# NEW AUTHENTICATION USING SYMBOL-BASED PASSWORD COMBINED WITH KEYSTROKE DYNAMICS

Mr. Nattapong Jeanjaitrong

A Thesis Submitted in Partial Fulfillment of the Requirements
for the Degree of Master of Science Program in Computer Science and Information Technology
Department of Mathematics and Computer Science
Faculty of Science
Chulalongkorn University
Academic Year 2013

# การระบุตัวตนแบบใหม่โดยใช้รหัสผ่านเชิงสัญลักษณ์ร่วมกับพลวัตการเคาะแป้นพิมพ์

นายณัฐพงศ์ จีนใจตรง

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต
สาขาวิชาวิทยาการคอมพิวเตอร์และเทคโนโลยีสารสนเทศ ภาควิชาคณิตศาสตร์และวิทยาการคอมพิวเตอร์
คณะวิทยาศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
ปีการศึกษา 2556

| | |
|---|---|
| Thesis Title | NEW AUTHENTICATION USING SYMBOL-BASED PASSWORD COMBINED WITH KEYSTROKE DYNAMICS |
| By | Mr. Nattapong Jeanjaitrong |
| Field of Study | Computer Science and Information Technology |
| Thesis Advisor | Assistant Professor Pattarasinee Bhattarakosol, Ph.D. |

Accepted by the Faculty of Science, Chulalongkorn University in Partial Fulfillment of the Requirements for the Master's Degree

................................................................................Dean of the Faculty of Science

(Professor Supot Hannongbua, Dr.rer.nat.)

THESIS COMMITTEE

................................................................................Chairman

(Assistant Professor Nagul Cooharojananone, Ph.D.)

................................................................................Thesis Advisor

(Assistant Professor Pattarasinee Bhattarakosol, Ph.D.)

................................................................................External Examiner

(Adisak Sukul, Ph.D.)

ณัฐพงศ์ จีนใจตรง : การระบุตัวตนแบบใหม่โดยใช้รหัสผ่านเชิงสัญลักษณ์ร่วมกับพลวัตการเคาะแป้นพิมพ์. (NEW AUTHENTICATION USING SYMBOL-BASED PASSWORD COMBINED WITH KEYSTROKE DYNAMICS) อ.ที่ปรึกษาวิทยานิพนธ์หลัก: ผศ. ดร. ภัทรสินี ภัทรโกศล, 119 หน้า.

ปัจจุบัน อุปกรณ์พกพาประเภทโทรศัพท์มือถือสมาร์ทโฟนหรือแทบเล็ต ได้กลายเป็นส่วนหนึ่งในชีวิตประจำวันของผู้คนส่วนใหญ่ ซอฟต์แวร์ประยุกต์ เพื่อช่วยอำนวยความสะดวกในหลายๆ ด้านได้ถูกพัฒนาขึ้นและใช้กันอย่างแพร่หลาย ไม่ว่าจะเป็นซอฟต์แวร์ประยุกต์ที่เกี่ยวข้องกับธุรกรรมทางการเงิน หรือแม้แต่การสำรองข้อมูลรหัสบัตรเครดิต บัตรเอทีเอ็มต่างๆ ไว้บนอุปกรณ์ อุปกรณ์พกพาเหล่านี้ถูกใช้เป็นแหล่งสำรองข้อมูลสำคัญของผู้ใช้ ซึ่งข้อมูลนั้นเสี่ยงต่อการถูกโจรกรรมเป็นอย่างมาก ระบบยืนยันตัวตนจึงเข้ามามีบทบาทในการช่วยคัดกรองระหว่างผู้ใช้จริงกับปลอม แต่ถึงกระนั้นแล้ว การใช้ปัจจัยเพียงอย่างเดียวเพื่อยืนยันตัวตน เช่น ชื่อผู้ใช้หรือรหัสผ่าน อาจไม่เพียงพอเมื่อเปรียบเทียบกับเทคโนโลยีทางอาชญากรรมที่ก้าวหน้าขึ้น ดังนั้น การผสมผสานการใช้หลายปัจจัยเพื่อยืนยันตัวตนบุคคลจึงเป็นทางเลือกที่ดีกว่า ในระบบการยืนยันตัวตนนั้น ชนิดของปัจจัยที่ใช้มีหลายประเภท หนึ่งในนั้นคือการใช้สิ่งที่ผู้ใช้เป็นอยู่มาเป็นปัจจัย หรือก็คือ ข้อมูลชีวมาตร ข้อมูลชีวมาตรเป็นปัจจัยที่สามารถใช้บ่งชี้ตัวผู้ใช้ได้ หนึ่งในข้อมูลชีวมาตรทางพฤติกรรมที่มีการใช้อย่างแพร่หลายคือพลวัตรการเคาะแป้นพิมพ์ แต่พลวัตรการเคาะแป้นพิมพ์นั้นโดยปกติจะกระทำบนแป้นพิมพ์จริง จึงเป็นหัวข้อที่น่าสนใจหากจะนำกลไกของพลวัตรการเคาะแป้นพิมพ์มาใช้บนอุปกรณ์พกพาระบบหน้าจอสัมผัส นอกจากนั้นแล้ว การใช้รหัสผ่านเชิงสัญลักษณ์แทนรหัสผ่านแบบดั้งเดิมก็เป็นตัวเลือกที่น่าสนใจ เพื่อเพิ่มความปลอดภัยในขึ้นตอนของการยืนยันตัวตน ดังนั้น งานวิจัยชิ้นนี้จึงมุ่งเน้นการผสมผสานการใช้รหัสผ่านเชิงสัญลักษณ์ ร่วมกับพลวัตรการเคาะแป้นพิมพ์ รวมถึงปัจจัยพฤติกรรมทางชีวมาตรอื่นๆ ที่สามารถรับค่าได้จากอุปกรณ์พกพามือถือหน้าจอระบบสัมผัส ผลงานวิจัยนี้พบว่า การผสมผสานการใช้งานรหัสผ่านเชิงสัญลักษณ์ ร่วมกับพลวัตรการเคาะแป้นพิมพ์และปัจจัยพฤติกรรมทางชีวมาตรอื่นๆ ให้ความแม่นยำในการระบุตัวตนได้ค่อนข้างสูง และสามารถนำไปปรับใช้บนอุปกรณ์พกพาหน้าจอระบบสัมผัสได้จริง

ภาควิชา คณิตศาสตร์และวิทยาการคอมพิวเตอร์

ลายมือชื่อนิสิต ..................................................

ลายมือชื่อ อ.ที่ปรึกษาวิทยานิพนธ์หลัก ..............

สาขาวิชา วิทยาการคอมพิวเตอร์และเทคโนโลยีสารสนเทศ

ปีการศึกษา 2556

# # 5572603123 : MAJOR COMPUTER SCIENCE AND INFORMATION TECHNOLOGY
KEYWORDS: KEYSTROKE DYNAMIC / TOUCHSCREEN / SYMBOL-BASED PASSWORD / BEHAVIORAL BIOMETRIC

NATTAPONG JEANJAITRONG: NEW AUTHENTICATION USING SYMBOL-BASED PASSWORD COMBINED WITH KEYSTROKE DYNAMICS. ADVISOR: ASST. PROF. PATTARASINEE BHATTARAKOSOL, Ph.D., 119 pp.

Presently, mobile devices such as Smartphone or tablet become a part of people’s life. Many facilitate applications has been developed and widely used on those devices, such as financial transaction application, virtual credit and debit card application. These devices are used as personal information storage for users which that information is high risk for being stolen. The authentication process was brought to authenticate between the real user and intruders. Thus, using only single-factor authentication such as username or password might not be enough compared to the high-technology crimes. So, using multi-factor in authentication process is a better way. In the authentication process, there are many types of factors. One of the types of factors is using something that people are, Biometrics. Biometrics is a unique factor which can be used to identify a person. One of the most using behavioral biometrics is keystroke dynamics. Unfortunately, the keystroke dynamic mechanism usually works on an actual keyboard. So it is an interesting issue to apply the keystroke dynamic mechanism onto the touchscreen mobile device. Furthermore, using a symbol-based password instead of the traditional password is an interesting option to increase higher security in the authentication process. So, this research focuses on the use of combination between symbol-based password with keystroke dynamics, included other behavioral biometrics which can be retrieved from the touchscreen mobile device. The result of this study shows that using the combination of the symbol-based password with keystroke dynamics and other behavioral biometrics provides a high accuracy in the authentication process and can be used in an actual touchscreen mobile device.

Department: Mathematics and Computer Science
Field of Study: Computer Science and Information Technology
Academic Year: 2013

Student's Signature ....................................
Advisor's Signature ....................................

## ACKNOWLEDGEMENTS

I would like to express my deep gratitude to Asst. Prof. Pattarasinee Bhattarakosol, Ph.D., my research adviser, for her patient guidance, enthusiastic encouragement and useful critiques of this research work.

Beside my adviser, I am particularly grateful for the assistance given by Assistant Professor Nagul Cooharojananone, Ph.D. and Adisak Sukul, Ph.D., my thesis committee.

I would like to express my very great appreciation to Professor Aizawa Akiko from National Institute of Informatics, Japan (NII), my research adviser while i'm an internship student at Japan, for her support and concern of my thesis even the topic of internship's research and my thesis are different.

My special thanks are extended to all of my friends who have participate in my research as a subject in the experiment.

Finally, I wish to thank my parents and friends for their support and encouragement throughout my study.

## CONTENTS

Page

Page

Page

## LIST OF ILLUSTRATIONS

Page

# LIST OF TABLES

# CHAPTER I
# INTRODUCTION

This chapter consists of information about the background and importance of this research. It is also included objective, scope of this study, its constraints, and expected outcome of the experiment. To make all readers clearly understand all contents, some of important keywords have been described in the definition section. Lastly, the structure of leftover chapters has been explained in the last section of this chapter.

## 1.1 Background and Importance

Currently, people cannot deny that mobile device is becoming a part of their life. From mobile phone to computer tablet, people communicate to each other through these devices. Since technology is developing rapidly, many activities beyond communication can be performed on those devices. Many applications have been developed to serve people comfortable, such as money transaction, password storage, and email accessing, etc. Developed as fast as technology, crime also developed in the same speed. With some sort of defect on technology and user's careless on the fundamental authentication method, user's stored information may be robbed very easily.

In the authentication process, there are three factors that use to identify users to the system: a knowledge factor, a possession factor, and an inherence factor. The first factor is something that the user knows just like username or password. The second factor is involving about something that the user has. The last factor is about something that user is. Currently, most of authentication method on mobile device is only just the knowledge factor, like passcode. Many researches show the results of using multi-factor in authentication phase provide a better result due to the increasing of the security issue.

Keystroke dynamics on keyboard has been proved that can be used as a behavioral biometric, which is one type of factors that can be used in authentication process. Biometrics, both physical and behavioral, is unique factor from human which can use to identify person to each other with a very effective performance.

From those reasons above, this thesis concentrate in the study about a chance to use multi-factor authentication on mobile devices by studying the feasibility of using keystroke dynamic on touch-screen device, including the study of other factors that may helpful in authentication along the keystroke dynamics. This also studies about the use of symbol-based password combining with keystroke dynamics mechanism to increase accuracy to the system.

## 1.2 Objective

This thesis has aims to perform the following tasks

1) To increase authentication accuracy using a combination of symbol-based password and keystroke dynamics mechanism.
2) To replaced CAPTCHA method with new authentication mechanism.

## 1.3 Scope of Thesis and Constraint

There are many types of biometrics which can be used in authentication mechanism. This research only focuses on behavioral biometrics. The behavioral that has been selected to study is keystroke dynamic due to the limitation of factor that can be retrieved from device. The following list is the scope and constraint of this research.

1) The sample size of this subject is 25 persons who have iPhone smartphone.
2) Age range of subject is between 21 to 30 years old due to the maturity and familiar with new gadget and technology.
3) The data collecting application is developed based on web-based application.
4) iPhone smartphone has been selected to use in the research due to the its size which can be used as control variable.
5) The password that has been delivered to all subjects is the same.
6) Each subject has to do the task of pressing password on application for at least 3 times a day with a minimum length of 4 hours.

7) In each time of doing the task, subject has been assigned to press the password on the screen with 3 posture of hand-gripping. All hand posture will appear by randomly.

## 1.4 Expected Outcome

1) The combination of symbol-based password and keystroke dynamics mechanism can increase the accuracy to the authentication process.
2) This new authentication mechanism can replaced CAPTCHA method.

## 1.5 Definition

In the data collecting and analyzing process on this research, there is some of keyword that reader might not familiar with. This section will give a short explanation of those keyword so reader will more understand when found it in the further chapters.

**Dwell Time** : The time that subject used to press and release a symbol (password), as show in Figure 1-1.

**Interval Time** : The time that subject used to move from the previous symbol to the next symbol, as show in Figure 1-1.

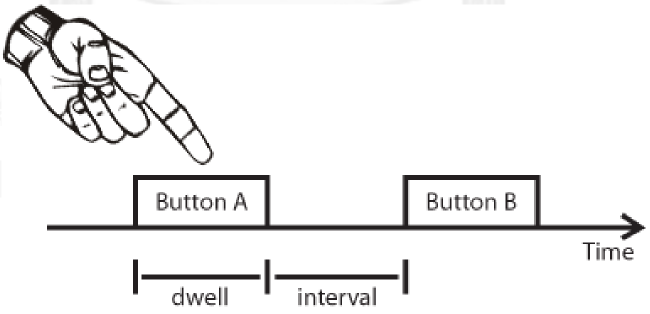


**Figure 1-1 Illustration of Dwell Time and Interval Time**

**Interval Timing Ratio** : A ratio between interval time and the time that using on that round (total time)

**Distance** : In each button of password, the area of button has been separated into small grid. The distance in this experiment means a length from one button of password to the next button of password by calculating from the position that has been pressed on that particular button, shown as a line in Figure 1-2.

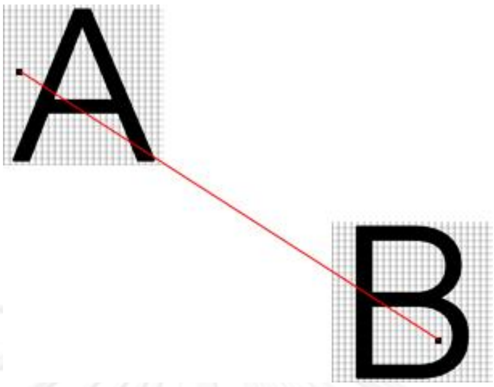


**Figure 1-2 Illustration of distance between button A and B**

## 1.6 Thesis Structure

The remaining part of this thesis consists of four chapters. Chapter 2 describes about fundamental knowledge and literature review which related to this study. Chapter 3 consists of information about methodology of this study and data collecting application. Result of data after collecting and analyzing will be showed on Chapter 4. Lastly, Chapter 5 will present the discussion and conclusion of all study.

# CHAPTER II
# FUNDAMENTAL KNOWLEDGE AND LITERATURE REVIEW

This chapter provides the fundamental knowledge and literature review which support this thesis. The background of authentication is describes in Section 2.1. The fundamental knowledge of Biometrics is provided in Section 2.2. Section 2.3 represents the information of keystroke dynamic. And finally, literature review is stated in Section 2.4.

## 2.1 Authentications

'Authentication' is the Greek word ***'αὐθεντικός'*** means the acting or processing to confirm and identify the truth of individual or attribute. In security system, authentication is a process to confirm a truly identity of a person or user by giving their identity documents or objects to the system. Authentication process can be shown in variety way such as using a digital certificate in validating a website or using a carbon dating to prove the age of an artifact. Authentication is different from Authorization. Normally, authorization will occur after the process of authentication [1, 2].

Authentication is normally performed through using logon password [3]. The knowing of that particular username and password is assumed to guarantee the user's authentic, which those username and password can be assigned information from automatic system or user's self-declared.

In authentication process, there are 3 types of factor that can be used to identify people. Each authentication factor consists of a different range of elements that are used to authenticate or verify the identity of a person. Each type of authentication factors requires a different way of using. The use of each authentication factor may just a simple asking of identity id or more complex methods like signing an actual document. These 3 types are:

1) **Knowledge factors** : something that the user **knows**, such as password, pin code, etc.

2) **Ownership factors** : something that the user **has or possess**, such as an ID card, token, etc.

3) **Inherence factors** : something that the user **is** or **does**, which is biometrics, such as DNA sequence, retinal, fingerprint, or even behavioral such as keystroke dynamic, etc.

Normally, only one factor will be used in the authentication process. However, in some system requires more than one factor in the authentication process, called *Multi-Factor Authentication*. The example of using multi-factor authentication is using a passcode combine with a keycard to turn on a laptop or using a combination of biometrics factors to access the system. There are several researches that show the efficiency of using multi-factor authentication. Esla et al [4] presented a method which combine fingerprints and user-specific random projection to generate a pattern for use in authentication process. They evaluate the performance of the proposed system using the Receiver Operating Characteristic (ROC) curves. Results show a very low error equal rate (EER) at 0.4%. Hisham et al [5] proposed a method that uses a multi-factor biometrics in the authentication process. They use fingerprint, iris, and face as a factor in their proposed system. The results show that using two biometrics factors in authenticating provides the best result which is near zero of error equal rate (EER).

Authentication is one of the methods which can increase the security in computer system with a high accuracy of user classification.

## 2.2 Biometrics

Biometrics (Greek word “Bio” and “Metric”), meaning “life measurement”, are the measuring of human characteristics and traits that are used as an identification in computer science. Biometric identifiers are unique and used to label and describe each user. There are two types of biometrics which are physiological (physical) biometrics and behavioral biometrics. Physiological biometrics are related to the outer shape of particular organ, such as face shape, hand, ear shape, lip, and also included fingerprint, iris, retina, DNA, etc. as shown in Figure 2-1. Behavioral biometrics is related to pattern of behavior of a person, such as keystroke, signature, voice, etc. [6, 7]

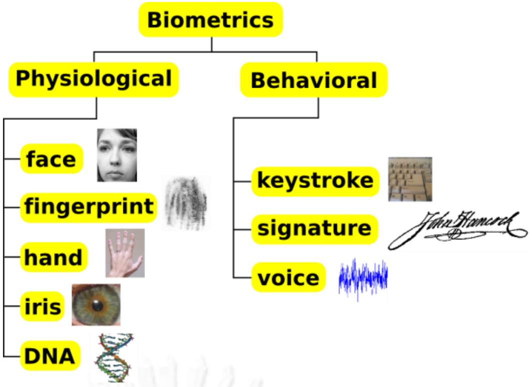


Figure 2-1 Types of Biometrics

Biometrics is the one of many authentication methods which was accepted that affective due to its reliable and safe [8]. There are several researches that studying about keystroke dynamics which is one kind of behavioral biometrics. H. Saevanee and P. Bhattarakosol [9] proposed a method which used keystroke dynamic combine with finger pressure in authentication. Saevanee and Bhattarakosol combine these two factors and study the feasibility of being a behavioral biometrics using machine learning, Probabilistic Neural Network (PNN). The result gives an accuracy of authentication at 99%. Giroux et al. [10] also proposed a method that used a keystroke dynamics to give a high accuracy of authentication. Giroux et al adapted the use of keystroke dynamic into a keypress interval timing ratio, which provided a low false acceptance rate (FAR) and false reject rate (FRR). Same as ERR rate, the low FAR rate and FRR rate gives a better accuracy of system.

Biometrics is now popular to be used as a factor in the authentication process. The results of verifying the identity of person by biometrics are quite accurate and reliable because it is difficult for an imposter to reproduce the identity of physical or behavior of a person to use in the authentication process.

## 2.3 Keystroke Dynamics

Keystroke dynamics, which is considered as one of the behavioral biometrics, is the information of timing when typing on a keyboard. That information is the time that the key was pressed or released [11]. Keystroke dynamics is the technology that used to separate individual among users based on person’s manner when typing on a keyboard, which is considered that there is a characteristic way of person when types on a keyboard [12]. In short term, keystroke dynamics are the patterns of rhythm and timing that created when person types [13].

The concept of using keystroke dynamics as a behavioral biometrics is based on the measurement of individual's typing rhythm. It collects the interesting features of typing pattern from particular user. The examples of features are the time that pressing a key, the time that releasing a key, the total time that a user spend on typing username and password, and the length of time when a user types successive keys. These pattern and features are believed to be presented the uniqueness of an individual and it should be very difficult for attackers to copy or duplicate [14].

The origin of keystroke dynamics go back to the early days of telegraph, when persons developed distinctive patterns that identified them. This pattern was known as a telegraph operator's "fist". During World War II, a methodology known as the "fist of the sender" helped to identify the source of Morse code and confirm that a particular message was, in fact, from a valid source.

The studies on keystroke dynamics in computer science have been proposed since the past few decades. In 1985, the experiment of Umphress et al. [15], which conducted with the group of seventeen people who were experienced programmers but the range of typing skills are from experienced touch-typists to those with no formal typing skills. This research's results indicated that the timing aspects and rhythm of typing can be used to identify a person in verification process. Moreover, several researchers have developed an authentication system based on keystroke dynamics to strengthening traditional password verification [16-18]. The studies on keystroke dynamics have not only focused on the adapting this biometric with the use of password but some studies also have focused on applying it with the long-text input [19].

### 2.4 Literature Review

Authentication process is becoming an important process in most systems due to various attacks to the system in present day. Unfortunately, using only single factor in the authentication process obviously seems to be unsecure. Multi-factor authentication in the authentication process has been used more widely, such as a research from Ren and Wu [20] who use two-factor in their proposed system. Ren and Wu use the combination of ownership factor (something user's has or possess in that particular time) which is MAC address of user's to be the source of OTP generating. With the combination of those possess factors and time factor synchronization, they conclude that their authentication schemes provide a more secure and low overhead authentication manner. Additionally, it is also secure enough to confront with many attacks.

There are many researches study about using keystroke dynamics as a factor in the authentication mechanism. Pin Shen The et al [21] proposed a new method of using keystroke dynamics by calculating the dwell time and the flight time of user's key pressing and calculate mean and standard deviation. After they received all features from keystroke, they classify user by Gaussian similarity score and Direction Similarity Measure (DSM). The result shows that the combination of dwell time and flight time shows a better result than using individually.

Karnan and N.Krishnaraj [22] also studies about using keystroke dynamics as a factor in authentication mechanism. They asked users to type a pin code to collect the interested factor from keystroke dynamics, which are duration, latency, and digraph. By performing an optimization technique such as particle Swam Optimization (PSO), Genetic Algorithm (GA), and Ant colony Optimization (ACO), those data are classified by Back propagation Neural Network (BPNN) algorithm. The conclusion of this study shows that the combination of all features gives a high accuracy with low error rate. Nonsrichai and Bhattarakosol [23] also proposed a new authentication using the combination of keystroke dynamics and the eye vision ability as a multi-factor biometrics. In [23], attributes that retrieved from web applications can be divided into two parts, the keystroke part and the eye visual part. In the keystroke part, the dwell time and the interval time are captured. In the eye vision part, the retrieval of the vision time, the dwell time and also the interval time are performed. [23] proposed that the relation of hand in keystroke dynamics and the eye vision can provide the better accuracy.

Morris Chang et al [24] also proposed the use of keystroke dynamics in the authentication process. Chang uses two different classifier techniques to build two different authentication system, which is support vector machine (SVM) and kernel ridge regression (KRR). The data which has been collected while users type on desktop considered as three types, short sentence, short essay, and web browsing. The result from Chang experiment shows the effective with a low value of FAR and FRR from both SVM and KRR. Chang also leads to an opinion that this mechanism is very interesting to do the experiment on a mobile phone device.

There is an interesting research from Chang et all [25] about using a graphical-based password combined with keystroke dynamics in authentication for touchscreen handheld mobile device. They use the combination of graphical-based password with time and pressure which retrieved from user's password pressing. By multi-factor authentication in the process, even the password which is graphical-based has been stole from shoulder surfing attack (SSA), their system still have a full protection from intruders due to the combination of keystroke dynamics features.

Besides the interesting issue which this thesis related to, there is some study that also an interesting issue for this thesis. Hoober [26] has studied about how user's interact with their mobile phone. Figure 2-2 shows the summary of how people hold and interact with their mobile phones.

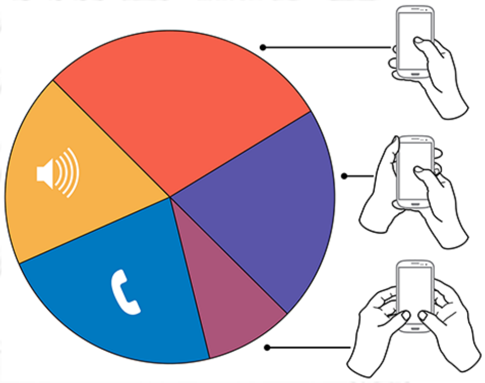


Figure 2-2 Summary of how people hold and interact with mobile phones

Hoober observes about user's hand posture while they are interacting with it. The result of observation shows that each user has many postures with their device due to the activity that they are currently do. The user who Hoober observed held their phone in three basic ways, one handed, cradled, and two handed.

