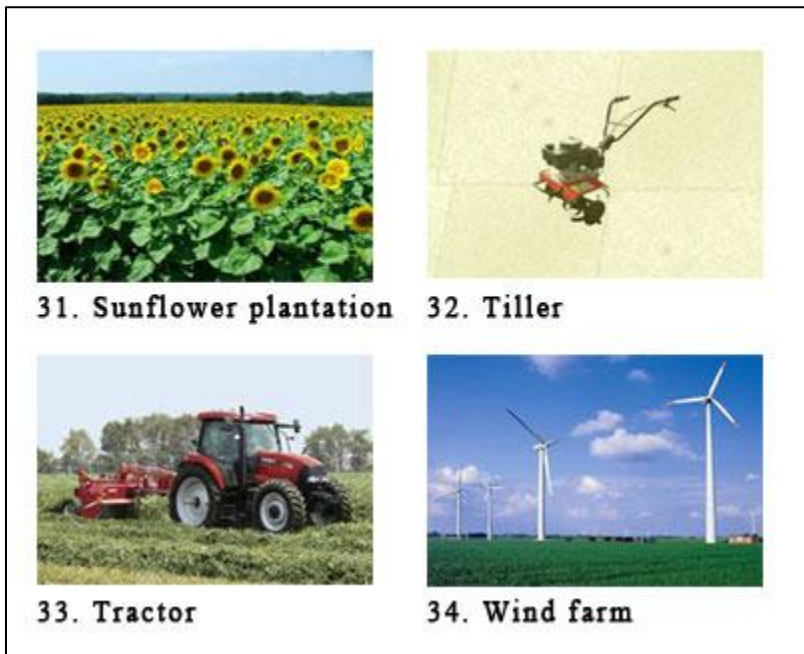


Figure H6. Images 31 to 34 used in the biometric test. Adapted from: 31. ThisIsCT.net, <http://www.thisisct.net/2007/07/buttonwood-farm-sunflowers.html>; 32. Alibaba.com, http://cqweiyou.en.alibaba.com/product/503491435-212873449/WY_400_Power_Farm_Tillers_Cultivators_Agricultural_Machines_Farming_Tools.html; 33. Merco Press. (South Atlantic News Agency), <http://en.mercopress.com/2010/11/12/as-argentine-farming-recovers-machinery-sales-soar>; 34. REVE (Wind Energy and Electric Vehicle Review), <http://www.evwind.es/2012/08/01/wind-energy-development-in-tanzania/20721>

Appendix I

Brief Description of Biometrics and the Biometric Traits

Captured in this Study

Biometrics refers to any physiological and/or behavioral characteristic that can be used to uniquely identify a person. Biometrics takes advantage of an individual's unique characteristics for identification. This uniqueness makes biometric identifiers essentially more reliable than knowledge-based and token-based methods in differentiating between an authorized user and an impostor.

Biometric authentication has been mainly used for identity verification and for identification. Identity verification compares a user's data against the records in a database when the system receives an enrollment request. Identification matches the user's biometric data against all its records because the user's identity is unknown.

All biometric systems are divided into two categories: physiological and behavioral. Physiological biometric systems are based on an individual's distinctive characteristics like fingerprints, iris, retina, facial images, and hand geometry. Behavioral biometric systems are based on the way people do things. They are based on the premise that distinctive traits are generated when people do different things.

The application that you used is based on this premise that distinctive traits are generated when people move their fingers over a touchscreen while scrolling vertically or

horizontally. The application captured the several biometric traits for each one of the fingers that made contact with the touchscreen.

Appendix J

User's Disposition Questionnaire

Participant # _____

Date _____

Please, rate your level of agreement with the following sentences.

1. I would be in favor of biometrics being adopted as a mean of verifying identity

_____ Strongly agree

_____ Agree

_____ Neither agree nor disagree

_____ Disagree

_____ Strongly disagree

2. I feel comfortable with a system, like the one tested, that continuously captures biometric data

_____ Strongly agree

_____ Agree

_____ Neither agree nor disagree

_____ Disagree

_____ Strongly disagree

3. I should be aware if biometric data is being captured while using a device.

_____ Strongly agree

_____ Agree

_____ Neither agree nor disagree

_____ Disagree

_____ Strongly disagree

Please answer the following questions:

1. A monitoring system may falsely reject a legitimate user, believing them to be an impostor. How frequently are you willing to tolerate such errors?

_____ I don't consider it a problem

_____ less than 20% of the time

_____ less than 15% of the time

_____ less than 10% of the time

_____ less than 5% of the time

_____ 0 % (Never)

2. A behavioral biometric system needs to create a behavioral profile, how long are you willing to spend creating one?

_____ no time

_____ less than 1 minute

_____ 1 to 3 minutes

_____ 3 to 5 minutes

_____ up to 10 minutes

_____ up to 30 minutes

_____ up to 60 minutes

_____ beyond 60 minutes

3. If you should use a biometric method like this, who do you think should have access to your biometric pattern?

- only yourself
- yourself and (you can select more than one)
 - your telephone/Internet provider
 - your employer/school
 - your bank office
 - the government (county, state, federal)
 - whoever you buy something from
 - other _____

Appendix K

Technology Acceptance Model for Biometrics Questionnaire

Participant # _____

Date _____

A. Perceived Need for Security and Privacy

Please, rate your level of agreement with the following sentences.

1. I feel that the safeguarding from potential external threats of my physical being is important to me.

_____ Strongly agree

_____ Agree

_____ Neither agree nor disagree

_____ Disagree

_____ Strongly disagree

2. I feel that my personal security at my home or in my vehicle is important to me.

_____ Strongly agree

_____ Agree

_____ Neither agree nor disagree

_____ Disagree

_____ Strongly disagree

3. I feel that my personal security at my place of work or other work related places is important to me.

_____ Strongly agree
_____ Agree
_____ Neither agree nor disagree
_____ Disagree
_____ Strongly disagree

4. My security at places of public access, such as a mall or airport, or special public events, such as the Olympics or the Super Bowl, is important to me.

_____ Strongly agree
_____ Agree
_____ Neither agree nor disagree
_____ Disagree
_____ Strongly disagree

5. I feel that the security of my tangible assets (such as my home, vehicle, etc.) is important to me.

_____ Strongly agree
_____ Agree
_____ Neither agree nor disagree
_____ Disagree
_____ Strongly disagree

6. I feel that keeping my personal possessions, such as jewelry, money, electronics, etc. safe is important to me.

- _____ Strongly agree
- _____ Agree
- _____ Neither agree nor disagree
- _____ Disagree
- _____ Strongly disagree

7. I feel that the safekeeping of my informational assets contained in digital or paper format is important to me (such as financial records, medical records, etc.).

- _____ Strongly agree
- _____ Agree
- _____ Neither agree nor disagree
- _____ Disagree
- _____ Strongly disagree

8. I feel that the security of my personal information, such as my PC files or personal records (financial, medical, etc.) is important to me.

