

MULTIPLE BIOMETRICS FOR AUTHENTICATION SYSTEM BY EYE VISION WITH  
KEYSTROKE DYNAMICS

Miss Kranogwan Krasaesat



จุฬาลงกรณ์มหาวิทยาลัย

CHULALONGKORN UNIVERSITY

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

บทคัดย่อและแฟ้มข้อมูลฉบับเต็มของวิทยานิพนธ์ตั้งแต่ปีการศึกษา 2554 ที่ให้บริการในคลังปัญญาจุฬาฯ (CUIR)  
Copyright of Chulalongkorn University  
เป็นแฟ้มข้อมูลของนิสิตเจ้าของวิทยานิพนธ์ ที่ส่งผ่านทางบัณฑิตวิทยาลัย

The abstract and full text of theses from the academic year 2011 in Chulalongkorn University Intellectual Repository (CUIR)  
are the thesis authors' files submitted through the University Graduate School.

ชีวมาตรพหุคุณสำหรับระบบระบุตัวตนโดยการเห็นด้วยตัวร่วมกับพลวัตการเคาะแป้นพิมพ์



นางสาวกนกวรรณ กระแสสัตย์

จุฬาลงกรณ์มหาวิทยาลัย

CHULALONGKORN UNIVERSITY

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต  
สาขาวิชาวิทยาการคอมพิวเตอร์และเทคโนโลยีสารสนเทศ ภาควิชาคณิตศาสตร์และวิทยาการ  
คอมพิวเตอร์

คณะวิทยาศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย

ปีการศึกษา 2556

ลิขสิทธิ์ของจุฬาลงกรณ์มหาวิทยาลัย

Thesis Title	MULTIPLE BIOMETRICS FOR AUTHENTICATION SYSTEM BY EYE VISION WITH KEYSTROKE DYNAMICS
By	Miss Kranogwan Krasaesat
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 Chooharajanone, Ph.D.)

.....Thesis Advisor  
(Assistant Professor Pattarasinee Bhattarakosol, Ph.D.)

.....External Examiner  
(Kanokwan Atchariyachanvanich, Ph.D.)

กนกวรรณ กระแสสัตย์ : ชีวิตมาตรพหุคูณสำหรับระบบระบุตัวตนโดยการเห็นด้วยตา ร่วมกับพลวัตการเคาะแป้นพิมพ์. (MULTIPLE BIOMETRICS FOR AUTHENTICATION SYSTEM BY EYE VISION WITH KEYSTROKE DYNAMICS) อ.ที่ปรึกษาวิทยานิพนธ์หลัก: ผศ. ดร. ภัทรลีนี ภัทรโกศล, 58 หน้า.

ปัจจุบันการระบุตัวบุคคลด้วยข้อมูลทางชีวภาพนั้นเป็นเทคโนโลยีที่นำมาใช้ในการรักษาความปลอดภัยของข้อมูลทางคอมพิวเตอร์อย่างกว้างขวาง เนื่องจากเป็นเทคโนโลยีที่ให้ผลลัพธ์ที่มีประสิทธิภาพและความแม่นยำสูง อย่างไรก็ตามส่วนใหญ่การระบุตัวบุคคลด้วยข้อมูลทางชีวภาพนั้นต้องอาศัยอุปกรณ์พิเศษเพิ่มเติมในการรับข้อมูลการระบุตัวบุคคลโดยอาศัยข้อมูลจังหวะในการพิมพ์ของแต่ละคนนั้นเป็นหนึ่งในวิธีในการระบุตัวบุคคลด้วยข้อมูลทางชีวภาพที่ไม่ต้องอาศัยอุปกรณ์พิเศษใดๆ เพิ่มเติมนอกจากแป้นพิมพ์ ดังนั้นเทคโนโลยีจึงมีประโยชน์อย่างมากในการเอามาประยุกต์ใช้กับระบบต่างๆ บนอินเทอร์เน็ตแต่นำเสียดายที่ยังมีข้อบกพร่องของการระบุตัวบุคคลโดยใช้ข้อมูลจังหวะในการเคาะพิมพ์ของบุคคลอยู่ เมื่ออารมณ์ของบุคคลนั้นๆ เปลี่ยนไป ผลลัพธ์ที่ได้ก็ไม่ถูกต้องสมบูรณ์ ดังนั้นความแม่นยำของการระบุตัวบุคคลด้วยข้อมูลจังหวะในการเคาะแป้นพิมพ์นี้สามารถเพิ่มขึ้นได้โดยการประยุกต์รวมใช้กับวิธีการระบุตัวบุคคลด้วยข้อมูลทางชีวภาพอื่นๆ อาทิ การสแกนลายนิ้วมือและม่านตา เป็นต้น แต่การนำเอาวิธีเหล่านี้มารวมกันก็ไม่เหมาะสมนักเนื่องจากเทคนิคเหล่านี้ล้วนต้องอาศัยอุปกรณ์พิเศษเพิ่มเติมในขั้นตอนการระบุตัวบุคคล ดังนั้นเพื่อเป็นการกำจัดความต้องการเหล่านั้น งานวิจัยนี้จึงนำเสนอการพัฒนาวิธีการระบุตัวบุคคลโดยอาศัยจังหวะในการเคาะแป้นพิมพ์ โดยปรับใช้ร่วมกับความสามารถในการมองเห็นของแต่ละบุคคลเพื่อเพิ่มความแม่นยำในการระบุตัวบุคคล โดยการแก้ปัญหาที่เสนอว่าขั้นตอนการระบุตัวบุคคลด้วยข้อมูลทางชีวภาพนั้นสามารถทำงานได้โดยอาศัยแค่อุปกรณ์ธรรมดาทั่วไปอย่างแป้นพิมพ์คอมพิวเตอร์

จุฬาลงกรณ์มหาวิทยาลัย  
CHULALONGKORN UNIVERSITY

ภาควิชา	คณิตศาสตร์และวิทยาการคอมพิวเตอร์	ลายมือชื่อนิสิต .....
สาขาวิชา	วิทยาการคอมพิวเตอร์และเทคโนโลยีสารสนเทศ	ลายมือชื่อ อ.ที่ปรึกษาวิทยานิพนธ์หลัก .....
ปีการศึกษา	2556	

# # 5572601923 : MAJOR COMPUTER SCIENCE AND INFORMATION TECHNOLOGY  
 KEYWORDS: AUTHENTICATION BIOMETRIC BEHAVIORAL BIOMETRICS CHARACTER'S  
 LOCATION EYE VISION KEYSTROKE DYNAMICS MULTI-BIOMETRIC.

KRANOGWAN KRASAESAT: MULTIPLE BIOMETRICS FOR AUTHENTICATION  
 SYSTEM BY EYE VISION WITH KEYSTROKE DYNAMICS. ADVISOR: ASST.  
 PROF. PATTARASINEE BHATTARAKOSOL, Ph.D., 58 pp.

Presently, the security of information significantly becomes an important issue for all users over the Internet. Since the single password is insufficient to protect attack from attackers as proved by various researchers, the biometrics has been applied as a new alternative for classifying and identifying users. Keystroke dynamics is a behavioral biometrics with individual characteristic patterns. Meanwhile, each person has a unique typing pattern that might cause from individual skills of typing the keypress. In addition, a research had proved that the eye vision can be counted as a biometric that can identify an individual person with higher accuracy when combining with keystroke dynamics. However, this research has found that the measurement times in the keystroke dynamics mechanism is related to the typing character's location. Therefore, this research has objective to propose that the vision speed and the location of typing unknown character should be integrated in the authentication mechanism to gain higher accuracy.



Department: Mathematics and  
 Computer Science

Student's Signature .....

Advisor's Signature .....

Field of Study: Computer Science and  
 Information Technology

Academic Year: 2013

## ACKNOWLEDGEMENTS

I would never have been able to finish this study without support of everyone whom involved in this thesis. I would like to take this opportunity to express my sincere gratitude to my advisor Asst. Prof. Dr. PattarasineeBhattarakosol for her helpful advice, support, motivation and patience.

Besides my advisor, I also would like to thank my thesis committee: Asst. Prof. NagulCooharojananone and Dr. KanokwanAtchariyachanvanichfor their encouragement and insightful comment.

Moreover, thank you to all the volunteers in this experiment for donating their time to participate on my study without them this experiment would not be possible.

Finally, I would like to thank my friends in INSET lab and my family for cheering up and supporting me with their best wishes.

## CONTENTS

	Page
THAI ABSTRACT .....	v
ENGLISH ABSTRACT .....	vi
ACKNOWLEDGEMENTS .....	vi
CONTENTS .....	vii
LIST OF TABLES .....	ix
LIST OF FIGURES .....	x
CHAPTER I .....	1
1.1 Background and importance .....	1
1.2 Objectives .....	3
1.3 Scopes of thesis and Constraints .....	3
1.4 Expected outcomes .....	4
1.5 Definition .....	4
1.6 Thesis structure .....	5
CHAPTER II .....	6
2.1 Background of Biometrics .....	6
2.2 Keystroke dynamics biometric .....	8
2.3 Multi-Biometrics .....	9
2.4 Literature review .....	10
CHAPTER III .....	14
3.1 Experimental Design .....	14
3.2 Proposed Method .....	18
3.3 Use Case Diagram .....	21
3.4 Class Diagram .....	24
3.5 Data Gathering Method .....	25
3.6 Code Implementation .....	29
3.7 Data Analysis Methods .....	33
CHAPTER IV .....	34

	Page
4.1 Statistical Analysis Results .....	34
4.2 Neural Network Analysis Results .....	41
CHAPTER V .....	45
5.1 Discussion .....	45
5.2 Conclusion .....	46
5.3 Future work .....	47
REFERENCES .....	48
VITA.....	58



จุฬาลงกรณ์มหาวิทยาลัย  
CHULALONGKORN UNIVERSITY



## LIST OF TABLES

	Page
Table 4.1 Categories of data in the Naive Bayes network classification .....	41
Table 4.2 ANN classification results of single keystroke (dwell and interleave) .....	41
Table 4.3 ANN classification results of combined eye vision with keystroke .....	42
Table 4.4 ANN classification results of combined eye vision with keystroke .....	43



## LIST OF FIGURES

	Page
Figure 1.1 Measurement methods of times capture.....	5
Figure 3.1 Screen pattern for eye testing .....	15
Figure 3.2 Separation group of character.....	16
Figure 3.3 Design experiment of 9*9 Greco-Latin Square.....	17
Figure 3.4 Key Pattern Collector Systems (KPCS) Architecture .....	19
Figure 3.5 Entity Relationship Diagram of elements in the PattnDB.....	21
Figure 3.6 Use case diagram of the UIM .....	21
Figure 3.7 Use case diagram of the PCM .....	22
Figure 3.8 Use case diagram of the ECM .....	23
Figure 3.9 the class diagram of the KPCS .....	24
Figure 3.10 Sequences diagram of the KPCS .....	26
Figure 3.11 Flowcharts of the KPCS.....	28
Figure 3.12 Example of records of a user in the UsersInfo table .....	30
Figure 3.13 Example of records of a user in the PasswordTime table.....	31
Figure 3.14 Records of a user in the ExperimentTime table .....	32
Figure 4.1 Mean Dwell Times from 15 random samples .....	34
Figure 4.2 Mean Interleave Times from 15 random samples.....	35

## CHAPTER I

### INTRODUCTION

This chapter describes about background and importance. Details in this chapter include objectives, scopes and constraints of the experiment and the expected outcomes. Moreover, definitions of technical terms are clarified so readers will have the same understanding for each technical term. Furthermore, the advantage of thesis is presented followed by the structure of the entire thesis.

#### 1.1 Background and importance

Currently, the computer technology is rapidly developed. Most of the daily people's activities use computer for performing their tasks or transactions. Since the Internet scale has grown up, most transaction flow over the Internet like the financial transaction, order product online and apply job online. Each transaction requires individual information of users. Thus, the method to identify user's authority is needed.

Generally, the traditional authentication system is the use of username and password for identifying who is the authorized user. Although, the computer technology is rapidly changed to support users for their tasks, the use of single password is insufficient solution to protect the users' information. The single password is the vulnerability for attackers since they try to use all kinds of techniques to break through. For example, the guessing of brute force attack in trial and error until the right password is disclosed, the dictionary attack that is the method of breaking into a password by systematically entering every word in the password's dictionary. Therefore, using only one password is insufficient solution to protect the personal information. Thus, the system developers try to figure out methods to prevent such problems by increasing complication of the password for conjecture or more of time consumed. Nevertheless, this solution cannot be completely fixed this problem. As a consequence, the authentication system has to be continuously developed.

According to the problem above, the approaches for human authentication are relied on 3 principals of the authentication method. Firstly, begin from something you know (eg. password), this is the most common kind of authentication used for identifying a person. Unfortunately, it can be stolen from malicious software. Secondly, the approach considers in something you have (eg. smart card); it is like a key for opening the door that only just fits to the specific key. However, this technique cannot identify the person because the key can be stolen. Lastly, the approach that focuses in something you are (eg. fingerprint, iris, keystroke dynamics). This refers to something about a person that cannot be changed, such as fingerprints, face recognition, iris, voice recognition and keystroke dynamics. Consequently, these factors can be applied as an identifying factor in the verification process. Moreover, it is significantly hard to copy or break all these biometrics when comparing with previous approaches. Therefore, the biometrics authentication is the most powerful technique that can protect the private information.