According to Hoober's research, each posture of device holding also has a slightly different detail. Such as one-handed holding, users tend to use right thumb on the screen for 67% and left thumb on screen for 33%. Also with cradling which users tend to use thumb on screen for about 72% and use finger on the screen for about 28%. And user who cradling with left hand is about 79% while cradling with right hand for 21%. Also with two-handed posture which user for about 90% hold it in portrait mode and 10% hold it in landscape mode.

This information of device’s holding is very interesting and it might be able to use as one of the authentication factor, which needed to be study more.

There still are many researches that studying in the use of the multi-factor authentication and biometrics. The target of all studies is trying to find a new method to increase security in the authentication process based on a new and unique factor that may prevent the traditional attack. Therefore, this study will focus on using the combination of keystroke dynamics and other behavioral biometrics, based on the touch-screen mobile devices.

# CHAPTER III
# METHODOLOGY

To propose this new authentication mechanism by using the combination of keystroke dynamic and symbol-based password, the specific application has been designed for collect the data. The structure of overall system will be demonstrated by using use case diagrams, class diagrams, sequence diagrams, activity diagrams, and others information which helpful to explain this proposed mechanism.

## 3.1 Preliminary Experiment and Results

There preliminary experiment is an experiment to test the hypothesis of performance comparing between an actual keyboard and touchscreen device. This result is a part of study from Jeanjaitrong and Bhattarakosol [27]. In the experiment, 10 subjects are assigned to press 4 symbol-passwords on the touchscreen mobile device (Figure 3-1). The experiment collects data which can be calculated into dwell time, interval time, interval timing ratio, and distance.

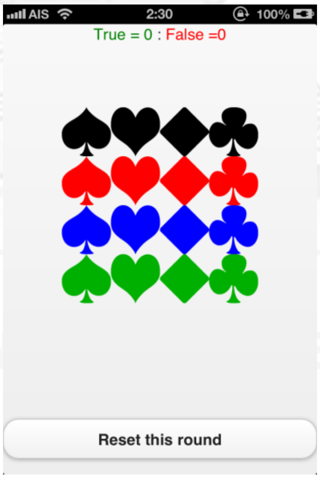


Figure 3-1 Password Pressing Screen of Preliminary Experiment

In their experiments also set another experiment which use 10 same subjects to type on an actual keyboard, by typing 4 characters password on the screen. This second application collects data which be calculated to dwell time and interval time.

Both set of results from two experiments is classified into user's correct class by Bayesian Network from Weka® Machine Learning. The result from learning machine can show as Table 3-1.

**Table 3-1 The comparing of accuracy indicator between an actual keyboard and touchscreen device.**

| Keystroke Dynamic Device | Accuracy Indicator | | |
|---|---|---|---|
| | Dwell Time FAR | Dwell Time FRR | Dwell Time Accuracy (%) |
| Actual Keyboard | 0.060 | 0.498 | 50.23 |
| Touchscreen Device | **0.050** | **0.447** | **55.29** |
| | Interval Time FAR | Interval Time FRR | Interval Time Accuracy (%) |
| Actual Keyboard | 0.046 | 0.391 | 60.93 |
| Touchscreen Device | **0.042** | **0.374** | **62.64** |
| | Dwell + Interval FAR | Dwell + Interval FRR | Dwell + Interval Accuracy (%) |
| Actual Keyboard | 0.027 | **0.223** | **77.67** |
| Touchscreen Device | **0.026** | 0.236 | 76.44 |

The preliminary results from this research shows that the accuracy indicator from an actual keyboard and a touchscreen device is pretty much nearing to each other. The conclusion confirms that the keystroke dynamics mechanism can be applied on the touch-screen mobile, with the efficiency as equal as on the actual keyboard, based on the result from Table 3-1. This thesis is the extended study from this work, using almost the same procedures with more of interesting factors.

### 3.2 Experimental Design

This research mainly focuses on using the combination of keystroke dynamics and a symbol-based password. So, the specific application has been developed to collect interesting factors from any mobile screen device. These interesting factors are pressing position and keystroke. The pressing position has been retrieved from the coordinated x and y which can be detected on the mobile screen and keystroke can be calculated from times that user pressed and released on the screen. Since this experiment focused on iPhone, due to the strict of iOS application store which has a lot of complication, this application has to choose other ways to developed. Web-based application, especially on iOS web-based application, has an ability to gather all of interesting factors and have much less complication compared to the native application. So, the specific application has been developed based on web.

By focusing on the use of a symbol-based password, special symbols have been selected to use as password. These experiments, geometric shapes that have been selected are triangle, circle, x mark, and square. These symbols are the simple geometric shape that can be easily to distinguish by users. In addition, the use as a label of button on game controllers of a well-known game console, Playstation® (Figure 3-2). Each shape has been assigned to 4 colors, which are red, green, blue, and black. These colors have been selected from the model of RGB color that has been used in most of the mobile phone display.

Figure 3-2 Playstation® Game Controller Button Label

With 4 different shapes and 4 different colors, 16 different symbols has been used as a main keypad of data collecting system. The password of this system that has the length of 4 has been determined from those symbols. Every subject will be assigned to use the same password. While pressing the sequence of password, every subject must hold a device and press on a screen in the determined postures that the order of it will be random in each time of data collecting. Those postures are one handed, cradled, and two handed (Figure 3-3).

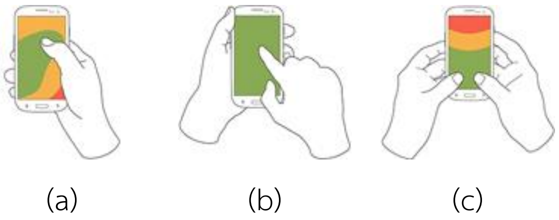


Figure 3-3 Device grip postures

(a) One Handed (b) Cradled (c) Two Handed

Before beginning the collecting of data, each subject will have to register to the system. In the register progress, vital information of each subject will be collected, those are age, gender, device model, handedness, most device's gripping posture, etc.

After logging in to the data collecting system, each subject will hold the device in the posture follows the system. In each hand posture, the subject has to press the sequence of password for 5 rounds. After finishing, the system will inform the subject to change the posture of hand gripping. The subject has to complete all of hand-posture, which are 15 rounds of sequence-password pressing in total. That's 1 time of data collecting. The subject must perform this task for 3 times per one day, which can be explained as a chart as below:

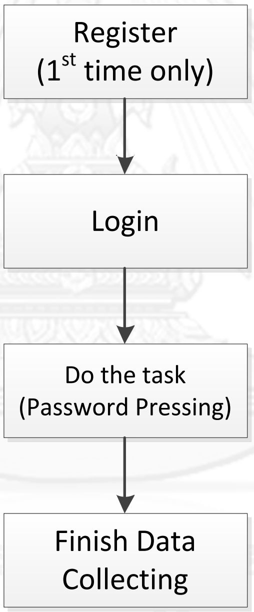


Figure 3-4 Process of Data Collecting for 1 time

- Register : The subject who just start using this system for the first time has to register to the system before beginning the data collecting process.
- Login : After finishing the register process, the subject has to login to the system by typing their username. If the username is correct, the subject can proceed to the next step of process.
- Do the task : In this step, the subject will be informed by the system about the hand-posture. After that, the subject will enter to the password-pressing

page. The subject has to press the password following the given one. Each hand posture, the subject has to press the correct password for 5 rounds. The subject has to finish all 3 hand postures of password pressing.

- Finish Data Collecting : After finishing all hand postures of the password pressing, system will count this whole process as a finishing of 1 time data collecting. The subject has to perform this task for 3 times a day in a different time of day.

### 3.3 Flow Chart

The working of data collecting process can be explained in flow chart Figure 3-5 as follow:

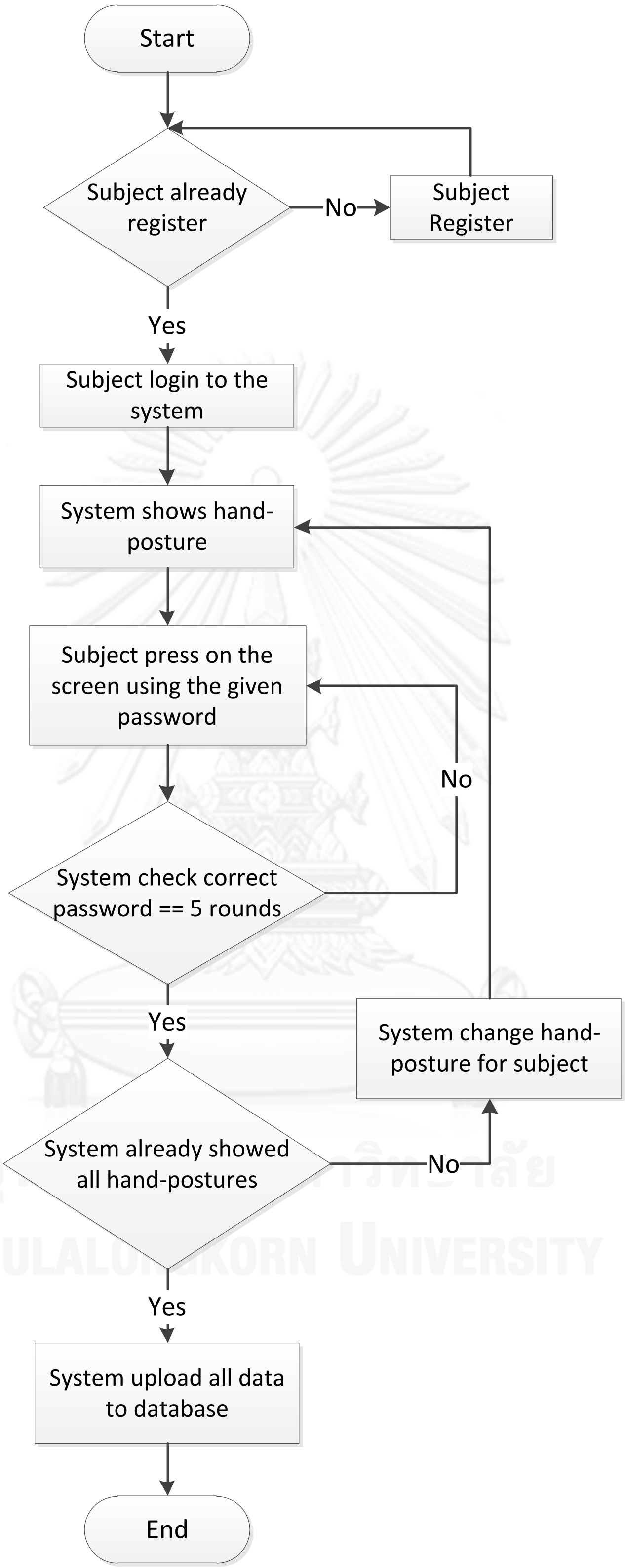

Start
Subject already register
No
Subject Register
Yes
Subject login to the system
System shows hand-posture
Subject press on the screen using the given password
No
System check correct password == 5 rounds
Yes
System change hand-posture for subject
System already showed all hand-postures
No
Yes
System upload all data to database
End

Figure 3-5 Flow Chart of the Data Collecting Process

From Figure 3-5, the process will start from registration process. The system will ask for the Username of the subject. If the subject already has it, the work flow will continue. If the subject still has no the Username, it means that the subject still does not register to the system. So, the subject needs to register before proceeding to the next process, which is logging in to the system. After logging in to the system, the system will check that the input Username matches with the Username that collected in the database or not. After passing through the login process, the process of data collection will begins. The data collecting process begins by the showing of hand postures that the subject needs to hold the device in that posture. After that, the password pressing screen will be displayed. The subject has to press the password which has been provided since the registration process. The subject must press the password correctly according to the color and order of the password. After 5 correct rounds of the password pressing, the system will change the hand posture. The system requires subject to press the password until all hand postures are completed, and then all data that have been collected will be uploaded to the database. After that, the system will inform the subject the status of data upload, and that is the finish of password collecting for 1 round.

### 3.4 Use Case Diagram

The data collecting system, that has been described as above, can be illustrated as a use case diagram in Figure 3-6.

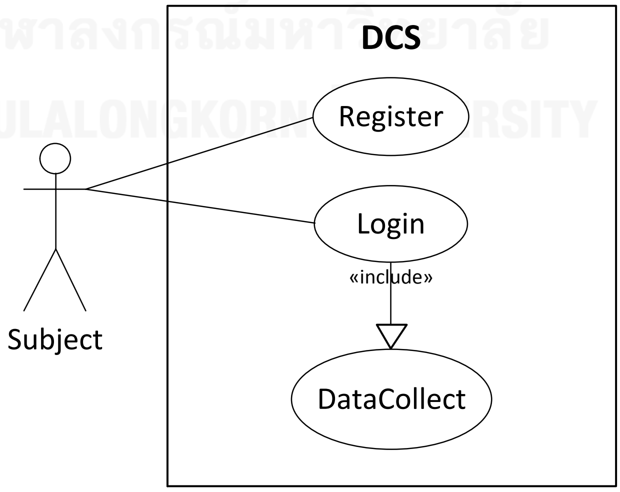


**Figure 3-6 Use Case Diagram of Data Collecting System**

### 3.4.1 Template of Use Case

Name : Data Collecting System
Participant Actor : Subject
Entry Condition : Subject starts system
Flow Event:

1. Subject registers to the system
2. Subject logins to the system
   2.1 Subject starts doing DataCollect

Exit Condition : Subject finishes DataCollect

### 3.4.2 Scenario of Use Case

Name : Data Collecting System
Participant Actor : Piti
Entry Condition : Piti starts system
Flow Event:

1. Piti registers to the system
2. Piti logins to the system
   2.1 Piti starts doing DataCollect

Exit Condition : Piti finishes DataCollect

### 3.5 Class Diagram

This data collecting system contains 4 main classes: the Subject class, the AppPage class, the DataList class, and the UserList class. The relationship between each class can be shown as follows:

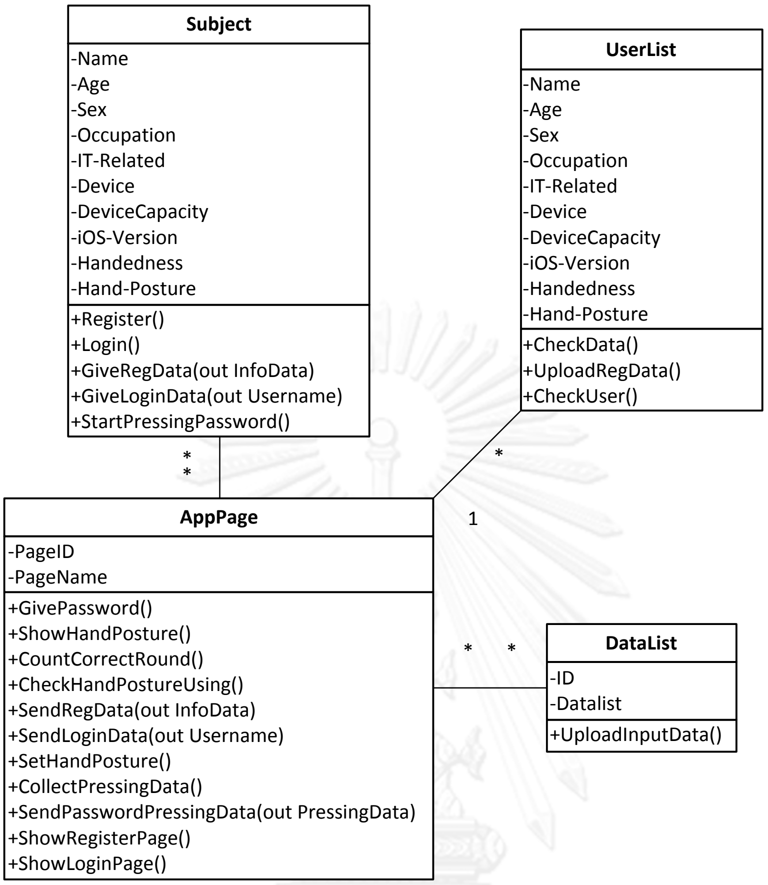


**Figure 3-7 Class Diagram of Data Collecting System**

Figure 3-7 can be described that this system consists of four classes, which are the Subject class, the UserList class, the AppPage class, and the Datalist Class. The Subject class means the subject who participates in this experiment; attributes that are defined in the class are personal information of the subject. Methods that subjects can do are register to the system, login to the system, give their data in register process, give their username in login process, and start doing the password pressing for this system. All of subject’s information will be collected in the UserList class, which has the same attributes with the Subject class. The UserList class stores the information that sent from the Subject class, and also checked the data in the login and password pressing process. AppPage class is the class that contains all pages show to the subject along the registration process and the password pressing process. The AppPage, is the main class that manages all tasks in this system, both the registration process and the password pressing process. The data from the password pressing process will be sent to the DataList class which has a function to upload the list of pressed-password to the database.

### 3.6 Sequence Diagram

In this system, the main process has been split into 2 sequence diagrams, which are the sequence of registration and the sequence of logging into the system, including doing the task. These sequence diagrams can be explained as follows:

#### 3.6.1 Sequence Diagram of Registration

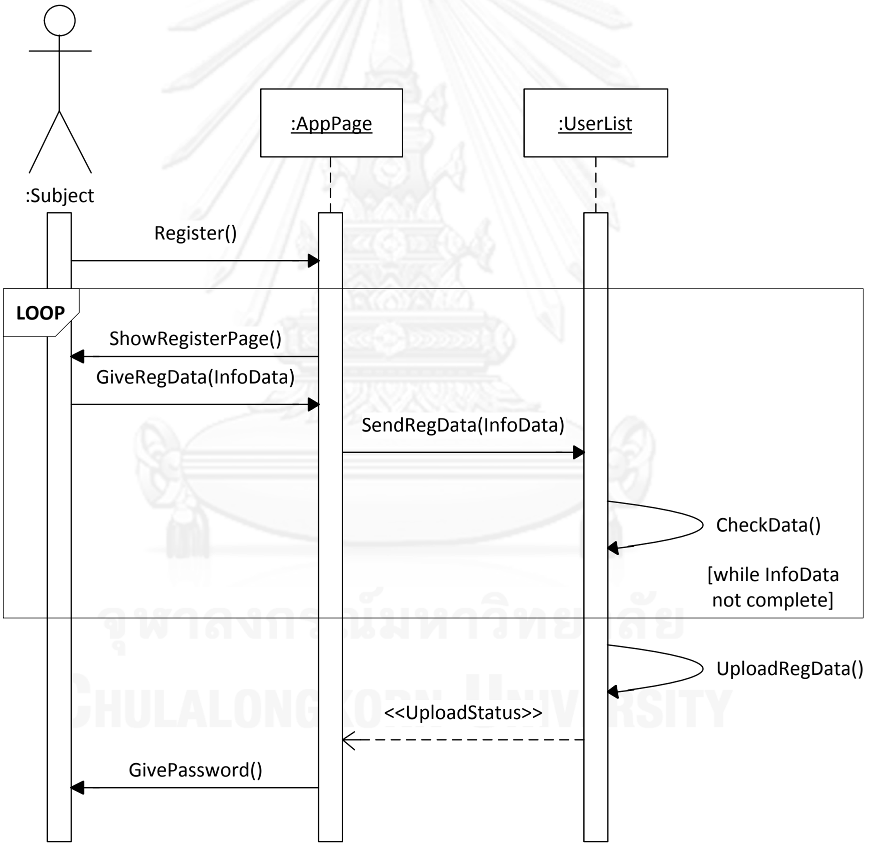


Figure 3-8 Sequence Diagram of Registration

*Processing Narrative*

This sequence occurs when the subject requests to register to the system, which has descriptions as follows:

*Interface Description*

1. Subject requests to register to the AppPage
2. AppPage shows the registration page
3. Subject gives data to AppPage
4. AppPage sends the data to UserList
5. UserList checks the correction of data. In this method, if data completed and conforms to the requested format, UserList will process to the next step. If data is not completed and not conformed to the format, UserList will ask the subject to re-input data again by returning to step number 2
6. UserList uploads data to the database
7. UserList sends upload status to AppPage
8. AppPage provides password to Subject

### 3.6.2 Sequence Diagram of System's Logging in and Subject's Task Performing Interface Description.

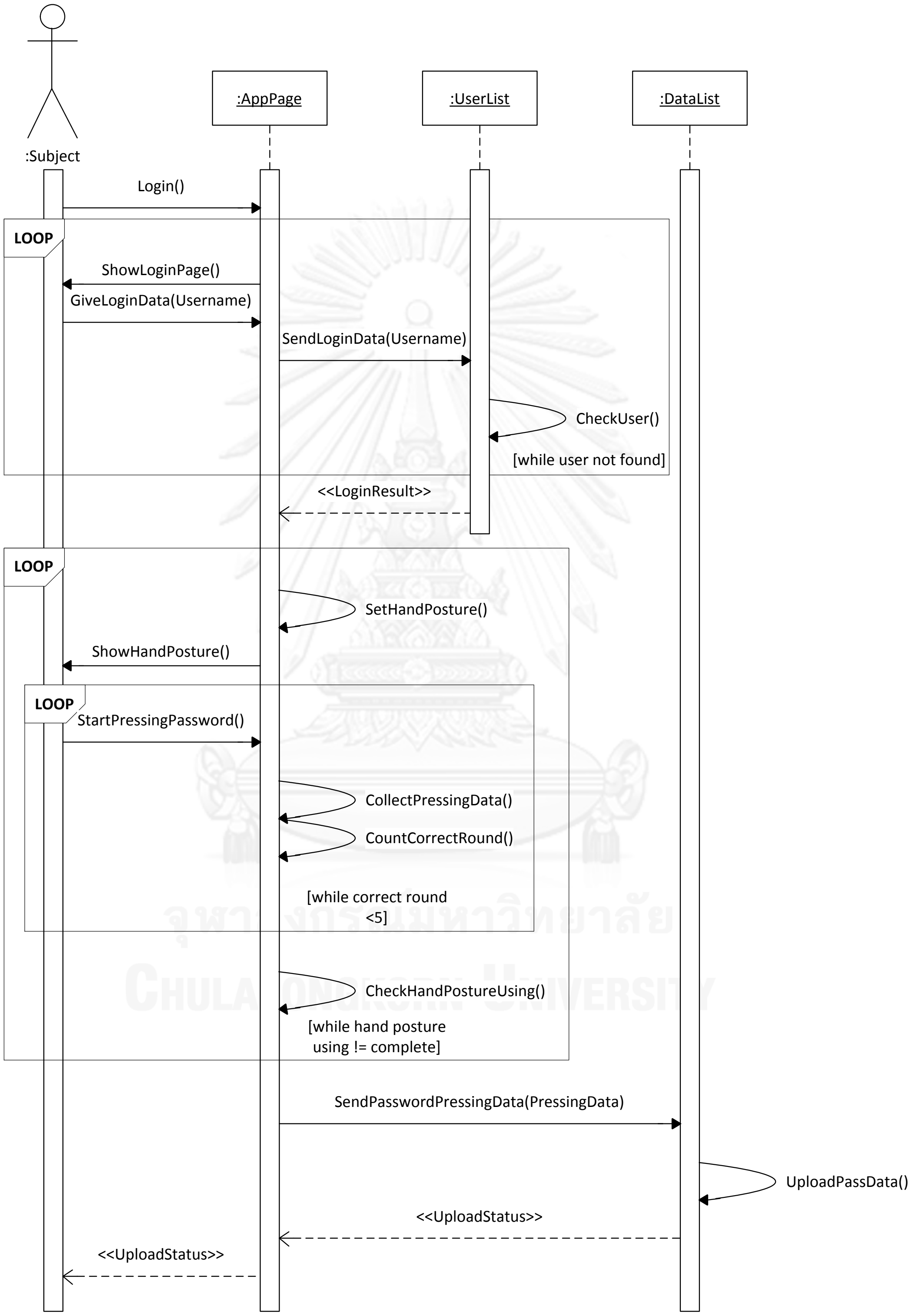


Figure 3-9 Sequence Diagram of System's Logging in and Subject's Task Performing

*Processing Narrative*

From Figure 3-9, this sequence will occur when the subject requests to login to the system, which has descriptions as follows:

*Interface Description*

1. Subject requests to login to the AppPage
2. AppPage shows Login Page
3. Subject gives their Username
4. AppPage send Username to UserList
5. UserList checks Username with data in the database. If found, the next step will be process, if not, the system will require the subject to provide Username again by going back to step number 2
6. UserList sends the success status of login to AppPage
7. AppPage sets the hand posture by randomly
8. AppPage shows hand posture which the subject has to hold the device
9. Subject starts pressing the order of password according to the given password from the registration process
10. AppPage collects the data and counts the correct round of password. If correct round < 5, AppPage will ask Subject for more pressing of the password sequence.
11. When the correct round of pressing password equal to 5, AppPage will check the using of hand posture. If the using of hand posture still not complete, the process returns to step 7, which is set the hand posture.
12. After all hand postures have been used, all password pressing data will be sent to DataList
13. DataList uploads input data to database
14. DataList reports back the upload status to AppPage
15. AppPage reports back the upload status to Subject

## 3.7 Activity Diagram

According to the sequence diagrams, the activity diagram has been illustrated to show the activity that has been occurred in each class. The main activity in this system can be separated into 2 activity diagrams, which are the activity diagram of the registration process and the activity diagram of password pressing process.