- _____ Strongly agree
- _____ Agree
- _____ Neither agree nor disagree
- _____ Disagree
- _____ Strongly disagree

9. I feel that the safekeeping of information I have provided to a corporation or other entity is important to me.

- _____ Strongly agree
- _____ Agree

_____ Neither agree nor disagree

_____ Disagree

_____ Strongly disagree

10. I feel my privacy is very important to me.

_____ Strongly agree

_____ Agree

_____ Neither agree nor disagree

_____ Disagree

_____ Strongly disagree

11. I feel that my control over my personal information is very important to me.

_____ Strongly agree

_____ Agree

_____ Neither agree nor disagree

_____ Disagree

_____ Strongly disagree

12. I feel that it is important not to release sensitive information to any entity.

_____ Strongly agree

_____ Agree

_____ Neither agree nor disagree

_____ Disagree

_____ Strongly disagree

13. I feel it is important to avoid having personal information released that I think could be financially damaging.

- _____ Strongly agree
- _____ Agree
- _____ Neither agree nor disagree
- _____ Disagree
- _____ Strongly disagree

14. I feel it is important to avoid having personal information released that I think could be socially damaging to me.

- _____ Strongly agree
- _____ Agree
- _____ Neither agree nor disagree
- _____ Disagree
- _____ Strongly disagree

15. I feel it is important to avoid having personal information about me released that may go against social morals and attitudes.

- _____ Strongly agree
- _____ Agree
- _____ Neither agree nor disagree
- _____ Disagree
- _____ Strongly disagree

16. I feel that the release of personal information to individuals with whom I have a high comfort level is unacceptable.

- _____ Strongly agree
- _____ Agree

_____ Neither agree nor disagree

_____ Disagree

_____ Strongly disagree

17. I feel that the release of personal information to entities where I feel as though I am anonymously providing the information is unacceptable.

_____ Strongly agree

_____ Agree

_____ Neither agree nor disagree

_____ Disagree

_____ Strongly disagree

18. I feel that the use of personal information that has been released by me but is used in a manner not intended by me is unacceptable.

_____ Strongly agree

_____ Agree

_____ Neither agree nor disagree

_____ Disagree

_____ Strongly disagree

B. The Biometric Application

The application that you used is based on the premise that distinctive traits are generated when people move their fingers over a touchscreen while scrolling vertically or horizontally. The application captured several biometric traits for each one of the fingers that made contact with the touchscreen.

Please, rate your level of agreement with the following sentences.

1. I think this biometric device is useful.

_____ Strongly agree

_____ Agree

_____ Neither agree nor disagree

_____ Disagree

_____ Strongly disagree

2. I think this biometric device is easy to use.

_____ Strongly agree

_____ Agree

_____ Neither agree nor disagree

_____ Disagree

_____ Strongly disagree

3. I think one of the reasons this device is useful is because of its ease of use.

_____ Strongly agree

_____ Agree

_____ Neither agree nor disagree

_____ Disagree

_____ Strongly disagree

4. I think that this device would be physically invasive.

_____ Strongly agree

_____ Agree

_____ Neither agree nor disagree

_____ Disagree

_____ Strongly disagree

5. I think I would use this device.

_____ Strongly agree

_____ Agree

_____ Neither agree nor disagree

_____ Disagree

_____ Strongly disagree

Appendix L

Amount of Time Needed to Complete the Biometric Test and Number of Strokes Captured for Each Participant

Table L1

Participants' Times during the Biometric Tests

Participant	Minutes
1	15.31
2	26.12
3	16.27
4	21.00
5	12.55
6	12.59
7	19.80
8	15.29
9	13.14
10	12.89
11	18.88
12	10.69
13	11.68
14	17.91
15	14.42
16	13.89
17	17.06
18	10.38
19	14.51
20	13.95
21	15.27
22	17.51
23	19.81
24	22.56
25	16.69
26	24.04
27	12.04
28	14.85
29	14.83
30	13.57
31	13.98

32	18.15
33	16.11
34	20.29
35	14.95
36	12.43
37	15.95
38	13.83
39	16.60
40	10.90
average	15.82
standard deviation	3.61
median	15.11
minimum	10.38
maximum	26.12

Table L2

Number of Strokes Captured per Participant during Horizontal and Vertical Scrolling

Participant	Horizontal	Vertical
1	191	226
2	86	124
3	115	394
4	65	78
5	102	298
6	45	45
7	209	403
8	128	222
9	78	230
10	104	141
11	82	142
12	70	69
13	68	236
14	119	168
15	45	88
16	79	142
17	130	145
18	63	88
19	76	101
20	52	82
21	49	151
22	125	190
23	100	119
24	112	170
25	70	246
26	191	100
27	67	101
28	46	70
29	49	76
30	52	145
31	69	62
32	167	157
33	62	102
34	102	260
35	49	71
36	86	249
37	25	44
38	37	82
39	111	104
40	62	133

average	88.45	151.35
standard deviation	43.11	85.78
minimum	25	44
maximum	209	403

Note. Red means below the target of 50 strokes.

Appendix M

Biometric Test Results for Different Biometric Traits Combinations

Table M1

Accuracy and FRR Results from Different Parameter Combinations in the Down

Horizontal Motion Event

Biometric Trait Combination	Accuracy	FRR
touchmajor	86.75%	13.25%
size (area), touchmajor	84.99%	15.01%
touchminor	84.99%	15.01%
size (area)	84.96%	15.04%
size (area), speed	84.96%	15.04%
size (area), distance	84.96%	15.04%
size (area), distance, angle	84.96%	15.04%
size (area), distance, speed	84.96%	15.04%
size (area), angle	84.96%	15.04%
size (area), distance, speed, angle, counter	84.96%	15.04%
size (area), touchmajor, touchminor, distance, counter	83.09%	16.91%
all	83.09%	16.91%
size (area), touchmajor, touchminor, counter	83.09%	16.91%
size (area), touchmajor, touchminor, distance, speed, angle	83.09%	16.91%
size (area), touchmajor, touchminor, 8, angle, counter	83.09%	16.91%
size (area), touchmajor, touchminor, angle, counter	83.09%	16.91%
size (area), touchmajor, touchminor, distance, angle, counter	83.09%	16.91%
size (area), touchmajor, touchminor, distance, speed, counter	83.09%	16.91%
size (area), touchmajor, touchminor, distance, speed, angle	83.09%	16.91%
size (area), touchmajor, touchminor	82.72%	17.28%
size (area), touchmajor, touchminor	82.72%	17.28%
size (area), touchminor	81.62%	18.38%
size (area), touchminor, distance, speed, angle, counter	81.62%	18.38%
touchmajor, touchminor	81.00%	19.00%
touchmajor, touchminor, distance, speed, angle,	81.00%	19.00%

counter		
touchminor, distance, speed, angle, counter	69.94%	30.06%
touchminor	68.19%	31.81%
distance	0.00%	100.00%
speed	0.00%	100.00%
angle	0.00%	100.00%
distance, speed	0.00%	100.00%
distance, angle	0.00%	100.00%
speed, angle	0.00%	100.00%
distance, speed, angle, counter	0.00%	100.00%

Table M2

*Accuracy and FRR Results from Different Parameter Combinations in the Down Vertical**Movement*