Biometrics authentication is a technology that detects physical or behavioral of human. Biometrics can be divided in two main classes. The first is physiological (eg. fingerprint, face recognition, etc.); these physiological can provide very high accurate verification result. Since the hereditary characteristic of each person will never be changed, thereby, this technique is high accuracy result of identifying individual person. However, the devices used in these techniques are complicated.

The second is behavioral (eg. keystroke dynamics, voice, etc.); behavioral characteristics is the individual of human trait which cannot be imitated. Keystroke dynamics is a class of behavioral biometrics that captures the typing style of a user. The typing style includes the length of time taken when typing the login name and password, the time between characters when a user presses over the keyboard, and the pressing time per key of each user. According to [1, 2] the eye vision has proved that there are some impacts from the keyboard typing which related to the keystroke dynamics concept. Meanwhile, merge of eye vision and skills of keystroke dynamic will be create a uniquely individual pattern to be identify person who are genuine or imposter user

Finally, various techniques have been proposed and implemented. Some techniques require a special device that depends on the type of biometrics. Nonetheless, the keystroke dynamics is the one that uses the basic keyboard and has been implemented to the authentication process. Additionally, some proposed techniques are proven under a specific environment; thus, it might not be possible for the real use. Therefore, this research will focus on the possibility of implementing biometrics in the real usage under the low cost of implementation. The proposed technique will combine the basic keystroke dynamics and human's eye vision with the character's location.

## **1.2 Objectives**

This research has aims to perform the following tasks;

1. To implement the classification authentication system using the Eye Vision Ability and keystroke dynamics.
2. To verify the accuracy of the proposed method with single biometrics value from eye vision or keystroke dynamics.

## **1.3 Scopes of thesis and Constraints**

Biometrics authentication methods are the verification of a human's identity. This research focuses in partial on the behavioral biometrics, called as the keystroke dynamics. It is a keystroke rhythm typing style of an individual person which does not require any additional hardware. Moreover, it can be applied on any system over the Internet. The study is based on the experiment on a group of samples. The following list is the scope and constraints of this research.

1. The sample size of this experiment is 30 persons with different careers but these samples use computer as their daily equipment.
2. The sample data-collection is 90 times within 30 days, three times (morning, afternoon and evening) per day.
3. The samples are in between 18-30 years of age because these ages are the working age and mostly familiar with computers.
4. The experiment focuses on the time that a sample consumes to type a password and responds to the displayed character.

5. The experiment required between 2 hands of the sample testing.
6. All interesting time values are captured and stored in the database if and only if the typing password is correct.
7. The samples have to use the desktop or laptop computers with the QWERTY keyboard only.
8. The program is developed as a web-based application to collect the data.

#### 1.4 Expected outcomes

According to the defined objectives, the expected outcomes of this research are listed below.

1. The authentication system using the proposed technique can prevent unauthorized users easily and accurately.
2. The new mechanism of authentication process using multi-biometrics between keystroke dynamics of character's location with eye vision ability of a person.
3. The proposed authentication system can be implemented in various computers without additional expensive equipment.
4. The keystroke dynamics authentication can be high accuracy result as physiological biometrics.

#### 1.5 Definition

In this research, the capturing data for keystroke dynamics includes the dwell time and interleave time, as shown in Figure 1.1. During the eye evaluations, the significant values are the typing time after the randomly assigned character appears within one of the nine areas of the eye vision test, called as the vision time. Figure 1.1 shows the measurement methods of times.

**Dwell time:** the period of time that a user used to press and release a key.

**Interleave time:** the period of time that a user used to move from a key to another consecutive key.

**Vision time:** the period of time that a user used to response with the displayed character on the eye vision test screen by pressing a key which matched with the appeared character.

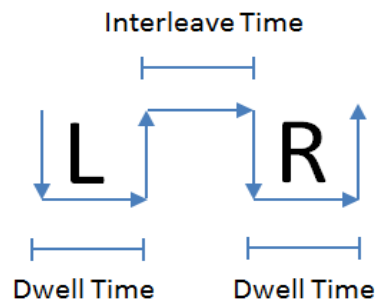


Figure 1.1 Measurement methods of times capture

## 1.6 Thesis structure

The remaining parts of this thesis consist of four chapters as follows. Chapter 2 informs about the fundamental of knowledge and literature review related to this thesis study. Chapter 3 describes the designed and methodology of this research, including the proposed method. The results of this study will be demonstrated in Chapter 4. The discussion and conclusions are presented in Chapter 5.

## CHAPTER II

### FUNDAMENTAL KNOWLEDGE AND LITERATURE REVIEW

This chapter provides the fundamental knowledge and literature reviews for this thesis. The background of the biometrics is demonstrated in Section 2.1. The fundamental knowledge of keystroke dynamics biometric and multi-biometrics are described in Section 2.2 and 2.3. Then, the literature review is stated in Section 2.4.

#### 2.1 Background of Biometrics

Biometrics is the science and technology that measures a biological data [3, 4]. The term biometrics is composed of the two Greek words: “bios” as “bio”, and “metros” as “metric”. The use of biometrics is under two objectives: elaboration of biological, and identification of persons. Biometrics is used as a part to identify and verify a person; this is the procedure to determine the authorized or imposters. Biometrics usually refers to some parts of human’s organ or behavior, such as fingerprints, eye retinas and irises, voice recognition, face recognition, and keystroke dynamics. The traditional methods of identification are PIN number, and single password. Unfortunately, these basic methods cannot protect or detect the illegal accesses by man.

According to the reason above, biometrics technologies were implemented to replace or support the fundamental authentication methods. In addition, biometrics application is implemented as an automated method in the identification process. Since there are various types of biometrics, these can be classified in the following categories.

- Physiological biometrics: this biometrics is based on direct measurement of existing genetic trait which can be derived from a certain part of human’s organ, such as fingerprint, retina scan, iris, and face recognition. This physiological biometrics is usually much accurate and more reliable comparing with behavioral biometrics because human’s genetic trait is unique.



- Behavioral biometrics: this biometrics is based on the action of human characteristics, such as voice recognition and keystroke dynamics. Normally, the collected data under this biometrics does not require additional special devices and the cost of implementation is low when comparing with the physiological biometrics.

Base on the concepts of biometrics above, the characteristics of biometrics must satisfy the following conditions [5]:

1. *Universal*: The process should be support with every person. And can be found around us or everyone has the same.
2. *Invariance of properties*: They should not be change although time has passed.
3. *Measurability*: The attributes data should be easy to gather and easy to evaluate.
4. *Singularity*: The attribute of each person must be unique to the individual. The sufficient of attribute can be indicating the unique properties to distinguish person from any other. Height, weight, hair and eye color are all attributes that are unique characteristics of the individual person.
5. *Acceptance*: The accepted ratio should be in the large scale of the population. Except, the particularly invasive technologies, i.e. technologies which require a part of the human body to be taken.
6. *Reducibility*: The size of captured data should be reducing those will be easy to manage and manipulate.
7. *Reliability and tamper-resistance*: The process of captured data and manipulate should be repeated to ensure that attributes are correct. Therefore, the result will be high reliability.
8. *Privacy*: The privacy of the person is most important. Thereby, the process should not be disclosing the privacy.
9. *Comparable*: The captured data can be able to reduce the similar attribute when compare with any others. And should be able to find the different point of the attribute.
10. *Inimitable*: the process should be able to find the unique of individual and protect an imitated of the imposter.

Biometrics authentication is growing and counted as a controversial field in which civil liberties groups express their concern over the privacy and identity

issues. Currently, biometric laws and regulations are in process and biometrics industry standards are being tested.

Presently, information of organizations requires high security, using of the biometrics techniques are the best optimum solution to protect the information. However, event required the highest technology, the cost of implement will also high. Thereby, the implement of keystroke dynamics is the one solution that should be considered.

## 2.2 Keystroke dynamics biometric

Keystroke dynamics is a class of behavioral biometrics that captures the typing styles of users [4]. The keystroke verification techniques can be either static or dynamic. The static keystroke verification technique refers to asked user taken in the same text or fixed characters. And another is dynamics; this keystroke verification technique refers to monitoring the user's typing behavior or free text. Meanwhile, the characteristic of keystroke verification techniques applied for finding the individual user's typing pattern. The common classifying of keystroke dynamics comes from the time capturing of user's typing rhythm of a user interacting with a keyboard. Therefore, [6] it has potential applications for the automatic recognition of users interacting with personal computers, ATMs, cellular phones, and any other devices with keys. The primary observations that each user has a unique way of typing until the end of the nineteenth century, since the telegraphists were able to identify other operators listening to the rhythm of Morse code sequences stroke. Meanwhile, the characteristics of individual person cannot be easily imitated.

Base on the reason above, the timing capture is the criteria of keystroke dynamics used to verifying person. Many researches [7, 8] defined the several today's measurements that using to verifying is show below:

1. Latency keystroke (dwell time).
2. Duration of keystroke (interleave time).
3. Overall typing speed.
4. Variations of speed moving between specific keys (hand's movement).

5. Frequency of errors (how often user has used backspace).
6. Rate of typing (mean times per character).

Referring to the measurement of keystroke dynamics above, in an early of researches have studied the typing behavior of users using keypress or dwell time as a base measurement unit. The suggestion from Gentner [9], that separate the user into two types as expert typists and novice typists. The person which is using computer for working in everyday life we assume that is the expert typists. For novice typist is use the computer but not much familiar for typing of the keyboard. As a result of [9], presented the median keypress of the expert typists is approximately 96 millisecond, while at that of novice typists is 825 millisecond. The various researches in today required more variable for using to be verifying the keystroke typing rhythm of human. Meanwhile, using keypress or dwell time is insufficient to be verifying person, another measurement unit of keystroke dynamics stated on above should be considered.

However, keystroke dynamics is a nonintrusive biometric trait, which is also widely accepted from end users. The data acquisition does not require either special hardware device to develop on this biometrics. This technology is based on software solution which costs less comparing with other biometrics which requires both special hardware and software.

### 2.3 Multi-Biometrics

Using password was the original authentication system that can secure the personal information from unauthorized users to steal or impostor users for their illegal benefits. Although, the computer technology has rapidly changed to support users for their tasks, unfortunately, these flexibilities also support intruders for breaking to the system in a short time, such as the brute force attack, dictionary attack, and etc. Therefore, using only password is insufficient solution to protect the personal information although the system developers try to figure out how to prevent such problems by increasing complication of the password for conjecture or more of time consumed. Nevertheless, this solution cannot be completely fixed the problems. Thus, the authentication system has to be continuously developed.

Referring to the study of [10, 30], the multi-biometrics has been applied to implement the authentication system. The study of [10], using the multi-factors biometrics by using the fingerprint and face recognition, the result shows that it is to achieve and perfect performance (0% EER) base on using two factors of biometrics. Whereas, the result of single biometrics shows 0.1 Fault Acceptance Rate (FAR) of fingerprint and 0.67 FAR of face recognition.

Since, the research proposed by [1], was applied the multi-biometrics in part of behavioral biometrics. The combination of keystroke dynamics and speed of eye vision was applied to the identification process. The studied of [1] proved that the speed of eye vision that interacting with keyboard can be identify the behavior in each person when combine with keystroke trait. Therefore, the experiment was test eye vision ability and participation of typing character those display on the screen. As a result of experiment was show the unique individual typing pattern.

#### **2.4 Literature review**

Generally, the authentication system is a common process that every user cannot avoid. This authentication system has an aim to protect illegal users in accessing resources over the network, especially accesses through web-applications. Although passwords are used to protect the system before users are enable to access the required files or CPU, this password mechanism is too weak to protect intruders. Thus, biometrics is applied and implemented to the authentication mechanism so the real users can be identified; all these biometrics are such as fingerprint, face recognition, iris, speaker recognition, keystroke dynamics, etc.

Various studies have indicated that using the biometrics in the authentication system can easily and accurately identify persons since human characteristics are much difficult to be forged. As a result, authenticated person can be distinguished from unauthorized users [11]. One basic technique that is implemented in various systems is keystroke dynamics.

Keystroke dynamics is a type of behavioral biometrics that captures characteristics of users, mainly related to the time capturing in various aspects. A time value can be measured in different criteria, such as a dwell time which is the

pressing time over a key on the keyboard. Another time value is the interleave time that is the time measured the hand's movement from one key to the next key on the keyboard. In addition, the correctness of the used of this method can be indicated using one of these values: False Rejection Rate (FRR), False Acceptance Rate (FAR), and Equal Error Rate (ERR). FRR is the percentage of authorized users is identified as imposters; FAR is the percentage of imposters is identified as a valid users; and ERR is the crossover point at which FRR equals FAR [12, 13].