### 3.7.1 Activity Diagram of Registration

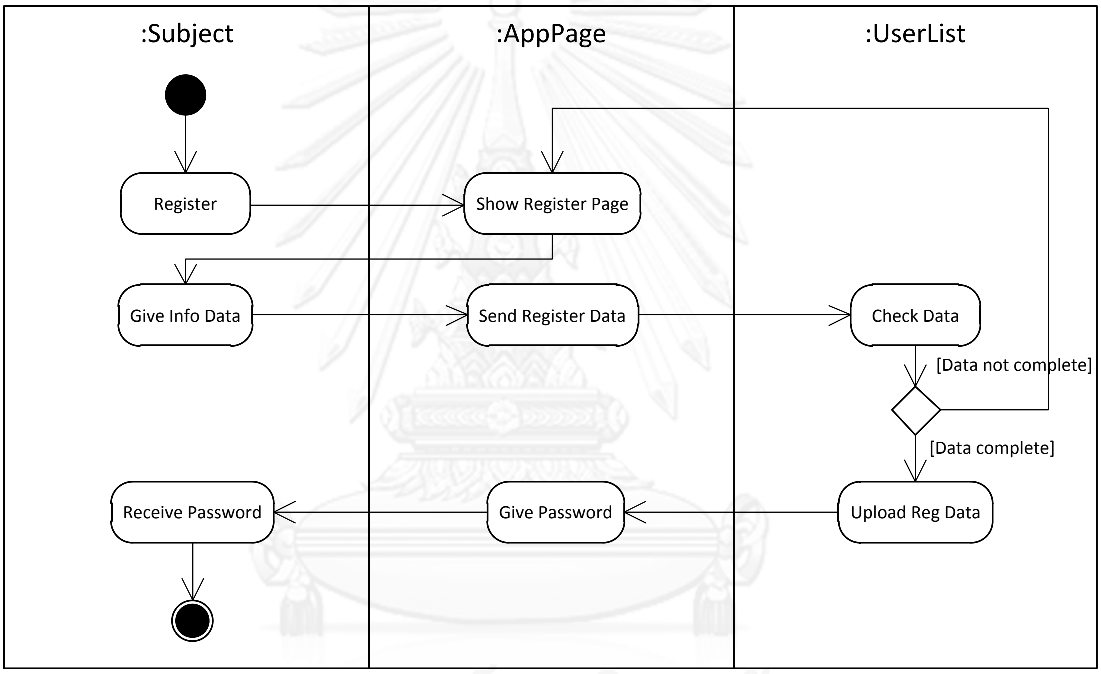


Figure 3-10 Activity Diagram of Registration

In this activity, 3 classes have been involved, which are Subject class, AppPage class, and UserList class. The flow starts from Subject requires registering, then AppPage class shows the register page. After that, Subject gives the info data, then AppPage class send the data that check at UserList Class. If the data is incomplete, the process will return to AppPage to show register page again. If the data complete, UserList will upload data to the database and sends the upload status to AppPage. AppPage will give password to Subject.

### 3.7.2 Activity Diagram of Password Pressing

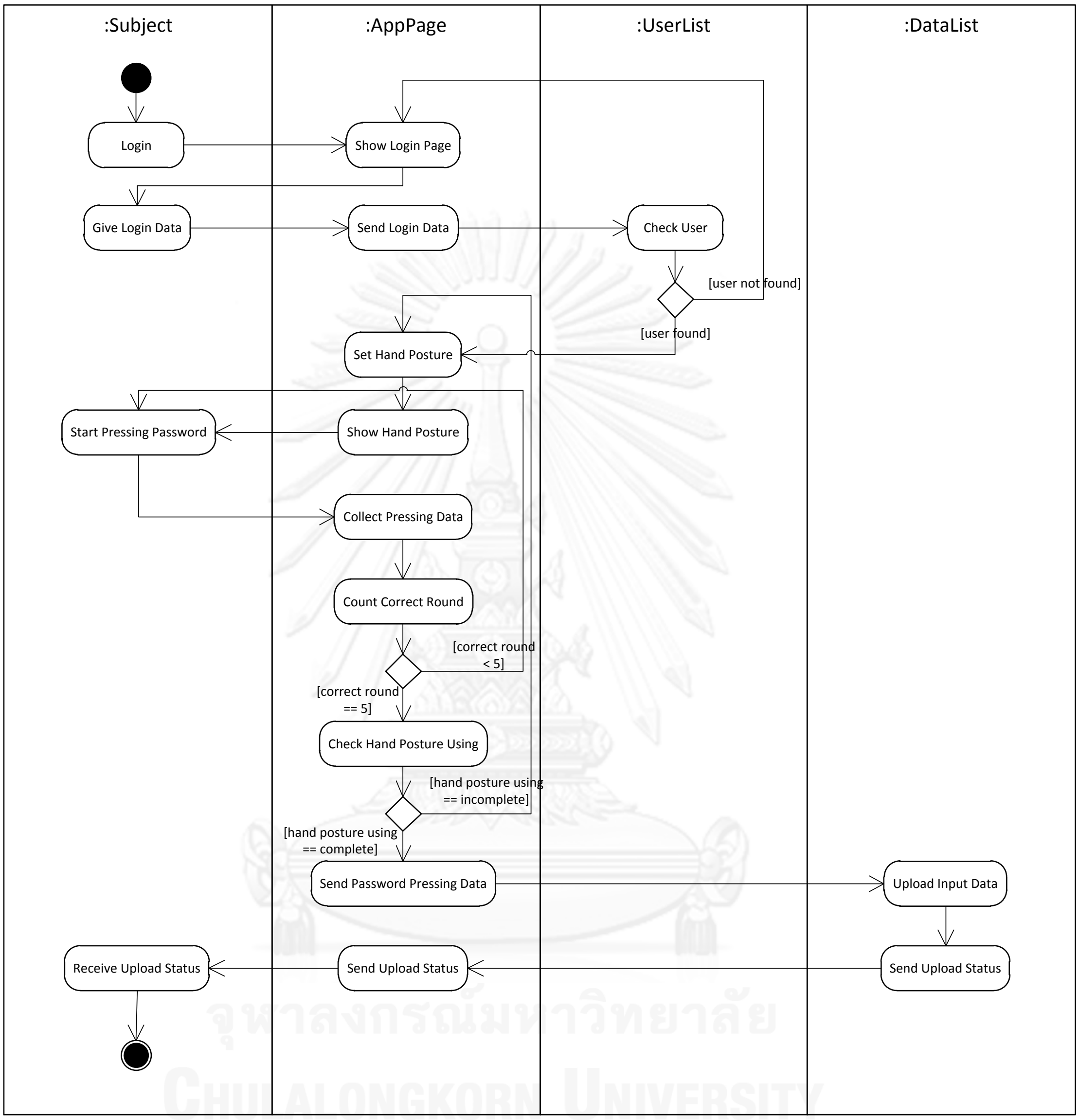


**Figure 3-11 Activity Diagram of Password Pressing**

In this activity, 4 classes have been involved, which are Subject class, AppPage class, UserList class, and DataList class. The flow starts after Subject request to login. The AppPage class will show the login page. Then Subject gives their Username to AppPage. AppPage will send the Username to UserList Class. UserList class will check the input Username with the stored data in database. If UserList could not find the match in the database, it will return to AppPage to show the login page again. If the match was found, Userlist will send the success status to AppPage and AppPage will set the hand posture. After that, AppPage will show the hand posture and Subject will start pressing the password. AppPage will collect the data and count correct round. This step will recurring until AppPage counts 5 correct round. Then, AppPage will check the using of hand posture. If the use of hand posture still incompletes, the step will repeat in hand posture setting step. If all postures have been used, all pressing data will send to DataList class. DataList class will upload the data to the database and then send the upload status to AppPage, which will forward that status to Subject.

### 3.8 Database Design

In this studying, the database contains 2 main tables as shown in Table 3-2.

Table 3-2 Detail of Databases

| Database No. | Name of Table | Description |
|---|---|---|
| 1 | UserList | The table which keep the information of all subject in this study |
| 2 | DataList | The table which keep the collecting data from subject, obtained from mobile device |

The details of each table can be explained as follows:

#### 3.8.1 UserList Table

UserList table is the table which keeps information of all subjects who have participate in this study. The structure and all fields of this table can be described as follows:

- **Name** : variable VARCHAR type with the maximum length of values equals to 50 characters. This field keeps the username of the subject and has been used in the login process.

- **Age** : variable INT type with the maximum length of values equals to 2 characters. This field keeps the age range of subjects. The age range of age which will be kept in this field can be separated into 5 groups: less than 15 years old, 15 to 20 years old, 21 to 25 years old, 26 to 30 years old, and more than 30 years old.

- **Gender** : variable VARCHAR type with the maximum length of values equals to 1 characters. This field keeps gender of the subject: M (Male) and F (Female).

- **Occupation** : variable VARCHAR type with the maximum length of values equals to 1 characters. This field keeps the occupation of subject. It can be divided into 3 groups: S (Student), E (Employee), and U (Unemployed).

- **ITRelated** : variable INT type with the maximum length of values equals to 1 characters. This field keeps the status of the subject's current occupation that the current occupation of the subject has involved with IT or not. (1 = has involved, 0 = not)

- **Device** : variable VARCHAR type with the maximum length of values equals to 5 characters. This field keeps the model of the subject's input device: 3gs (iPhone 3GS), 4 (iPhone 4), 4s (iPhone 4S), 5 (iPhone 5), 5c (iPhone 5C), 5s (iPhone 5S), and itouch (iPod Touch).

- **DeviceCapacity** : variable INT type with the maximum length of values equals to 2 characters. This field keeps the capacity of subject's device: 16 (16 GB), 32 (32 GB), and 64 (64 GB).

- **iOS-Version** : variable VARCHAR type with the maximum length of values equals to 5 characters. This field keeps the number of version of subject's device: ios6 (iOS Version 6), ios7 (iOS Version 7), and other (Other Version of iOS).

- **Handedness** : variable VARCHAR type with the maximum length of values equals to 2 characters. This field keeps the information of subject's handedness: L (Left-Handedness), R (Right-Handedness), and LR (Two-Handedness).

- **Hand-Posture** : variable INT type with the maximum length of values equals to 1 characters. This field keeps the number that represents the most grip posture that the subject uses to grip the device. The possible value which can be kept in this field are 1 (One Handed), 2 (Cradled), and 3 (Two Handed).

From this information, can be shown into table as table 3.-3.

**Table 3-3 UserList Table**

| Name | Type | Description | Extra |
|---|---|---|---|
| Name | VARCHAR (50) | Username | Primary Key, Not null |
| Age | INT (2) | Subject's Age range | Not null |
| Gender | VARCHAR (1) | Subject's gender | Not null |
| Occupation | VARCHAR (1) | Subject's occupation | Not null |
| ITRelated | INT (1) | Occupation relate to IT or not | Not null |
| Device | VARCHAR (5) | Subject's device model | Not null |
| DeviceCapacity | INT (2) | Subject's device capacity | Not null |
| iOS-Version | VARCHAR (5) | Version of subject's device | Not null |
| Handedness | VARCHAR (2) | Subject's handedness | Not null |
| Hand-Posture | INT (1) | Subject's handedness | Not null |

### 3.8.2 DataList Table

DataList table is the table which keeps input data after the subject finishing the password pressing for 1-full-round. The structure and all fields of this table can be described as follows:

- ID : variable INT type with the maximum length of values equals to 5 characters. This field keeps the number of input row. It can be used as a primary key of each input data as well.

- DataList : variable LONGTEXT type. This field keeps the long-string of data which generated from the input application. This long string consists of all-needed information from subject's password pressing and it will be split into each variable in the step of the data analysis process.

From this information, can be shown into table as Table 3-4.

**Table 3-4 DataList Table**

| Name | Type | Description | Extra |
|---|---|---|---|
| ID | INT (5) | Number of row of data | Primary Key, Not null |
| DataList | LONGTEXT | Long-string input data | Not null |

### 3.9 User Interface Design

User interface design is one of the most important processes because every interface that has been created will be directly communicated to all subjects. So every command or request that this study needs from subjects has to be very clearly and easily to understand. In the meantime, behind those ease of use of interface, the programming part which will collected the needed information in this study has to be well-programed and conformed to those user interface.

User interface design of this system can be discuss into 4 groups, which are:

1. Main Interface Design
2. Description Page Interface Design
3. Registration Page Interface Design
4. Data Collecting Page Interface Design

### 3.9.1 Main Interface Design

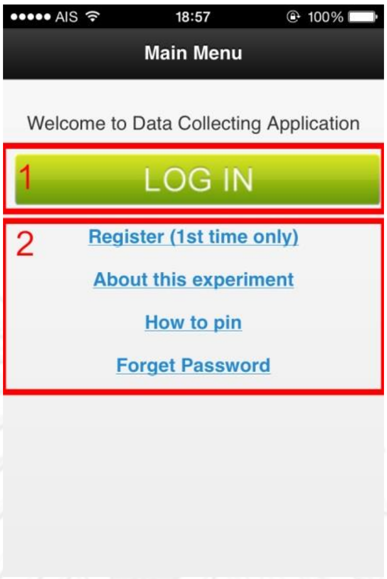


Figure 3-12 Main Interface

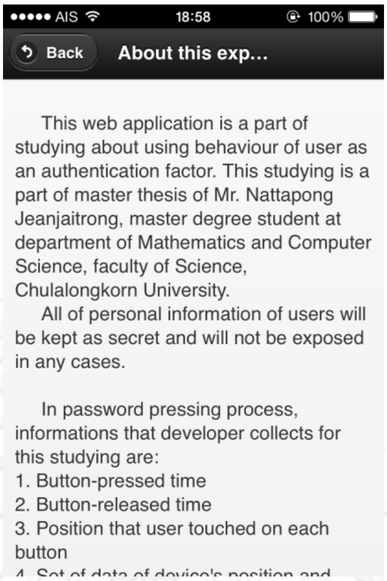
Main interface (Figure 3-12) is the first page that will be seen by the subject. So, every command and direction on this page has to be very clear and easy to understand. This page can be divided into 2 sections as:

1. *Login Command:* This command is the most important command of this system because retrieving all needed information in this study, system requires the subject to login and do all the tasks. So, that's the reason why this command is the most attractive on this page.
2. *Another Command:* This section consists of another command that also work in this system, but isn't the main command like *login*. So the size of each command is smaller than *login* command. All commands in this section can be seen very easily due to the using of text color and background color.

### 3.9.2 Description Page Interface Design

Description Page Interface is the page that consists of information for subject to read and understands about how's system works. In this system has many description pages, which can be explained as follows:

### *3.9.2.1) 'About this Experiment' Page Interface*



This web application is a part of studying about using behaviour of user as an authentication factor. This studying is a part of master thesis of Mr. Nattapong Jeanjaitrong, master degree student at department of Mathematics and Computer Science, faculty of Science, Chulalongkorn University.

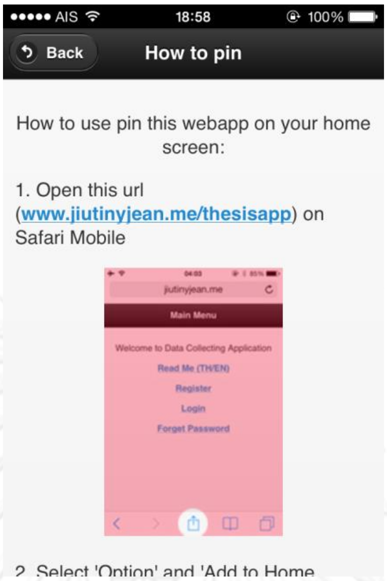
All of personal information of users will be kept as secret and will not be exposed in any cases.

In password pressing process, informations that developer collects for this studying are:
1. Button-pressed time
2. Button-released time
3. Position that user touched on each button
4. Set of data of device's position and

**Figure 3-13 'About this Experiment' Page Interface**

This page (Figure 3-13) is the page which explains about the reason of this studying to the subject. So, the subject can understand the reason of data collecting and how to do it properly. This page is only an explanation so there is no fancy, only black text with the proper text-size to read.

*3.9.2.2) 'How to Pin' Page Interface*



How to use pin this webapp on your home screen:

1. Open this url (www.jiutinyjean.me/thesisapp) on Safari Mobile

2. Select 'Option' and 'Add to Home

Figure 3-14 'How to Pin' Page Interface

This page (Figure 3-14) is the page which explains about how to put the shortcut icon of this application onto the home screen of device, called 'Pinning'. So, this page consists of both text explanation and images. The theme color of text and link are also the same with the previous page.

*3.9.2.3) 'Forget Password' Page Interface*

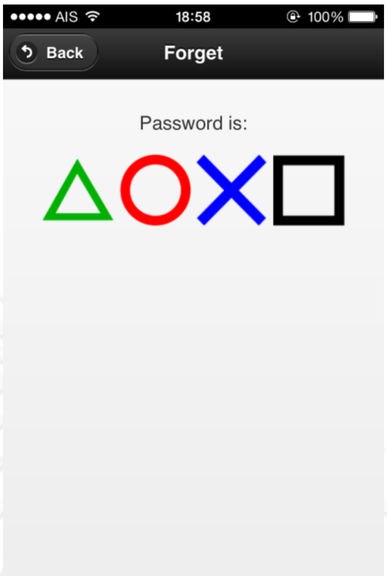
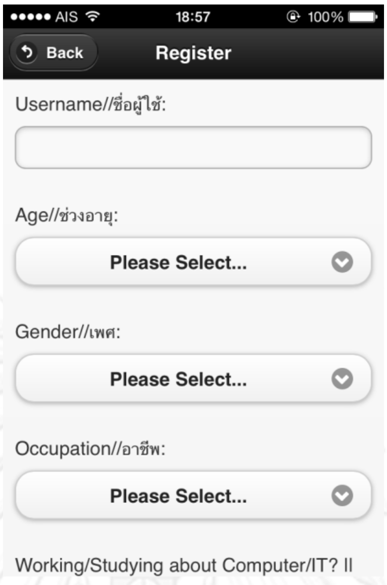


Figure 3-15 'Forget Password' Page Interface

This page (Figure 3-15) is the page that shows the password that all subjects have been given to. Every subject will receive this same set of password. In this page consists of only image of the password. So, the size of each symbol is quite bigger than the symbol that represent in the data collecting process.

### 3.9.3 Registration Page Interface Design



Register

Username//ชื่อผู้ใช้:

Age//ช่วงอายุ:

Please Select...

Gender//เพศ:

Please Select...

Occupation//อาชีพ:

Please Select...

Working/Studying about Computer/IT? ll

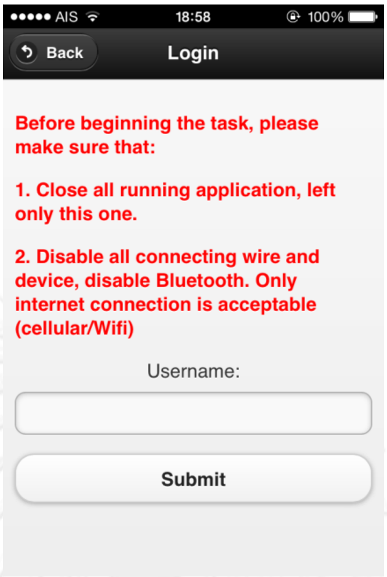
Figure 3-16 ‘Registration’ Page Interface

Registration page (Figure 3-16) is the page that will collect the personal information from the subject. Subject will use this page only at the first time of using this system. Since this page requires a lot of information from subjects, all input fields have been designed to be very easy for subjects to provide their data to the system. Most of input fields are drop-down list, only the username field which the subject has to type it by themselves.

### 3.9.4 Data Collecting Page Interface Design

Data Collecting Page is the main heart of this study. All subjects have to do the task, pressing password, on these pages of system. The Data Collecting section can be divided into sub-pages as follows:

*3.9.4.1) 'Login' Page Interface*



Before beginning the task, please make sure that:

1. Close all running application, left only this one.

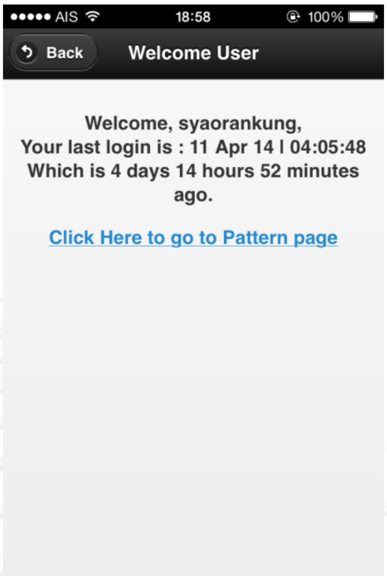
2. Disable all connecting wire and device, disable Bluetooth. Only internet connection is acceptable (cellular/Wifi)

Username:

Figure 3-17 'Login' Page Interface

Login Page (Figure 3-17) is the page after subject select "Login" button from the main page. This page consists of 2 main sections. First section is top-half of the screen which has a warning text. This warning text was written in red to make sure that this text will get an attention from the subject. The warning text is describing about things that the subject needs to complete before doing the next process. The second section is bottom-half of page that contains textbox. The subject has to type the username into this textbox then submit it. If the username is right, the system will bring the subject to the next process.

### *3.9.4.2) 'Welcome User' Page Interface*



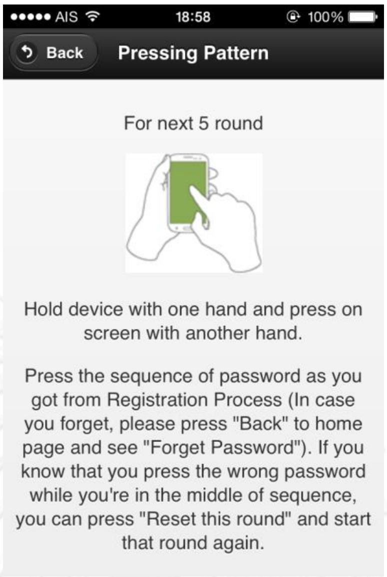
Welcome, syaorankung,
Your last login is : 11 Apr 14 I 04:05:48
Which is 4 days 14 hours 52 minutes ago.

Click Here to go to Pattern page

Figure 3-18 'Welcome User' Page Interface

Welcome User (Figure 3-18) page is the page that describes subjects about their last login to the system. Due to the rule of task-doing, subjects have to take a gap at least 4 hours between each complete round of task. So with this page, subjects can check the time by themselves. Text color on this page is black and link color is blue according to the theme color that has been used in this system.

### *3.9.4.3) 'Pressing Pattern' Page Interface*



For next 5 round

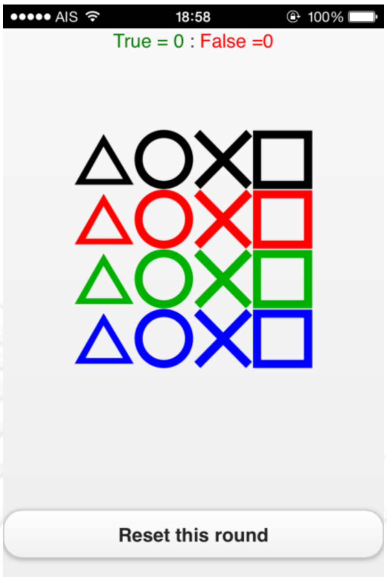
Hold device with one hand and press on screen with another hand.

Press the sequence of password as you got from Registration Process (In case you forget, please press "Back" to home page and see "Forget Password"). If you know that you press the wrong password while you're in the middle of sequence, you can press "Reset this round" and start that round again.

**Figure 3-19 'Pressing Pattern' Page Interface**

Pressing Pattern (Figure 3-19) page is the page that will explain subjects about how to press password in the next screen and also show the hand posture that subjects need to grip the device. The picture of hand posture is clearly shown at the top-half of the page, and the bottom-half is a description of the password-pressing process. At the bottom of this page is a link that leads the subjects to the password-pressing page

### *3.9.4.4) 'Password Pressing' Page Interface*



True = 0 : False =0

Figure 3-20 'Password Pressing' Page Interface

Password Pressing page (Figure 3-20) is the most important page of all. Subjects will have to press the sequence of password on this page. This page can be divided into 3 sections.

The first section is the top of page, contains of round-counter. The green text is correct round-counter, the number of it will change when subjects press the correct sequence of password. Also with the red text, it acts as an incorrect round-counter.

Next section is the middle of page which contains of 16 different symbols. The shape and color has already been explained in the experimental design (3.1). Each symbol has a size of 50x50 pixels.

Last section of this page is the 'Reset this round' button which located at the bottom of the page. This button is used when the subject realizes that the wrong sequence of password was pressed before the sequence is finish. The size of the button makes it can be seen very easily.