Biometric Trait Combination	Accuracy	FRR
size (area)	80.05%	19.9%5
size (area), speed	80.05%	19.95%
size (area), distance	80.05%	19.95%
size (area), distance, angle	80.05%	19.95%
size (area), distance, speed	80.05%	19.95%
size (area), angle	80.05%	19.95%
size (area), distance, speed, angle, counter	80.05%	19.95%
touchmajor	79.50%	20.50%
size (area), touchmajor	79.10%	20.90%
size (area), touchmajor, distance, speed, angle, counter	79.10%	20.90%
touchmajor, touchminor	76.74%	23.26%
touchmajor, touchminor, distance, speed, angle, counter	76.74%	23.26%
size (area),touchmajor, touchminor, distance, speed, angle	75.95%	24.05%
size (area),touchmajor, touchminor, speed, angle, counter	75.95%	24.05%
size (area),touchmajor, touchminor, angle, counter	75.95%	24.05%
size (area),touchmajor, touchminor, distance, angle, counter	75.95%	24.05%
size (area),touchmajor, touchminor, distance, speed, counter	75.95%	24.05%
size (area),touchmajor, touchminor, distance, speed, angle	75.95%	24.05%
size (area),touchmajor, touchminor, distance, counter	75.95%	24.05%
all	75.95%	24.05%
size (area),touchmajor, touchminor, counter	75.95%	24.05%
size (area), touchminor	75.69%	24.31%
size (area), touchminor-counter	75.69%	24.31%
touchminor, distance, speed, angle, counter	75.62%	24.38%
touchminor	75.62%	24.38%
size (area), touchmajor, touchminor	74.24%	25.76%
size (area), touchmajor, touchminor	74.24%	25.76%
distance	0.00%	100.00%
speed	0.00%	100.00%
angle	0.00%	100.00%
distance, speed	0.00%	100.00%

distance, angle	0.00%	100.00%
speed, angle	0.00%	100.00%
distance, speed, angle, counter	0.00%	100.00%

Table M3

*Accuracy and FRR Results from Different Parameter Combinations in the Move**Horizontal Movement*

Biometric Trait Combination	Accuracy	FRR
touchmajor	57.29%	42.71%
touchminor	56.53%	43.47%
size (area)	52.66%	47.34%
distance	51.23%	48.77%
speed	50.93%	49.07%
angle	50.80%	49.20%
size (area), touchmajor, touchminor	50.44%	49.57%
size (area), touchmajor, touchminor	50.44%	49.57%
size (area), touchminor	49.61%	50.39%
size (area), touchmajor	49.50%	50.50%
touchmajor, touchminor	49.37%	50.63%
size (area), angle	49.05%	50.95%
distance, speed	49.04%	50.96%
size (area), speed	49.00%	51.00%
size (area), distance, speed	48.97%	51.03%
speed, angle	48.97%	51.03%
distance, angle	48.95%	51.05%
distance, speed, angle, counter	48.94%	51.06%
size (area), distance	48.93%	51.07%
touchminor, distance, speed, angle, counter	48.92%	51.08%
size (area), distance, angle	48.91%	51.09%
touchmajor, touchminor, distance, speed, angle, counter	48.91%	51.09%
size (area), distance, speed, angle, counter	48.90%	51.10%
size (area), touchminor-counter	48.90%	51.10%
size (area),touchmajor, touchminor, counter	48.88%	51.12%
size (area),touchmajor, touchminor, distance, speed, angle	48.86%	51.14%
size (area),touchmajor, touchminor, distance, speed, angle	48.86%	51.14%
size (area),touchmajor, touchminor, distance, counter	48.86%	51.14%
size (area),touchmajor, touchminor, angle, counter	48.86%	51.14%
size (area), touchmajor, touchminor, speed, angle, counter	48.85%	51.15%
size (area),touchmajor, touchminor, distance, speed, counter	48.85%	51.15%
size (area),touchmajor, touchminor, distance, angle, counter	48.85%	51.15%

size (area), touchmajor, distance, speed, angle, counter	48.85%	51.15%
all	48.83%	51.17%

Table M4

*Accuracy and FRR Results from Different Parameter Combinations in the Move Vertical**Movement*

Biometric Trait Combination	Accuracy	FRR
touchminor	56.35%	43.65%
touchmajor	52.65%	47.35%
size (area)	52.16%	47.84%
distance	51.48%	48.52%
speed	50.78%	49.22%
angle	50.60%	49.40%
size (area), touchmajor	50.57%	49.43%
size (area), touchminor	50.56%	49.44%
touchmajor, touchminor	50.37%	49.63%
size (area), touchmajor, touchminor	50.36%	49.64%
size (area), touchmajor, touchminor	50.36%	49.64%
distance, speed	50.34%	49.66%
size (area), touchmajor, touchminor, counter	50.21%	49.79%
distance, angle	50.21%	49.79%
size (area), distance	50.18%	49.82%
size (area), distance, speed	50.17%	49.83%
size (area), angle	50.16%	49.84%
speed, angle	50.16%	49.84%
size (area), distance, speed, angle, counter	50.15%	49.85%
distance, speed, angle, counter	50.15%	49.85%
touchmajor, touchminor, distance, speed, angle, counter	50.14%	49.86%
size (area), touchmajor, distance, speed, angle, counter	50.13%	49.87%
touchminor, distance, speed, angle, counter	50.13%	49.87%
size (area), distance, angle	50.12%	49.88%
size (area), touchmajor, touchminor, distance, speed, angle	50.12%	49.88%
size (area), touchmajor, touchminor, distance, speed, angle	50.12%	49.88%
all	50.12%	49.88%
size (area), touchmajor, touchminor, angle, counter	50.11%	49.89%
size (area), touchmajor, touchminor, distance, counter	50.11%	49.89%
size (area), speed	50.11%	49.89%
size (area), touchminor-counter	50.11%	49.89%
size (area), touchmajor, touchminor, speed, angle, counter	50.10%	49.90%
size (area), touchmajor, touchminor, distance, speed, counter	50.08%	49.92%

counter		
size (area),touchmajor, touchminor, distance, angle,	50.07%	49.93%
counter		

Table M5

*Accuracy and FRR Results from Different Parameter Combinations in the Up Horizontal**Movement*

Biometric Trait Combination	Accuracy	FRR
angle	72.13%	27.87%
distance	71.56%	28.44%
touchminor	71.06%	28.94%
speed	70.21%	29.79%
distance, angle	70.16%	29.84%
touchmajor	70.01%	29.99%
size (area)	69.47%	30.53%
size (area), touchminor	69.02%	30.98%
distance, speed	69.01%	30.99%
speed, angle	68.62%	31.38%
size (area), touchmajor	68.60%	31.40%
size (area), angle	68.46%	31.54%
size (area), speed	68.21%	31.79%
touchmajor, touchminor	68.11%	31.89%
size (area), distance	67.65%	32.35%
size (area), distance, angle	67.21%	32.79%
size (area), touchmajor, touchminor	66.59%	33.41%
size (area), touchmajor, touchminor	66.59%	33.41%
size (area), distance, speed	65.68%	34.32%
size (area), touchmajor, touchminor, counter	65.01%	34.99%
distance, speed, angle, counter	64.88%	35.12%
size (area), touchmajor, touchminor, distance, counter	63.35%	36.65%
size (area), touchmajor, touchminor, angle, counter	62.35%	37.65%
touchminor, distance, speed, angle, counter	62.21%	37.79%
size (area), distance, speed, angle, counter	62.03%	37.97%
size (area), touchmajor, touchminor, distance, angle, counter	60.52%	39.48%
size (area), touchmajor, touchminor, speed, angle, counter	60.25%	39.75%
size (area), touchmajor, touchminor, distance, speed, counter	60.17%	39.83%
size (area), touchmajor, distance, speed, angle, counter	59.73%	40.27%
size (area), touchminor-counter	59.60%	40.40%
touchmajor, touchminor, distance, speed, angle, counter	59.53%	40.47%
size (area), touchmajor, touchminor, distance, speed,	59.28%	40.72%

angle		
size (area),touchmajor, touchminor, distance, speed,	59.28%	40.72%
angle		
all	57.69%	42.31%

Table M6

*Accuracy and FRR Results from Different Parameter Combinations in the Up Vertical**Movement*