Although the keystroke dynamics is an efficient method in identifying authenticated users, all measurement indexes mentioned previously still show some mistaken identification. Therefore, many recent researchers proposed the combination of keystroke dynamics and another biometrics value to increase accuracy of the authentication process.

According to Obaidat and Sadoun [14], they studied the differences between statistical-based and neural network-based classification methods with keystroke dynamics. This study concluded that neural network-based methods provided better results as compared with statistical methods in keystroke patterns classification. In other words, the neural networks were trained in advance not only using legitimate users' sample, but also intruders' samples. Hence the classifier is expected to produce better results with low FAR.

In addition, the researches of [15, 16] also studied the typing pattern and discovered that the combination of keystroke pattern and users' passwords will lead to a high accuracy result. However, using password as a combining factor may not secure enough since the password can be captured easily by bots or imposters. Thus, using multi-biometrics in the authentication process should be a better alternative. Thus, using multi-biometrics can provide the highest accuracy result than using only single biometrics. Based on the studied of [23], the proposed multimodal biometric system with fingerprint and iris recognition shows the significant improvement of the biometrics system. In the year 2011, the multi-biometric system by fusion of finger-knuckle-print and palm print was applied for an efficient person recognition [24]. Moreover, this study provided a fusion scheme that improves the

result to be 0.003 % of equal error rate (EER). Thus, in the same year 2011, the studied of Lang, Z. and Qi, H. [25] shows the result process of matching finger geometry and palm print will be fast and highly active. Thereby, the effective fusion strategy is necessary for combining information from several single biometric systems. Especially, the multi-biometrics system, the result of used multi-biometrics shows the highest accuracy than used of the single biometrics.

Referring to the research combined keystroke dynamics with some part of biometrics, in the year 2010, [26] the multimodal biometric system based on keystroke dynamics and 2D face recognition was applied for improving a good performances, acceptability, and respect of privacy, the results by obtaining an EER of 2.22% in their best scheme. The study of Freire, J. and et.al [28] performed an Identity verification through fusion of features from keystroke dynamics and speech. FAR and FRR were applied to outperform decision fusion and calculate EER, the result provided better of EER. In the past decade, the principal disadvantage of keystroke dynamics method is their performance that are still lower than the biometric methods based on physical characteristics. Currently, the fusion of keystroke dynamics with some another biometrics will provide the high accuracy result [29].

Base on the research of Nonsrichai, and Bhattarakosol [1], the biometrics under the eye vision had been proven that there are some impacts to keyboard typing which related keystroke dynamics. Meanwhile, the combination between eye vision and skills of keystroke dynamics will create an individual pattern to identify persons. The study of [1] was use the static and dynamics keystroke verification techniques. The first part was generate the fixed password to all of sample or called static, the meant of fixed password for investigating the different typing pattern of each sample. Whereas, the dynamics of [1] was gather from experiment random the character on the screen, this experiment was combined eye vision and keystroke dynamics for study the relation of speed of vision with hand's movement. In the past, many researches have been studied the human eye movements in the eye vision, because it can be identify the character style and comes through behavioral for classifying the person [17, 18].

Moreover, [21, 32] the neural network approaches was applied for classifying data. While the back propagation model used to be classify an instance. The result of [22] using BPNN shows excellent verification accuracy by using the median values. The classification average error of 0.063% is reported. According to the study of [31], Bayesian Network was applied to increase accuracy of user classification and authentication, the standard metrics of accuracy: Precision, Recall, F-measure, FRR, FAR and ROC area.

Over the years, researches in keystroke biometrics applied many existing machine learning and classification techniques. All those researches meant to find the best classifying method in the highest accuracy of result and the lowest error rate. Therefore, this study will use multi-biometric based eye vision with keystroke dynamics to form characteristic patterns in the identification process.

## CHAPTER III

### METHODOLOGY

This chapter will describe the experimental design by demonstrating the proposed system in the structure of overall system, use case diagrams, class diagrams, sequence diagrams and the designed database.

#### 3.1 Experimental Design

This research focused on presenting the results of individual's keystroke typing style of each person using the multi-biometrics authentication. On the research proposed by [1], has proven that the eye vision ability has impacts to keyboard typing which related to the keystroke dynamics concept. So the combination of keystroke dynamics and speed of eye vision is applied to the new identification process. Nevertheless, this research will be combine character's location with keystroke dynamic and also using eye vision ability to gain higher accuracy result. The experiment will be implemented on the web-based application for collecting of user's behavioral keystroke typing style.

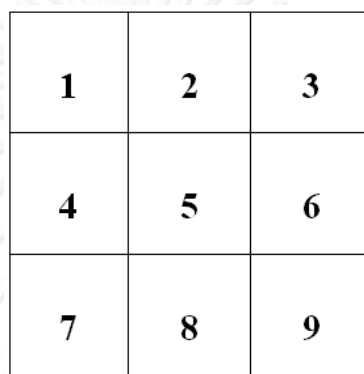
The propose idea for this authentication technique is that the timing capture of keystroke dynamics in case of keypress (dwell time), time between character (interleave time) and times for presented characters (vision time). All participants in this experiment are students and staffs from private sections; furthermore, they must use computers in their daily life. Each volunteer was assigned a fixed 8-character length password. The reason that they were assigned the fixed password is to cut the bias from different passwords and the consideration of hand's movement of each volunteer is clear to figure out the sample's keystroke pattern.

After logging on the state one, all samples will past to state two of the experiment that considers in eye vision and character's location testing. Each volunteer has to type characters that are popped up on screen; this state also measures times as the collected data as same as the state one.

In order to prove assumption stated in the previous section, the sample must be collected under the controlled conditions. The sample size of this



experiment is 30 volunteers whose age is between 18-30 years old and they are daily computer users. The data collection was performed on the user's desktop or laptop with the standard QWERTY keyboard. Each person enters to the testing application by browsing to the web-based application that was developed for recording all keystrokes as required. In this experiment, the participants must login to the system and participate in the test of the eye vision section. The test of the eye vision section is performed by divided the screen into nine segments as shown in Figure 3.1.



<b>1</b>	<b>2</b>	<b>3</b>
<b>4</b>	<b>5</b>	<b>6</b>
<b>7</b>	<b>8</b>	<b>9</b>

**Figure 3.1** Screen pattern for eye testing

Referring to Figure 3.1, the system will display the random character over those 9 segments. The experiment capturing time of keystroke, including the dwell time (the time between keypress of each character), interleave time (the time between character up to another character), start time (the start experiment time), and total time (the time that capturing begin until end of the experiment). These values are used for testing the eye vision of users. The random character will be display on all nine segments per one round and the next display of position will not be repeated.

According to the separation of the display screen, the experiment has been divided into nine groups as shown in Figure 3.2 blow. As the fact that most computer users are familiar with the QWERTY keyboard so this research will use the QWERTY keyboard for collecting data and use for screen pattern under the eye testing procedure.

~	!	@	#	\$	%	^	&	*	(	)	-	=	←	
1	2	3	4	5	6	7	8	9	0	-	=	←	Backspace	
Tab	Q	W	E	R	T	Y	U	I	O	P	{	}		
↔	←	→	←	→	←	→	←	→	←	→	←	→	↵	
Caps Lock	A	S	D	F	G	H	J	K	L	:	"	'	Enter	
⬆	⬆	⬆	⬆	⬆	⬆	⬆	⬆	⬆	⬆	⬆	⬆	⬆	⬆	
Shift	Z	X	C	V	B	N	M	<	>	?	Shift	↵	↵	
⬆	⬆	⬆	⬆	⬆	⬆	⬆	⬆	⬆	⬆	⬆	⬆	⬆	⬆	
Ctrl	Win Key	Alt									Alt	Win Key	Menu	Ctrl

Figure 3.2 Separation group of character

Referring to Figure 3.2, each group represents the set of the character as shown below:

Group1. q, w, e, r

Group2. t, y

Group3. u, i, o, p

Group4. a, s, d

Group5. f, g, h

Group6. j, k, l

Group7. z, x, c

Group8. v, b

Group9. n, m

The display mechanism is that characters of each group will be randomly selected once. When the displayed character was typed, the next character from another group will be selected and performed the same task. The reason of random a character in separated group is to check the differences of typing styles of users whenever the typing hand is changed. Though, the detail of randomly for selecting characters and presenting area will be stated in the next section.

Since, the experiment components (screen pattern for eye testing and separation group of character) have been designed, this research studies the

relationship between eye vision and hand's movement of character location those effected with the keystroke typing pattern. Then, the 9x9Graeco-Latin Square is applied to define the display character of experiment, as shown in Figure 3.3.

1,6	2,5	9,7	3,4	8,8	4,3	7,9	5,2	6,1
2,7	3,6	1,8	4,5	9,9	5,4	8,1	6,3	7,2
3,8	4,7	2,9	5,6	1,1	6,5	9,2	7,4	8,3
4,9	5,8	3,1	6,7	2,2	7,6	1,3	8,5	9,4
5,1	6,9	4,2	7,8	3,3	8,7	2,4	9,6	1,5
6,2	7,1	5,3	8,9	4,4	9,8	3,5	1,7	2,6
7,3	8,2	6,4	9,1	5,5	1,9	4,6	2,8	3,7
8,4	9,3	7,5	1,2	6,6	2,1	5,7	3,9	4,8
9,5	1,4	8,6	2,3	7,7	3,2	6,8	4,1	5,9

**Figure 3.3 Design experiment of 9\*9 Greco-Latin Square.**

According to the Figure 3.3, the number that represented (x, y) is the method for displaying a character. The first number (x) represents the area of the display screen (Figure 3.1 pattern for eye testing), and the second number (y) represents a group of character set (Figure 3.2 separation group of character). For example, the number of (1,6) means the experiment will random to one character from the group# 6 (i.e. j, k, l) and the selected character will be displayed in the screen area# 1.

In order to collecting data, the experiment has been generated nine sets follow as Figure 3.3 in vertical line. Each set will represent nine characters, using all those possible 9 areas of display screen and nine groups of character. For example, a set pattern in this experiment is ((1,6),(2,5),(9,7),(3,4),(8,8),(4,3),(7,9), (5,2),(6,1)). According to the example of the set pattern, it shows that the system will use all those nine possible display screen and group of character.

## 3.2 Proposed Method

Base on the experimental design above, this section presents details of the proposed method and processes of the collecting system. The Keystroke Pattern Collector System (KPCS) is implemented for collecting data that will interpret as the individual's pattern. The KPCS is composed of three main modules as listed below.

- 3.2.1. User Information Module (UIM): This module responsible for collecting the basic information of samples. In addition, this module will be integrated with other modules for sharing the samples' information. The main process of this module is to receive the user's registration at the first time before entering the login process of the experiment. This module required sample's information as name, last name, age, gender, email and occupation. After the sample submits information, the system will generate the username and password back to the sample. All entered information will be stored in the Database (PattnDB). When the sample logs in for starting the experiment, the system will call this data for the authorized checking.
- 3.2.2. Password Capturing Module (PCM): This module responsible for authorize of logging in and capturing the keystroke typing password of the sample whenever the login process starts. The capturing process will begin when the sample types the first character until the end of that password. Parameters that the system collected are Dwell time, Interleave time and Total time. Then, the system will send the username and the password to the method for checking the authorized user.
- 3.2.3. Experimental Capturing Module (ECM): This module is responsible for capturing the basic of sample's typing rhythm which can be classified as the eye vision ability of the sample and the sample's hand-move. Therefore, the parameters that the system will be collected are dwell time, interleave time, vision time, and total time. This experiment will test by random the character's display area, the sample is assumed to type the presented character correctly; the correct typing result will be stored in the PattnDB.