### 3.10 Application Storyboard

This section illustrates the storyboard of this application as follow:

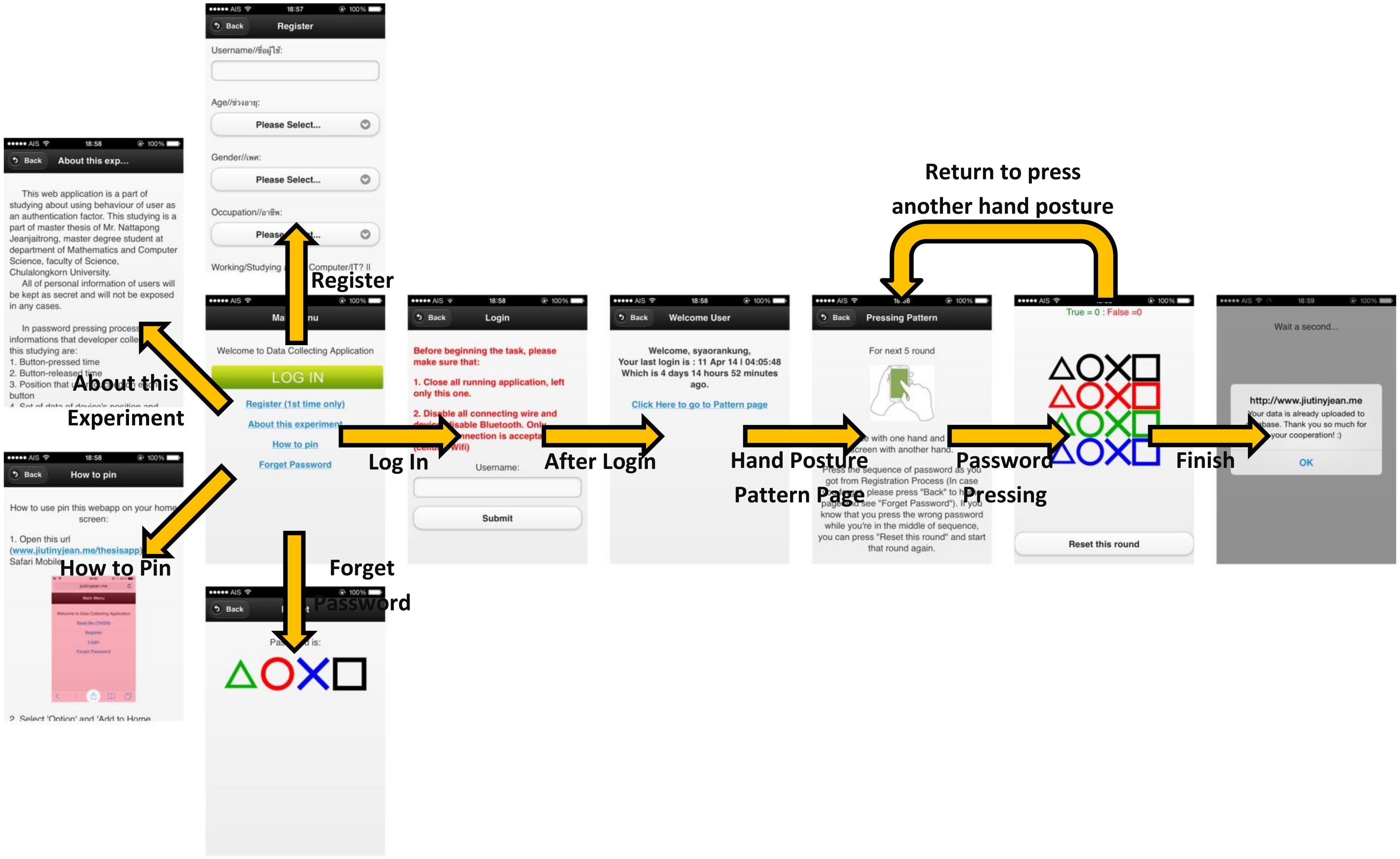


Figure 3-21 Application Flowchart

# CHAPTER IV
# EXPERIMENTAL RESULTS

This chapter demonstrates the experimental results from collected data from the proposed mechanism. The process of data preparing before analyzing will be described in Section 4.1 and machine learning analysis results by Weka will be illustrated in Section 4.2. Section 4.3 will be analyzed the using of distance in each user by SPSS statistical application.

## 4.1 Data Preparing

Since the data collecting application collects all in a form of long string (due to the ease of collecting). So, the preparing process is one of the most important in this step to prepare data in a suitable form before analyzing in machine learning in the next process.

### 4.1.1 Raw Data

The raw data is a long string data which keeps all information that has been gathered in the data collecting process. One row of raw data contains one time of the password pressing, which is username, the order of hand-posture, and all round of password pressing which is minimum at 15 rounds in case that the subject presses all correct passwords. But if the subject presses a wrong password, the wrong round off password will also be an addition to the raw data. Each set of variable will be separated by symbol “//”. The example of one row of raw data will show in Figure 4-1.

```
syaorankung//2*1*3//trigreen;92,211;1392644122905;1392644122965|cirred;134,164;1392644123047;13
92644123109|xblue;198,266;1392644123253;1392644123334|sqblack;250,98;1392644123478;13926441
23539|***true//trigreen;98,212;1392644123972;1392644124035|cirred;155,161;1392644124134;1392644
124195|xblue;185,259;1392644124341;1392644124404|sqblack;235,96;1392644124549;1392644124612|
***true//trigreen;97,214;1392644126755;1392644126818|cirred;136,168;1392644126932;13926441269 7
9|xblue;172,265;1392644127139;1392644127186|sqblack;233,118;1392644127332;1392644127378|***tr
ue//trigreen;95,215;1392644129666;1392644129713|cirred;150,156;1392644129844;1392644129872|xbl
ue;193,267;1392644130034;1392644130081|sqblack;247,104;1392644130227;1392644130273|***true//t
rigreen;100,211;1392644130756;1392644130801|cirred;152,149;1392644130929;1392644130963|xblue;1
98,252;1392644131141;1392644131167|sqblack;246,99;1392644131332;1392644131361|***true//trigree
n;89,207;1392644133841;1392644133886|cirred;147,152;1392644134082;1392644134174|sqblue;210,25
6;1392644134322;1392644134431|sqblack;249,113;1392644134642;1392644134703|***false//trigreen;9
4,214;1392644138590;1392644138717|cirred;142,147;1392644138863;1392644138971|xblue;181,254;13
92644139152;1392644139260|sqblack;233,111;1392644139438;1392644139533|***true//trigreen;89,210
;1392644141628;1392644141723|cirred;141,157;1392644141917;1392644142012|xblue;178,258;139264
4142206;1392644142299|sqblack;237,118;1392644142510;1392644142603|***true//trigreen;99,202;139
2644143116;1392644143259|cirred;150,152;1392644143420;1392644143531|xblue;192,258;1392644143
709;1392644143833|triblue;93,235;undefined;undefined|***false//trigreen;97,217;1392644147065;1392
644147178|cirred;146,165;1392644147388;1392644147529|xblue;186,258;1392644147724;13926441478
48|sqblack;237,110;1392644148044;1392644148154|***true//trigreen;97,205;1392644148620;13926441
48745|cirred;153,156;1392644148923;1392644149017|xblue;190,272;1392644149274;1392644149385|s
qblack;243,124;1392644149610;1392644149689|***true//trigreen;99,214;1392644150202;13926441503 1
3|cirred;149,157;1392644150491;1392644150584|xblue;200,259;1392644150843;1392644150888|sqblac
k;248,114;1392644151162;1392644151255|***true//trigreen;90,213;1392644155200;1392644155295|cirr
ed;126,163;1392644155472;1392644155532|xblue;193,261;1392644155663;1392644155759|sqblack;248
,102;1392644156000;1392644156078|***true//trigreen;89,226;1392644156465;1392644156526|cirred;12
3,161;1392644156719;1392644156799|xblue;191,263;1392644156944;1392644157021|sqblack;239,96;1
392644157264;1392644157341|***true//trigreen;80,219;1392644157759;1392644157854|cirred;130,162;
1392644158032;1392644158078|xblue;170,265;1392644158271;1392644158318|sqblack;232,112;13926
44158592;1392644158670|***true//trigreen;85,217;1392644159072;1392644159165|cirred;132,155;1392
644159360;1392644159420|xblue;172,275;1392644159584;1392644159645|sqblack;233,104;139264415
9903;1392644159965|***true//trigreen;86,219;1392644160366;1392644160444|cirred;142,162;13926441
60622;1392644160685|xblue;175,277;1392644160896;1392644160956|sqblack;248,97;1392644161198;1
392644161261|***true//
```

Figure 4-1 Example of one row of raw data

As mentioned before that each set of variable has been separated by symbol “//”. So the string of raw data can be interpreted as follows:

**Username** : Username is the first variable that can be extracted from the raw data string, as shown in Figure 4-1 ‘Syaorankung’. Username is the name that subject named in the registration process. And this username will be used as a classification’s class name in analyzing process.

**Order Number of Hand-Postures** : The next set of variable is the order number of hand-posture (As Figure 4-1 is //2*1*3//). The order number is the number that random by application itself. This order number will be used as a decision for application to shows subject the hand-posture that subject needs to hold and press device with that posture. Each hand posture needs the subject to press a right round of the password for 5 rounds, before changing to the next postures until all posture in the order or list have been completed. As Figure 4-1 that subject need to hold and press the password with the posture number 2 then number 1 and 3 respectively.

**Password-Pressing Data** : Following after order number of hand-postures is password-pressing data. In each set of password-pressing data consists of the name of the symbol, position x, position y, time that subject presses finger on the screen, times that subject releases finger. The last symbol of round will concatenate with the status of correctness, if that round of pressing of correct, the word “true” will be followed after separate symbol “***”. The example in Figure 4-2 shows only one round of password-pressing. The full complete of one time of password pressing will contain at least 15 correct rounds.

```
trigreen;92,211;1392644122905;1392644122965|cirred;134,164;1392644
123047;1392644123109|xblue;198,266;1392644123253;1392644123334
|sqblack;250,98;1392644123478;1392644123539|***true
```

**Figure 4-2 Example of one round of password-pressing**

### 4.1.2 Data Calculating and Preparing

After retrieving the long string of information, each features will be extracted and calculated into the factor that needed in machine learning. Factors that have been needed in machine learning are:

**Dwell Time** : As mentioned in the first chapter, dwell time is the time that user spent on pressing one symbol since start until release that symbol. The dwell time can be calculated very easily, only a calculation within the same set of data. This is the easiest factor that can be calculated from raw data.

**Interval Time** : The interval time is the duration of time since the subject releases from the first symbol until press the next symbol. Mostly, the interval time is longer than the dwell time. The calculation of Interval time is by calculates the difference of button-pressed-time from current button and button-released-time from previous button.

**Interval Timing Ratio** : The interval timing ratio is the factor that comes from an idea from another research, as mention in chapter 2. The interval timing ration is the ration between the interval time (from the previous step) and the total time that has been used in that round of pressing.

**Distance** : Distance is the factor that has been proposed on this thesis. The idea of using distance between symbol (or button) comes from the further study from writer's senior project of bachelor's degree. Back in that time, factors that have been proposed to use as new factors are positions x and y that the subject touched on screen. In this thesis, position x and y have been transformed into a distance between each symbol. The calculation of a using the distance equation as show in Figure 4-3.

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

Figure 4-3 Distance Equation

After all interested factor has been calculated, the data has been arranged into CSV form, which will be used in machine learning process in the next step. The look of data after transform into CSV form can be illustrated as Figure 4-4, which the top row of it is the name of each factor, and the second row is the data which accord to the top row.

```
hand,dwell1,interval1,ratio1,dist1,dwell2,interval2,ratio2,dist2,
dwell3,interval3,ratio3,dist3, dwell4,correction,user

2,163,252,0.21668099742046,64.660652641309,99,234,0.2012
03783319,104.6231331972,100,233,0.20034393809114,174.88
853593075,82,true,hedpor
```

**Figure 4-4 Example of one row data in CSV file**

From 25 subjects, each subject's data has been calculated and transformed into CSV form. Each CSV file of each subject will be used as a learning data in the next process.

### 4.2 Machine Learning Analysis Results

In this section, all data that have been collected from all subjects which have been already calculated and prepared in the previous step will be learned and classified by Weka® Machine Learning. The analysis will be separated into different categories depends on the interesting factor.

In each analysis, the CSV file that contains the normalized data from subjects will be used. After loading the data into the application, the application will translate those text and number data into graphs. Each graph represents the plotting between each factor that collected, as shown in Figure 4-5.

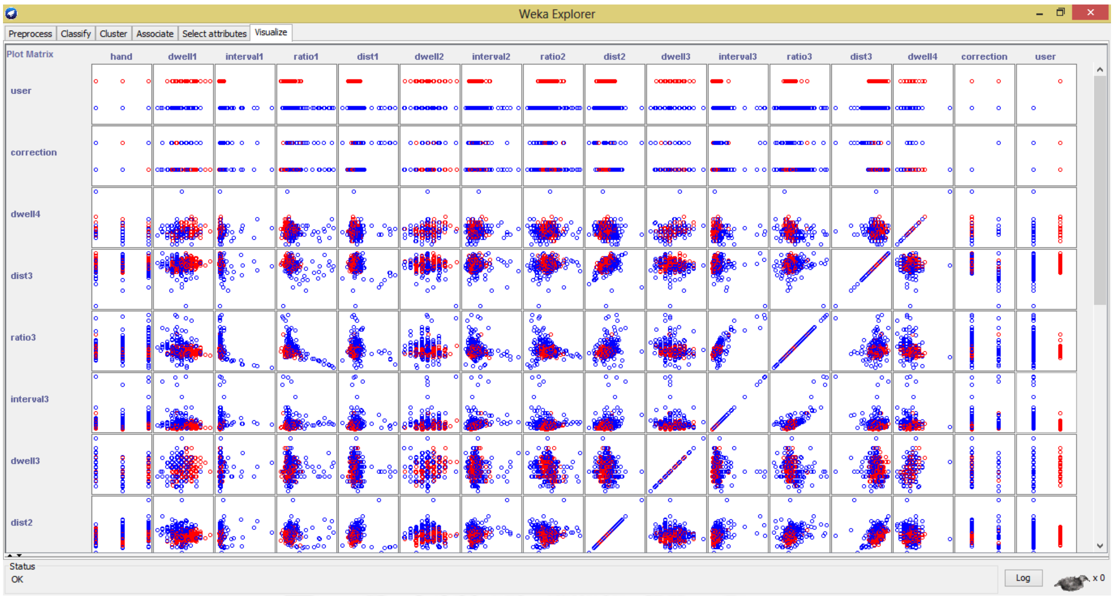


Figure 4-5 Scatter Plot of each factor between 2 Subjects

From Figure 4-5, scatter plots show the distribution of data from each subject. Some pair of factor shows the clearly separate of 2 subjects. Each scatter plot shows the distribution with the color of data that represent the different subject. From the graph, it can be concluded that each factor might have a potential to be used as a factor in authentication mechanism.

### 4.2.1 All Data Analysis

In the authentication process, there are only 2 outputs after logging in that tells user whether the user's status is the right person or not. The login process on the mobile device requires only one user at a time. So, it means that only 2 classes are needed to be classified by machine learning, which is the right class and the wrong class.

From 25 subjects whose their data have been collected, their data have been paired to make 2 different classes in one file. In this experiment, 13 pairs have been generated among 25 subjects. Each pair will perform a machine learning process using Weka® Machine Learning. The classifier that has been selected to classify the data is Bayesian Network. The main result that needs to be studied is the percentage of accuracy, false acceptance rate (FAR), and false rejection rate (FRR).

In the result, each pair of subject will be represented by the combination of subject’s number. The example is, the combination pair from subject number 1 and subject number 2 is p0102.

Table 4-1 Result of Classification from random pair of subjects, All Factors

| Pair of Subjects | Accuracy (%) | FAR | FRR |
|---|---|---|---|
| p0102 | 90.45 | 0.095 | 0.096 |
| p0304 | 100 | 0 | 0 |
| p0506 | 93.8 | 0.062 | 0.062 |
| p0708 | 99.9 | 0.001 | 0.001 |
| p0910 | 99.6 | 0.004 | 0.004 |
| p1112 | 82.25 | 0.177 | 0.178 |
| p1314 | 100 | 0 | 0 |
| p1516 | 99.8 | 0.002 | 0.002 |
| p1718 | 99.45 | 0.005 | 0.006 |
| p1920 | 97.45 | 0.025 | 0.026 |
| p2122 | 95.1 | 0.049 | 0.049 |
| p2324 | 93.7 | 0.063 | 0.063 |
| p0225 | 100 | 0 | 0 |
| **Average** | **96.26923** | **0.037154** | **0.037462** |

Table 4-1 shows the results from 13 random pair from 25 subjects and the average results. The result shows the percentage of accuracy by using the combination of all factors, which has accuracy at 96.27% with false acceptance rate and false rejection rate at 0.0371 and 0.0374 respectively.

The above result based on only behavioral data which are retrieved from password pressing. All subjects press the same password. So this is the result from the combination of using behavioral biometrics, which gives quite impressive results.

### 4.2.2 Hand Gripping Posture Analysis

Another factor that has been interested is device's hand gripping posture. To prove that hand gripping posture is one of the behavioral biometrics and can be used as a factor in the authentication method, all data of subjects has been separated according to their hand gripping posture, as shown in Table 4-2.

Table 4-2 Information of subject’s handedness and device gripping posture

| UID | Username | Handedness | Gripping Posture |
|---|---|---|---|
| u01 | ball | L | 1 |
| u02 | btas01 | R | 1 |
| u03 | elle_nlatt | R | 2 |
| u04 | flookkung | R | 2 |
| u05 | flukiefluka | R | 1 |
| u06 | fuckmefuckmu | R | 1 |
| u07 | 'hathaiwinee wisitkard' | R | 2 |
| u08 | hedbow | R | 1 |
| u09 | hedpor | R | 1 |
| u10 | ipao | LR | 1 |
| u11 | jedsada | R | 2 |
| u12 | lumluk | R | 1 |
| u13 | mikichocobanana | R | 3 |
| u14 | mink | R | 1 |
| u15 | natt | R | 1 |
| u16 | nitingale | LR | 3 |
| u17 | ohmoomtang | R | 2 |
| u18 | pond01234 | R | 3 |
| u19 | poomer | L | 2 |
| u20 | printer555 | R | 3 |
| u21 | pt.skoolz | R | 1 |
| u22 | saimorke | R | 2 |
| u23 | setsquare | L | 1 |
| u24 | specture | L | 1 |
| u25 | syaorankung | R | 3 |

### *4.2.2.1) Experiment between same group of hand gripping posture*

In this experiment, data of all subjects have been grouped according to the gripping posture. Finally, three groups of data has been set. Each group of data has been random paired as same as the previous experiment. The comparing result in the same group of data between focusing on gripping posture and non-focusing can show as follows:

**Table 4-3 Comparing result between non-focusing of gripping posture and focusing on gripping posture of gripping posture Number 1**

| Pair ID | Non-Focusing on Gripping Posture | | | Focusing on Gripping Posture | | |
|---|---|---|---|---|---|---|
| | % | FAR | FRR | % | FAR | FRR |
| p0102 | 90.45 | 0.095 | 0.096 | 80.9 | 0.191 | 0.191 |
| p0224 | 91.95 | 0.08 | 0.081 | 94.5 | 0.055 | 0.055 |
| p0506 | 93.8 | 0.062 | 0.062 | 96.27 | 0.037 | 0.037 |
| p0809 | 91.8 | 0.082 | 0.082 | 90.06 | 0.099 | 0.099 |
| p1012 | 99.1 | 0.009 | 0.009 | 99.41 | 0.006 | 0.006 |
| p1415 | 87.55 | 0.124 | 0.125 | 73.02 | 0.27 | 0.271 |
| p2123 | 89.9 | 0.101 | 0.101 | 94.83 | 0.052 | 0.052 |
| AVERAGE | **92.08** | **0.0790** | **0.0794** | **89.86** | **0.1014** | **0.1015** |

Table 4-3 shows the comparing result between non-focusing of gripping posture and focusing on gripping posture of gripping posture number 1. The result shows that focusing on non-gripping posture can provide an obvious accuracy better that focusing for about 2.5% in posture number 1, with the lower of FAR and FRR.

**Table 4-4 Comparing result between non-focusing of gripping posture and focusing on gripping posture of gripping posture Number 2**

| Pair ID | Non-Focusing on Gripping Posture | | | Focusing on Gripping Posture | | |
|---|---|---|---|---|---|---|
| | % | FAR | FRR | % | FAR | FRR |
| p0304 | 100 | 0 | 0 | 100 | 0 | 0 |
| p0322 | 96.8 | 0.032 | 0.032 | 98.15 | 0.019 | 0.018 |
| p0711 | 99.95 | 0 | 0.001 | 99.25 | 0.007 | 0.007 |
| p1719 | 86.4 | 0.136 | 0.136 | 85.67 | 0.143 | 0.144 |
| AVERAGE | **95.79** | **0.0420** | **0.0422** | **95.77** | **0.04225** | **0.04225** |

Table 4-4 shows the comparing results between non-focusing of gripping posture and focusing on the gripping posture of the gripping posture number 2. The accuracy of non-focusing on gripping posture are slightly better than focusing, with the slightly lower of FAR and FRR.

**Table 4-5 Comparing result between non-focusing of gripping posture and focusing on gripping posture of gripping posture number 1**

| Pair ID | Non-Focusing on Gripping Posture | | | Focusing on Gripping Posture | | |
|---|---|---|---|---|---|---|
| | % | FAR | FRR | % | FAR | FRR |
| p1316 | 93.85 | 0.061 | 0.062 | 99.54 | 0.005 | 0.005 |
| p1820 | 93.45 | 0.065 | 0.066 | 91.99 | 0.08 | 0.08 |
| p1325 | 95.95 | 0.04 | 0.041 | 98.95 | 0.01 | 0.011 |
| AVERAGE | **94.42** | **0.0553** | **0.0563** | **96.83** | **0.0317** | **0.0320** |

Table 4-5 shows the comparing results between non-focusing of gripping posture and focusing on gripping posture of the gripping posture number 3. The accuracy of focusing on gripping posture are better that non-focusing for almost 2%, with the lower of FAR and FRR.

Table 4-6 Average results from all group of gripping posture

| Group | Non-Focusing on Gripping Posture | | | Focusing on Gripping Posture | | |
|---|---|---|---|---|---|---|
| | % | FAR | FRR | % | FAR | FRR |
| Posture 1 | 92.08 | 0.079 | 0.0794 | 89.86 | 0.1014 | 0.1015 |
| Posture 2 | 95.79 | 0.042 | 0.0422 | 95.77 | 0.0423 | 0.0423 |
| Posture 3 | 94.42 | 0.0553 | 0.0563 | 96.83 | 0.0317 | 0.0320 |
| **AVERAGE** | **93.64** | **0.0633** | **0.0638** | **93.04** | **0.0695** | **0.0697** |

From results above show that random paired of each group of gripping posture shows an almost equal result when focusing on hand gripping (89.85%, 95.77%, and 96.83%). The average result from all posture can be illustrated as Table 4-6.

This can be the concluded that the device's gripping posture has no effect to the accuracy

### *4.2.2.2) Experiment between different groups of hand gripping posture*

On the previous experiment is the comparing between subjects who have the same posture of device's hand gripping. This experiment will compare between different groups of hand gripping posture among subjects. 10 pairs of subjects have been selected in this experiment. Each subject in a pair comes from different groups of gripping posture. The result of comparing between subjects from different groups of hand gripping postures can be illustrated in Table 4-7

Table 4-7 Comparing result between different groups of hand gripping posture

| Pair ID | % | FAR | FRR |
|---|---|---|---|
| p0103 | 94.88 | 0.051 | 0.053 |
| p0204 | 99.85 | 0.001 | 0.001 |
| p0507 | 99.41 | 0.006 | 0.006 |
| p0613 | 98.63 | 0.014 | 0.014 |
| p0816 | 99.54 | 0.005 | 0.005 |
| p0918 | 93.68 | 0.063 | 0.063 |
| p1019 | 84.13 | 0.159 | 0.159 |
| p1120 | 88.08 | 0.119 | 0.119 |
| p1222 | 96.9 | 0.031 | 0.031 |
| **AVERAGE** | **91.64** | **0.084** | **0.083** |

Table 4-7 shows that even each subject from each pair comes from different hand gripping posture group, the average result still have a high accuracy with low FAR and FRR. The results between comparing the same group and comparing different groups have a slightly different due to the different numbers of input pairs.

### 4.2.3 Handedness Analysis

The next factor that has been interested is handedness. There are three types of handedness among 25 subjects, which are left-handedness, both handedness, and right handedness. Each subject has been separated into their handedness and paring with the member in the same group. The results from machine learning shows in Table 4-8.

**Table 4-8 Result from pairing in the member of Left-Handedness**

| Pair ID | % | FAR | FRR |
|---|---|---|---|
| p0103 | 96.25 | 0.037 | 0.036 |
| p0204 | 96 | 0.04 | 0.04 |
| **AVERAGE** | **96.125** | **0.0385** | **0.038** |

From the Left-Handedness group, the results show an average accuracy at 96.13% with FAR and FRR at 0.0385 and 0.038 respectively.