Biometric Trait Combination	Accuracy	FRR
touchmajor	71.58%	28.42%
size (area)	70.09%	29.91%
size (area), touchmajor	68.87%	31.13%
angle	68.58%	31.42%
touchmajor, touchminor	67.82%	32.18%
distance	67.80%	32.20%
touchminor	67.60%	32.40%
speed	67.25%	32.75%
size (area), speed	66.75%	33.25%
size (area), distance	66.75%	33.25%
size (area), touchminor	66.32%	33.68%
distance, angle	66.29%	33.71%
size (area), angle	66.16%	33.84%
speed, angle	65.09%	34.91%
distance, speed	64.65%	35.35%
size (area), touchmajor, touchminor	64.14%	35.86%
size (area), touchmajor, touchminor	64.14%	35.86%
size (area), distance, angle	63.61%	36.39%
size (area), distance, speed	62.31%	37.69%
size (area), touchmajor, touchminor, counter	62.14%	37.86%
distance, speed, angle, counter	60.37%	39.63%
size (area), touchmajor, touchminor, distance, counter	58.40%	41.60%
size (area), touchmajor, touchminor, angle, counter	58.29%	41.71%
size (area), distance, speed, angle, counter	57.99%	42.01%
touchminor, distance, speed, angle, counter	57.40%	42.60%
size (area), touchmajor, distance, speed, angle, counter	55.90%	44.10%
size (area), touchmajor, touchminor, distance, angle, counter	55.73%	44.27%
touchmajor, touchminor, distance, speed, angle, counter	55.55%	44.45%
size (area), touchmajor, touchminor, distance, speed, counter	55.46%	44.54%
size (area), touchmajor, touchminor, speed, angle, counter	55.22%	44.78%
size (area), touchminor-counter	55.13%	44.87%
size (area), touchmajor, touchminor, distance, speed, angle	53.79%	46.21%

size (area),touchmajor, touchminor, distance, speed, angle	53.79%	46.21%
all	53.17%	46.83%

Appendix N

Comments about Participants during Biometric Tests

Table N1

General Remarks about Participants during the Biometric Tests

Participant	General Remarks
2	Changed fingers
5	Changed fingers
12	Used the tablet in the upright position and continued that way throughout the test
13	Used the tablet in the upright position and continued that way throughout the test and also changed fingers
14	Everything was consistent
17	Everything was consistent
18	Was left handed,
19	Everything was consistent
21	was left-handed,.
25	Was left-handed.
26	Was left-handed.
28	No change on fingers.
33	Was consistent on both parts.

Note: Red means major concern, green means minor concern, and black means no concern.

Table N2

Comments on Participants during Horizontal Stroke Portion of the Biometric Tests

Participant	General Remarks
15	Changed hands on one occasion
16	Changed hands on one occasion and fingers
21	Began using the middle finger but changed fingers
22	used the middle finger.
23	changed between thumb and middle finger, also changed hands.
24	changed fingers.
27	used left hand although right handed.
28	used right hand.
29	changed fingers.
30	changed fingers and hand
31	used the left hand and changed fingers although is right handed.
32	began with left hand but later changed to right hand.
34	began with left hand but later changed to right hand although is right handed.
35	began with the left hand but later changed to right hand although is right handed.
36	used the right hand all the time.
37	began with the left hand but later changed to right hand although is right handed.
38	used the left hand although is right handed.
39	took the tablet on his hand and used the right hand to move
40	took the tablet on his hand and used the index finger of the right hand to move. Later put the tablet over the table and afterwards changed to the left hand.

Note: Red means major concern, green means minor concern.

Table N3

Comments on Participants during Vertical Stroke Portion of the Biometric Tests

Participant	General Remarks
18	used the right hand for the vertical portion
20	changed fingers
21	changed hands.
22	used the middle finger.
24	used thumb finger.
25	began with thumb but later changed fingers.
26	began with thumb but later changed fingers.
27	used right hand.
28	used right hand.
29	changed fingers.
30	changed fingers.
31	used the left hand also but don't changed fingers.
32	used thumb but changed fingers sometimes,
34	used the right hand since the beginning. Used different fingers while going up or down.
35	began to alternate hands.
36	used the same hand but changed fingers.
37	used the right hand since the beginning and used the same finger.
38	used the thumb finger.
39	took the tablet on his hand and used the right hand to move.
40	began with the right hand but later changed to the left hand.

Note: Red means major concern, green means minor concern.

Appendix O

FRR for Participants with Less than 50 Strokes

Table O1

Results for Different Parameter Combinations in the Down Horizontal Motion

Biometric Traits	FRR	FAR
touchmajor	31.84%	57.02%
size (area), touchmajor	13.54%	54.98%
touchminor	43.62%	24.36%
size (area)	12.72%	54.56%

Table O2

Results for Different Parameter Combinations in the Down Vertical Motion

Biometric Traits	FRR	FAR
size (area)	9.45%	66.19%
touchmajor	10.46%	68.75%
size (area), touchmajor	9.28%	66.23%
touchmajor, touchminor	14.41%	66.05%

Table O3

Results for Different Parameter Combinations in the Up Horizontal Motion

Biometric Traits	FRR	FAR
angle	28.17%	58.54%
distance	26.97%	51.76%
touchminor	25.01%	43.86%
speed	33.11%	44.30%

Table O4

Results for Different Parameter Combinations in the Up Vertical Motion

Biometric Traits	FRR	FAR
touchmajor	40.57%	43.16%
size (area)	48.77%	35.34%
size (area), touchmajor	47.35%	37.09%
angle	32.91%	27.45%

Appendix P

FRR for Participants with Changes in their Scrolling Behavior

Table P1

Results for Different Parameter Combinations in the Down Horizontal Motion

Biometric Traits	FRR	FAR
touchmajor	18.80%	65.16%
size (area), touchmajor	17.54%	60.84%
touchminor	38.33%	46.92%
size (area)	16.05%	53.36%

Table P2

Results for Different Parameter Combinations in the Down Vertical Motion

Biometric Traits	FRR	FAR
size (area)	23.27%	54.67%
touchmajor	29.54%	50.52%
size (area), touchmajor	25.95%	55.17%
touchmajor, touchminor	28.85%	62.43%

Table P3

Results for Different Parameter Combinations in the Up Horizontal Motion

Biometric Traits	FRR	FAR
angle	24.84%	53.49%
distance	26.50%	55.68%
touchminor	25.75%	58.08%
speed	28.09%	58.73%

Table P4

Results for Different Parameter Combinations in the Up Vertical Motion

Biometric Traits	FRR	FAR
touchmajor	23.25%	71.76%
size (area)	27.44%	59.16%
size (area), touchmajor	25.87%	61.86%
angle	30.80%	51.67%

Appendix Q

Raw Collected Data for User's Disposition Questionnaire

Table Q1

Answer to Participants' Level of Agreement of the User's Disposition Questionnaire

Participant	Questions		
	1. I would be in favor of biometrics being adopted as a mean of verifying identity	2. I feel comfortable with a system, like the one tested, that continuously captures biometric data	3. I should be aware if biometric data is being captured while using a device
1	2	2	3
2	2	3	3
3	2	2	1
4	1	1	1
5	2	2	1
6	2	2	1
7	2	2	3
8	2	2	3
9	2	3	1
10	1	1	3
11	2	2	3
12	1	1	1
13	1	1	3
14	2	2	2
15	2	3	1
16	2	2	2
17	2	4	1
18	2	1	2
19	1	2	1
20	1	2	2
21	2	3	1
22	2	2	1
23	2	2	2
24	1	2	3
25	2	3	1
26	2	2	1
27	2	2	2
28	2	2	1
29	4	4	1