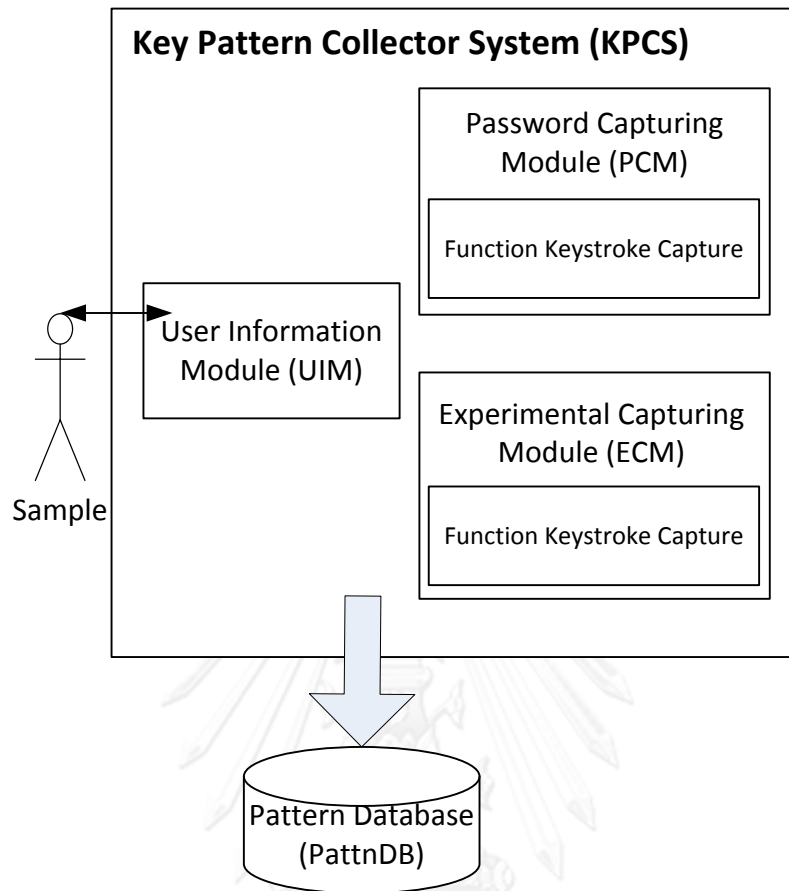


Figure 3.4 Key Pattern Collector Systems (KPCS) Architecture

Figure 3.4 shows the architecture of Key Pattern Collector System (KPCS); it has three sub-modules. The UIM is a registration process, the first process of the system, to generate the username and password to all samples. After the registration process, every sample can insert their username and password into the login form for checking authorization of users before starting the experiment. The PCM module will capture time when first character has been typed and when the last password character has been typed the time capture will stop. Then, the system will send the typed password to the checking method in order to indicate the authorized user. If the typed password is incorrect, the system will request the sample to retype the password again. After the checking has been confirmed, the time capturing of the previous process will be stored into the PattnDB which are separated into two parameters. The first parameter is the Dwell time all of the

password character those sample has been typed, and the second parameter is the Interleave time. In order to store times to the PattnDB, the PCM has to retrieve User ID of each sample through the UIM.

After the login process, the second part of the test is to consider the individual sample's typing pattern. The process for time measurement begins when the sample clicks the button to start the test, and the character and its location on the display area are randomly chosen. The time starts counting when the character is presented until the keyboard is pressed.

The parameters from the second process of the ECM are the character's location and the vision time. The time capturing is almost the same as the PCM, only corrected of sample typing character will be stored into database, otherwise the experiment will request the sample to restart the test again from the beginning. The ECM retrieves the sample's information and the log test from the UIM (more details will be explained in the next section). Moreover, the system will randomly select the testing pattern from the 9 test sets. As represented in Figure 3.3 Design experiment of 9x9 Greco-Latin Square.

Based on the structure of KPCS above, the Entity Relationship Diagram of elements is presented in Figure 3.5. Referring to Figure 3.5, there are three tables in the PattnDB: UsersInfo table, PasswordTime table, and ExperimentalTime table. Each table belongs to one module. The UserInfo table belongs to the UIM; this will store the user's information of the KPCS. The PasswordTime table belongs to the PCM; this stores the sample keystroke typing of password. The last table is ExperimentTime that belongs to the ECM; this stores the testing results of eye vision and character's location based on each sample. Figure 3.5 presents attributes of each table.

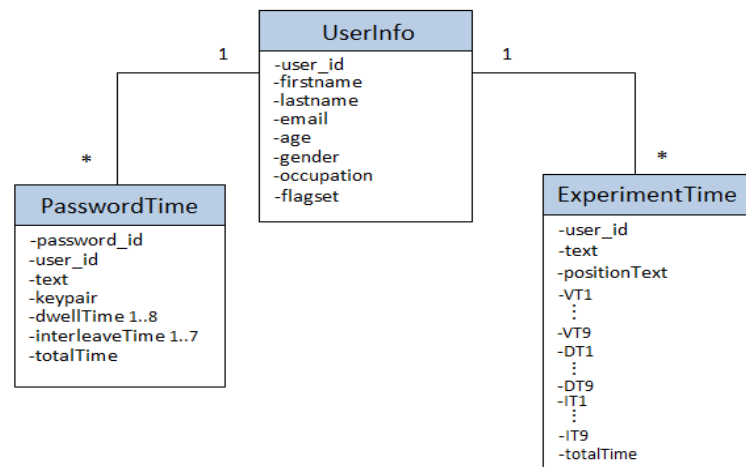


Figure 3.5 Entity Relationship Diagram of elements in the PattnDB

### 3.3 Use Case Diagram

Referring to the structure of KPCS mentioned previously, it can be illustrated as use case diagrams of two main modules bellows.

3.3.1. Use Case Diagram of User Information Module (UIM) which is responsible for the registration process of samples.

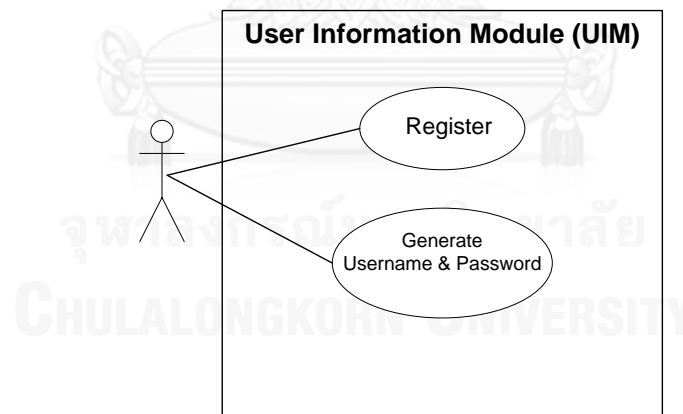


Figure 3.6 Use case diagram of the UIM

Use case diagram: Template

- *Use case name:* User Information Module (UIM)
- *Participant actors:*
  1. User

- *Flow of events*
  1. The UIM require user to register into the system.
  2. The information of user is stored into the PattnDB in table of UserInfo.
  3. The UIM generate username and password, then sends back to the user.
- *Exit condition*
  1. The user receives a username and password to log in to the experiment.

3.3.2. Use Case Diagram of Password Capturing Module (PCM) which is responsible for the capturing the sample keystroke typing rhythms, the parameter that collecting are dwell time and interleave time of users. The time capturing of each parameter will collect in millisecond.

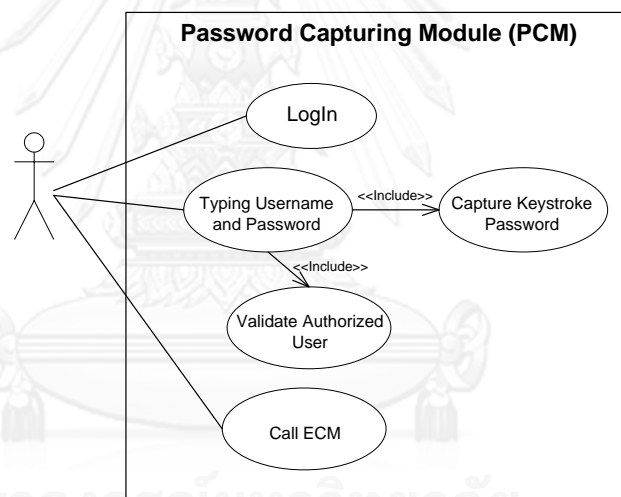


Figure 3.7 Use case diagram of the PCM

#### Use case diagram: Template

- *Use case name:* Password Capturing Module (PCM)
- *Participant actors:*
  1. User
- *Entry condition:*
  1. The user is already registered and got username and password of the KPCS.



- *Flow of events*
  1. The user log in to the system.
  2. The typing each of character will be capture the dwell and interleave time in every character that user has typed.
  3. The validation of user authorized verify in username and password of the user.
  4. The system calls the ECM access to start the experiment.

3.3.3. Use Case Diagram of Password Capturing Module (ECM) which is responsible for the test the vision ability and character's location of the user. This module will test the speed of vision those concern with the typing of the character. The parameters in this module are the dwell time, interleave time and vision time. By random the character based on the design patterns in Figure 3.3.

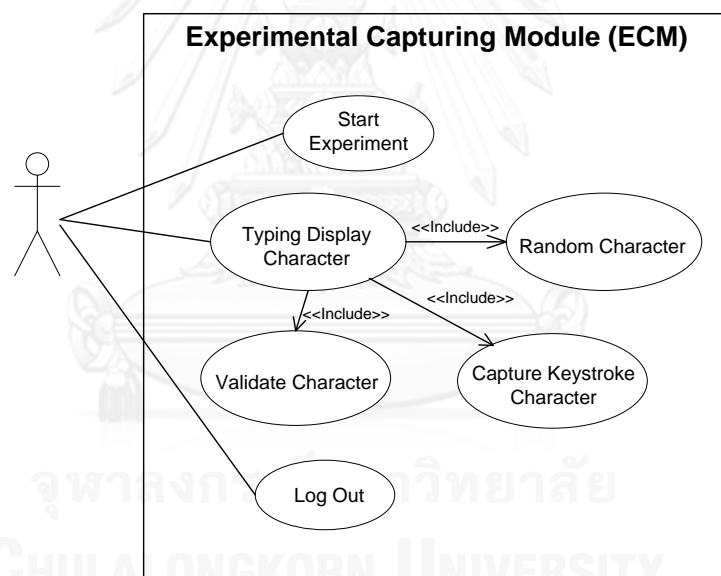


Figure 3.8 Use case diagram of the ECM

#### Use case diagram: Template

- *Use case name:* Experimental Capturing Module (ECM)
- *Participant actors:*
  1. User

- *Entry condition:*
  1. The user is already log in by validate of authorized to access into the system.
- *Flow of events*
  1. The user clicks to start the experiment.
  2. A displayed character and presented area are random and display on the screen.
  3. The user types the character based on the displayed one on the screen.
  4. The system captures the vision time, the dwell time and the interleave time.
  5. Validation of the typed character with the displayed character.
  6. The system will random the next character to display on the screen.
  7. The system shows the log out screen.
- *Exit conditions*
  1. The user types all 9 characters correctly.

### 3.4 Class Diagram

The KPCS composes of 4 main classes: class User, class PCM, class Watch, and class ECM, as shown in Figure 3.9.

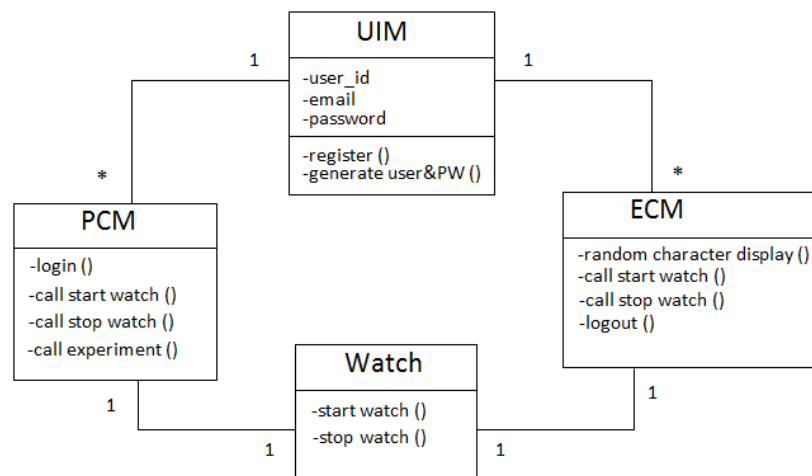


Figure 3.9 the class diagram of the KPCS

Referring to Figure 3.9, each user can register only one time because the registered email can be used only once. After passing the first step and obtained a login name with a password, the user is able to login to the system under the process of the PCM. For each typing password's character, the PCM will capture the keystroke time. When the user submits full password, the PCM will validate the typed password for user's authorization. After passing the authorization process, the user can precede to the next step of the ECM. Otherwise, the user is requested to retype the password again.

When entering to the process of the ECM, the user is requested to type the characters that are displayed on the screen. Every typing character will be triggered to capture times of user's vision and keystroke. Each displayed character is random after the previous character was correctly typed else the display process will restart for the new round of the test.

### **3.5 Data Gathering Method**

In order to capture data as needed, the data collecting mechanism must be determined as described in the sequence diagram in Figure 3.10 below.