**Table 4-9 Result from pairing in the member of Both-Handedness**

| Pair ID | % | FAR | FRR |
|---|---|---|---|
| p1016 | 89.95 | 0.1 | 0.101 |

From the Both-Handedness group, the results show an accuracy at 89.95% with FAR and FRR at 0.1 and 0.101 respectively.

Table 4-10 Result from pairing in the member of Right-Handedness

| Pair ID | % | FAR | FRR |
|---|---|---|---|
| p0205 | 91.55 | 0.084 | 0.085 |
| p0225 | 100 | 0 | 0 |
| p0608 | 92.8 | 0.072 | 0.072 |
| p0321 | 69.75 | 0.302 | 0.303 |
| p0407 | 81.8 | 0.172 | 0.182 |
| p0912 | 86.7 | 0.133 | 0.133 |
| p1117 | 99.65 | 0.003 | 0.004 |
| p1322 | 99.7 | 0.003 | 0.003 |
| p1415 | 87.55 | 0.124 | 0.125 |
| p1820 | 93.45 | 0.065 | 0.066 |
| **AVERAGE** | **90.295** | **0.0958** | **0.0973** |

From the Right-Handedness group, the results show an average accuracy at 90.30% with FAR and FRR at 0.096 and 0.097 respectively.

To sum up, the average result from three groups of handedness can be shown in Table 4-11.

Table 4-11 The average result of all handedness

| Handedness | % | FAR | FRR |
|---|---|---|---|
| Left-Handedness | 96.125 | 0.0385 | 0.038 |
| Both-Handedness | 89.95 | 0.1 | 0.101 |
| Right-Handedness | 90.295 | 0.0958 | 0.0973 |
| **AVERAGE** | **92.12333** | **0.0781** | **0.078767** |

The average results from three groups of handedness show the accuracy at 92.12% with FAR and FRR at 0.0781 and 0.0787 respectively. When comparing the result with all-factor or hand-gripping posture, the result from handedness shows a slightly different from them, especially when comparing to non-focus hand-gripping posture that has an accuracy result at 93%. So, it might be a conclusion that handedness has a slightly influence to be a factor in the authentication process.

### 4.3 Statistical Analysis

Among many factors that have been collected in this experiment, distance is a factor that has been questioned whether it is a unique factor to represent each subject or not. The data of distance has been analyzed using SPSS® Statistic Software. This analysis uses nonparametric test; the test field is the distance data classified by subjects. The analysis compares distributions across groups by Mann-Whitney U with 2 samples with the significant level at 0.05. The following result shows the result from random pair of subject, as same as 4.2.1.

From Table 4-12, the random pair has been selected to represent the whole data of this experiment. Each table row shows the significance values of distance 1 to distance 3. The null hypothesis of each distance can be shown as follows:

1. The distribution of dist1 is the same across categories of users.
2. The distribution of dist2 is the same across categories of users.
3. The distribution of dist3 is the same across categories of users.

From the table, there are some distances of pairs that accept the null hypothesis. However, most of results reject the null hypothesis. Moreover, the average significance values show the rejection of null hypothesis. So, it means that the distance factors of each pair of subject are different to each other and can be used as a unique factor in the authentication process.

Table 4-12 Result of Mann-Whitney U Test from random pair of subject

| Pair of Subject | dist1 sig | dist2 sig | dist3 sig |
|---|---|---|---|
| p0102 | 0.000 | 0.000 | 0.000 |
| p0304 | 0.000 | 0.023 | 0.000 |
| p0506 | 0.000 | 0.000 | 0.000 |
| p0708 | 0.000 | 0.000 | 0.256 |
| p0910 | 0.000 | 0.000 | 0.000 |
| p1112 | 0.000 | 0.000 | 0.000 |
| p1314 | 0.000 | 0.000 | 0.000 |
| p1516 | 0.000 | 0.002 | 0.000 |
| p1718 | 0.000 | 0.000 | 0.000 |
| p1920 | 0.000 | 0.000 | 0.154 |
| p2122 | 0.000 | 0.251 | 0.000 |
| p2324 | 0.000 | 0.001 | 0.000 |
| p0225 | 0.000 | 0.000 | 0.000 |
| **AVERAGE** | **0.000** | **0.021** | **0.032** |

# CHAPTER V
# DISCUSSION AND CONCLUSION

In this chapter, the discussion of all experiment will be described in Section 5.1. Section 5.2 will stated the conclusion of all experiments. Finally, the future work from this study will be discussed in Section 5.3

## 5.1 Discussion

Since the mobile devices can be used as various functions, including storing important personal information like credit card id, password, bank account, etc. The cyber-crime occurring rate also increases. To protect the data from these crimes, an authentication mechanism must be implemented before entering to the system. Many researches indicated that using multi-factor in the authentication process provides a better result than the use of single-factor. This thesis studies the feasibility of applying keystroke dynamics with the touch-screen mobile devices by the symbol-based password, plus the extended study of other behavioral factor. This work focuses on prominent factors that can retrieve from a touch-screen pressing, these factors are the dwell time, the interval time, the interval timing ratio and the distance between buttons. Bayesian network classifier was applied to analyze the accuracy and performance of this biometrics. The results from random pair among subjects, which included all interest factors, show that the multi-factor authentication gains the accuracy at 96.27% followed by FAR and FRR at 0.0371 and 0.0374 consequently. With focusing on hand gripping posture gives the accuracy at 93.04% with FAR and FRR in 0.0695 and 0.0697 respectively while non-focusing on hand-gripping posture shows the result at 93.64% with FAR and FRR in 0.0633 and 0.0638 consequently. The accuracy of focusing in term of handedness shows the average result at 92.12% with FAR and FRR 0.0781 and 0.0787 respectively. The statistical analyze result of distance using nonparametric test with Mann-Whitney U test with 2 samples shows that the average significance value of distance 1 is 0.000, the average significance value of distance 2 is 0.021, and the average significance value of distance 3 is 0.032. The significant level that will accept the null hypothesis is 0.05. This means that the average significance value reject null hypothesis. From the results, there is some value which value is more than acceptance significant value such as dist3 sig in p0104 (Table B-1 in Appendix B). In dist3 sig of p0104, the significant value is equal to 0.999. This maybe shows the possibility that the pressing position of subject number 1 and number 4 is very similar to each other.

## 5.2 Conclusion

This research proposes a study of applying keystroke dynamics on the touchscreen mobile devices in order to gain a new authentication method. This study starts from reviewing involved researches, which are the use of the multi-factor in the authentication system, such as keystroke dynamics and graphical-based password. Due to the fact that most of the touch-screen mobile devices have no specific input sensor to detect physical biometrics, keystroke dynamics was selected to be applied on mobile devices. Moreover, keystroke dynamics is the most convenient factor that can be retrieved from mobile users. This research study the use of four factors obtained from keystroke dynamics, which are the dwell time, the interval time, the interval timing ratio and the distance between buttons. Based on Bayesian network classifier in the machine learning process, each factor and combined factors provided a different accuracy results. The best result is obtained from combination of four factors with accuracy at 92.27%% with FAR and FRR at 0.0371 and 0.0374 respectively.

Furthermore, this research also focus and comparing the other interesting factors such as hand gripping posture and handedness. The results show that both hand gripping posture and handedness gives almost equal accuracy, which can lead to the conclusion that both hand gripping posture and handedness did not have much effect to the accuracy in the authentication process.

The distance factor has been analyzed using SPSS® statistical software. The result shows that the average significance value rejects the null hypothesis, which means that the distance factor can be used as a unique factor in the authentication mechanism.

Based on the results presented above, this research leads to the conclusion that the keystroke dynamics mechanism can be applied on the touch-screen mobile. The combination of using keystroke dynamics and symbol-based password provides a high accuracy with low error rate.

### 5.3 Future Works

This research study about applying keystroke dynamics onto touchscreen device combines with symbol-based password. There might be other factors from mobile devices which can be retrieved and used as a behavioral biometrics. So, the future work might be finding the new factors from the use of touchscreen mobile device. Plus the combination with other types of password such as graphical-based which have a lot of technique to design and experiment with. This thesis might be the beginning of a new way of authentication on touchscreen mobile device.

# REFERENCES

1. Wikipedia_Contributors. *Authentication*. 2014 13 April 2014 17:35 UTC 23 April 2014 16:04 UTC]; Available from: http://en.wikipedia.org/w/index.php?title=Authentication&oldid=604036165.
2. Team, W. *What is Authentication?* 2014 23 April 2014]; Available from: http://www.webopedia.com/TERM/A/authentication.html.
3. Rouse, M. *Authentication*. 2007 [cited 2014; Available from: http://searchsecurity.techtarget.com/definition/authentication.
4. Anzaku, E.T., H. Sohn, and Y.M. Ro. *Multi-factor authentication using fingerprints and user-specific random projection*. in *Web Conference (APWEB), 2010 12th International Asia-Pacific*. 2010. IEEE.
5. Al-Assam, H., H. Sellahewa, and S. Jassim. *On security of multi-factor biometric authentication*. in *Internet Technology and Secured Transactions (ICITST), 2010 International Conference for*. 2010. IEEE.
6. contributors, W. *Biometrics*. 2014 22 April 2014 23:00 UTC 23 April 2014 19:25 UTC]; Available from: http://en.wikipedia.org/w/index.php?title=Biometrics&oldid=605366567.
7. Portal, E.T.o.B.N. *What are biometrics?* 2014 [cited 2014; Available from: http://www.biometricnewsportal.com/biometrics_definition.asp.
8. Ao, S., W. Ren, and S. Tang. *Analysis and Reflection on the Security of Biometrics System*. in *Wireless Communications, Networking and Mobile Computing, 2008. WiCOM'08. 4th International Conference on*. 2008. IEEE.
9. Saevanee, H. and P. Bhattarakosol. *Authenticating user using keystroke dynamics and finger pressure*. in *Consumer Communications and Networking Conference, 2009. CCNC 2009. 6th IEEE*. 2009. IEEE.
10. Giroux, S., R. Wachowiak-Smolikova, and M.P. Wachowiak. *Keypress interval timing ratios as behavioral biometrics for authentication in computer security*. in *Networked Digital Technologies, 2009. NDT'09. First International Conference on*. 2009. IEEE.
11. contributors, W. *Keystroke dynamics*. 2014 26 March 2014 17:33 UTC 23 April 2014 20:49 UTC]; Available from: http://en.wikipedia.org/w/index.php?title=Keystroke_dynamics&oldid=601381545.
12. Jones, L.A. and S.J. Lederman, *Human hand function*. 2006: Oxford University Press.
13. Rouse, M. *Keystroke Dynamics*. 2008 [cited 2014; Available from: http://searchsecurity.techtarget.com/definition/keystroke-dynamics.
14. Bolle, R., *Guide to biometrics*. 2004: Springer.

15.Umphress, D. and G. Williams, *Identity verification through keyboard characteristics.* International journal of man-machine studies, 1985. **23**(3): p. 263-273.

16.Joyce, R. and G. Gupta, *Identity authentication based on keystroke latencies.* Communications of the ACM, 1990. **33**(2): p. 168-176.

17.Meszaros, A., Z. Banko, and L. Czuni. *Strengthening passwords by keystroke dynamics*. in *Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, 2007. IDAACS 2007. 4th IEEE Workshop on*. 2007. IEEE.

18.Giroux, S., R. Wachowiak-Smolikova, and M.P. Wachowiak. *Keystroke-based authentication by key press intervals as a complementary behavioral biometric*. in *Systems, Man and Cybernetics, 2009. SMC 2009. IEEE International Conference on*. 2009. IEEE.

19.Zack, R.S., C.C. Tappert, and S.-H. Cha. *Performance of a long-text-input keystroke biometric authentication system using an improved k-nearest-neighbor classification method*. in *Biometrics: Theory Applications and Systems (BTAS), 2010 Fourth IEEE International Conference on*. 2010. IEEE.

20.Ren, X. and X.-W. Wu. *A novel dynamic user authentication scheme*. in *Communications and Information Technologies (ISCIT), 2012 International Symposium on*. 2012. IEEE.

21.Teh, P.S., et al. *Statistical fusion approach on keystroke dynamics*. in *Signal-Image Technologies and Internet-Based System, 2007. SITIS'07. Third International IEEE Conference on*. 2007. IEEE.

22.Karnan, M. and N. Krishnaraj. *Bio password—keystroke dynamic approach to secure mobile devices*. in *Computational Intelligence and Computing Research (ICCIC), 2010 IEEE International Conference on*. 2010. IEEE.

23.Nonsrichai, K. and P. Bhattarakosol. *A new alternative of an authentication system using the eye vision ability*. in *Computing and Convergence Technology (ICCCT), 2012 7th International Conference on*. 2012. IEEE.

24.Chang, M., et al., *Capturing Cognitive Fingerprints from Keystroke Dynamics for Active Authentication.* 2013.

25.Chang, T.-Y., C.-J. Tsai, and J.-H. Lin, *A graphical-based password keystroke dynamic authentication system for touch screen handheld mobile devices.* Journal of Systems and Software, 2012. **85**(5): p. 1157-1165.

26.Hoober, S. *How Do Users Really Hold Mobile Devices?* 2013 18 February 2013 11 November 2013]; Available from: http://www.uxmatters.com/mt/archives/2013/02/how-do-users-really-hold-mobile-devices.php.

27.Jeanjaitrong, N. and P. Bhattarakosol. *Feasibility study on authentication based keystroke dynamic over touch-screen devices*. in *Communications and Information Technologies (ISCIT), 2013 13th International Symposium on*. 2013.

# APPENDIX

# APPENDIX A
## Result of Classification

This section consists of the classification result by Weka® Machine Learning. In classification process, all factors which have been gathered in data collecting process are used. Each result table presents the percentage of accuracy, false acceptance rate (FAR), and false rejection rate (FRR) from each pair of subject. The name of pair represents the combination of two subjects, such as p0102 comes from subject number 1 and subject number 2. The result shows the pairing start from subject number 1 to subject number 25 as follows:

Table A-1 Result of Classification: Subject 01 paring to all subjects, All Factors

| Pair of Subjects | Accuracy (%) | FAR | FRR |
|---|---|---|---|
| p0101 | 100 | 0 | 0 |
| p0102 | 81.7 | 0.183 | 0.183 |
| p0103 | 86.2 | 0.138 | 0.138 |
| p0104 | 99.95 | 0 | 0.001 |
| p0105 | 93.95 | 0.06 | 0.061 |
| p0106 | 85.2 | 0.148 | 0.148 |
| p0107 | 99.95 | 0 | 0.001 |
| p0108 | 90.5 | 0.095 | 0.095 |
| p0109 | 89.05 | 0.109 | 0.11 |
| p0110 | 99.45 | 0.005 | 0.006 |
| p0111 | 87.8 | 0.122 | 0.122 |
| p0112 | 91.1 | 0.089 | 0.089 |
| p0113 | 99.65 | 0.003 | 0.004 |
| p0114 | 79.1 | 0.209 | 0.209 |
| p0115 | 83.85 | 0.161 | 0.162 |
| p0116 | 99.65 | 0.003 | 0.004 |
| p0117 | 99.45 | 0.005 | 0.006 |
| p0118 | 81.95 | 0.18 | 0.181 |
| p0119 | 97 | 0.03 | 0.03 |
| p0120 | 89.45 | 0.105 | 0.106 |
| p0121 | 85.5 | 0.145 | 0.145 |
| p0122 | 87.35 | 0.126 | 0.127 |
| p0123 | 85.5 | 0.145 | 0.145 |
| p0124 | 81.2 | 0.188 | 0.188 |
| p0125 | 100 | 0 | 0 |
| **AVERAGE** | **90.98** | **0.08996** | **0.09044** |

Table A-2 Result of Classification: Subject 02 paring to all subjects, All Factors

| Pair of Subjects | Accuracy (%) | FAR | FRR |
|---|---|---|---|
| p0201 | 81.7 | 0.183 | 0.183 |
| p0202 | 100 | 0 | 0 |
| p0203 | 80.5 | 0.195 | 0.195 |
| p0204 | 99.75 | 0.002 | 0.003 |
| p0205 | 90.2 | 0.098 | 0.098 |
| p0206 | 88.35 | 0.116 | 0.117 |
| p0207 | 99.85 | 0.001 | 0.002 |
| p0208 | 89.4 | 0.106 | 0.106 |
| p0209 | 86.15 | 0.138 | 0.139 |
| p0210 | 99.55 | 0.004 | 0.005 |
| p0211 | 84.9 | 0.151 | 0.151 |
| p0212 | 86.25 | 0.137 | 0.138 |
| p0213 | 99.85 | 0.001 | 0.002 |
| p0214 | 74.5 | 0.255 | 0.255 |
| p0215 | 76.55 | 0.234 | 0.235 |
| p0216 | 99.55 | 0.004 | 0.005 |
| p0217 | 99.55 | 0.004 | 0.005 |
| p0218 | 87.55 | 0.124 | 0.125 |
| p0219 | 98.15 | 0.018 | 0.019 |
| p0220 | 85.35 | 0.146 | 0.147 |
| p0221 | 76.8 | 0.232 | 0.232 |
| p0222 | 92.6 | 0.074 | 0.074 |
| p0223 | 91.2 | 0.088 | 0.088 |
| p0224 | 89 | 0.33 | 0.11 |
| p0225 | 99.95 | 0 | 0.001 |
| **AVERAGE** | **90.288** | **0.10564** | **0.0974** |

Table A-3 Result of Classification: Subject 03 paring to all subjects, All Factors

| Pair of Subjects | Accuracy (%) | FAR | FRR |
|---|---|---|---|
| 86.2 | 0.138 | 0.138 | 86.2 |
| 80.5 | 0.195 | 0.195 | 80.5 |
| 100 | 0 | 0 | 100 |
| 100 | 0 | 0 | 100 |
| 83.45 | 0.165 | 0.166 | 83.45 |
| 85.25 | 0.147 | 0.148 | 85.25 |
| 100 | 0 | 0 | 100 |
| 80.9 | 0.191 | 0.191 | 80.9 |
| 85.35 | 0.146 | 0.147 | 85.35 |
| 99.55 | 0.004 | 0.005 | 99.55 |
| 74.95 | 0.25 | 0.251 | 74.95 |
| 79.35 | 0.206 | 0.207 | 79.35 |
| 99.95 | 0 | 0.001 | 99.95 |
| 68.25 | 0.317 | 0.318 | 68.25 |
| 70.95 | 0.29 | 0.291 | 70.95 |
| 99.6 | 0.004 | 0.004 | 99.6 |
| 99.7 | 0.003 | 0.003 | 99.7 |
| 93.6 | 0.064 | 0.064 | 93.6 |
| 99.05 | 0.009 | 0.01 | 99.05 |
| 78.35 | 0.216 | 0.217 | 78.35 |
| 80.8 | 0.192 | 0.192 | 80.8 |
| 95.75 | 0.042 | 0.043 | 95.75 |
| 84.1 | 0.159 | 0.159 | 84.1 |
| 86.6 | 0.134 | 0.134 | 86.6 |
| 100 | 0 | 0 | 100 |
| **88.488** | **0.11488** | **0.11536** | **88.488** |

Table A-4 Result of Classification: Subject 04 paring to all subjects, All Factors

| Pair of Subjects | Accuracy (%) | FAR | FRR |
|---|---|---|---|
| p0401 | 99.95 | 0 | 0.001 |
| p0402 | 99.75 | 0.002 | 0.003 |
| p0403 | 100 | 0 | 0 |
| p0404 | 100 | 0 | 0 |
| p0405 | 99.9 | 0.001 | 0.001 |
| p0406 | 99.95 | 0 | 0.001 |
| p0407 | 76.75 | 0.232 | 0.233 |
| p0408 | 100 | 0 | 0 |
| p0409 | 100 | 0 | 0 |
| p0410 | 93.35 | 0.066 | 0.067 |
| p0411 | 99.95 | 0 | 0.001 |
| p0412 | 99.75 | 0.002 | 0.003 |
| p0413 | 97 | 0.03 | 0.03 |
| p0414 | 100 | 0 | 0 |
| p0415 | 99.95 | 0 | 0.001 |
| p0416 | 86.45 | 0.135 | 0.136 |
| p0417 | 91.25 | 0.087 | 0.088 |
| p0418 | 100 | 0 | 0 |
| p0419 | 93.5 | 0.065 | 0.065 |
| p0420 | 99.8 | 0.002 | 0.002 |
| p0421 | 100 | 0 | 0 |
| p0422 | 99.95 | 0 | 0.001 |
| p0423 | 100 | 0 | 0 |
| p0424 | 99.95 | 0 | 0.001 |
| p0425 | 73.95 | 0.26 | 0.261 |
| **AVERAGE** | **96.446** | **0.03528** | **0.0358** |

Table A-5 Result of Classification: Subject 05 paring to all subjects, All Factors

| Pair of Subjects | Accuracy (%) | FAR | FRR |
|---|---|---|---|
| p0501 | 93.95 | 0.06 | 0.061 |
| p0502 | 90.2 | 0.098 | 0.098 |
| p0503 | 83.45 | 0.165 | 0.166 |
| p0504 | 99.9 | 0.001 | 0.001 |
| p0505 | 100 | 0 | 0 |
| p0506 | 90.7 | 0.093 | 0.093 |
| p0507 | 99.75 | 0.002 | 0.003 |
| p0508 | 82 | 0.18 | 0.18 |
| p0509 | 73.7 | 0.263 | 0.263 |
| p0510 | 98.8 | 0.012 | 0.012 |
| p0511 | 86.3 | 0.137 | 0.137 |
| p0512 | 83.45 | 0.165 | 0.166 |
| p0513 | 99.3 | 0.007 | 0.007 |
| p0514 | 80.25 | 0.197 | 0.198 |
| p0515 | 81.5 | 0.185 | 0.185 |
| p0516 | 98.9 | 0.011 | 0.011 |
| p0517 | 98.5 | 0.015 | 0.015 |
| p0518 | 96.6 | 0.034 | 0.034 |
| p0519 | 98.1 | 0.019 | 0.019 |
| p0520 | 71.1 | 0.289 | 0.289 |
| p0521 | 84.4 | 0.156 | 0.156 |
| p0522 | 96.75 | 0.032 | 0.033 |
| p0523 | 87.95 | 0.12 | 0.121 |
| p0524 | 87.9 | 0.121 | 0.121 |
| p0525 | 99.75 | 0.002 | 0.003 |
| **AVERAGE** | **90.528** | **0.09456** | **0.09488** |

Table A-6 Result of Classification: Subject 06 paring to all subjects, All Factors

| Pair of Subjects | Accuracy (%) | FAR | FRR |
|---|---|---|---|
| p0601 | 85.2 | 0.148 | 0.148 |
| p0602 | 88.35 | 0.116 | 0.117 |
| p0603 | 85.25 | 0.147 | 0.148 |
| p0604 | 99.95 | 0 | 0.001 |
| p0605 | 90.7 | 0.093 | 0.093 |
| p0606 | 100 | 0 | 0 |
| p0607 | 99.85 | 0.001 | 0.002 |
| p0608 | 84.35 | 0.156 | 0.157 |
| p0609 | 90.15 | 0.098 | 0.099 |
| p0610 | 99.35 | 0.006 | 0.007 |
| p0611 | 83 | 0.17 | 0.17 |
| p0612 | 85.3 | 0.147 | 0.147 |
| p0613 | 99.9 | 0.001 | 0.001 |
| p0614 | 83.25 | 0.167 | 0.168 |
| p0615 | 86.05 | 0.139 | 0.14 |
| p0616 | 99.4 | 0.006 | 0.006 |
| p0617 | 98.9 | 0.011 | 0.011 |
| p0618 | 88.2 | 0.118 | 0.118 |
| p0619 | 98.4 | 0.016 | 0.016 |
| p0620 | 84.6 | 0.154 | 0.154 |
| p0621 | 88.05 | 0.119 | 0.12 |
| p0622 | 91.9 | 0.081 | 0.081 |
| p0623 | 76 | 0.24 | 0.24 |
| p0624 | 87.05 | 0.129 | 0.13 |
| p0625 | 99.95 | 0 | 0.001 |
| AVERAGE | **90.924** | **0.09052** | **0.091** |

Table A-7 Result of Classification: Subject 07 paring to all subjects, All Factors

| Pair of Subjects | Accuracy (%) | FAR | FRR |
|---|---|---|---|
| p0701 | 99.95 | 0 | 0.001 |
| p0702 | 99.85 | 0.001 | 0.002 |
| p0703 | 100 | 0 | 0 |
| p0704 | 76.75 | 0.232 | 0.233 |
| p0705 | 99.75 | 0.002 | 0.003 |
| p0706 | 99.85 | 0.001 | 0.002 |
| p0707 | 100 | 0 | 0 |
| p0708 | 99.95 | 0 | 0.001 |
| p0709 | 99.9 | 0.001 | 0.001 |
| p0710 | 88.75 | 0.112 | 0.113 |
| p0711 | 99.95 | 0 | 0.001 |
| p0712 | 99.95 | 0 | 0.001 |
| p0713 | 90 | 0.1 | 0.1 |
| p0714 | 100 | 0 | 0 |
| p0715 | 100 | 0 | 0 |
| p0716 | 89.2 | 0.108 | 0.108 |
| p0717 | 86.15 | 0.138 | 0.139 |
| p0718 | 99.7 | 0.003 | 0.003 |
| p0719 | 90.55 | 0.094 | 0.095 |
| p0720 | 99.55 | 0.004 | 0.005 |
| p0721 | 99.9 | 0.001 | 0.001 |
| p0722 | 99.8 | 0.002 | 0.002 |
| p0723 | 99.95 | 0 | 0.001 |
| p0724 | 99.45 | 0.005 | 0.006 |
| p0725 | 84.6 | 0.154 | 0.154 |
| **AVERAGE** | **96.14** | **0.03832** | **0.03888** |