30	2	2	1
31	1	1	1
32	2	2	4
33	2	3	1
34	2	2	2
35	2	2	1
36	2	2	2
37	1	1	2
38	2	3	1
39	1	1	2
40	1	1	1

Table Q2

Answer to Questions One and Two from Part Two of the User's Disposition

Questionnaire

Participant	Questions	
	1. A monitoring system may falsely reject a legitimate user, believing them to be an impostor. How frequently are you willing to tolerate such errors?	2. A behavioral biometric system needs to create a behavioral profile, how long are you willing to spend creating one?
1	less than 15% of the time	3 to 5 minutes
2	less than 5% of the time	3 to 5 minutes
3	less than 20% of the time	1 to 3 minutes
4	less than 10% of the time	up to 10 minutes
5	less than 5% of the time	less than 1 minute
6	less than 5% of the time	3 to 5 minutes
7	I don't consider it a problem	3 to 5 minutes
8	0 % (Never)	less than 1 minute
9	less than 10% of the time	1 to 3 minutes
10	less than 10% of the time	3 to 5 minutes
11	less than 5% of the time	up to 30 minutes
12	less than 5% of the time	beyond 60 minutes
13	I don't consider it a problem	up to 10 minutes
14	less than 5% of the time	up to 10 minutes
15	less than 5% of the time	up to 10 minutes
16	less than 5% of the time	beyond 60 minutes
17	0 % (Never)	1 to 3 minutes
18	less than 10% of the time	up to 10 minutes
19	less than 10% of the time	3 to 5 minutes
20	less than 20% of the time	beyond 60 minutes
21	0 % (Never)	up to 60 minutes
22	less than 5% of the time	3 to 5 minutes
23	less than 10% of the time	3 to 5 minutes
24	less than 10% of the time	up to 10 minutes
25	less than 10% of the time	1 to 3 minutes
26	0 % (Never)	up to 10 minutes
27	less than 5% of the time	up to 10 minutes
28	less than 15% of the time	3 to 5 minutes
29	0 % (Never)	no time
30	less than 5% of the time	up to 10 minutes
31	0 % (Never)	less than 1 minute
32	less than 15% of the time	up to 10 minutes
33	less than 20% of the time	up to 30 minutes

34	less than 10% of the time	up to 30 minutes
35	less than 15% of the time	3 to 5 minutes
36	less than 5% of the time	3 to 5 minutes
37	less than 5% of the time	beyond 60 minutes
38	less than 5% of the time	up to 10 minutes
39	less than 20% of the time	up to 60 minutes
40	less than 5% of the time	3 to 5 minutes

Table Q3

Answer to Question Three (If You Should Use a Biometric Method Like This, Who Do You Think Should Have Access to Your Biometric Pattern?) from Part Two of the User's Disposition Questionnaire

User	who	Options					other
		your telephone/ Internet provider	your employer /school	your bank office	government (county, state, federal)	whoever you buy something from	
1	yourself and ...			1	1		
2	yourself and ...	1					
3	yourself and ...		1	1			
4	only yourself						
5	yourself and ...						People I know
6	yourself and ...			1			
7	yourself and ...	1					
8	only yourself						
9	only yourself						
10	only yourself						
11	only yourself						
12	yourself and ...		1				
13	only yourself						
14	only yourself						
15	only yourself						
16	yourself and ...					1	
17	only yourself						
18	yourself and ...	1					
19	only yourself						
20	yourself and ...	1	1	1			
21	yourself and ...				1		
22	only yourself						

23	yourself and ...				the person that I choose
24	only yourself				
25	only yourself				
26	yourself and ...			1	
27	only yourself				
28	yourself and ...		1		
29	only yourself				
30	yourself and ...			1	family
31	only yourself				
32	only yourself				
33	only yourself				
34	yourself and ...	1			
35	only yourself				
36	yourself and ...		1		
37	only yourself				
38	only yourself				
39	yourself and ...		1	1	
40	only yourself				

Appendix R

Raw Collected Data for Technology Acceptance Model for Biometrics

Questionnaire

Table R1

Answer for Perceived Need for Security (Questions 1 – 9) and Perceived Need for

Privacy (Questions 10 – 18) of the TAM for Biometrics Questionnaire

P	<u>Questions</u>																	
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
1	1	1	1	1	1	2	1	1	1	2	1	3	1	1	2	1	3	1
2	1	1	1	2	2	3	1	2	1	2	1	3	3	3	3	3	4	3
3	1	1	1	1	2	2	1	1	1	1	1	1	1	1	1	3	1	1
4	2	1	1	1	1	1	1	1	1	1	1	1	1	1	2	3	2	3
5	3	1	1	1	1	1	1	1	2	1	2	1	1	2	2	3	5	1
6	1	1	1	1	1	3	1	2	1	1	1	1	1	1	1	3	2	1
7	2	1	1	2	3	1	1	1	2	1	1	3	1	1	5	4	2	5
8	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
9	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
10	2	1	1	1	1	1	1	1	1	1	2	1	1	1	1	1	1	1
11	1	1	1	1	2	3	1	1	1	1	1	2	1	2	2	2	1	1
12	1	1	1	1	1	1	1	1	1	1	1	2	2	1	1	1	1	1
13	1	1	1	1	1	1	1	1	1	1	1	1	1	1	3	3	2	1
14	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
15	1	1	1	1	2	2	1	1	1	1	1	1	1	2	2	3	3	1
16	2	2	2	2	2	2	1	1	2	1	1	1	1	2	1	2	1	1
17	1	1	1	1	2	5	1	2	2	1	1	1	1	1	1	2	1	1
18	2	1	1	1	1	1	1	1	1	1	1	1	1	2	1	1	1	1
19	1	1	1	1	2	4	1	2	1	2	2	2	2	3	1	4	4	2
20	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2	4	1	1
21	2	1	2	2	2	3	1	1	1	1	1	1	1	2	2	2	1	1
22	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2	2	1
23	1	1	1	1	1	2	1	1	1	1	1	1	1	2	2	3	1	1
24	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	3	1
25	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2	1	1
26	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2	3	1	1

27	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
28	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2	1	1
29	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
30	1	1	1	1	1	2	1	1	1	1	2	1	2	2	2	2	1	1
31	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
32	2	2	2	2	2	2	1	1	1	2	1	2	2	2	2	2	3	3
33	2	1	1	1	1	2	1	1	1	2	1	1	3	3	3	3	2	2
34	2	1	1	1	2	1	1	1	1	1	1	2	2	2	2	1	2	2
35	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
36	2	2	2	1	1	2	1	1	1	2	2	2	1	2	3	3	3	2
37	1	1	1	1	1	1	1	1	3	1	1	2	1	1	2	3	3	3
38	2	1	1	2	1	1	1	1	1	1	1	2	1	1	1	1	1	1
39	1	2	1	2	1	1	1	1	1	1	1	1	2	1	1	3	2	2
40	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2	1	1

Note: P = Participant.