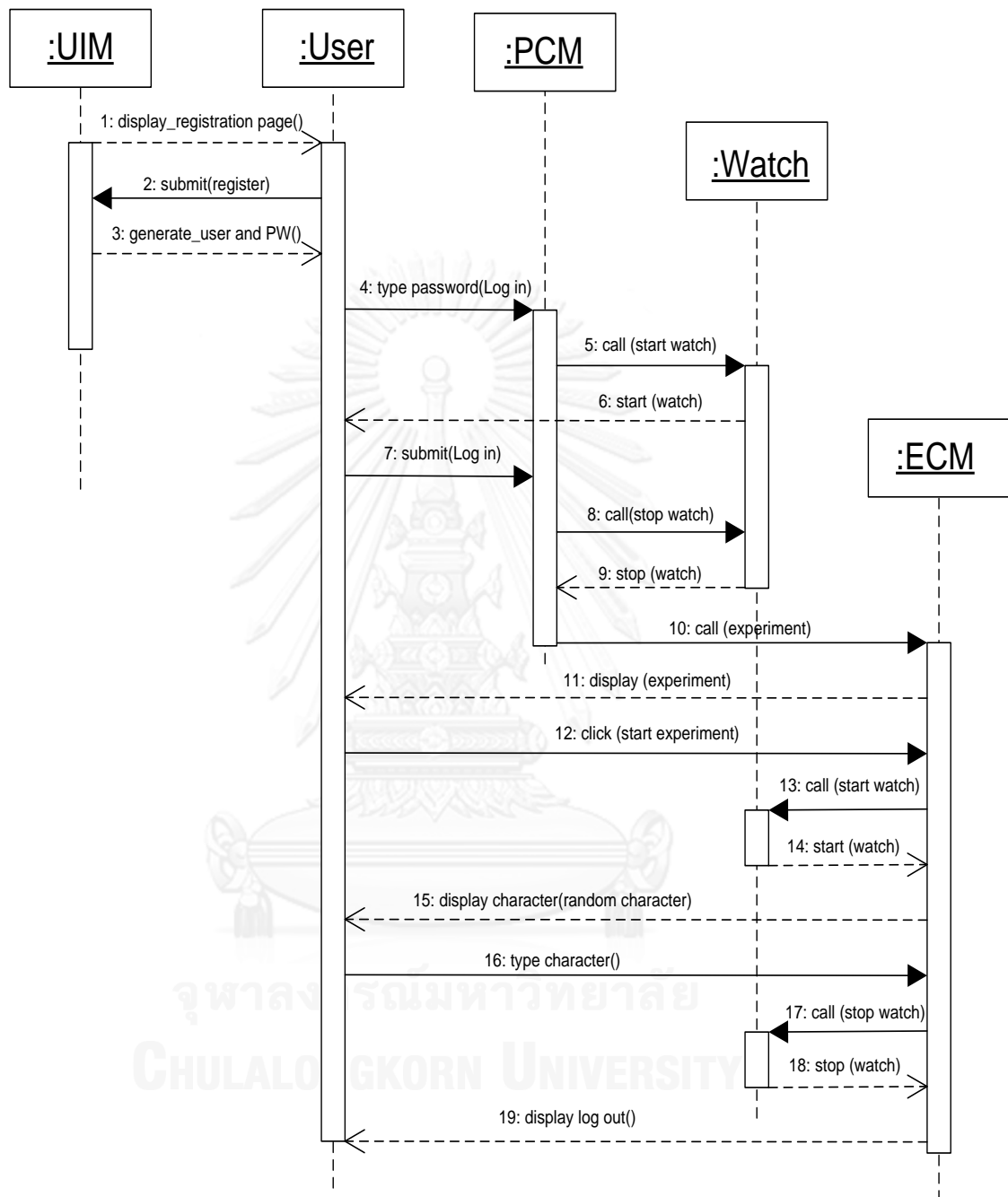


Figure 3.10 Sequences diagram of the KPCS

From Figure 3.10, the data collecting process can be described as follow.

- 1: The UIM requires the user to register at the first time in order to enter user information.
- 2: The user fills personal information and submits to the system.
- 3: The UIM generates a username and a password to the user.
- 4: The user types the received password for logging into the system.
- 5: When the user starts typing, the PCM will trigger the keystroke times.
- 6: The computer's watch begins to count the time.
- 7: When the user submits the full password, the PCM will validate the password.
- 8: The PCM triggers the watch to stop the time.
- 9: The watch stops the time capturing and the PCM sends the captured times to store in the PasswordTime table.
- 10: After the user has successfully logged in, the PCM will transfer the user to ECM.
- 11: The ECM displays the experiment page to user.
- 12: The user clicks the start button to begin the test.
- 13: The ECM triggers the watch to record the user's keystroke time when the first character is displayed.
- 14: The watch begins to count the time.
- 15: The ECM random a character and a display.

16: The user types a character matching with the displayed and the ECM validates the typed character.

17: After the last character has been typed, the ECM will trigger the watch to stop the time.

18: The watch stops the time capturing.

19: The ECM sends the times to store in the PattrnDB database and presents the log out page to the user.

As mentioned above, the KPCS was developed as a web-application using PHP, JavaScript, HTML and JQuery. This web consists of three main pages. The first page is the registration to generate a username and a password to a new user. The second page is the login interface which has the recording keystroke function when the user starts typing password in the input textbox until submits the full password. The last main page is the evaluation of the eye vision ability, and character's location based on random character and displayed location.

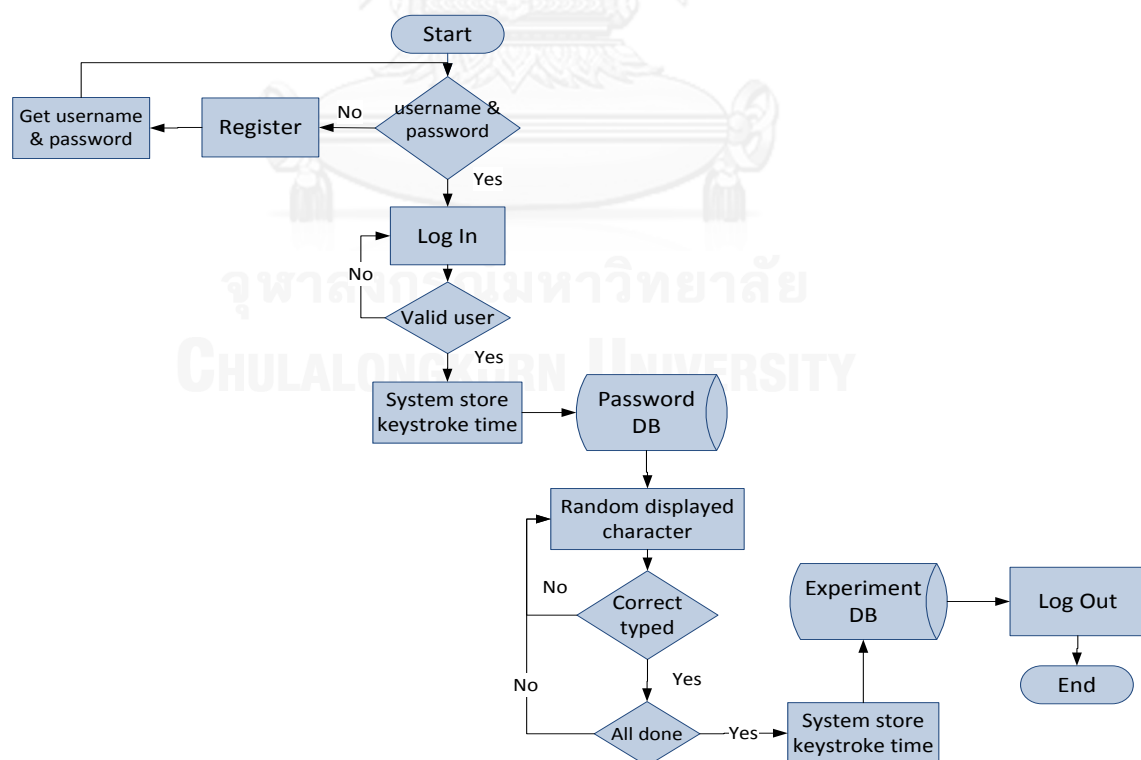


Figure 3.11 Flowcharts of the KPCS

Referring to Figure 3.11, it shows the workflow of procedures in the Key Pattern Collector System (KPCS). The KPCS starts the web page for registering and logging, the user has to register his/her personal information, then the system will generate a username and a password for the user for system login. After completing the registration, the user must login to the next step. During the login process, the system will capture times from keystroke typing and store in a temporary storage until the full entering password is confirmed its correctness. Otherwise, the system will require the user retype the password again. Then, the test for eye vision and hand's movement begin whenever the user presses the start button. The system will randomly generate a character and present to a random location on screen. The user needs to type the displayed character once it appears. The test in this process will repeat for nine times with nine random sets. However, if the user types any incorrect character, the test will restart from the beginning again. After the user finishes all correctly typing, all the keystroke dynamics data will be stored into the PattnDB database; the user signs out to finish the test.

### 3.6 Code Implementation

Base on the scenario above, the KPCS was developed and implemented as a web-based application that was programmed in PHP language, JavaScript, HTML, JQuery, and MySQL database. The KPCS consists of three main subsystems: the registration subsystem, the login subsystem and the experiment evaluation subsystem. The next section will present procedures of each subsystem and the programming technique.

**3.6.1. The registration subsystem:** this subsystem is responsible for users' registration, storing the user information, and generates a username and a password to the user after the registration success. The code implemented in this subsystem is PHP for connecting and interpreting data from HTML to store in the MySQL database.

**3.6.2. The login subsystem:** this subsystem is responsible for the login process. The meant of this subsystem is to capture the user's keystroke typing rhythm, using JQuery to capture the keystroke times. As soon as the user submits the

password, the validation process begins to check the correctness of the typing password. If the password is right, the keystroke times will be stored in the PattnDB; otherwise the system requires the user to retype the password again. The webpage of the login process is also developed using PHP and HTML.

**3.6.3. The experimental evaluation subsystem:** this subsystem is responsible for testing the eye vision ability and character' location of uses. The random a character and location to display on the screen come from as electing function of the test set for the user. This method is implemented by JQuery and JavaScript. All data will be record into a temporary storage, and after finished the test, the system will transfer data to store in the PattnDB. This part is implemented by JQuery Jason files, PHP, and MySQL database. All recorded data in the PattnDB is presented in the Figure 3.12.

user_id	firstname	lastname	email	age	gender	occupation	flagset
183	nansinee	luesakon	i.fern@hotmail.com	24	Female	Computers	0
184	nansinee	luesakon	tatoo9929@hotmail.com	18	Female	Computers	1
185	Maethika	Yisunsaeng	maethika2533@gmail.com	24	Female	Computers	3
186	toom	sara	toomsara@gmail.com	26	Male	Computers	0
187	Thanita	Wongkanha	thanita.wongkanha@gmail.com	22	Female	Administrative	1
188	Kamol	Rodyou	krommon@gmail.com	30	Male	Student	6
189	Tanat	Sirirattanakul	auxtopuz@hotmail.com	22	Male	Computers	1
190	Amornrat	Muangkaew	i.olive.ohlala@gmail.com	24	Female	Computers	0
191	Sopida	Sommun	nla_new1@hotmail.com	24	Female	Banking/Financial	0
192	Nuttawat	Ruensukon	n.ruensukon@gmail.com	24	Male	Computers	1
193	Nattapat	Peerachaidecho	khem129@hotmail.com	21	Male	Computers	2
194	Kittipong	Boonnan	ougogood@hotmail.com	24	Male	Banking/Financial	1

Figure 3.12 Example of records of a user in the UsersInfo table

Referring to Figure 3.12, it shows the screen captured of recorded data in the UsersInfo table from the phpMyadmin which is a tool for record user information. As seen from this figure, the UsersInfo table consists of eight attributes: User\_id, Firstname, Lastname, Email, Age, Gender, Occupation, and Flagset.

Meanwhile, the recorded data from login process is stored into the PasswordTime table that consists of seven attributes: Passwordlog\_id, User\_id, text, dwellTime, KeyPair, InterleaveTime, and TotalTime. Examples of records of users in the PassowrdTime table are shown in Figure 3.13 below.



passwordlog_id	user_id	text	dwellTime	KeyPair	interleaveTime	totaltime
1	1	Q.L.A.M.W.X.T.V	108,177,138,140,106,143,142,143	Q.L.L.A.A.M.M.W.W.X.X.T.T.V	453,3,54,32,156,128,146	3428
2	2	Q.L.A.M.W.X.T.V	159,80,96,96,112,112,96,112	Q.L.L.A.A.M.M.W.W.X.X.T.T.V	672,768,528,384,1040,320,784	7433
3	2	Q.L.A.M.W.X.T.V	224,144,128,95,207,128,96,160	Q.L.L.A.A.M.M.W.W.X.X.T.T.V	1824,416,1792,785,817,352,480	8942
410	10	Q.L.A.M.W.X.T.V	153,132,142,118,101,187,95,96	Q.L.L.A.A.M.M.W.W.X.X.T.T.V	114,172,189,84,147,116,293	4019
5	1	Q.L.A.M.W.X.T.V	95,128,112,96,96,96,112,96	Q.L.L.A.A.M.M.W.W.X.X.T.T.V	32,16,32,16,144,112,128	1630
6	1	Q.L.A.M.W.X.T.V	95,96,112,96,96,96,96,96	Q.L.L.A.A.M.M.W.W.X.X.T.T.V	32,48,64,32,144,96,144	1726
7	1	Q.L.A.M.W.X.T.V	80,97,112,96,128,112,112,128	Q.L.L.A.A.M.M.W.W.X.X.T.T.V	31,31,32,48,160,144,144	1998
8	1	Q.L.A.M.W.X.T.V	112,128,144,96,96,112,96,112	Q.L.L.A.A.M.M.W.W.X.X.T.T.V	128,64,80,48,177,144,192	12332
9	1	Q.L.A.M.W.X.T.V	104,152,112,88,96,104,88,112	Q.L.L.A.A.M.M.W.W.X.X.T.T.V	96,0,120,56,192,168,240	2939
10	3	Q.L.A.M.W.X.T.V	120,104,136,88,112,112,88,128	Q.L.L.A.A.M.M.W.W.X.X.T.T.V	488,168,72,936,232,1056,6760	13022
11	4	Q.L.A.M.W.X.T.V	184,144,152,192,200,152,160,152	Q.L.L.A.A.M.M.W.W.X.X.T.T.V	736,4623,2928,448,2056,376,848	15407

Figure 3.13 Example of records of a user in the PasswordTime table

Finally, the last table that records data is the ExperimentTime table which consists of 30:User\_id, Text, PositionText, VT1 – VT9, DT1– DT9, IT1–8, and Total. These attributes are shown in Figure 3.14. Figure 3.14 (a) shows all attributes of vision times of some users, namely VT1 to VT9. Figure 3.14 (b) presents all attributes of dwell times of some users, namely DT1 to DT9. Figure 3.14 (c) presents all attributes of interleave times of some users, namely IT1 to IT8.