Table A-8 Result of Classification: Subject 08 paring to all subjects, All Factors

| Pair of Subjects | Accuracy (%) | FAR | FRR |
|---|---|---|---|
| p0801 | 90.5 | 0.095 | 0.095 |
| p0802 | 89.4 | 0.106 | 0.106 |
| p0803 | 80.9 | 0.191 | 0.191 |
| p0804 | 100 | 0 | 0 |
| p0805 | 82 | 0.18 | 0.18 |
| p0806 | 84.35 | 0.156 | 0.157 |
| p0807 | 99.95 | 0 | 0.001 |
| p0808 | 100 | 0 | 0 |
| p0809 | 86.5 | 0.135 | 0.135 |
| p0810 | 99.7 | 0.003 | 0.003 |
| p0811 | 82.6 | 0.174 | 0.174 |
| p0812 | 80.15 | 0.198 | 0.199 |
| p0813 | 99.9 | 0.001 | 0.001 |
| p0814 | 80.35 | 0.196 | 0.197 |
| p0815 | 77.25 | 0.227 | 0.228 |
| p0816 | 99.55 | 0.004 | 0.005 |
| p0817 | 99.7 | 0.003 | 0.003 |
| p0818 | 94.9 | 0.051 | 0.051 |
| p0819 | 99.4 | 0.006 | 0.006 |
| p0820 | 81.8 | 0.182 | 0.182 |
| p0821 | 86 | 0.14 | 0.14 |
| p0822 | 95.75 | 0.042 | 0.043 |
| p0823 | 80.7 | 0.193 | 0.193 |
| p0824 | 88.1 | 0.119 | 0.119 |
| p0825 | 100 | 0 | 0 |
| **AVERAGE** | **90.378** | **0.09608** | **0.09636** |

Table A-9 Result of Classification: Subject 09 paring to all subjects, All Factors

| Pair of Subjects | Accuracy (%) | FAR | FRR |
|---|---|---|---|
| p0901 | 89.05 | 0.109 | 0.11 |
| p0902 | 86.15 | 0.138 | 0.139 |
| p0903 | 85.35 | 0.146 | 0.147 |
| p0904 | 100 | 0 | 0 |
| p0905 | 73.7 | 0.263 | 0.263 |
| p0906 | 90.15 | 0.098 | 0.099 |
| p0907 | 99.9 | 0.001 | 0.001 |
| p0908 | 86.5 | 0.135 | 0.135 |
| p0909 | 100 | 0 | 0 |
| p0910 | 99.4 | 0.006 | 0.006 |
| p0911 | 84.1 | 0.159 | 0.159 |
| p0912 | 87.1 | 0.129 | 0.129 |
| p0913 | 99.85 | 0.001 | 0.002 |
| p0914 | 77.95 | 0.22 | 0.221 |
| p0915 | 81.85 | 0.181 | 0.182 |
| p0916 | 99.65 | 0.003 | 0.004 |
| p0917 | 99.35 | 0.006 | 0.007 |
| p0918 | 94.95 | 0.05 | 0.051 |
| p0919 | 99.1 | 0.009 | 0.009 |
| p0920 | 85 | 0.15 | 0.15 |
| p0921 | 72 | 0.28 | 0.28 |
| p0922 | 96.85 | 0.031 | 0.032 |
| p0923 | 84.8 | 0.152 | 0.152 |
| p0924 | 80.75 | 0.192 | 0.193 |
| p0925 | 99.95 | 0 | 0.001 |
| **AVERAGE** | **90.138** | **0.09836** | **0.09888** |

Table A-10 Result of Classification: Subject 10 paring to all subjects, All Factors

| Pair of Subjects | Accuracy (%) | FAR | FRR |
|---|---|---|---|
| p1001 | 99.45 | 0.005 | 0.006 |
| p1002 | 99.55 | 0.004 | 0.005 |
| p1003 | 99.55 | 0.004 | 0.005 |
| p1004 | 93.35 | 0.066 | 0.067 |
| p1005 | 98.8 | 0.012 | 0.012 |
| p1006 | 99.35 | 0.006 | 0.007 |
| p1007 | 88.75 | 0.112 | 0.113 |
| p1008 | 99.7 | 0.003 | 0.003 |
| p1009 | 99.4 | 0.006 | 0.006 |
| p1010 | 100 | 0 | 0 |
| p1011 | 99.4 | 0.004 | 0.006 |
| p1012 | 99.65 | 0.003 | 0.004 |
| p1013 | 81.2 | 0.188 | 0.188 |
| p1014 | 99.75 | 0.002 | 0.003 |
| p1015 | 99.6 | 0.004 | 0.004 |
| p1016 | 89.4 | 0.106 | 0.106 |
| p1017 | 82.7 | 0.173 | 0.173 |
| p1018 | 99.2 | 0.008 | 0.008 |
| p1019 | 75.85 | 0.241 | 0.242 |
| p1020 | 98.1 | 0.019 | 0.019 |
| p1021 | 99.45 | 0.005 | 0.006 |
| p1022 | 99.15 | 0.008 | 0.009 |
| p1023 | 99.75 | 0.002 | 0.003 |
| p1024 | 98.1 | 0.019 | 0.019 |
| p1025 | 93.7 | 0.063 | 0.063 |
| AVERAGE | **95.716** | **0.04252** | **0.04308** |

Table A-11 Result of Classification: Subject 11 paring to all subjects, All Factors

| Pair of Subjects | Accuracy (%) | FAR | FRR |
|---|---|---|---|
| p1101 | 87.8 | 0.122 | 0.122 |
| p1102 | 84.9 | 0.151 | 0.151 |
| p1103 | 74.95 | 0.25 | 0.251 |
| p1104 | 99.95 | 0 | 0.001 |
| p1105 | 86.3 | 0.137 | 0.137 |
| p1106 | 83 | 0.17 | 0.17 |
| p1107 | 99.95 | 0 | 0.001 |
| p1108 | 82.6 | 0.174 | 0.174 |
| p1109 | 84.1 | 0.159 | 0.159 |
| p1110 | 99.4 | 0.004 | 0.006 |
| p1111 | 100 | 0 | 0 |
| p1112 | 82.7 | 0.173 | 0.173 |
| p1113 | 99.9 | 0.001 | 0.001 |
| p1114 | 77.15 | 0.228 | 0.229 |
| p1115 | 80.1 | 0.199 | 0.199 |
| p1116 | 99.55 | 0.004 | 0.005 |
| p1117 | 99.25 | 0.007 | 0.008 |
| p1118 | 92.55 | 0.074 | 0.075 |
| p1119 | 98.5 | 0.015 | 0.015 |
| p1120 | 79.4 | 0.206 | 0.206 |
| p1121 | 80.2 | 0.198 | 0.198 |
| p1122 | 95.05 | 0.049 | 0.05 |
| p1123 | 80.9 | 0.191 | 0.191 |
| p1124 | 87.4 | 0.126 | 0.126 |
| p1125 | 99.95 | 0 | 0.001 |
| **AVERAGE** | **89.422** | **0.10552** | **0.10596** |

Table A-12 Result of Classification: Subject 12 paring to all subjects, All Factors

| Pair of Subjects | Accuracy (%) | FAR | FRR |
|---|---|---|---|
| p1201 | 91.1 | 0.089 | 0.089 |
| p1202 | 86.25 | 0.137 | 0.138 |
| p1203 | 79.35 | 0.206 | 0.207 |
| p1204 | 99.75 | 0.002 | 0.003 |
| p1205 | 83.45 | 0.165 | 0.166 |
| p1206 | 85.3 | 0.147 | 0.147 |
| p1207 | 99.95 | 0 | 0.001 |
| p1208 | 80.15 | 0.198 | 0.199 |
| p1209 | 87.1 | 0.129 | 0.129 |
| p1210 | 99.65 | 0.003 | 0.004 |
| p1211 | 82.7 | 0.173 | 0.173 |
| p1212 | 100 | 0 | 0 |
| p1213 | 99.85 | 0.001 | 0.002 |
| p1214 | 77.75 | 0.222 | 0.223 |
| p1215 | 81.8 | 0.182 | 0.182 |
| p1216 | 99.5 | 0.005 | 0.005 |
| p1217 | 99.1 | 0.009 | 0.009 |
| p1218 | 94.7 | 0.053 | 0.053 |
| p1219 | 98.95 | 0.01 | 0.011 |
| p1220 | 75.6 | 0.244 | 0.244 |
| p1221 | 86.95 | 0.13 | 0.131 |
| p1222 | 91.65 | 0.083 | 0.084 |
| p1223 | 89.45 | 0.105 | 0.106 |
| p1224 | 87.65 | 0.123 | 0.124 |
| p1225 | 99.95 | 0 | 0.001 |
| **AVERAGE** | **90.306** | **0.09664** | **0.09724** |

Table A-13 Result of Classification: Subject 13 paring to all subjects, All Factors

| Pair of Subjects | Accuracy (%) | FAR | FRR |
|---|---|---|---|
| p1301 | 99.65 | 0.003 | 0.004 |
| p1302 | 99.85 | 0.001 | 0.002 |
| p1303 | 99.95 | 0 | 0.001 |
| p1304 | 97 | 0.03 | 0.03 |
| p1305 | 99.3 | 0.007 | 0.007 |
| p1306 | 99.9 | 0.001 | 0.001 |
| p1307 | 90 | 0.1 | 0.1 |
| p1308 | 99.9 | 0.001 | 0.001 |
| p1309 | 99.85 | 0.001 | 0.002 |
| p1310 | 81.2 | 0.188 | 0.188 |
| p1311 | 99.9 | 0.001 | 0.001 |
| p1312 | 99.85 | 0.001 | 0.002 |
| p1313 | 100 | 0 | 0 |
| p1314 | 99.8 | 0.002 | 0.002 |
| p1315 | 99.9 | 0.001 | 0.001 |
| p1316 | 92.65 | 0.073 | 0.074 |
| p1317 | 88.9 | 0.111 | 0.111 |
| p1318 | 99.6 | 0.004 | 0.004 |
| p1319 | 81.25 | 0.187 | 0.188 |
| p1320 | 99.1 | 0.009 | 0.009 |
| p1321 | 100 | 0 | 0 |
| p1322 | 99.1 | 0.009 | 0.009 |
| p1323 | 99.8 | 0.002 | 0.002 |
| p1324 | 98.65 | 0.013 | 0.014 |
| p1325 | 97.75 | 0.022 | 0.023 |
| AVERAGE | **96.914** | **0.03068** | **0.03104** |

Table A-14 Result of Classification: Subject 14 paring to all subjects, All Factors

| Pair of Subjects | Accuracy (%) | FAR | FRR |
|---|---|---|---|
| p1401 | 79.1 | 0.209 | 0.209 |
| p1402 | 74.5 | 0.255 | 0.255 |
| p1403 | 68.25 | 0.317 | 0.318 |
| p1404 | 100 | 0 | 0 |
| p1405 | 80.25 | 0.197 | 0.198 |
| p1406 | 83.25 | 0.167 | 0.168 |
| p1407 | 100 | 0 | 0 |
| p1408 | 80.35 | 0.196 | 0.197 |
| p1409 | 77.95 | 0.22 | 0.221 |
| p1410 | 99.75 | 0.002 | 0.003 |
| p1411 | 77.15 | 0.228 | 0.229 |
| p1412 | 77.75 | 0.222 | 0.223 |
| p1413 | 99.8 | 0.002 | 0.002 |
| p1414 | 100 | 0 | 0 |
| p1415 | 67.9 | 0.321 | 0.321 |
| p1416 | 99.9 | 0.001 | 0.001 |
| p1417 | 99.7 | 0.003 | 0.003 |
| p1418 | 90.8 | 0.092 | 0.092 |
| p1419 | 98.6 | 0.014 | 0.014 |
| p1420 | 74.8 | 0.252 | 0.252 |
| p1421 | 79.55 | 0.204 | 0.205 |
| p1422 | 91.65 | 0.083 | 0.084 |
| p1423 | 84.1 | 0.159 | 0.159 |
| p1424 | 82.8 | 0.172 | 0.172 |
| p1425 | 100 | 0 | 0 |
| **AVERAGE** | **86.716** | **0.13264** | **0.13304** |

Table A-15 Result of Classification: Subject 15 paring to all subjects, All Factors

| Pair of Subjects | Accuracy (%) | FAR | FRR |
|---|---|---|---|
| p1501 | 83.85 | 0.161 | 0.162 |
| p1502 | 76.55 | 0.234 | 0.235 |
| p1503 | 70.95 | 0.29 | 0.291 |
| p1504 | 99.95 | 0 | 0.001 |
| p1505 | 81.5 | 0.185 | 0.185 |
| p1506 | 86.05 | 0.139 | 0.14 |
| p1507 | 100 | 0 | 0 |
| p1508 | 77.25 | 0.227 | 0.228 |
| p1509 | 81.85 | 0.181 | 0.182 |
| p1510 | 99.6 | 0.004 | 0.004 |
| p1511 | 80.1 | 0.199 | 0.199 |
| p1512 | 81.8 | 0.182 | 0.182 |
| p1513 | 99.9 | 0.001 | 0.001 |
| p1514 | 67.9 | 0.321 | 0.321 |
| p1515 | 100 | 0 | 0 |
| p1516 | 99.55 | 0.004 | 0.005 |
| p1517 | 99.6 | 0.004 | 0.004 |
| p1518 | 94.3 | 0.057 | 0.057 |
| p1519 | 98.35 | 0.016 | 0.017 |
| p1520 | 82.7 | 0.173 | 0.173 |
| p1521 | 76.9 | 0.231 | 0.231 |
| p1522 | 95.95 | 0.04 | 0.041 |
| p1523 | 82.95 | 0.17 | 0.171 |
| p1524 | 85.65 | 0.143 | 0.144 |
| p1525 | 100 | 0 | 0 |
| **AVERAGE** | **88.128** | **0.11848** | **0.11896** |

Table A-16 Result of Classification: Subject 16 paring to all subjects, All Factors

| Pair of Subjects | Accuracy (%) | FAR | FRR |
|---|---|---|---|
| p1601 | 99.65 | 0.003 | 0.004 |
| p1602 | 99.55 | 0.004 | 0.005 |
| p1603 | 99.6 | 0.004 | 0.004 |
| p1604 | 86.45 | 0.135 | 0.136 |
| p1605 | 98.9 | 0.011 | 0.011 |
| p1606 | 99.4 | 0.006 | 0.006 |
| p1607 | 89.2 | 0.108 | 0.108 |
| p1608 | 99.55 | 0.004 | 0.005 |
| p1609 | 99.65 | 0.003 | 0.004 |
| p1610 | 89.4 | 0.106 | 0.106 |
| p1611 | 99.55 | 0.004 | 0.005 |
| p1612 | 99.5 | 0.005 | 0.005 |
| p1613 | 92.65 | 0.073 | 0.074 |
| p1614 | 99.9 | 0.001 | 0.001 |
| p1615 | 99.55 | 0.004 | 0.005 |
| p1616 | 100 | 0 | 0 |
| p1617 | 82.4 | 0.176 | 0.176 |
| p1618 | 99.2 | 0.008 | 0.008 |
| p1619 | 89 | 0.11 | 0.11 |
| p1620 | 97.95 | 0.02 | 0.021 |
| p1621 | 99.75 | 0.002 | 0.003 |
| p1622 | 99.75 | 0.002 | 0.003 |
| p1623 | 100 | 0 | 0 |
| p1624 | 98.85 | 0.011 | 0.012 |
| p1625 | 84.25 | 0.157 | 0.158 |
| **AVERAGE** | **96.146** | **0.03828** | **0.0388** |

Table A-17 Result of Classification: Subject 17 paring to all subjects, All Factors

| Pair of Subjects | Accuracy (%) | FAR | FRR |
|---|---|---|---|
| p1701 | 99.45 | 0.005 | 0.006 |
| p1702 | 99.55 | 0.004 | 0.005 |
| p1703 | 99.7 | 0.003 | 0.003 |
| p1704 | 91.25 | 0.087 | 0.088 |
| p1705 | 98.5 | 0.015 | 0.015 |
| p1706 | 98.9 | 0.011 | 0.011 |
| p1707 | 86.15 | 0.138 | 0.139 |
| p1708 | 99.7 | 0.003 | 0.003 |
| p1709 | 99.35 | 0.006 | 0.007 |
| p1710 | 82.7 | 0.173 | 0.173 |
| p1711 | 99.25 | 0.007 | 0.008 |
| p1712 | 99.1 | 0.009 | 0.009 |
| p1713 | 88.9 | 0.111 | 0.111 |
| p1714 | 99.7 | 0.003 | 0.003 |
| p1715 | 99.6 | 0.004 | 0.004 |
| p1716 | 82.4 | 0.176 | 0.176 |
| p1717 | 100 | 0 | 0 |
| p1718 | 98.9 | 0.011 | 0.011 |
| p1719 | 81.1 | 0.189 | 0.189 |
| p1720 | 97.4 | 0.026 | 0.026 |
| p1721 | 99.6 | 0.004 | 0.004 |
| p1722 | 99.1 | 0.009 | 0.009 |
| p1723 | 99.6 | 0.004 | 0.004 |
| p1724 | 97.8 | 0.022 | 0.022 |
| p1725 | 94.15 | 0.058 | 0.059 |
| AVERAGE | **95.674** | **0.04312** | **0.0434** |

Table A-18 Result of Classification: Subject 18 paring to all subjects, All Factors

| Pair of Subjects | Accuracy (%) | FAR | FRR |
|---|---|---|---|
| p1801 | 81.95 | 0.18 | 0.181 |
| p1802 | 87.55 | 0.124 | 0.125 |
| p1803 | 93.6 | 0.064 | 0.064 |
| p1804 | 100 | 0 | 0 |
| p1805 | 96.6 | 0.034 | 0.034 |
| p1806 | 88.2 | 0.118 | 0.118 |
| p1807 | 99.7 | 0.003 | 0.003 |
| p1808 | 94.9 | 0.051 | 0.051 |
| p1809 | 94.95 | 0.05 | 0.051 |
| p1810 | 99.2 | 0.008 | 0.008 |
| p1811 | 92.55 | 0.074 | 0.075 |
| p1812 | 94.7 | 0.053 | 0.053 |
| p1813 | 99.6 | 0.004 | 0.004 |
| p1814 | 90.8 | 0.092 | 0.092 |
| p1815 | 94.3 | 0.057 | 0.057 |
| p1816 | 99.2 | 0.008 | 0.008 |
| p1817 | 98.9 | 0.011 | 0.011 |
| p1818 | 100 | 0 | 0 |
| p1819 | 95.5 | 0.045 | 0.045 |
| p1820 | 92.1 | 0.079 | 0.079 |
| p1821 | 91.8 | 0.082 | 0.082 |
| p1822 | 74.25 | 0.257 | 0.258 |
| p1823 | 88.65 | 0.113 | 0.114 |
| p1824 | 93.95 | 0.06 | 0.061 |
| p1825 | 100 | 0 | 0 |
| **AVERAGE** | **93.718** | **0.06268** | **0.06296** |

Table A-19 Result of Classification: Subject 19 paring to all subjects, All Factors

| Pair of Subjects | Accuracy (%) | FAR | FRR |
|---|---|---|---|
| p1901 | 97 | 0.03 | 0.03 |
| p1902 | 98.15 | 0.018 | 0.019 |
| p1903 | 99.05 | 0.009 | 0.01 |
| p1904 | 93.5 | 0.065 | 0.065 |
| p1905 | 98.1 | 0.019 | 0.019 |
| p1906 | 98.4 | 0.016 | 0.016 |
| p1907 | 90.55 | 0.094 | 0.095 |
| p1908 | 99.4 | 0.006 | 0.006 |
| p1909 | 99.1 | 0.009 | 0.009 |
| p1910 | 75.85 | 0.241 | 0.242 |
| p1911 | 98.5 | 0.015 | 0.015 |
| p1912 | 98.95 | 0.01 | 0.011 |
| p1913 | 81.25 | 0.187 | 0.188 |
| p1914 | 98.6 | 0.014 | 0.014 |
| p1915 | 98.35 | 0.016 | 0.017 |
| p1916 | 89 | 0.11 | 0.11 |
| p1917 | 81.1 | 0.189 | 0.189 |
| p1918 | 95.5 | 0.045 | 0.045 |
| p1919 | 100 | 0 | 0 |
| p1920 | 97.05 | 0.029 | 0.03 |
| p1921 | 98.2 | 0.018 | 0.018 |
| p1922 | 97.1 | 0.029 | 0.029 |
| p1923 | 99.1 | 0.009 | 0.009 |
| p1924 | 96.85 | 0.031 | 0.032 |
| p1925 | 93.65 | 0.063 | 0.064 |
| AVERAGE | **94.892** | **0.05088** | **0.05128** |

Table A-20 Result of Classification: Subject 20 paring to all subjects, All Factors

| Pair of Subjects | Accuracy (%) | FAR | FRR |
|---|---|---|---|
| p2001 | 89.45 | 0.105 | 0.106 |
| p2002 | 85.35 | 0.146 | 0.147 |
| p2003 | 78.35 | 0.216 | 0.217 |
| p2004 | 99.8 | 0.002 | 0.002 |
| p2005 | 71.1 | 0.289 | 0.289 |
| p2006 | 84.6 | 0.154 | 0.154 |
| p2007 | 99.55 | 0.004 | 0.005 |
| p2008 | 81.8 | 0.182 | 0.182 |
| p2009 | 85 | 0.15 | 0.15 |
| p2010 | 98.1 | 0.019 | 0.019 |
| p2011 | 79.4 | 0.206 | 0.206 |
| p2012 | 75.6 | 0.244 | 0.244 |
| p2013 | 99.1 | 0.009 | 0.009 |
| p2014 | 74.8 | 0.252 | 0.252 |
| p2015 | 82.7 | 0.173 | 0.173 |
| p2016 | 97.95 | 0.02 | 0.021 |
| p2017 | 97.4 | 0.026 | 0.026 |
| p2018 | 92.1 | 0.079 | 0.079 |
| p2019 | 97.05 | 0.029 | 0.03 |
| p2020 | 100 | 0 | 0 |
| p2021 | 84.2 | 0.158 | 0.158 |
| p2022 | 93.55 | 0.064 | 0.065 |
| p2023 | 88.55 | 0.114 | 0.115 |
| p2024 | 86.5 | 0.135 | 0.135 |
| p2025 | 99.9 | 0.001 | 0.001 |
| AVERAGE | **88.876** | **0.11108** | **0.1114** |

Table A-21 Result of Classification: Subject 21 paring to all subjects, All Factors

| Pair of Subjects | Accuracy (%) | FAR | FRR |
|---|---|---|---|
| p2101 | 85.5 | 0.145 | 0.145 |
| p2102 | 76.8 | 0.232 | 0.232 |
| p2103 | 80.8 | 0.192 | 0.192 |
| p2104 | 100 | 0 | 0 |
| p2105 | 84.4 | 0.156 | 0.156 |
| p2106 | 88.05 | 0.119 | 0.12 |
| p2107 | 99.9 | 0.001 | 0.001 |
| p2108 | 86 | 0.14 | 0.14 |
| p2109 | 72 | 0.28 | 0.28 |
| p2110 | 99.45 | 0.005 | 0.006 |
| p2111 | 80.2 | 0.198 | 0.198 |
| p2112 | 86.95 | 0.13 | 0.131 |
| p2113 | 100 | 0 | 0 |
| p2114 | 79.55 | 0.204 | 0.205 |
| p2115 | 76.9 | 0.231 | 0.231 |
| p2116 | 99.75 | 0.002 | 0.003 |
| p2117 | 99.6 | 0.004 | 0.004 |
| p2118 | 91.8 | 0.082 | 0.082 |
| p2119 | 98.2 | 0.018 | 0.018 |
| p2120 | 84.2 | 0.158 | 0.158 |
| p2121 | 100 | 0 | 0 |
| p2122 | 94.2 | 0.058 | 0.058 |
| p2123 | 86.8 | 0.132 | 0.132 |
| p2124 | 82.5 | 0.175 | 0.175 |
| p2125 | 99.95 | 0 | 0.001 |
| **AVERAGE** | **89.34** | **0.10648** | **0.10672** |