Table R2

*Answer to Question 1 -5 from the Second Part (The Biometric Application) of the TAM
for Biometrics Questionnaire*

Participant	Questions				
	1	2	3	4	5
1	2	2	1	2	2
2	3	1	2	3	3
3	1	1	1	2	1
4	1	1	2	2	1
5	2	2	3	6	3
6	2	1	1	4	2
7	2	1	2	3	2
8	2	2	4	3	3
9	1	2	2	3	2
10	2	1	1	1	1
11	2	2	2	4	2
12	2	1	1	1	1
13	1	1	1	4	1
14	2	3	3	2	3
15	2	3	3	3	2
16	2	2	2	3	2
17	2	2	3	3	3
18	1	2	2	2	2
19	1	1	1	1	1
20	1	1	1	5	1
21	2	2	2	3	3
22	3	1	3	4	4
23	2	1	1	3	2
24	1	1	1	4	1
25	2	2	2	4	2
26	2	1	1	3	2
27	1	2	2	2	2
28	2	2	2	3	2
29	2	2	2	2	2
30	2	1	1	2	2
31	1	1	1	1	1
32	2	2	2	3	2
33	2	2	3	2	2
34	2	2	2	2	2
35	2	1	1	3	3
36	2	2	2	3	2
37	1	1	1	5	2

38	1	2	3	3	1
39	1	1	1	2	1
40	1	2	2	4	2

References

- Ahmed, A. E. & Traore, I. (2007). A new biometric technology based on mouse dynamics. *IEEE Transactions on Dependable and Secure Computing*, 4(3), 165 – 179. doi: 10.1109/TDSC.2007.70207
- Alhussain, T., Drew, S., & Alfarraj, O. (2010). Biometric authentication for mobile government security. *International Conference on Intelligent Computing and Intelligent Systems*, 114 – 118. doi:10.1109/ICICISYS.2010.5658854
- Android Developers. (n.d.a). MotionEvent. Retrieved November 20, 2014 from <http://developer.android.com/reference/android/view/MotionEvent.html>
- Android Developers. (n.d.b). MotionEvent.PointerCoords. Retrieved November 20, 2014 from <http://developer.android.com/reference/android/view/MotionEvent.PointerCoords.html>
- Athanassoulis, N. & Wilson, J. (2009). When is deception in research ethical? *Clinical Ethics*, 4 (1) 44 - 49. doi: 10.1258/ce.2008.008047
- Bhalla, M. R. & Bhalla, A. V. (2010). Comparative study of various touchscreen technologies. *International Journal of Computer Applications*, 6(8), 12 – 18. Retrieved from http://www.jips-k.org/dlibrary/JIPS_v04_no4_paper5.pdf
- Bednarik, R., Kinnunen, T., Mihaila, A., & Fränti, P. (2005). Eye-movements as a biometric. *Image Analysis*, 16 – 26. doi: 10.1007/11499145_79
- Beecher, J. A., Penna, J. A., & Bittinger, M. L. (2011). *Algebra and trigonometry* (Fourth ed., pp. 59-101, 705-719). Boston, MA, USA: Addison-Wesley.
- Ben-Hur, A., & Weston, J. (2010). A user's guide to support vector machines. *Data Mining Techniques for the Life Sciences*, 223-239.
- Bhattacharyya, D., Ranjan, R., Das, P., Kim, T., & Bandyopadhyay, S. K. (2009). Biometric authentication techniques and its future possibilities. *Second International Conference on Computer and Electrical Engineering*, 2, 652 – 655. doi: 10.1109/ICCEE.2009.103
- Bours, P. & Barghouthi, H. (2009). Continuous authentication using biometric keystroke dynamics. The Norwegian Information Security Conference, 1 – 12.
- Brase, C. H. & Brase, C. P. (2007). *Understanding basic statistics*. (4th ed.). Boston, MA, USA: Houghton Mifflin Company.
- Brömme, A., & Al-Zubi, S. (2003). Multifactor biometric sketch authentication. *Proceedings of the First Conference on Biometrics and Electronic Signatures of the GI Working Group BIOSIG*, 81-90. Retrieved from:

<http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.10.129&rep=rep1&type=pdf>.

- Burges, C. J. C. (1998). A Tutorial on support vector machines for pattern recognition. *Data Mining and Knowledge Discovery*, 2, 121-167. doi: 10.1023/A:1009715923555
- Chen, Y. & Ku, W. (2009). Self-encryption scheme for data security in mobile devices. *6th IEEE Consumer Communications and Networking Conference*, 1 – 5. doi: 10.1109/CCNC.2009.4784733
- Chang, C. C. & Lin, C. J. (2011). LIBSVM: a library for support vector machines. *ACM Transactions on Intelligent Systems and Technology*, 2(3).
- Cinar, O. (2012). *Android apps with eclipse* (First ed., pp. 2 – 3). New York, New York, USA: Apress, Inc.
- Cortes, C., & Vapnik, V. (1995). Support-vector networks. *Machine learning*, 20(3), 273-297. doi: 10.1023/A:1022627411411
- Creswell, J. W. (2012) *Educational research: Planning, conducting, and evaluating quantitative and qualitative research* (Fourth ed.). Boston, MA, USA: Pearson.
- Davis, F. D. (1993). User acceptance of information technology: systems characteristics, user perceptions, and behavioral impacts. *International Journal on Man-Machine Studies*, 38, 475 – 487. doi: 10.1006/imms.1993.1022
- Definition of entropy. (2013). Retrieved June 23, 2013 from <http://oxforddictionaries.com/definition/english/entropy>.
- De Luis-García, R., Alberola-López, C., Aghzout, O., & Ruiz-Alzola, J. (2003). Biometric identification systems. *Signal Processing*, 83(12), 2539 – 2557. doi: 10.1016/j.sigpro.2003.08.001
- De Marsico, M., Nappi, M., Riccio, D., & Tortora, G. (2011). NABS: Novel approaches for biometric systems. *IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews*, 41(4), 481 – 493. doi: 10.1109/TSMCC.2010.2060326
- El-Abed, M., Giot, R., Hemery, B., & Rosenberger, C. (2010). A study of users' acceptance and satisfaction of biometric systems. *IEEE International Carnahan Conference on Security Technology*, 170 – 178. doi: 10.1109/CCST.2010.5678678
- El-Abed, M., Giot, R., Hemery, B., & Rosenberger, C. (2012). Evaluation of biometric systems: A study of users' acceptance and satisfaction. *International Journal of Biometrics*, 4(3), 265-290. doi: 10.1504/IJBM.2012.047644