User_id	Text	PositionText	DT1	DT2	DT3	DT4	DT5	DT6	DT7	DT8	DT9
84	k,g,z,a,b,p,m,y,q	1,2,9,3,8,4,7,5,6	85	96	134	138	128	106	101	96	107
84	c,k,v,f,m,a,e,p,y	2,3,1,4,9,5,8,6,7	112	115	133	133	101	149	107	117	80
84	b,x,n,k,q,f,y,a,o	3,4,2,5,1,6,9,7,8	87	143	80	105	111	105	72	145	80
84	n,b,w,c,y,j,u,f,a	4,5,3,6,2,7,1,8,9	48	112	80	96	80	64	64	80	112
84	e,n,t,b,o,c,a,l,g	5,6,4,7,3,8,2,9,1	96	64	96	96	96	96	112	64	64
84	t,w,i,n,a,b,f,z,j	6,7,5,8,4,9,3,1,2	64	96	80	64	129	128	96	80	64
84	p,t,s,q,h,n,j,b,z	7,8,6,9,5,1,4,2,3	96	96	112	64	64	64	64	96	112
84	a,o,f,y,j,e,x,m,b	8,9,7,1,6,2,5,3,4	95	80	96	80	64	80	112	64	80
84	g,s,k,o,x,t,b,q,n	9,1,8,2,7,3,6,4,5	80	112	80	80	128	80	95	80	64

(a)

User_id	Text	PositionText	IT1	IT2	IT3	IT4	IT5	IT6	IT7	IT8
84	k,g,z,a,b,p,m,y,q	1,2,9,3,8,4,7,5,6	1168	993	911	1163	1115	965	949	1059
84	c,k,v,f,m,a,e,p,y	2,3,1,4,9,5,8,6,7	740	784	988	805	673	1246	711	842
84	b,x,n,k,q,f,y,a,o	3,4,2,5,1,6,9,7,8	856	1697	727	864	920	943	800	823
84	n,b,w,c,y,j,u,f,a	4,5,3,6,2,7,1,8,9	737	768	912	624	736	768	800	832
84	e,n,t,b,o,c,a,l,g	5,6,4,7,3,8,2,9,1	672	768	688	656	736	592	672	879
84	t,w,i,n,a,b,f,z,j	6,7,5,8,4,9,3,1,2	640	704	928	608	639	881	752	576
84	p,t,s,q,h,n,j,b,z	7,8,6,9,5,1,4,2,3	815	736	848	704	912	608	720	768
84	a,o,f,y,j,e,x,m,b	8,9,7,1,6,2,5,3,4	656	640	800	656	672	752	689	832
84	g,s,k,o,x,t,b,q,n	9,1,8,2,7,3,6,4,5	720	784	704	800	800	688	687	640

(b)

User_id	Text	PositionText	VT1	VT2	VT3	VT4	VT5	VT6	VT7	VT8	VT9
84	k,g,z,a,b,p,m,y,q	1,2,9,3,8,4,7,5,6	1077	926	908	825	1062	994	877	862	977
84	c,k,v,f,m,a,e,p,y	2,3,1,4,9,5,8,6,7	773	649	697	892	719	575	904	624	745
84	b,x,n,k,q,f,y,a,o	3,4,2,5,1,6,9,7,8	1046	778	1624	653	791	846	873	728	750
84	n,b,w,c,y,j,u,f,a	4,5,3,6,2,7,1,8,9	856	722	753	900	609	720	748	783	816
84	e,n,t,b,o,c,a,l,g	5,6,4,7,3,8,2,9,1	713	659	756	672	640	722	568	656	864
84	t,w,i,n,a,b,f,z,j	6,7,5,8,4,9,3,1,2	815	624	690	908	582	624	768	734	557
84	p,t,s,q,h,n,j,b,z	7,8,6,9,5,1,4,2,3	950	793	716	833	687	890	593	702	753
84	a,o,f,y,j,e,x,m,b	8,9,7,1,6,2,5,3,4	677	639	625	784	640	658	728	674	811
84	g,s,k,o,x,t,b,q,n	9,1,8,2,7,3,6,4,5	796	703	768	682	781	784	672	649	623

(c)

Figure 3.14 Records of a user in the ExperimentTime table

Since, the ExperimentTime table is too long for presenting in one peace; Figure 3.14 presents the splitting of attributes those separated into 3 figures. Figure 3.14 (a) presents all attributes of the vision time of users using the name of VT1 until VT9. Figure 3.14 (b) presents all attributes of the dwell time of users using the name of DT1 until DT9. Figure 3.14 (c) presents all attributes of the interleave time of users using the name of IT1 until IT8. These parameters will be applied in the analytical process by SPSS v.17.0 and Weka 3.6.10.

### 3.7 Data Analysis Methods

The total participants in this experiment are 30 volunteers. The data are obtained from the typing of the fixed password, and typing from the experiment of eye vision's speed. All data are analyzed using SPSS v.17.0; Scheffe and Tukey are applied to test the mean time differences among various factors. Moreover, these data are also analyzed by Weka 3.6.10. The objective of this analysis is to determine the characteristics of each sample based on various biometrics.



## CHAPTER IV

### EXPERIMENTAL RESULTS

This chapter demonstrates the experimental results from the gathered data of the proposed method. The statistical results which are shown in this chapter were processed by SPSS v.17 will be described in Section 4.1 and the neural network analysis results will be illustrated in Section 4.2.

#### 4.1 Statistical Analysis Results

##### Phase 1: Test of time differences based on fixed password

Based on the collected data from 30 persons, 15 samples are random chosen to draw a line graph for comparing among mean times of each sample dwell times and mean times of each sample interleave times during typing the password, as shown in Figure 4.1 and Figure 4.2. From Figure 4.1 and Figure 4.2, they are clear that each person has unique pattern of their typing times. Thus, the analysis to determine these differences of samples must be performed.

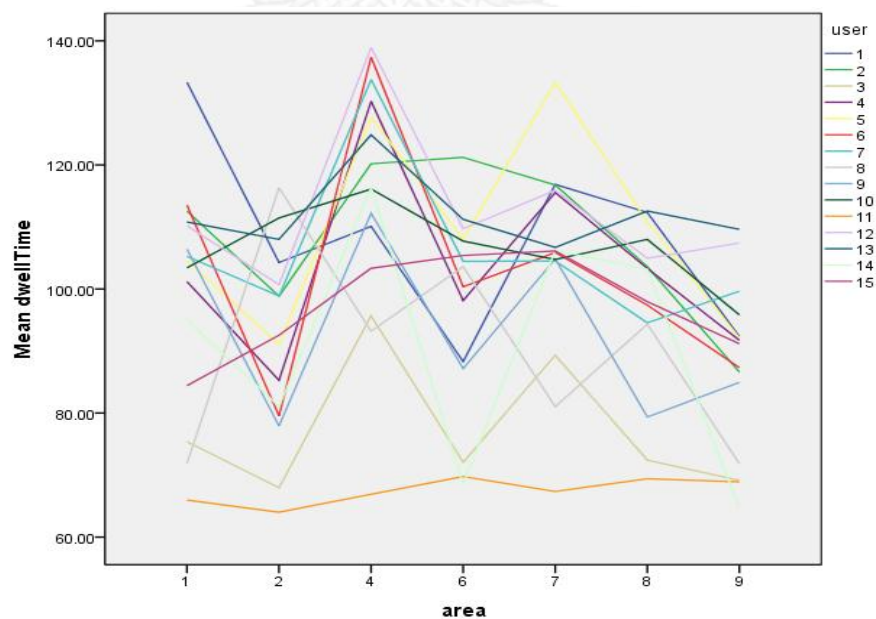


Figure 4.1 Mean Dwell Times from 15 random samples

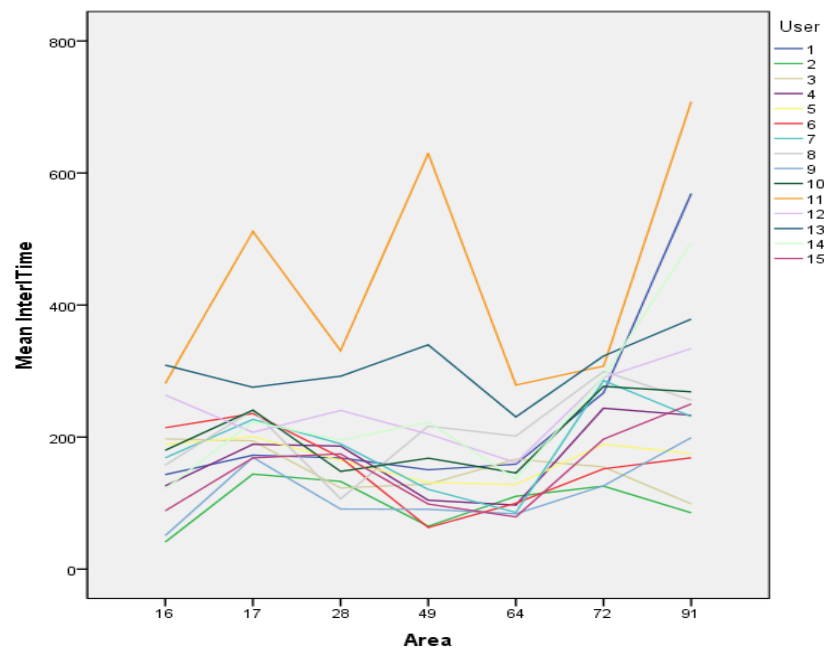


Figure 4.2 Mean Interleave Times from 15 random samples

In the first phase, the data from typing the fixed password will be analyzed using complete randomized design (CRD) with significant level ( $\alpha$ )= 0.05.

Let mean values of each person's dwell times be represented as MDT. The testing hypothesis is listed below.

$H_0$ : There is no significant difference among MDT of difference areas.

$H_1$ : There is at least one MDT of an area that has a significant difference from other areas.

Since the homogeneity of variance test indicates that there is at least one variance of an area that has significant difference from others. Thus, the Kruskal-Wallis test of non-parametric is applied for testing hypothesis above, the calculated p-value =  $0.00 < 0.05 = \alpha$ . Thus, it can conclude that there is at least one MDT of an area that has a significant difference from other areas.

$H_0$ : There is no significant difference among MDT of difference samples.

$H_1$ : There is at least one MDT of a sample that has a significant difference from other samples.

Since the homogeneity of variance test indicates that there is at least one variance of a sample that has significant difference from others. Thus, the Kruskal-Wallis test of non-parametric is applied for testing hypothesis above, the calculated p-value =  $0.00 < 0.05 = \alpha$ . Thus, it can conclude that there is at least one MDT of a sample that has a significant difference from other samples.

$H_0$ : There is no significant difference between MDT of two samples.

$H_1$ : There is significant difference between MDT of two samples.

Moreover, the analysis for comparing the different of between persons will be stated as a follows. Thus, the Independent-Samples Mann-Whitney nonparametric test is also applied for testing the different of pressing between two persons. Based on the collected data from 30 persons, 15 pairs are randomly chosen to test the different of Dwell Time (keypress). In the first pair comes from the Dwell Time of samples person 1 and 2, and another pairs are arranged in sequence remaining of the samples. According to the calculated result, it shows the significant in almost of samples are less than 0.05 or equal zero of different except the pair of samples 21 and 22. The calculation from pair of samples 21 and 22 shows the significant are 0.186, it mean that the sample person 21 and 22 has no significant different of mean time of dwell time when the character was pressed (see in APPENDIX, Table A1: Results comparing between users of Dwell Time).

Considering the interleave times obtained during the test, the differences of interleave times from all samples are analyzed. Moreover, the interleave times of the pressing areas of the keyboard are also investigated. Let mean values of each person's interleave times be represented as MIT. The testing hypothesis is listed below.

$H_0$ : There is no significant different between among of MIT within the sample group.

$H_1$ : There is at least one MIT within the sample group that has a significant different from other mean values.