Table A-22 Result of Classification: Subject 22 paring to all subjects, All Factors

| Pair of Subjects | Accuracy (%) | FAR | FRR |
|---|---|---|---|
| p2201 | 87.35 | 0.126 | 0.127 |
| p2202 | 92.6 | 0.074 | 0.074 |
| p2203 | 95.75 | 0.042 | 0.043 |
| p2204 | 99.95 | 0 | 0.001 |
| p2205 | 96.75 | 0.032 | 0.033 |
| p2206 | 91.9 | 0.081 | 0.081 |
| p2207 | 99.8 | 0.002 | 0.002 |
| p2208 | 95.75 | 0.042 | 0.043 |
| p2209 | 96.85 | 0.031 | 0.032 |
| p2210 | 99.15 | 0.008 | 0.009 |
| p2211 | 95.05 | 0.049 | 0.05 |
| p2212 | 91.65 | 0.083 | 0.084 |
| p2213 | 99.1 | 0.009 | 0.009 |
| p2214 | 91.65 | 0.083 | 0.084 |
| p2215 | 95.95 | 0.04 | 0.041 |
| p2216 | 99.75 | 0.002 | 0.003 |
| p2217 | 99.1 | 0.009 | 0.009 |
| p2218 | 74.25 | 0.257 | 0.258 |
| p2219 | 97.1 | 0.029 | 0.029 |
| p2220 | 93.55 | 0.064 | 0.065 |
| p2221 | 94.2 | 0.058 | 0.058 |
| p2222 | 100 | 0 | 0 |
| p2223 | 91.25 | 0.087 | 0.088 |
| p2224 | 94.15 | 0.058 | 0.059 |
| p2225 | 99.85 | 0.001 | 0.002 |
| AVERAGE | **94.898** | **0.05068** | **0.05136** |

Table A-23 Result of Classification: Subject 23 paring to all subjects, All Factors

| Pair of Subjects | Accuracy (%) | FAR | FRR |
|---|---|---|---|
| p2301 | 85.5 | 0.145 | 0.145 |
| p2302 | 91.2 | 0.088 | 0.088 |
| p2303 | 84.1 | 0.159 | 0.159 |
| p2304 | 100 | 0 | 0 |
| p2305 | 87.95 | 0.12 | 0.121 |
| p2306 | 76 | 0.24 | 0.24 |
| p2307 | 99.95 | 0 | 0.001 |
| p2308 | 80.7 | 0.193 | 0.193 |
| p2309 | 84.8 | 0.152 | 0.152 |
| p2310 | 99.75 | 0.002 | 0.003 |
| p2311 | 80.9 | 0.191 | 0.191 |
| p2312 | 89.45 | 0.105 | 0.106 |
| p2313 | 99.8 | 0.002 | 0.002 |
| p2314 | 84.1 | 0.159 | 0.159 |
| p2315 | 82.95 | 0.17 | 0.171 |
| p2316 | 100 | 0 | 0 |
| p2317 | 99.6 | 0.004 | 0.004 |
| p2318 | 88.65 | 0.113 | 0.114 |
| p2319 | 99.1 | 0.009 | 0.009 |
| p2320 | 88.55 | 0.114 | 0.115 |
| p2321 | 86.8 | 0.132 | 0.132 |
| p2322 | 91.25 | 0.087 | 0.088 |
| p2323 | 100 | 0 | 0 |
| p2324 | 84.55 | 0.154 | 0.155 |
| p2325 | 100 | 0 | 0 |
| AVERAGE | **90.626** | **0.09356** | **0.09392** |

Table A-24 Result of Classification: Subject 24 paring to all subjects, All Factors

| Pair of Subjects | Accuracy (%) | FAR | FRR |
|---|---|---|---|
| p2401 | 81.2 | 0.188 | 0.188 |
| p2402 | 89 | 0.33 | 0.11 |
| p2403 | 86.6 | 0.134 | 0.134 |
| p2404 | 99.95 | 0 | 0.001 |
| p2405 | 87.9 | 0.121 | 0.121 |
| p2406 | 87.05 | 0.129 | 0.13 |
| p2407 | 99.45 | 0.005 | 0.006 |
| p2408 | 88.1 | 0.119 | 0.119 |
| p2409 | 80.75 | 0.192 | 0.193 |
| p2410 | 98.1 | 0.019 | 0.019 |
| p2411 | 87.4 | 0.126 | 0.126 |
| p2412 | 87.65 | 0.123 | 0.124 |
| p2413 | 98.65 | 0.013 | 0.014 |
| p2414 | 82.8 | 0.172 | 0.172 |
| p2415 | 85.65 | 0.143 | 0.144 |
| p2416 | 98.85 | 0.011 | 0.012 |
| p2417 | 97.8 | 0.022 | 0.022 |
| p2418 | 93.95 | 0.06 | 0.061 |
| p2419 | 96.85 | 0.031 | 0.032 |
| p2420 | 86.5 | 0.135 | 0.135 |
| p2421 | 82.5 | 0.175 | 0.175 |
| p2422 | 94.15 | 0.058 | 0.059 |
| p2423 | 84.55 | 0.154 | 0.155 |
| p2424 | 100 | 0 | 0 |
| p2425 | 99.95 | 0 | 0.001 |
| AVERAGE | **91.014** | **0.0984** | **0.09012** |

Table A-25 Result of Classification: Subject 25 paring to all subjects, All Factors

| Pair of Subjects | Accuracy (%) | FAR | FRR |
|---|---|---|---|
| p2501 | 100 | 0 | 0 |
| p2502 | 99.95 | 0 | 0.001 |
| p2503 | 100 | 0 | 0 |
| p2504 | 73.95 | 0.26 | 0.261 |
| p2505 | 99.75 | 0.002 | 0.003 |
| p2506 | 99.95 | 0 | 0.001 |
| p2507 | 84.6 | 0.154 | 0.154 |
| p2508 | 100 | 0 | 0 |
| p2509 | 99.95 | 0 | 0.001 |
| p2510 | 93.7 | 0.063 | 0.063 |
| p2511 | 99.95 | 0 | 0.001 |
| p2512 | 99.95 | 0 | 0.001 |
| p2513 | 97.75 | 0.022 | 0.023 |
| p2514 | 100 | 0 | 0 |
| p2515 | 100 | 0 | 0 |
| p2516 | 84.25 | 0.157 | 0.158 |
| p2517 | 94.15 | 0.058 | 0.059 |
| p2518 | 100 | 0 | 0 |
| p2519 | 93.65 | 0.063 | 0.064 |
| p2520 | 99.9 | 0.001 | 0.001 |
| p2521 | 99.95 | 0 | 0.001 |
| p2522 | 99.85 | 0.001 | 0.002 |
| p2523 | 100 | 0 | 0 |
| p2524 | 99.95 | 0 | 0.001 |
| p2525 | 100 | 0 | 0 |
| **AVERAGE** | **96.848** | **0.03124** | **0.0318** |

# APPENDIX B
# Result of Mann-Whitney U Test

This section consists of the result of SPSS® Statistic Software by focusing the significance of distance values. This analysis uses distance values that collected in the data collecting process and analyze by using a nonparametric test. Mann-Whitney U test has been selected to test the null hypothesis, which means the distribution of selected value is the same across categories of user. The Significant level is equal to 0.05, which means that the null hypothesis will be rejected if significant value is less than 0.05. Each result table presents the. significant value from distance1, distance 2, and distance3. The name of the pair represents the combination of two subjects, such as p0102 comes from subject number 1 and subject number 2. The result shows the pairing start from subject number 1 to subject number 25 as follows:

Table B-1 Result of Mann-Whitney U Test: Subject 01 paring to all subjects

| Pair of Subject | dist1 sig | dist2 sig | dist3 sig |
|---|---|---|---|
| p0102 | 0.000 | 0.000 | 0.000 |
| p0103 | 0.000 | 0.000 | 0.000 |
| p0104 | 0.000 | 0.000 | 0.999 |
| p0105 | 0.000 | 0.000 | 0.000 |
| p0106 | 0.000 | 0.000 | 0.002 |
| p0107 | 0.000 | 0.100 | 0.000 |
| p0108 | 0.000 | 0.000 | 0.000 |
| p0109 | 0.046 | 0.006 | 0.000 |
| p0110 | 0.000 | 0.000 | 0.000 |
| p0111 | 0.000 | 0.621 | 0.000 |
| p0112 | 0.000 | 0.000 | 0.008 |
| p0113 | 0.000 | 0.515 | 0.000 |
| p0114 | 0.000 | 0.000 | 0.002 |
| p0115 | 0.000 | 0.003 | 0.000 |
| p0116 | 0.000 | 0.000 | 0.000 |
| p0117 | 0.000 | 0.000 | 0.000 |
| p0118 | 0.008 | 0.167 | 0.000 |
| p0119 | 0.018 | 0.000 | 0.000 |
| p0120 | 0.000 | 0.000 | 0.000 |
| p0121 | 0.000 | 0.908 | 0.000 |
| p0122 | 0.255 | 0.270 | 0.000 |
| p0123 | 0.000 | 0.000 | 0.000 |
| p0124 | 0.680 | 0.000 | 0.000 |
| p0125 | 0.000 | 0.000 | 0.582 |
| AVERAGE | **0.042** | **0.108** | **0.066** |

Table B-2 Result of Mann-Whitney U Test: Subject 02 paring to all subjects

| Pair of Subject | dist1 sig | dist2 sig | dist3 sig |
|---|---|---|---|
| p0201 | 0.000 | 0.000 | 0.000 |
| p0203 | 0.000 | 0.000 | 0.003 |
| p0204 | 0.067 | 0.000 | 0.000 |
| p0205 | 0.000 | 0.565 | 0.000 |
| p0206 | 0.000 | 0.000 | 0.000 |
| p0207 | 0.052 | 0.000 | 0.408 |
| p0208 | 0.000 | 0.000 | 0.042 |
| p0209 | 0.000 | 0.000 | 0.000 |
| p0210 | 0.000 | 0.000 | 0.000 |
| p0211 | 0.006 | 0.000 | 0.468 |
| p0212 | 0.127 | 0.380 | 0.000 |
| p0213 | 0.000 | 0.000 | 0.000 |
| p0214 | 0.000 | 0.073 | 0.000 |
| p0215 | 0.001 | 0.000 | 0.032 |
| p0216 | 0.000 | 0.000 | 0.002 |
| p0217 | 0.003 | 0.000 | 0.000 |
| p0218 | 0.000 | 0.000 | 0.097 |
| p0219 | 0.000 | 0.000 | 0.171 |
| p0220 | 0.473 | 0.000 | 0.790 |
| p0221 | 0.000 | 0.000 | 0.000 |
| p0222 | 0.000 | 0.000 | 0.000 |
| p0223 | 0.004 | 0.000 | 0.000 |
| p0224 | 0.000 | 0.000 | 0.010 |
| p0225 | 0.000 | 0.000 | 0.000 |
| **AVERAGE** | **0.031** | **0.042** | **0.084** |

Table B-3 Result of Mann-Whitney U Test: Subject 03 paring to all subjects

| Pair of Subject | dist1 sig | dist2 sig | dist3 sig |
|---|---|---|---|
| p0301 | 0.000 | 0.000 | 0.000 |
| p0302 | 0.000 | 0.000 | 0.003 |
| p0304 | 0.000 | 0.023 | 0.000 |
| p0305 | 0.000 | 0.000 | 0.000 |
| p0306 | 0.006 | 0.003 | 0.000 |
| p0307 | 0.000 | 0.000 | 0.043 |
| p0308 | 0.000 | 0.020 | 0.398 |
| p0309 | 0.000 | 0.000 | 0.000 |
| p0310 | 0.000 | 0.000 | 0.000 |
| p0311 | 0.000 | 0.000 | 0.031 |
| p0312 | 0.000 | 0.000 | 0.000 |
| p0313 | 0.000 | 0.000 | 0.000 |
| p0314 | 0.000 | 0.000 | 0.000 |
| p0315 | 0.000 | 0.340 | 0.000 |
| p0316 | 0.000 | 0.022 | 0.953 |
| p0317 | 0.000 | 0.000 | 0.000 |
| p0318 | 0.000 | 0.000 | 0.095 |
| p0319 | 0.000 | 0.000 | 0.000 |
| p0320 | 0.000 | 0.000 | 0.011 |
| p0321 | 0.000 | 0.000 | 0.024 |
| p0322 | 0.000 | 0.000 | 0.000 |
| p0323 | 0.000 | 0.000 | 0.000 |
| p0324 | 0.000 | 0.000 | 0.816 |
| p0325 | 0.000 | 0.000 | 0.000 |
| **AVERAGE** | **0.000** | **0.017** | **0.099** |

Table B-4 Result of Mann-Whitney U Test: Subject 04 paring to all subjects

| Pair of Subject | dist1 sig | dist2 sig | dist3 sig |
|---|---|---|---|
| p0401 | 0.000 | 0.000 | 0.999 |
| p0402 | 0.067 | 0.000 | 0.000 |
| p0403 | 0.000 | 0.023 | 0.000 |
| p0405 | 0.000 | 0.000 | 0.000 |
| p0406 | 0.000 | 0.861 | 0.002 |
| p0407 | 0.978 | 0.000 | 0.000 |
| p0408 | 0.000 | 0.848 | 0.000 |
| p0409 | 0.000 | 0.000 | 0.000 |
| p0410 | 0.000 | 0.000 | 0.000 |
| p0411 | 0.000 | 0.000 | 0.000 |
| p0412 | 0.695 | 0.000 | 0.007 |
| p0413 | 0.000 | 0.000 | 0.000 |
| p0414 | 0.000 | 0.000 | 0.001 |
| p0415 | 0.185 | 0.003 | 0.000 |
| p0416 | 0.000 | 0.977 | 0.000 |
| p0417 | 0.425 | 0.000 | 0.000 |
| p0418 | 0.000 | 0.000 | 0.000 |
| p0419 | 0.000 | 0.000 | 0.000 |
| p0420 | 0.007 | 0.000 | 0.000 |
| p0421 | 0.000 | 0.000 | 0.000 |
| p0422 | 0.000 | 0.000 | 0.000 |
| p0423 | 0.492 | 0.000 | 0.000 |
| p0424 | 0.000 | 0.000 | 0.000 |
| p0425 | 0.000 | 0.000 | 0.579 |
| **AVERAGE** | **0.119** | **0.113** | **0.066** |

Table B-5 Result of Mann-Whitney U Test: Subject 05 paring to all subjects

| Pair of Subject | dist1 sig | dist2 sig | dist3 sig |
|---|---|---|---|
| p0501 | 0.000 | 0.000 | 0.000 |
| p0502 | 0.000 | 0.565 | 0.000 |
| p0503 | 0.000 | 0.000 | 0.000 |
| p0504 | 0.000 | 0.000 | 0.000 |
| p0506 | 0.000 | 0.000 | 0.000 |
| p0507 | 0.000 | 0.000 | 0.000 |
| p0508 | 0.000 | 0.000 | 0.000 |
| p0509 | 0.000 | 0.000 | 0.106 |
| p0510 | 0.522 | 0.000 | 0.000 |
| p0511 | 0.000 | 0.000 | 0.000 |
| p0512 | 0.000 | 0.203 | 0.000 |
| p0513 | 0.000 | 0.000 | 0.001 |
| p0514 | 0.000 | 0.228 | 0.000 |
| p0515 | 0.000 | 0.000 | 0.000 |
| p0516 | 0.128 | 0.000 | 0.000 |
| p0517 | 0.000 | 0.000 | 0.005 |
| p0518 | 0.000 | 0.000 | 0.000 |
| p0519 | 0.000 | 0.000 | 0.000 |
| p0520 | 0.000 | 0.000 | 0.000 |
| p0521 | 0.000 | 0.000 | 0.000 |
| p0522 | 0.000 | 0.000 | 0.000 |
| p0523 | 0.000 | 0.000 | 0.043 |
| p0524 | 0.000 | 0.000 | 0.000 |
| p0525 | 0.000 | 0.000 | 0.000 |
| **AVERAGE** | **0.027** | **0.042** | **0.006** |

Table B-6 Result of Mann-Whitney U Test: Subject 06 paring to all subjects

| Pair of Subject | dist1 sig | dist2 sig | dist3 sig |
|---|---|---|---|
| p0601 | 0.000 | 0.000 | 0.002 |
| p0602 | 0.000 | 0.000 | 0.000 |
| p0603 | 0.006 | 0.003 | 0.000 |
| p0604 | 0.000 | 0.861 | 0.002 |
| p0605 | 0.000 | 0.000 | 0.000 |
| p0607 | 0.000 | 0.000 | 0.000 |
| p0608 | 0.000 | 0.869 | 0.000 |
| p0609 | 0.000 | 0.000 | 0.000 |
| p0610 | 0.000 | 0.000 | 0.000 |
| p0611 | 0.000 | 0.000 | 0.000 |
| p0612 | 0.000 | 0.000 | 0.000 |
| p0613 | 0.000 | 0.000 | 0.000 |
| p0614 | 0.007 | 0.000 | 0.822 |
| p0615 | 0.000 | 0.000 | 0.004 |
| p0616 | 0.000 | 0.800 | 0.000 |
| p0617 | 0.000 | 0.000 | 0.000 |
| p0618 | 0.000 | 0.000 | 0.000 |
| p0619 | 0.000 | 0.000 | 0.000 |
| p0620 | 0.000 | 0.000 | 0.000 |
| p0621 | 0.000 | 0.000 | 0.000 |
| p0622 | 0.000 | 0.000 | 0.000 |
| p0623 | 0.000 | 0.000 | 0.000 |
| p0624 | 0.000 | 0.000 | 0.000 |
| p0625 | 0.000 | 0.000 | 0.000 |
| **AVERAGE** | **0.001** | **0.106** | **0.035** |

Table B-7 Result of Mann-Whitney U Test: Subject 07 paring to all subjects

| Pair of Subject | dist1 sig | dist2 sig | dist3 sig |
|---|---|---|---|
| p0701 | 0.000 | 0.100 | 0.000 |
| p0702 | 0.052 | 0.000 | 0.408 |
| p0703 | 0.000 | 0.000 | 0.043 |
| p0704 | 0.978 | 0.000 | 0.000 |
| p0705 | 0.000 | 0.000 | 0.000 |
| p0706 | 0.000 | 0.000 | 0.000 |
| p0708 | 0.000 | 0.000 | 0.256 |
| p0709 | 0.000 | 0.222 | 0.000 |
| p0710 | 0.000 | 0.000 | 0.000 |
| p0711 | 0.000 | 0.014 | 0.963 |
| p0712 | 0.758 | 0.000 | 0.000 |
| p0713 | 0.000 | 0.007 | 0.000 |
| p0714 | 0.000 | 0.000 | 0.000 |
| p0715 | 0.168 | 0.000 | 0.006 |
| p0716 | 0.000 | 0.000 | 0.034 |
| p0717 | 0.434 | 0.000 | 0.000 |
| p0718 | 0.000 | 0.000 | 0.513 |
| p0719 | 0.000 | 0.000 | 0.047 |
| p0720 | 0.007 | 0.000 | 0.657 |
| p0721 | 0.000 | 0.041 | 0.000 |
| p0722 | 0.000 | 0.002 | 0.000 |
| p0723 | 0.567 | 0.000 | 0.000 |
| p0724 | 0.000 | 0.027 | 0.081 |
| p0725 | 0.000 | 0.000 | 0.000 |
| AVERAGE | **0.124** | **0.017** | **0.125** |

Table B-8 Result of Mann-Whitney U Test: Subject 08 paring to all subjects

| Pair of Subject | dist1 sig | dist2 sig | dist3 sig |
|---|---|---|---|
| p0801 | 0.000 | 0.000 | 0.000 |
| p0802 | 0.000 | 0.000 | 0.042 |
| p0803 | 0.000 | 0.020 | 0.398 |
| p0804 | 0.000 | 0.848 | 0.000 |
| p0805 | 0.000 | 0.000 | 0.000 |
| p0806 | 0.000 | 0.869 | 0.000 |
| p0807 | 0.000 | 0.000 | 0.256 |
| p0809 | 0.000 | 0.000 | 0.000 |
| p0810 | 0.000 | 0.000 | 0.000 |
| p0811 | 0.000 | 0.000 | 0.206 |
| p0812 | 0.000 | 0.000 | 0.000 |
| p0813 | 0.000 | 0.000 | 0.000 |
| p0814 | 0.000 | 0.000 | 0.000 |
| p0815 | 0.000 | 0.002 | 0.000 |
| p0816 | 0.000 | 0.879 | 0.372 |
| p0817 | 0.000 | 0.000 | 0.000 |
| p0818 | 0.000 | 0.000 | 0.472 |
| p0819 | 0.000 | 0.000 | 0.001 |
| p0820 | 0.000 | 0.000 | 0.103 |
| p0821 | 0.004 | 0.000 | 0.003 |
| p0822 | 0.002 | 0.000 | 0.000 |
| p0823 | 0.000 | 0.000 | 0.000 |
| p0824 | 0.000 | 0.000 | 0.570 |
| p0825 | 0.000 | 0.000 | 0.000 |
| **AVERAGE** | **0.000** | **0.109** | **0.101** |

Table B-9 Result of Mann-Whitney U Test: Subject 09 paring to all subjects

| Pair of Subject | dist1 sig | dist2 sig | dist3 sig |
|---|---|---|---|
| p0901 | 0.046 | 0.006 | 0.000 |
| p0902 | 0.000 | 0.000 | 0.000 |
| p0903 | 0.000 | 0.000 | 0.000 |
| p0904 | 0.000 | 0.000 | 0.000 |
| p0905 | 0.000 | 0.000 | 0.106 |
| p0906 | 0.000 | 0.000 | 0.000 |
| p0907 | 0.000 | 0.222 | 0.000 |
| p0908 | 0.000 | 0.000 | 0.000 |
| p0910 | 0.000 | 0.000 | 0.000 |
| p0911 | 0.000 | 0.000 | 0.000 |
| p0912 | 0.000 | 0.000 | 0.000 |
| p0913 | 0.000 | 0.000 | 0.000 |
| p0914 | 0.000 | 0.000 | 0.000 |
| p0915 | 0.000 | 0.000 | 0.000 |
| p0916 | 0.008 | 0.000 | 0.000 |
| p0917 | 0.000 | 0.000 | 0.000 |
| p0918 | 0.676 | 0.000 | 0.000 |
| p0919 | 0.842 | 0.002 | 0.000 |
| p0920 | 0.000 | 0.000 | 0.000 |
| p0921 | 0.000 | 0.001 | 0.073 |
| p0922 | 0.000 | 0.000 | 0.000 |
| p0923 | 0.000 | 0.000 | 0.780 |
| p0924 | 0.092 | 0.234 | 0.000 |
| p0925 | 0.000 | 0.000 | 0.000 |
| **AVERAGE** | **0.069** | **0.019** | **0.040** |

Table B-10 Result of Mann-Whitney U Test: Subject 10 paring to all subjects

| Pair of Subject | dist1 sig | dist2 sig | dist3 sig |
|---|---|---|---|
| p1001 | 0.000 | 0.000 | 0.000 |
| p1002 | 0.000 | 0.000 | 0.000 |
| p1003 | 0.000 | 0.000 | 0.000 |
| p1004 | 0.000 | 0.000 | 0.000 |
| p1005 | 0.522 | 0.000 | 0.000 |
| p1006 | 0.000 | 0.000 | 0.000 |
| p1007 | 0.000 | 0.000 | 0.000 |
| p1008 | 0.000 | 0.000 | 0.000 |
| p1009 | 0.000 | 0.000 | 0.000 |
| p1011 | 0.000 | 0.000 | 0.000 |
| p1012 | 0.000 | 0.000 | 0.000 |
| p1013 | 0.000 | 0.000 | 0.000 |
| p1014 | 0.000 | 0.000 | 0.000 |
| p1015 | 0.000 | 0.000 | 0.000 |
| p1016 | 0.026 | 0.000 | 0.000 |
| p1017 | 0.000 | 0.692 | 0.000 |
| p1018 | 0.000 | 0.000 | 0.000 |
| p1019 | 0.000 | 0.155 | 0.000 |
| p1020 | 0.000 | 0.000 | 0.000 |
| p1021 | 0.000 | 0.000 | 0.000 |
| p1022 | 0.000 | 0.000 | 0.685 |
| p1023 | 0.000 | 0.376 | 0.000 |
| p1024 | 0.000 | 0.012 | 0.000 |
| p1025 | 0.000 | 0.000 | 0.000 |
| **AVERAGE** | **0.023** | **0.051** | **0.029** |

Table B-11 Result of Mann-Whitney U Test: Subject 11 paring to all subjects

| Pair of Subject | dist1 sig | dist2 sig | dist3 sig |
|---|---|---|---|
| p1101 | 0.000 | 0.621 | 0.000 |
| p1102 | 0.006 | 0.000 | 0.468 |
| p1103 | 0.000 | 0.000 | 0.031 |
| p1104 | 0.000 | 0.000 | 0.000 |
| p1105 | 0.000 | 0.000 | 0.000 |
| p1106 | 0.000 | 0.000 | 0.000 |
| p1107 | 0.000 | 0.014 | 0.963 |
| p1108 | 0.000 | 0.000 | 0.206 |
| p1109 | 0.000 | 0.000 | 0.000 |
| p1110 | 0.000 | 0.000 | 0.000 |
| p1112 | 0.000 | 0.000 | 0.000 |
| p1113 | 0.000 | 0.841 | 0.000 |
| p1114 | 0.095 | 0.000 | 0.000 |
| p1115 | 0.000 | 0.003 | 0.006 |
| p1116 | 0.000 | 0.000 | 0.027 |
| p1117 | 0.000 | 0.000 | 0.000 |
| p1118 | 0.000 | 0.412 | 0.404 |
| p1119 | 0.000 | 0.000 | 0.048 |
| p1120 | 0.172 | 0.000 | 0.662 |
| p1121 | 0.000 | 0.551 | 0.000 |
| p1122 | 0.000 | 0.672 | 0.000 |
| p1123 | 0.000 | 0.000 | 0.000 |
| p1124 | 0.000 | 0.000 | 0.068 |
| p1125 | 0.684 | 0.000 | 0.000 |
| **AVERAGE** | **0.040** | **0.130** | **0.120** |