- Ellis, T. J., & Levy, Y. (2009). Towards a guide for novice researchers on research methodology: Review and proposed methods. *Issues in Informing Science and Information Technology*, 6, 323 – 337. Retrieved from <http://iisit.org/Vol6/IISITv6p323-337Ellis663.pdf>
- Faundez-Zanuy, M. (2005). Data fusion in biometrics. *IEEE Aerospace and Electronic Systems Magazine*, 20(1), 34 – 38. doi: 10.1109/MAES.2005.1396793
- Furnell, S.M., Dowland, P.S., Illingworth, H.M., & Reynolds, P.L. (2000). *Authentication and supervision: A survey of user attitudes*. *Computers & Security*, 19(6), 529-539. doi: 10.1016/S0167-4048(00)06027-2.
- Gamboa, H. & Fred, A. (2003). An identity authentication system based on human computer interaction behavior. *Proceedings of the Third International Workshop on Pattern Recognition in Information Systems*. Retrieved from <http://www.lx.it.pt/~afred/anawebit/articles/AFredSPIE2004.pdf>
- Gamboa, H., Fred, A. L. N., & Jain, A. K. (2007). Webbiometrics: User verification via web interaction. *Biometrics Symposium 2007*, 1 – 6. doi: 10.1109/BCC.2007.4430552
- Giot, R., El-Abed, M., & Rosenberger, C. (2009). Keystroke dynamics authentication for collaborative systems. *International Symposium on Collaborative Technologies and Systems*, 172 – 179. doi: 10.1109/CTS.2009.5067478
- Han, J., Kamber, M., & Pei, J. (2006). *Data mining concepts and techniques* (Third ed., pp. 403 – 411). Burlington, MA, USA: Morgan Kaufmann.
- Harrison, C., Sato, M., & Poupyrev, I. (2012). Capacitive fingerprinting: Exploring user differentiation by sensing electrical properties of the human body. *Proceedings of the 25th Annual ACM Symposium on User interface Software and Technology*, 537 – 544. doi: 10.1145/2380116.2380183
- Hashia, S., Pollett, C., & Stamp, M. (2005). On using mouse movements as a biometric. *Proceeding in the International Conference on Computer Science and its Applications*. Retrieved from <http://www.cs.sjsu.edu/faculty/pollett/masters/Semesters/Spring04/Shivani/shivanipaper.pdf>.
- Hearst, M.A., Dumais, S.T., Osman, E., Platt, J., & Scholkopf, B. (1998). Support vector machines. *IEEE Intelligent Systems and their Applications*, 13(4), 18 – 28. doi: 10.1109/5254.708428
- Hoggan, E., Brewster, S. A., & Johnston, J. (2008). Investigating the effectiveness of tactile feedback for mobile touchscreens. *Proceedings of the Twenty-Sixth Annual SIGCHI Conference on Human Factors in Computing Systems*, 1573 – 1582. doi: 10.1145/1357054.1357300

- Hsu, C. W., Chang, C. C., & Lin, C. J. (2003). A practical guide to support vector classification. *Technical Report Department of Computer Science National Taiwan University*, 1 – 16. Retrieved from <http://www.csie.ntu.edu.tw/~cjlin/papers/guide/guide.pdf>
- IBM X-Force. (2011). IBM X-Force 2011 mid-year trend and risk report (September 2011). Retrieved from IBM website: <http://public.dhe.ibm.com/common/ssi/ecm/en/wgl03009usen/WGL03009USEN.PDF>
- IBM X-Force. (2013). IBM X-Force 2013 mid-year trend and risk report (September 2013). Retrieved from: http://www.lsec.be/upload_directories/documents/IBM/IBM_XForce_2013_2013_report.pdf
- Jain, A. K., Griess, F. D., & Connell, S. D. (2002). On-line signature verification. *Pattern Recognition*, 35(12), 2963-2972. doi: 10.1016/S0031-3203(01)00240-0
- Jain, A.K, Hong, L., & Pankanti, S. (2000). Biometric identification. *Communications of the ACM*, 43(2), 90 – 98. doi: 10.1145/328236.328110
- Jain, A. K., Nandakumar, K., & Ross, A. (2005). Score normalization in multimodal biometric systems. *Pattern Recognition*, 38, 2270 – 2285. doi: 10.1016/j.patcog.2005.01.012
- Jain, A. K., Pankanti, S., Prabhakar, S., Hong, L., Ross, A., & Wayman, J. L. (2004). Biometrics: A grand challenge. *Proceedings of International Conference on Pattern Recognition*, 935 – 942. doi: 10.1109/ICPR.2004.1334413
- Jain, A. K., Ross, A., & Prabhakar, S. (2004). An introduction to biometric recognition. *IEEE Transactions on Circuits and Systems for Video Technology*, 14(1), 4- 20. doi: 10.1109/TCSVT.2003.818349
- James, T., Pirim, T., Boswell, K., Reithel, B., & Barkhi, R. (2008). An extension of the technology acceptance model to determine the intention to use biometric devices. In Clarke, S. (Ed.), *End User Computing Challenges and Technologies: Emerging Tools and Applications* (pp. 57-78). Hershey, PA: IGI Global.
- Jorgensen, Z. & Yu, T. (2011). On mouse dynamics as a behavioral biometric for authentication. *Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security*, 476 – 482. doi: 10.1145/1966913.1966983
- Kanneh, A. & Sakr, Z. (2008). Biometric user verification using haptics and fuzzy logic. *Proceeding of the 16th ACM international conference on Multimedia*, 937 – 940. doi: 10.1145/1459359.1459526

- Khan, S. S., & Madden, M. G. (2010). A survey of recent trends in one class classification. *Artificial Intelligence and Cognitive Science*, 188-197.
- Kohavi, R. (1995). A study of cross-validation and bootstrap for accuracy estimation and model selection. *International Joint Conference on Artificial Intelligence*, 14(2), 1137-1145.
- Kumar, A., Wong, D., Shen, H., & Jain, A. (2003). Personal verification using palmprint and hand geometry biometric. *Proceedings of the Fourth International Conference on Audio- and Video-based Biometric Person Authentication*, 668 – 678. doi: 10.1007/3-540-44887-X_78
- Lazar, J., Feng, J. H., & Hochheiser, H. (2010). Experimental research. In J. Lazar, J. H. Feng, & H. Hochheiser (Eds.), *Research methods in human-computer interaction* (pp. 19 – 40). West Sussex, United Kingdom: Wiley & Sons.
- Liu, S., & Silverman, M. (2001). A practical guide to biometric security technology. *IT Professional*, 3(1), 27-32. doi: 10.1109/6294.899930
- Luts, J., Ojeda, F., Van de Plas, R., De Moor, B., Van Huffel, S., & Suykens, J. A. (2010). A tutorial on support vector machine-based methods for classification problems in chemometrics. *Analytica Chimica Acta*, 665(2), 129 – 145. doi: 10.1016/j.aca.2010.03.030
- Manevitz, L. M. & Yousef, M. (2002). One-class svms for document classification. *The Journal of Machine Learning Research*, 2, 139-154.
- Matyas, V. & Riha, Z. (2003). Toward reliable user authentication through biometrics. *IEEE Security & Privacy*, 1(3), 45 – 49. doi: 10.1109/MSECP.2003.1203221
- Monwar, M.M. & Gavrilova, M. L. (2009). Multimodal biometric system using rank-level fusion approach. *IEEE Transactions on Systems, Man, and Cybernetics, Part B: Cybernetics*, 39(4), 867 – 878. doi: 10.1109/TSMCB.2008.2009071
- Müller, K.-R., Mika, S., Rätsch, G., Tsuda, K., & Schölkopf, B. (2001). An introduction to kernel-based learning algorithms. *IEEE Transactions on Neural Networks*, 12(2), 181 – 201. doi: 10.1109/72.914517
- Nandakumar, K., Chen, Y., Dass, S. C., & Jain, A. K. (2008). Likelihood ratio-based biometric score fusion. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 30(2), 342 – 347. doi: 10.1109/TPAMI.2007.70796
- Nazir, I., Zubair, I., & Islam, M. H. (2009). User authentication for mobile device through image selection. *First International Conference on Networked Digital Technologies*, 518 – 520. doi: 10.1109/NDT.2009.5272104