Since the homogeneity of variance test indicates that there is at least one variance of a sample that has significant difference from others. Thus, the Kruskal-Wallis test of non-parametric is applied for testing hypothesis above, the calculated p-value =  $0.00 < 0.05 = \alpha$ . Thus, it can conclude that there is at least one MIT of a sample that has a significant difference from other samples.

$H_0$ : There is no significant difference among MIT of difference keyboard's movement.

$H_1$ : There is at least one MIT of a keyboard's movement that has a significant difference from other keyboard's movements.

Since the homogeneity of variance test indicates that there is at least one variance of a keyboard's movement that has significant difference from others. Thus, the Kruskal-Wallis test of non-parametric is applied for testing hypothesis above, the calculated p-value =  $0.00 < 0.05 = \alpha$ . Thus, it can conclude that there is at least one MIT of a keyboard's movement that has a significant difference from other keyboard's movements.

$H_0$ : There is no significant difference between MIT of two samples.

$H_1$ : There is significant difference between MIT of two samples.

Moreover, the analysis for comparing the differences between persons will be stated as follows. Thus, the Independent-Samples Mann-Whitney nonparametric test is also applied for testing the different time consuming typing of the Interleave Time. However, the random 15 pairs are the same as the analysis above. Referring to the hypothesis, the result shows the distribution of the interleave time is the same across categories of users. Unfortunately, there is a significant difference between 3 pairs: pair 4, pair 12, and pair 15. The result provided over of the significance level is 0.05. Thus, it means that the interval time of all those 3 pairs are significant different (see in APPENDIX, Table A2: Results comparing between users of Interleave Time).

According to the variances' differences among groups and non-parametric is applied for all testes above, the multiple comparison to confirm the pair difference cannot be performed. Thus, this data set can conclude only there is a significance difference among considered factors. However, it also determines that the movement of hands based keyboard pressing is an important factor for personal distinguishing.

### Phase 2: Test of time differences based on displayed characters

This part describes the test of eye vision ability based on displayed characters on different display areas. The Randomized Complete Block Design (RCBD) is applied for analyzing this data set.

Let mean of vision times be represented as MVT. All hypotheses are drawn below.

$H_0$ : There is no significant difference between MVT based on different samples.

$H_1$ : There is at least one MVT of a sample that has a significant different from others.

The result shows that there is at least one sample that has the MVT significant dissimilar to others,  $p\text{-value}=0.00 < 0.05 = \alpha$ .

$H_0$ : There is no significant difference between MVT based on different combination between display location and the position of character on the keyboard.

$H_1$ : There is at least one MVT of a combination between display location and the position of character on the keyboard that has a significant different from others.

The result shows that there is at least one combination between display location and the position of character on the keyboard area that has the MVT significant dissimilar to others,  $p\text{-value}=0.00 < 0.05 = \alpha$ . As a consequence of results



above, it can conclude that the combination between display location and the position of character on the keyboard has affect to the time values.

$H_0$ : There is no significant difference between MVT of two samples.

$H_1$ : There is significant difference between MVT of two samples.

Moreover, the analysis for comparing the differences between persons will be stated as a follows. Thus, the Mann-Whitney nonparametric test is applied for testing. However, the random of 15 pairs are the same as the analysis in phase 1 above. Referring to the hypothesis, the result shows the distribution of the vision time is the same across categories of users. Furthermore, the result of analyzed between 15 pairs provided the significant difference from other users. Thus, the eye vision ability has impact with the keyboard typing in each sample user (see in APPENDIX, Table A3: Results comparing between users of Vision Time).

Besides the consideration of the vision time, the interleave time is also counted as another important factor. To indicate the differences among interleave times of every sample based on the position of each character, Factorial Experimental Design is applied to analyze impacts from such factors. Hypothesis of all tests are listed as follow.

$H_{01}$ : There is no significant difference between MIT based on hand's movement.

$H_{11}$ : There is at least one MIT of a hand's movement that has a significant different from others.

$H_{02}$ : There is no significant difference between MIT based on different typing round.

$H_{12}$ : There is at least one MIT based on a typing round that has a significant different from others.

$H_{03}$ : There is no significant difference between MIT of different samples.

H<sub>13</sub>: There is at least one MIT of a sample that has a significant different from others.

H<sub>04</sub>: There is no significant difference between MIT based on different hand's movement and typing rounds.

H<sub>14</sub>: There is at least one MIT of a hand's movement and a typing rounds that has a significant different from others.

H<sub>05</sub>: There is no significant difference between MIT based on different typing rounds and samples.

H<sub>15</sub>: There is at least one MIT based on a typing round and a sample that has a significant different from others.

H<sub>06</sub>: There is no significant difference between MIT based on different hand's movement and different samples.

H<sub>16</sub>: There is at least one MIT of a hand's movement and a sample that has a significant different from others.

H<sub>07</sub>: There is no significant difference between MIT based on different hand's movement, typing rounds, and different samples.

H<sub>17</sub>: There is at least one MIT of a hand's movement, a typing round, and a sample that has a significant different from others.

H<sub>01</sub> – H<sub>14</sub> are hypothesis that check impact from all main effects while H<sub>04</sub>–H<sub>17</sub> are hypothesis that check impact from interaction among factors. The analytical results show that only the interaction between typing rounds and samples has no impact to the MITs,  $p=0.242 > 0.05 = \alpha$ .

Based on all conclusions, it can imply that there is a possibility of personal differentiation under the use of typing locations and display positions, no matter which time values are used.

## 4.2 Neural Network Analysis Results

Referring to the results from the statistical analysis, there is at least one mean different among other mean values under individual sample and the character's location consideration. Thus, to confirm that the speed of eye vision interacts with keystroke and character's location can identify an individual person, the neural network analysis is applied.

As a consequence of every statistical test, factors that will be included in the neural network analysis are the typing location, the display area, the dwell time, the vision time, and the interleave time.

In this research, the neural network analysis was performed using machine learning for classification; Weka versions 3.6.10 is used. The analysis method is the Naive Bayes network; Naive Bayes classifier is a technique of Bayes Theorem. This technique uses the probabilistic classifier under the assumption that all samples are independent [31]. Based on Bayes probability theorem [31], the Naive Bayes network is used widely in the pattern classification and keystroke analysis. Moreover, the results of Naive Bayes classifiers are evaluated by the standard metrics of accuracy: Precision, Recall, F-measure, FRR, FAR and ROC area. These values are presented in the Confusion Matrix, as shown in Table 4.1.

In order to perform Naive Bayes network classification, the data must be separated into three sets of instances. Each set will be divided into two different classes: the authorized class (10%) and the imposter class (90%). Since the experiment is performed into two phases: fixed password testing, and eye vision testing, therefore, within each sets there are three data sets based on each phase. Table 4.1 shows the categories of data in the Naive Bayes network classification process.

Table 4.1 Categories of data in the Naive Bayes network classification

Set of Instances		Imposter	Authorize	Total
Set 1.	Dwell Time +	90%	10%	100%
	Interleave Time			
Set 2.	Dwell Time +	90%	10%	100%
	Interleave Time +			
	Vision Time			
Set 3.	Character's location+	90%	10%	100%
	Interleave Time			

#### Learning of Data in Phase I

After the training phase of data in both classes, the learning phase is performed. The result of the learning phase is presented in Table 4.2 which indicates that using only the dwell time and the interleave time can provide 70% classification accuracy.

Table 4.2 ANN classification results of single keystroke (dwell and interleave)

Correctly Classified Instances	70	70 %
Incorrectly Classified Instances	30	30 %
Precision	0.894	
Recall	0.7	
F-Measure	0.759	
ROC area	0.797	
FAR	0.3	
FRR	0.211	

Referring to Table 4.2 above, the result classification using single of keystroke dynamics; dwell and interleave time, It shows that the correctly classified

instances at 70%. In addition, there are 0.894 (precision), 0.7 (recall), 0.759 (F-measure), and 0.797 (ROC area). These mean, the precision result shows the retrieved incorrect in the wrong class. Whereas, the result answers that correct in the right class is high. The effective of classification in this phase is provided the low accuracy results.

### Learning of Data in Phase II

Table 4.3 shows the classification result of multi-biometrics, there is 91% for correctly classified instances when the classifier model consists of the typing location, the display area, the dwell time, the vision time, and the interleave time. In addition, there are 0.923 (precision), 0.91 (recall), 0.915 (F-measure), and 0.794 (ROC area). These mean, the precision result is higher than the precision result from phase I, whereas, the recall result in this phase is lower than the phase I. However, the effective of classification result is higher than the phase I.

**Table 4.3 ANN classification results of combined eye vision with keystroke**

Correctly Classified Instances	91	91 %
Incorrectly Classified Instances	9	9 %
Precision	0.923	
Recall	0.91	
F-Measure	0.915	
ROC area	0.794	
FAR	0.09	
FRR	0.277	

### Learning of Data in Phase III

According to the last phase, the classification to confirm the impact of character's location towards the time of hand's movement in each person is performed. The instances to be used for considering are character's location, and interleave time between the characters. The instance obtained from the collected data, 8 samples are random from 9 test sets for classifying the class of authorize and

imposter users. However, the classification of character's location on phase III is presented on the Table 4.4 below.

**Table 4.4 ANN classification results of character's location**

Correctly Classified Instances	96	96 %
Incorrectly Classified Instances	4	4 %
Precision	0.971	
Recall	0.96	
F-Measure	0.963	
ROC area	0.996	
FAR	0.04	
FRR	0.004	

Referring to Table 4.4, the result of classification using location of character and interleave time shows that the correctly classified instances at 96%. In addition, the correct classification on the authorize class provided a perfect corrected in the right class. These results confirm that the character's location has significant impact to the typing style of each person.

## CHAPTER V

### DISCUSSION AND CONCLUSION

In this chapter, the discussion is drawn in Section 5.1, and the conclusion of this study will be stated in Section 5.2. Finally, the future work is stated in Section 5.3.

#### 5.1 Discussion

Since many valuable resources are installed over the Internet, this persuades intruders to attack the existing system in tremendous ways. One direct technique is to steal the user name and password to gain access from the system. Therefore, many protection mechanisms are proposed and implemented to solve such problem. The most popular technique in the present world is the use of biometric. These biometric are obtained from personal characteristics, such as fingerprint, iris, face recognition, speaker recognition, and keystroke dynamics. Unfortunately, no such metrics can completely guarantee the correctness of the identification system. Therefore, multi-biometrics is applied to gain higher accuracy, such as a use of keystroke dynamics with face recognition.

Although multi-biometrics is applied, the weakness of this method is the use of specific equipment for biometrics capturing. Therefore, the eye vision is proposed by [1] to combine with the use of keystroke value since this technique needs no extra equipment and also can be applied to every keyboard system, including the touch screen technology. Nevertheless, this research discovers that the typing time might relate to the position of the typing character. Therefore, suitable parameters that should be deployed to the authentication process include the location of the typing character as well as the typing time when the character is displayed.

The result from the previous chapter indicates that the times captured from both phases are related to the physical characteristics of equipment which are the position of the character location over the keyboard and the position of the displayed character. Moreover, high accuracy of personal classification can be obtained when the classification module includes these physical characteristics in

the classification mechanism. So, in order to obtain high accuracy of intrusion protection, the multi-biometrics should be applied with the physical characteristics of equipment. Moreover, this result also indicates that the difficulty in hacking a password is also depended on the location and sequence of each character in the password itself.

## 5.2 Conclusion

The authentication process is a serious procedure because of increasing usage of the Internet. Many techniques have been proposed and implemented, especially the use of biometrics. Originally, the single biometrics is implemented in various systems, such as face recognition, fingerprint scan, iris scan, etc. However, these biometrics can be changed according to time or can be emulated by some special equipment. Thus, the protection of the system cannot be completed as wish.

This research has proved that the use of keystroke dynamic can increase its accuracy by combining this method with other biometrics and physical characteristics of equipment. The classification module that uses times from keystroke dynamics combining with locations of displayed and typing characters is able to detect an authenticated person with 91% accuracy. Times that are implemented in the classification module are dwell time, interleave time, and vision time.

The benefit of the proposed parameters is not only enhance the protection ability of the system, but also easy to be implemented in the real protection mechanism. Moreover, it is cost effective since there is no additional equipment required.



### 5.3 Future work

In this research, the measurement of detection in keystroke dynamics is presented based on the study of eye vision and character's location experimental benchmark data. Consequently, the implementation of mechanism to identify the authorized person using the random of Greco-Latin Square method should be developed for reality uses. The result shows the significant of character's location typing can be identify the person. Moreover, the future work should be tested more than 9 test sets which are collected on the proposed method. Moreover, Greco-Latin Square method can consider in many dimension of test set for enhance the accuracy result.