Table B-12 Result of Mann-Whitney U Test: Subject 12 paring to all subjects

| Pair of Subject | dist1 sig | dist2 sig | dist3 sig |
|---|---|---|---|
| p1201 | 0.000 | 0.000 | 0.008 |
| p1202 | 0.127 | 0.380 | 0.000 |
| p1203 | 0.000 | 0.000 | 0.000 |
| p1204 | 0.695 | 0.000 | 0.007 |
| p1205 | 0.000 | 0.203 | 0.000 |
| p1206 | 0.000 | 0.000 | 0.000 |
| p1207 | 0.758 | 0.000 | 0.000 |
| p1208 | 0.000 | 0.000 | 0.000 |
| p1209 | 0.000 | 0.000 | 0.000 |
| p1210 | 0.000 | 0.000 | 0.000 |
| p1211 | 0.000 | 0.000 | 0.000 |
| p1213 | 0.000 | 0.000 | 0.000 |
| p1214 | 0.000 | 0.032 | 0.000 |
| p1215 | 0.093 | 0.000 | 0.000 |
| p1216 | 0.000 | 0.000 | 0.000 |
| p1217 | 0.305 | 0.000 | 0.000 |
| p1218 | 0.000 | 0.000 | 0.000 |
| p1219 | 0.000 | 0.000 | 0.000 |
| p1220 | 0.014 | 0.000 | 0.000 |
| p1221 | 0.000 | 0.000 | 0.000 |
| p1222 | 0.000 | 0.000 | 0.000 |
| p1223 | 0.414 | 0.000 | 0.000 |
| p1224 | 0.000 | 0.000 | 0.000 |
| p1225 | 0.000 | 0.005 | 0.022 |
| **AVERAGE** | **0.100** | **0.026** | **0.002** |

Table B-13 Result of Mann-Whitney U Test: Subject 13 paring to all subjects

| Pair of Subject | dist1 sig | dist2 sig | dist3 sig |
|---|---|---|---|
| p1301 | 0.000 | 0.515 | 0.000 |
| p1302 | 0.000 | 0.000 | 0.000 |
| p1303 | 0.000 | 0.000 | 0.000 |
| p1304 | 0.000 | 0.000 | 0.000 |
| p1305 | 0.000 | 0.000 | 0.001 |
| p1306 | 0.000 | 0.000 | 0.000 |
| p1307 | 0.000 | 0.007 | 0.000 |
| p1308 | 0.000 | 0.000 | 0.000 |
| p1309 | 0.000 | 0.000 | 0.000 |
| p1310 | 0.000 | 0.000 | 0.000 |
| p1311 | 0.000 | 0.841 | 0.000 |
| p1312 | 0.000 | 0.000 | 0.000 |
| p1314 | 0.000 | 0.000 | 0.000 |
| p1315 | 0.000 | 0.000 | 0.000 |
| p1316 | 0.000 | 0.000 | 0.000 |
| p1317 | 0.000 | 0.000 | 0.887 |
| p1318 | 0.000 | 0.176 | 0.000 |
| p1319 | 0.000 | 0.000 | 0.000 |
| p1320 | 0.000 | 0.000 | 0.000 |
| p1321 | 0.335 | 0.577 | 0.000 |
| p1322 | 0.000 | 0.490 | 0.000 |
| p1323 | 0.000 | 0.000 | 0.000 |
| p1324 | 0.000 | 0.000 | 0.000 |
| p1325 | 0.000 | 0.000 | 0.000 |
| **AVERAGE** | **0.014** | **0.109** | **0.037** |

Table B-14 Result of Mann-Whitney U Test: Subject 14 paring to all subjects

| Pair of Subject | dist1 sig | dist2 sig | dist3 sig |
|---|---|---|---|
| p1401 | 0.000 | 0.000 | 0.002 |
| p1402 | 0.000 | 0.073 | 0.000 |
| p1403 | 0.000 | 0.000 | 0.000 |
| p1404 | 0.000 | 0.000 | 0.001 |
| p1405 | 0.000 | 0.228 | 0.000 |
| p1406 | 0.007 | 0.000 | 0.822 |
| p1407 | 0.000 | 0.000 | 0.000 |
| p1408 | 0.000 | 0.000 | 0.000 |
| p1409 | 0.000 | 0.000 | 0.000 |
| p1410 | 0.000 | 0.000 | 0.000 |
| p1411 | 0.095 | 0.000 | 0.000 |
| p1412 | 0.000 | 0.032 | 0.000 |
| p1413 | 0.000 | 0.000 | 0.000 |
| p1415 | 0.000 | 0.000 | 0.016 |
| p1416 | 0.000 | 0.000 | 0.000 |
| p1417 | 0.000 | 0.000 | 0.000 |
| p1418 | 0.000 | 0.000 | 0.000 |
| p1419 | 0.000 | 0.000 | 0.000 |
| p1420 | 0.003 | 0.000 | 0.000 |
| p1421 | 0.000 | 0.000 | 0.000 |
| p1422 | 0.000 | 0.000 | 0.000 |
| p1423 | 0.000 | 0.000 | 0.000 |
| p1424 | 0.000 | 0.000 | 0.000 |
| p1425 | 0.218 | 0.000 | 0.000 |
| **AVERAGE** | **0.013** | **0.014** | **0.035** |

Table B-15 Result of Mann-Whitney U Test: Subject 15 paring to all subjects

| Pair of Subject | dist1 sig | dist2 sig | dist3 sig |
|---|---|---|---|
| p1501 | 0.000 | 0.003 | 0.000 |
| p1502 | 0.001 | 0.000 | 0.032 |
| p1503 | 0.000 | 0.340 | 0.000 |
| p1504 | 0.185 | 0.003 | 0.000 |
| p1505 | 0.000 | 0.000 | 0.000 |
| p1506 | 0.000 | 0.000 | 0.004 |
| p1507 | 0.168 | 0.000 | 0.006 |
| p1508 | 0.000 | 0.002 | 0.000 |
| p1509 | 0.000 | 0.000 | 0.000 |
| p1510 | 0.000 | 0.000 | 0.000 |
| p1511 | 0.000 | 0.003 | 0.006 |
| p1512 | 0.093 | 0.000 | 0.000 |
| p1513 | 0.000 | 0.000 | 0.000 |
| p1514 | 0.000 | 0.000 | 0.016 |
| p1516 | 0.000 | 0.002 | 0.000 |
| p1517 | 0.483 | 0.000 | 0.000 |
| p1518 | 0.000 | 0.010 | 0.000 |
| p1519 | 0.000 | 0.000 | 0.269 |
| p1520 | 0.000 | 0.000 | 0.019 |
| p1521 | 0.000 | 0.000 | 0.000 |
| p1522 | 0.000 | 0.003 | 0.000 |
| p1523 | 0.373 | 0.000 | 0.000 |
| p1524 | 0.000 | 0.000 | 0.000 |
| p1525 | 0.000 | 0.000 | 0.000 |
| **AVERAGE** | **0.054** | **0.015** | **0.015** |

Table B-16 Result of Mann-Whitney U Test: Subject 16 paring to all subjects

| Pair of Subject | dist1 sig | dist2 sig | dist3 sig |
|---|---|---|---|
| p1601 | 0.000 | 0.000 | 0.000 |
| p1602 | 0.000 | 0.000 | 0.002 |
| p1603 | 0.000 | 0.022 | 0.953 |
| p1604 | 0.000 | 0.977 | 0.000 |
| p1605 | 0.128 | 0.000 | 0.000 |
| p1606 | 0.000 | 0.800 | 0.000 |
| p1607 | 0.000 | 0.000 | 0.034 |
| p1608 | 0.000 | 0.879 | 0.372 |
| p1609 | 0.008 | 0.000 | 0.000 |
| p1610 | 0.026 | 0.000 | 0.000 |
| p1611 | 0.000 | 0.000 | 0.027 |
| p1612 | 0.000 | 0.000 | 0.000 |
| p1613 | 0.000 | 0.000 | 0.000 |
| p1614 | 0.000 | 0.000 | 0.000 |
| p1615 | 0.000 | 0.002 | 0.000 |
| p1617 | 0.000 | 0.000 | 0.000 |
| p1618 | 0.015 | 0.000 | 0.058 |
| p1619 | 0.006 | 0.000 | 0.000 |
| p1620 | 0.000 | 0.000 | 0.008 |
| p1621 | 0.000 | 0.000 | 0.025 |
| p1622 | 0.000 | 0.000 | 0.000 |
| p1623 | 0.000 | 0.000 | 0.000 |
| p1624 | 0.000 | 0.000 | 0.776 |
| p1625 | 0.000 | 0.000 | 0.000 |
| **AVERAGE** | **0.008** | **0.112** | **0.094** |

Table B-17 Result of Mann-Whitney U Test: Subject 17 paring to all subjects

| Pair of Subject | dist1 sig | dist2 sig | dist3 sig |
|---|---|---|---|
| p1701 | 0.000 | 0.000 | 0.000 |
| p1702 | 0.003 | 0.000 | 0.000 |
| p1703 | 0.000 | 0.000 | 0.000 |
| p1704 | 0.425 | 0.000 | 0.000 |
| p1705 | 0.000 | 0.000 | 0.005 |
| p1706 | 0.000 | 0.000 | 0.000 |
| p1707 | 0.434 | 0.000 | 0.000 |
| p1708 | 0.000 | 0.000 | 0.000 |
| p1709 | 0.000 | 0.000 | 0.000 |
| p1710 | 0.000 | 0.692 | 0.000 |
| p1711 | 0.000 | 0.000 | 0.000 |
| p1712 | 0.305 | 0.000 | 0.000 |
| p1713 | 0.000 | 0.000 | 0.887 |
| p1714 | 0.000 | 0.000 | 0.000 |
| p1715 | 0.483 | 0.000 | 0.000 |
| p1716 | 0.000 | 0.000 | 0.000 |
| p1718 | 0.000 | 0.000 | 0.000 |
| p1719 | 0.000 | 0.457 | 0.000 |
| p1720 | 0.001 | 0.000 | 0.000 |
| p1721 | 0.000 | 0.000 | 0.000 |
| p1722 | 0.000 | 0.000 | 0.000 |
| p1723 | 0.820 | 0.248 | 0.000 |
| p1724 | 0.000 | 0.033 | 0.000 |
| p1725 | 0.000 | 0.000 | 0.000 |
| **AVERAGE** | **0.103** | **0.060** | **0.037** |

Table B-18 Result of Mann-Whitney U Test: Subject 18 paring to all subjects

| Pair of Subject | dist1 sig | dist2 sig | dist3 sig |
|---|---|---|---|
| p1801 | 0.008 | 0.167 | 0.000 |
| p1802 | 0.000 | 0.000 | 0.097 |
| p1803 | 0.000 | 0.000 | 0.095 |
| p1804 | 0.000 | 0.000 | 0.000 |
| p1805 | 0.000 | 0.000 | 0.000 |
| p1806 | 0.000 | 0.000 | 0.000 |
| p1807 | 0.000 | 0.000 | 0.513 |
| p1808 | 0.000 | 0.000 | 0.472 |
| p1809 | 0.676 | 0.000 | 0.000 |
| p1810 | 0.000 | 0.000 | 0.000 |
| p1811 | 0.000 | 0.412 | 0.404 |
| p1812 | 0.000 | 0.000 | 0.000 |
| p1813 | 0.000 | 0.176 | 0.000 |
| p1814 | 0.000 | 0.000 | 0.000 |
| p1815 | 0.000 | 0.010 | 0.000 |
| p1816 | 0.015 | 0.000 | 0.058 |
| p1817 | 0.000 | 0.000 | 0.000 |
| p1819 | 0.913 | 0.000 | 0.001 |
| p1820 | 0.000 | 0.000 | 0.175 |
| p1821 | 0.000 | 0.099 | 0.000 |
| p1822 | 0.000 | 0.528 | 0.000 |
| p1823 | 0.000 | 0.000 | 0.000 |
| p1824 | 0.020 | 0.000 | 0.197 |
| p1825 | 0.000 | 0.000 | 0.000 |
| **AVERAGE** | **0.068** | **0.058** | **0.084** |

Table B-19 Result of Mann-Whitney U Test: Subject 19 paring to all subjects

| Pair of Subject | dist1 sig | dist2 sig | dist3 sig |
|---|---|---|---|
| p1901 | 0.018 | 0.000 | 0.000 |
| p1902 | 0.000 | 0.000 | 0.171 |
| p1903 | 0.000 | 0.000 | 0.000 |
| p1904 | 0.000 | 0.000 | 0.000 |
| p1905 | 0.000 | 0.000 | 0.000 |
| p1906 | 0.000 | 0.000 | 0.000 |
| p1907 | 0.000 | 0.000 | 0.047 |
| p1908 | 0.000 | 0.000 | 0.001 |
| p1909 | 0.842 | 0.002 | 0.000 |
| p1910 | 0.000 | 0.155 | 0.000 |
| p1911 | 0.000 | 0.000 | 0.048 |
| p1912 | 0.000 | 0.000 | 0.000 |
| p1913 | 0.000 | 0.000 | 0.000 |
| p1914 | 0.000 | 0.000 | 0.000 |
| p1915 | 0.000 | 0.000 | 0.269 |
| p1916 | 0.006 | 0.000 | 0.000 |
| p1917 | 0.000 | 0.457 | 0.000 |
| p1918 | 0.913 | 0.000 | 0.001 |
| p1920 | 0.000 | 0.000 | 0.154 |
| p1921 | 0.000 | 0.000 | 0.000 |
| p1922 | 0.000 | 0.000 | 0.000 |
| p1923 | 0.000 | 0.024 | 0.000 |
| p1924 | 0.034 | 0.177 | 0.000 |
| p1925 | 0.000 | 0.000 | 0.000 |
| **AVERAGE** | **0.076** | **0.034** | **0.029** |

Table B-20 Result of Mann-Whitney U Test: Subject 20 paring to all subjects

| Pair of Subject | dist1 sig | dist2 sig | dist3 sig |
|---|---|---|---|
| p2001 | 0.000 | 0.000 | 0.000 |
| p2002 | 0.473 | 0.000 | 0.790 |
| p2003 | 0.000 | 0.000 | 0.011 |
| p2004 | 0.007 | 0.000 | 0.000 |
| p2005 | 0.000 | 0.000 | 0.000 |
| p2006 | 0.000 | 0.000 | 0.000 |
| p2007 | 0.007 | 0.000 | 0.657 |
| p2008 | 0.000 | 0.000 | 0.103 |
| p2009 | 0.000 | 0.000 | 0.000 |
| p2010 | 0.000 | 0.000 | 0.000 |
| p2011 | 0.172 | 0.000 | 0.662 |
| p2012 | 0.014 | 0.000 | 0.000 |
| p2013 | 0.000 | 0.000 | 0.000 |
| p2014 | 0.003 | 0.000 | 0.000 |
| p2015 | 0.000 | 0.000 | 0.019 |
| p2016 | 0.000 | 0.000 | 0.008 |
| p2017 | 0.001 | 0.000 | 0.000 |
| p2018 | 0.000 | 0.000 | 0.175 |
| p2019 | 0.000 | 0.000 | 0.154 |
| p2021 | 0.000 | 0.000 | 0.000 |
| p2022 | 0.000 | 0.000 | 0.000 |
| p2023 | 0.001 | 0.000 | 0.000 |
| p2024 | 0.000 | 0.000 | 0.028 |
| p2025 | 0.026 | 0.000 | 0.000 |
| **AVERAGE** | **0.029** | **0.000** | **0.109** |

Table B-21 Result of Mann-Whitney U Test: Subject 21 paring to all subjects

| Pair of Subject | dist1 sig | dist2 sig | dist3 sig |
|---|---|---|---|
| p2101 | 0.000 | 0.908 | 0.000 |
| p2102 | 0.000 | 0.000 | 0.000 |
| p2103 | 0.000 | 0.000 | 0.024 |
| p2104 | 0.000 | 0.000 | 0.000 |
| p2105 | 0.000 | 0.000 | 0.000 |
| p2106 | 0.000 | 0.000 | 0.000 |
| p2107 | 0.000 | 0.041 | 0.000 |
| p2108 | 0.004 | 0.000 | 0.003 |
| p2109 | 0.000 | 0.001 | 0.073 |
| p2110 | 0.000 | 0.000 | 0.000 |
| p2111 | 0.000 | 0.551 | 0.000 |
| p2112 | 0.000 | 0.000 | 0.000 |
| p2113 | 0.335 | 0.577 | 0.000 |
| p2114 | 0.000 | 0.000 | 0.000 |
| p2115 | 0.000 | 0.000 | 0.000 |
| p2116 | 0.000 | 0.000 | 0.025 |
| p2117 | 0.000 | 0.000 | 0.000 |
| p2118 | 0.000 | 0.099 | 0.000 |
| p2119 | 0.000 | 0.000 | 0.000 |
| p2120 | 0.000 | 0.000 | 0.000 |
| p2122 | 0.000 | 0.251 | 0.000 |
| p2123 | 0.000 | 0.000 | 0.108 |
| p2124 | 0.000 | 0.000 | 0.017 |
| p2125 | 0.000 | 0.000 | 0.000 |
| **AVERAGE** | **0.014** | **0.101** | **0.010** |

Table B-22 Result of Mann-Whitney U Test: Subject 22 paring to all subjects

| Pair of Subject | dist1 sig | dist2 sig | dist3 sig |
|---|---|---|---|
| p2201 | 0.255 | 0.270 | 0.000 |
| p2202 | 0.000 | 0.000 | 0.000 |
| p2203 | 0.000 | 0.000 | 0.000 |
| p2204 | 0.000 | 0.000 | 0.000 |
| p2205 | 0.000 | 0.000 | 0.000 |
| p2206 | 0.000 | 0.000 | 0.000 |
| p2207 | 0.000 | 0.002 | 0.000 |
| p2208 | 0.002 | 0.000 | 0.000 |
| p2209 | 0.000 | 0.000 | 0.000 |
| p2210 | 0.000 | 0.000 | 0.685 |
| p2211 | 0.000 | 0.672 | 0.000 |
| p2212 | 0.000 | 0.000 | 0.000 |
| p2213 | 0.000 | 0.490 | 0.000 |
| p2214 | 0.000 | 0.000 | 0.000 |
| p2215 | 0.000 | 0.003 | 0.000 |
| p2216 | 0.000 | 0.000 | 0.000 |
| p2217 | 0.000 | 0.000 | 0.000 |
| p2218 | 0.000 | 0.528 | 0.000 |
| p2219 | 0.000 | 0.000 | 0.000 |
| p2220 | 0.000 | 0.000 | 0.000 |
| p2221 | 0.000 | 0.251 | 0.000 |
| p2223 | 0.000 | 0.000 | 0.000 |
| p2224 | 0.141 | 0.000 | 0.000 |
| p2225 | 0.000 | 0.000 | 0.000 |
| **AVERAGE** | **0.017** | **0.092** | **0.029** |

Table B-23 Result of Mann-Whitney U Test: Subject 23 paring to all subjects

| Pair of Subject | dist1 sig | dist2 sig | dist3 sig |
|---|---|---|---|
| p2301 | 0.000 | 0.000 | 0.000 |
| p2302 | 0.004 | 0.000 | 0.000 |
| p2303 | 0.000 | 0.000 | 0.000 |
| p2304 | 0.492 | 0.000 | 0.000 |
| p2305 | 0.000 | 0.000 | 0.043 |
| p2306 | 0.000 | 0.000 | 0.000 |
| p2307 | 0.567 | 0.000 | 0.000 |
| p2308 | 0.000 | 0.000 | 0.000 |
| p2309 | 0.000 | 0.000 | 0.780 |
| p2310 | 0.000 | 0.376 | 0.000 |
| p2311 | 0.000 | 0.000 | 0.000 |
| p2312 | 0.414 | 0.000 | 0.000 |
| p2313 | 0.000 | 0.000 | 0.000 |
| p2314 | 0.000 | 0.000 | 0.000 |
| p2315 | 0.373 | 0.000 | 0.000 |
| p2316 | 0.000 | 0.000 | 0.000 |
| p2317 | 0.820 | 0.248 | 0.000 |
| p2318 | 0.000 | 0.000 | 0.000 |
| p2319 | 0.000 | 0.024 | 0.000 |
| p2320 | 0.001 | 0.000 | 0.000 |
| p2321 | 0.000 | 0.000 | 0.108 |
| p2322 | 0.000 | 0.000 | 0.000 |
| p2324 | 0.000 | 0.001 | 0.000 |
| p2325 | 0.000 | 0.000 | 0.000 |
| AVERAGE | **0.111** | **0.027** | **0.039** |

Table B-24 Result of Mann-Whitney U Test: Subject 24 paring to all subjects

| Pair of Subject | dist1 sig | dist2 sig | dist3 sig |
|---|---|---|---|
| p2401 | 0.680 | 0.000 | 0.000 |
| p2402 | 0.000 | 0.000 | 0.010 |
| p2403 | 0.000 | 0.000 | 0.816 |
| p2404 | 0.000 | 0.000 | 0.000 |
| p2405 | 0.000 | 0.000 | 0.000 |
| p2406 | 0.000 | 0.000 | 0.000 |
| p2407 | 0.000 | 0.027 | 0.081 |
| p2408 | 0.000 | 0.000 | 0.570 |
| p2409 | 0.092 | 0.234 | 0.000 |
| p2410 | 0.000 | 0.012 | 0.000 |
| p2411 | 0.000 | 0.000 | 0.068 |
| p2412 | 0.000 | 0.000 | 0.000 |
| p2413 | 0.000 | 0.000 | 0.000 |
| p2414 | 0.000 | 0.000 | 0.000 |
| p2415 | 0.000 | 0.000 | 0.000 |
| p2416 | 0.000 | 0.000 | 0.776 |
| p2417 | 0.000 | 0.033 | 0.000 |
| p2418 | 0.020 | 0.000 | 0.197 |
| p2419 | 0.034 | 0.177 | 0.000 |
| p2420 | 0.000 | 0.000 | 0.028 |
| p2421 | 0.000 | 0.000 | 0.017 |
| p2422 | 0.141 | 0.000 | 0.000 |
| p2423 | 0.000 | 0.001 | 0.000 |
| p2425 | 0.000 | 0.000 | 0.000 |
| **AVERAGE** | **0.040** | **0.020** | **0.107** |

Table B-25 Result of Mann-Whitney U Test: Subject 25 paring to all subjects

| Pair of Subject | dist1 sig | dist2 sig | dist3 sig |
|---|---|---|---|
| p2501 | 0.000 | 0.000 | 0.582 |
| p2502 | 0.000 | 0.000 | 0.000 |
| p2503 | 0.000 | 0.000 | 0.000 |
| p2504 | 0.000 | 0.000 | 0.579 |
| p2505 | 0.000 | 0.000 | 0.000 |
| p2506 | 0.000 | 0.000 | 0.000 |
| p2507 | 0.000 | 0.000 | 0.000 |
| p2508 | 0.000 | 0.000 | 0.000 |
| p2509 | 0.000 | 0.000 | 0.000 |
| p2510 | 0.000 | 0.000 | 0.000 |
| p2511 | 0.684 | 0.000 | 0.000 |
| p2512 | 0.000 | 0.005 | 0.022 |
| p2513 | 0.000 | 0.000 | 0.000 |
| p2514 | 0.218 | 0.000 | 0.000 |
| p2515 | 0.000 | 0.000 | 0.000 |
| p2516 | 0.000 | 0.000 | 0.000 |
| p2517 | 0.000 | 0.000 | 0.000 |
| p2518 | 0.000 | 0.000 | 0.000 |
| p2519 | 0.000 | 0.000 | 0.000 |
| p2520 | 0.026 | 0.000 | 0.000 |
| p2521 | 0.000 | 0.000 | 0.000 |
| p2522 | 0.000 | 0.000 | 0.000 |
| p2523 | 0.000 | 0.000 | 0.000 |
| p2524 | 0.000 | 0.000 | 0.000 |
| **AVERAGE** | **0.039** | **0.000** | **0.049** |

# VITA

Nattapong Jeanjaitrong is a master's degree student majoring in computer science and information technology at the faculty of science, Chulalongkorn University. He graduated in bachelor's degree with the same majoring in the year 2011. He has interest  in authentication mechanism by using behavioral biometrics since he was in a bachelor’s degree. His passion is to find new factors which can be used in authentication mechanism without using much equipment. He is now studying about other factors from mobile device to improve an accuracy of user’s classification.