- Ngugi, B., Kahn, B. K., & Tremaine, M. (2011). Typing biometrics: Impact of human learning on performance quality. *Journal of Data and Information Quality*, 2(2), 11:1 – 11:21. doi: 10.1145/1891879.1891884
- Niinuma, K., Park, U., & Jain, A. K.. (2010). Soft biometric traits for continuous user authentication. *IEEE Transactions on Information Forensics and Security*, 5(4), 771 – 780. doi: 10.1109/TIFS.2010.2075927
- Nova Southeastern University. (2011). Institutional review board adult/general informed consent. Retrieved from <http://www.nova.edu/irb>
- Orozco, M., Asfaw, Y., Adler, A., Shirmohammadi, S., El Saddik, A. (2005). Automatic identification of participants in haptic systems. *Proceedings of the IEEE Instrumentation and Measurement Technology Conference*, 2, 888 – 892. doi: 10.1109/IMTC.2005.1604262
- Orozco, M., Graydon, M., Shirmohammadi, S., & Saddik, A.E. (2006). Using haptic interfaces for user verification in virtual environments. *Proceedings of 2006 IEEE International Conference on Virtual Environments, Human-Computer Interfaces and Measurement Systems*, 25 – 30. doi: 10.1109/VECIMS.2006.250784
- Patrick, A. S., Long, A. C., & Flinn, S. (2003). HCI and security systems. *CHI '03 Extended Abstracts on Human Factors in Computing Systems*, 1056 – 1057. doi: 10.1145/765891.766146
- Pohsiang Tsai, P., Hintz, T., & Jan, T. (2007). Facial behavior as behavior biometric? An empirical study. *IEEE International Conference on Systems, Man and Cybernetics*, 3917 – 3922. doi: 10.1109/ICSMC.2007.4414085
- Puente-Rodriguez, L., Garcia-Crespo, A., Poza-Lara, M. J., & Ruiz-Mezcua, B. (2008). Study of different fusion techniques for multimodal biometric authentication. *IEEE International Conference on Wireless and Mobile Computing, Networking and Communications*, 666 – 671. doi: 10.1109/WiMob.2008.29
- Pusara, M. & Brodley, C. E. (2004). User re-authentication via mouse movements. *Proceedings of the 2004 ACM Workshop on Visualization and Data Mining for Computer Security*, 1 – 8. doi: 10.1145/1029208.1029210
- Ross, A. & Jain, A. K. (2004). Multimodal biometrics: An overview. *Proceedings of the 12th European Signal Processing Conference*, 1221 – 1224. Retrieved from http://www.csee.wvu.edu/~ross/pubs/RossMultimodalOverview_EUSIPCO04.pdf
- Sae-Bae, N., Ahmed, K., Isbister, K., & Memon, N. (2012). Biometric-rich gestures: A novel approach to authentication on multi-touch devices. *Proceedings of the 2012 ACM Annual Conference on Human Factors in Computing Systems*, 977 – 986. doi: 10.1145/2207676.2208543

- Saevanee, H. & Bhatarakosol, P. (2009). Authenticating user using keystroke dynamics and finger pressure. *6th IEEE Consumer Communications and Networking Conference*, 1 – 2. doi: 10.1109/CCNC.2009.4784783
- Scholkopf, B., Williamson, R. C., Smola, A. J., Shawe-Taylor, J., & Platt, J. C. (1999). Support Vector Method for Novelty Detection. *Advances in Neural Information Processing Systems*, 12, 582-588..
- Schulz, D.A.(2006). Mouse curve biometrics. *Biometric Consortium Conference*, 1-6. doi: 10.1109/BCC.2006.4341626
- Shneiderman, B. & Plaisant C. (2010). *Designing the user interface: Strategies for effective human-computer interaction* (Fifth ed., pp. 70, 311 – 313). Reading, MA, USA: Addison-Wesley Publishing Co.
- Snelick, R., Indovina, M., Yen, J., & Mink, A. (2003). Multimodal biometrics: issues in design and testing. *Proceedings of the 5th International Conference on Multimodal Interfaces*, 68 – 72. doi:10.1145/958432.958447
- Stroke. (2014). In Merriam-Webster.com. Retrieved November 20, 2014 from <http://www.merriam-webster.com/dictionary/stroke>
- Sulong, A., Wahyudi, & Siddiqi, M.U. (2009). Intelligent keystroke pressure-based typing biometrics authentication system using radial basis function network. *5th International Colloquium on Signal Processing & Its Applications*, 151 – 155. doi: 10.1109/CSPA.2009.5069206
- Sutcu, Y., Sencar, H. T., & Memon, N. (2005). A secure biometric authentication scheme based on robust hashing. *Proceedings of the Seventh Workshop on Multimedia and Security*, 111-116. doi: 10.1145/1073170.1073191
- Tax, D. M., & Duin, R. P. (2002). Uniform object generation for optimizing one-class classifiers. *The Journal of Machine Learning Research*, 2, 155-173.
- Triantaphyllou, E. (2000). Multi-Criteria Decision Making Methods. In Triantaphyllou, E. (Ed.), *Multi-criteria decision making methods: A comparative study* (pp. 5 - 21). Dordrecht, Netherlands: Kluwer Academic Publishers.
- Trujillo, M. O., Shakra, I., & El Saddik, A. (2005). Haptic: the new biometrics-embedded media to recognizing and quantifying human patterns. In *Proceedings of the 13th Annual ACM International Conference on Multimedia*, 387 – 390. doi: 10.1145/1101149.1101232
- Tu, J.V. (1996). Advantages and disadvantages of using artificial neural networks versus logistic regression for predicting medical outcomes. *Journal of Clinical Epidemiology*, 49(11), 1225 – 1231. doi: 10.1016/S0895-4356(96)00002-9.

- Tullis, T. & Albert, B. (2008). *Measuring the user experience: Collecting, analyzing, and presenting usability metrics* (First ed., pp. 123 – 146). Burlington, MA, USA: Morgan Kaufmann.
- UKPS biometric enrolment trial. (2005). *Biometric Technology Today*, 13(7), 6-7. doi: 10.1016/S0969-4765(05)70368-4.
- Wang, P. S. P. & Yanushkevich, S. N. (2007). Biometric technologies and applications. *Proceedings of the 25th IASTED International Multi-Conference: Artificial Intelligence and Applications*, 226 – 231. Retrieved from: <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.72.3174&rep=rep1&type=pdf>
- Wayman, J. L. (1999). Technical testing and evaluation of biometric identification devices. In Jain, Anil K., Bolle, Ruud, & Pankanti, Sharath (Eds.), *Biometrics: Personal Identification in Networked Society*, Norwell, MA: Kluwer.
- Witten, I. H., Frank, E. & Hall, M. A. (2011). *Data mining: Practical machine learning tools and techniques* (Third ed., pp. 191 - 372). Burlington, MA, USA: Morgan Kaufmann.
- Yager, N. & Dunstone, T. (2010). The biometric menagerie. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 32(2), 220 – 230. doi: 10.1109/TPAMI.2008.291
- Yampolskiy, R. V. (2007). Human computer interaction based intrusion detection. *Fourth International Conference on Information Technology*, 837 – 842. doi: 10.1109/ITNG.2007.101
- Yampolskiy, R. V. & Govindaraju, V. (2008). Behavioral biometrics: A survey and classification. *International Journal of Biometrics*, 1(1), 81 – 113. doi: 10.1504/IJBM.2008.018665
- Yoder, B. L. (2013). Engineering by the numbers. American Society for Engineering Education, 11 – 47. Retrieved from http://www.asee.org/papers-and-publications/publications/14_11-47.pdf.
- Yu, H. (2003). SVMC: single-class classification with support vector machines. *Proceedings of the 18th international joint conference on Artificial intelligence*, 567-572.
- Zhang, D. & Zuo, W. (2007). Computational intelligence-based biometric technologies. *IEEE Computational Intelligence Magazine*, 2(2), 26 – 36. doi: 10.1109/MCI.2007.353418