## REFERENCES

1. K. Nonsrichai, a.P.B., *A New Alternative of an Authentication System using the Eye Vision Ability*, in *Computing and Convergence Technology (ICCCCT)*. 2012, 7th International Conference on IEEE: Seoul, South Korea.
2. Debnath Bhattacharyya, R.R., FarkhodAlisherov A., and Minkyu Choi, *Biometric Authentication: A Review*. u- and e- Service, Science and Technology, 2009. **Vol. 2, No. 3**.
3. James Wayman, A.J., DavideMaltoni and Dario Maio, *An Introduction to Biometric Authentication Systems*. Biometric Systems - Technology, Design and Performance Evaluation, 2005: p. 1-20.
4. <http://www.intechopen.com/books/biometrics/keystroke-dynamics-overview>.
5. [http://www.cse.iitk.ac.in/users/biometrics/pages/what\\_is\\_biom\\_more.htm](http://www.cse.iitk.ac.in/users/biometrics/pages/what_is_biom_more.htm). 2011.
6. [http://www.infosecurityproductsguide.com/technology/2007/BioPassword\\_Authentication\\_Solutions\\_Whitepaper\\_FINAL.pdf](http://www.infosecurityproductsguide.com/technology/2007/BioPassword_Authentication_Solutions_Whitepaper_FINAL.pdf).
7. Ilonen, J., <http://www.it.lut.fi/kurssit/03-04/010970000/seminars/Ilonen.pdf>.
8. Shepherd, S.J., *Continuous Authentication by Analysis of Keyboard Typing Characteristics*, in *International Conference on European Convention on Security and Detection*. 1995, Conference publication No. 408, in IEEE.
9. Gentner. *Keystroke timing in transcription typing*. in *Cognitive Aspects of skilled typewriting*. 1993.
- 10.H. Al-Assam, H.S., and S. Jassim. *Multi-Factor Biometrics for Authentication: A False Sense of Security*. in *in the proceedings of the 12th ACM Workshop on Multimedia and Security*. September 2010. Rome, Italy.
- 11.Kenneth Revett, F.G., Marina Gorunescu and Marius Ene, *A machine learning approach to keystroke dynamics based user authentication*. international Journal of Electronic Security and Digital Forensics, 2007. **Vol. 1, No. 1**.
- 12.Salil P. Banerjee, a.D.L.W., *Biometric Authentication and Identification using Keystroke Dynamics: A Survey*. International Journal of Pattern Recognition Research 7, 2012.
- 13.F. Bergadano, a.e.a., *User Authentication through Keystroke Dynamics*. International Journal of ACM Transactions on Information and System Security, 2002. **Vol. 5, No. 4**.
- 14.Obaidat, M.S., Sadoun, *Verification of Computer Users using Keystroke Dynamics*, in *IEEE Transactions on Systems, Man, and Cybernetics, Part B: Cybernetics*. 1997, IEEE Press Piscataway, NJ, USA. p. 261-269.

- 15.S. Giroux, R.W.S., and Mark P. Wanchowiak. *Keypress Interval Timing Ratios as Behavioral Biometrics for Authentication in Computer Security*. in *In proceeding of: Networked Digital Technologies*. 2009.
- 16.Chang, W., *Improving Hidden Markov Models with a Similarity Histogram for Typing Pattern Biometrics*. in IEEE, 2005.
- 17.G.C. De Silva, J.M.L., S. Kawato and N. Tetsutani, *Human Factors Evaluation of a Vision-Based Facial Gesture Interface*, in *in Conference on Computer Vision and Pattern Recognition*. 2003. p. 52.
- 18.W. Kienzle, F.A.W., B. SchÖlkopf, and M.O. Franz, *Learning an Interest Operator from Human Eye Movements*, in *in IEEE Conference on Computer Vision and Pattern Recognition*. 2006. p. 1-8.
- 19.S. Bajaj, a.K., *Typing Speed Analysis of Human for Password Protection (Based On Keystrokes Dynamics)*. *International Journal of Innovative Technology and Exploring Engineering (IJITEE)*, 2013. **Vol. 3**.
- 20.G. Shin, J.C. *Vision-based Multimodal Human Computer Interface based on Parallel Tracking of Eye and Hand Motion*. in *In proceeding of: Convergence Information Technology, IEEE*. 2007.
- 21.B. Hussien, R.M.a.S.B., *An application of fuzzy algorithms in a computer access security system*. *Pattern Recognition Letters*, 1989.
- 22.M. Akila, S.S.K., *Improving Feature Extraction in Keystroke Dynamics using Optimization Technique and Neural Network*, in *International Conference on Sustainable Energy and Intelligence System (SEISCON 2011)*. 2011: India.
- 23.A. Jameer Basha, V.P., T. Purusothaman, *Fast multimodal biometric approach using dynamic fingerprint authentication and enhanced iris features*, in *Computational Intelligence and Computing Research (ICCIC)*. 2010, in IEEE: Coimbatore. p. 1-8.
- 24.Abdallah Meraoumia, S.C.a.A.B. *Fusion of Finger-Knuckle-Print and Palmprint for an Efficient Multi-biometric System of Person Recognition*. in *IEEE Communications Society subject matter experts for publication in the IEEE ICC 2011 proceedings*. 2011.
- 25.Hu, L.Z.a.Q., *The Research of Double-biometric Identification Technology Based on Finger Geometry & Palm print*, in *in IEEE*. 2011.
- 26.Romain Giot, B.H., and Christophe Rosenberger, *Low Cost and Usable Multimodal Biometric System Based on Keystroke Dynamics and 2D Face Recognition*, in *International Conference on Pattern Recognition (ICPR)*. 2010, in IEEE. p. 1128-1131.

27. Ning Wang, Q.L., Ahmed A. Abd El-Latif, Jialiang Peng and Xiamu Niu, *Multibiometrics Fusion for Identity Authentication: Dual Iris, Visible and Thermal Face Imagery*. International Journal of Security and Its Applications, 2012. **Vol. 7, No. 3**.
28. Freire, J.R.M.a.F.a.E.O., *Multimodal Biometric Fusion — Joint Typist (Keystroke) and Speaker Verification*, in *Telecommunication Symposium (ITS)*. 2006, in IEEE. p. 609-614.
29. Sylvain Hocquet, J.-Y.R., and Hubert Cardot, *Fusion of Methods for Keystroke Dynamic Authentication*, in *Automatic Identification Advanced Technologies*. 2005, in IEEE. p. 224-229.
30. Raut, T.S.I.a.S.D., *Person Identification based On Multi-biometric Characteristics*, in *International Conference on Emerging Trends in Computing, Communication and Nanotechnology (ICECCN 2013)*. 2013. p. 45-52.
31. L. Huijuan, C.K., and L. Bai, *Bayesian Network Based Behavior Prediction Model for Intelligent Location Based*, in *Industrial Electronics and Applications ICIEA 2007*. 2007, in IEEE Conference.
32. Anagun, A.S., *Designing A Neural Network Based Computer Access Security System: Keystroke Dynamics and/or Voice Patterns*. Smart Engineering System Design, 2002: p. 125-132.
33. F. Monroe, M.K.R.a.S.W. *Password Hardening Based on Keystroke Dynamics*. in *in Proceeding of the 6th ACM on Computer and communications security*. 1999. New York, USA.
34. Maxion, K.S.K.a.R.A. *Comparing Anomaly Detectors for Keystroke Dynamics*. in *in Proceedings of the 39th Annual International Conference on Dependable Systems and Networks (DSN-2009)*, in IEEE. 2009.



APPENDIX

จุฬาลงกรณ์มหาวิทยาลัย  
**CHULALONGKORN UNIVERSITY**

Table A1: Results comparing between users of Dwell Time

Hypothesis Test Summary				
	Pair of users	Null Hypothesis	Sig.	Decision
1	1 and 2	The distribution of pressing is the same across categories of user	0.000	Reject the null hypothesis.
2	3 and 4		0.000	
3	5 and 6		0.000	
4	7 and 8		0.000	
5	9 and 10		0.000	
6	11 and 12		0.000	
7	13 and 14		0.000	
8	15 and 16		0.000	
9	17 and 18		0.000	
10	19 and 20		0.000	
11	21 and 22		0.186	Retain the null hypothesis.
12	23 and 24		0.000	Reject the null hypothesis.
13	25 and 26		0.000	
14	27 and 28		0.001	
15	29 and 30		0.000	

Asymptotic significances are displayed. The significance level is .05.

Table A2: Results comparing between users of Interleave Time

Hypothesis Test Summary				
	Pair of users	Null Hypothesis	Sig.	Decision
1	1 and 2	The distribution of interval is the same across categories of user	0.000	Reject the null hypothesis.
2	3 and 4		0.019	
3	5 and 6		0.006	
4	7 and 8		0.197	Retain the null hypothesis.
5	9 and 10		0.000	Reject the null hypothesis.
6	11 and 12		0.000	
7	13 and 14		0.003	
8	15 and 16		0.000	
9	17 and 18		0.000	
10	19 and 20		0.000	Retain the null hypothesis.
11	21 and 22		0.000	
12	23 and 24		0.142	Retain the null hypothesis.
13	25 and 26		0.000	Reject the null hypothesis.
14	27 and 28		0.000	
15	29 and 30		0.223	Retain the null hypothesis.

Asymptotic significances are displayed. The significance level is .05.

Table A3: Results comparing between users of Vision Time

Hypothesis Test Summary				
	Pair of users	Null Hypothesis	Sig.	Decision
1	1 and 2	The distribution of vision time is the same across categories of user	0.000	Reject the null hypothesis.
2	3 and 4		0.000	
3	5 and 6		0.000	
4	7 and 8		0.000	
5	9 and 10		0.000	
6	11 and 12		0.000	
7	13 and 14		0.000	
8	15 and 16		0.000	
9	17 and 18		0.000	
10	19 and 20		0.000	
11	21 and 22		0.000	
12	23 and 24		0.000	
13	25 and 26		0.000	
14	27 and 28		0.000	
15	29 and 30		0.000	

Asymptotic significances are displayed. The significance level is .05.



Table A4: Results of classification data from single of keystroke dynamics

=== Stratified cross-validation ===							
=== Summary ===							
Correctly Classified Instances	70	70%					
Incorrectly Classified Instances	30	30%					
Kappa statistic	0.2268						
Mean absolute error	0.2968						
Root mean squared error	0.5224						
Relative absolute error	158.76%						
Root relative squared error	174.07%						
Total Number of Instances	100						
=== Detailed Accuracy By Class ===							
			FP		F-	ROC	
	TP Rate	Rate	Precision	Recall	Measure	Area	Class
	0.689	0.2	0.969	0.689	0.805	0.797	Imposter
	0.8	0.311	0.222	0.8	0.348	0.793	Authorize
Weighted Avg.	0.7	0.211	0.894	0.7	0.759	0.797	
=== Confusion Matrix ===							
a	b	← classified as					
62	28	a = Imposter					
2	8	b = Authorize					

Table A5: Results of classification data from Multi-Biometrics

```

=== Stratified cross-validation ===
=== Summary ===

Correctly Classified Instances      91   91%

Incorrectly Classified Instances      9   9%

Kappa statistic      0.5588
Mean absolute error      0.0994
Root mean squared error      0.2901
Relative absolute error      53.15%
Root relative squared error      96.65%
Total Number of Instances      100

=== Detailed Accuracy By Class ===

```

	TP Rate	FP Rate	Precision	Recall	F- Measure	ROC Area	Class
	0.933	0.3	0.966	0.933	0.949	0.79	Imposter
	0.7	0.067	0.538	0.7	0.609	0.787	Authorize
Weighted Avg.	0.91	0.277	0.923	0.91	0.915	0.794	

```

=== Confusion Matrix ===
a  b <-- classified as
84  6 | a = Imposter
 3  7 | b = Authorize

```

Table A6: Results of classification data from Character's location

=== Stratified cross-validation ===

=== Summary ===

Correctly Classified Instances	96	96%
Incorrectly Classified Instances	4	4%
Kappa statistic	0.8113	
Mean absolute error	0.0364	
Root mean squared error	0.182	
Relative absolute error	19.4914%	
Root relative squared error	60.6326%	
Total Number of Instances	100	

=== Detailed Accuracy By Class ===

	TP Rate	FP Rate	Precision	Recall	F-Measure	ROC Area	Class
	1	0.044	0.714	1	0.833	0.996	Imposter
	0.956	0	1	0.956	0.977	0.996	Authorize
Weighted Avg.	0.96	0.004	0.971	0.96	0.963	0.996	

=== Confusion Matrix ===

a b <-- classified as

86	4	a = Imposter
0	10	b = Authorize

## VITA

Miss KranogwanKrasaesat was born on May 21, 1990 in Phanakorn Sri Ayutthaya. She attended in the faculty of Business Administration, in department of International Bachelor of Business Administration, major in International Information System at Rajamangala University of Technology Thanyaburi for Bachelor in Business Administration, in the year 2011. After that, she continued her study in Master's degree in the year 2012 in faculty of Science, ChulalongkornUniversity, major in Computer Science and Information Technology.

Publication paper:

- Krasaesat, K., and Bhattarakosol, P. "The Significant of Character's Location in the Authentication Process," Proceeding on ACIT'14 International Conference on Advance in Computing and Information Technology. Bangkok, Thailand, 2014, pp. 10-14.