RANDOMNESS FINGERPRINT AUTHENTICATION WITH BARCODE

LEONG HUAY CHING

This report is submitted in partial fulfillment requirements for the
Bachelor of Computer Science (Computer Network)

FACULTY OF INFORMATION AND COMMUNICATIONS TECHNOLOGY
KOLEJ UNIVERSITI TEKNIKAL KEBANGSAAN MALAYSIA
2005

TESIS APPROVAL STATUS FORM

JUDUL: **RANDOMNESS FINGERPRINT AUTHENTICATION WITH BARCODE**

SESI PENGAJIAN: **2004 / 2005**

Saya **LEONG HUAY CHING**

mengaku membenarkan tesis (PSM/Sarjana/Doktor Falsafah) ini disimpan di Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dengan syarat-syarat kegunaan seperti berikut:

1. Tesis adalah hakmilik Kolej Universiti Teknikal Kebangsaan Malaysia.
2. Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dibenarkan membuat salinan untuk tujuan pengajian sahaja.
3. Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dibenarkan membuat salinan tesis ini sebagai bahan pertukaran antara institusi pengajian tinggi.
4. ** Sila tandakan (/)

_____	SULIT RASMI	(Mengandungi maklumat yang berdarjah keselamatan atau kepentingan Malaysia seperti yang termaktub di dalam AKTA RAHSIA 1972)
_____	TERHAD	(Mengandungi maklumat TERHAD yang telah ditentukan oleh organisasi/badan di mana penyelidikan dijalankan)
___/___	TIDAK TERHAD	

(TANDATANGAN PENULIS)

Alamat tetap : No 7, Lorong 1,
Taman K.S.M. ,
72100 Bahau, N.S.

Tarikh : 22/11/05

(TANDATANGAN PENYELIA)

Encik Nazrulazhar Bin Bahaman

Tarikh : 25/11/05

DECLARATION

I admitted that this project title name of

RANDOMNESS FINGERPRINT AUTHENTICATION WITH BARCODE

is written by me and is my own effort and that no part has been plagiarized without citations.

STUDENT : _____ Date : 22/11/05

(LEONG HUAY CHING)

SUPERVISOR : _____ Date : _____

(Mr. NAZRULAZHAR BIN BAHAMAN)

DEDICATION

To my beloved parents

ACKNOWLEDGEMENT

Through this PSM project, a lot of knowledge, skills and experience I have obtained during each different planning or implementation phase. To complete this project, I owe tremendous gratitude to many people that helped with the development of this report. I never would have accomplished this report without the help and advice of my project supervisor, Encik Nazurlazhar Hj Bahaman. I would like to thanks for his providing excellent guidance, cooperation and support thought the whole course of the project.

I would like to express many thanks also to all PSM committees for guiding and leading the way during the entire planning and implement project period. I receive valuable comments and suggestion from them on ways to improve the quality and structure of PSM report and project.

Most of all, I am grateful to my parents and family. Without their support, I never could undergo the trial of PSM and accomplish the project successfully. Thanks for their undying support and encouragement during study in Kolej Universiti Teknikal Kebangsaan Malaysia (KUTKM). At last, sincere appreciation to all my friends and all those who helped me in one way or another towards the success of this project.

ABSTRACT

The title of this thesis is "Randomness Fingerprint Authentication with Barcode". The main purpose of system is to be able to improve the efficiency and effectiveness of the current authentication security and attendance signature system. Most of the current authentication and attendance signature system is found that do not fulfill the criteria of security requirement. These current system have similar problem, it unable to guarantees authenticated the correct user with something that cannot be lost, forgotten, misplaced, shared or stolen. With this thesis, the feasibility of integrating the fingerprint authentication system with the barcode authentication technology will be researched and implemented. The "Randomness Fingerprint Authentication with Barcode" is a new scheme to solve the problems which was found on the traditional student attendance system and existing fingerprint authentication system. The system that proposed is not only using the static formula for request user fingerprint but will establish a randomized fingerprint algorithm. This randomized algorithm will be the most attractive and interesting features or function if compare with other authentication system. Besides, by combination of fingerprint verifying with bar code authentication mechanism, it can improves the effectively identification of the particular person in attendance signature process. In this thesis, some existing fingerprint authentication system is taken as investigate and analysis sample. Problem statement is established based on the analysis and requirement for the to-be system is captured. On the other hand, a preliminary design of the to-be system is established as well including system architecture, user interfaces design, and logical database design. As in conclusion, the wellness of "Randomness Fingerprint Authentication with Barcode" will represent through the completion of this thesis.

ABSTRAK

Tajuk tesis yand dihasilkan adalah "*Randomness Fingerprint Authentication with Barcode*". Tujuan utama sistem dihasilkan adalah untuk meningkatkan kecekapan dan keberkesanan sistem pengesahan dan sistem kehadiran yang sediada. Kebanyakan sistem pengesahan dan sistem kehadiran masa kini didapati tidak memenuhi kriteria keselamatan keperluan. Sistem yang sediada mempunyai masalah yang hampir sama, iaitu tidak berupaya menjamin dapat mengesahkan pengguna yang betul dengan sesuatu yang tidak akan dihilangkan, dilupai, disalah letakan, dikongsi dan dicuri. Dengan adanya tesis ini, kebolehlaksanaan untuk menyatukan sistem pengesahan cap jari dengan pengesahan kod-bar teknologi akan dikajiselidikan dan dilaksanakan. "*Randomness Fingerprint Authentication with Barcode*" merupakan satu skema yang baru untuk menyelesaikan masalah yang tertimbul dalam sistem kehadiran yang tradisional serta sistem penyesahan cap jari yang sediada. Sistem yang dicadangkan tidak menggunakan formula statik dalam proses permintaan pengimbasan cap jari, manakala formula kerawakan permintaan pengimbasan cap jari akan dibangunkan. Kerawakan algoritma yang diadakan dalam sistem "*Randomness Fingerprint Authentication with Barcode*" merupakan satu daya tarikan dan ciri atau fungsi yang amat menarikan jika berbanding dengan sistem pengesahan yang lain. Selain daripada itu, dengan adanya penggabungan pengesahan cap jari dengan mekanisme pengesahan kod- bar, ia dapat meningkatkan keberkesanan pengesahan pengguna dalam sistem tandatangan kehadiran. Dalam tesis ini, sesetengah sistem pengesahan cap jari yang sediaada akan dijadikan sebagai contoh untuk dikajiselidik dan dianalisiskan. Penerangan masalah juga akan dinyatakan berdasarkan analisis dan keperluan untuk sistem yang akan dibangunkan. Di samping itu, rekabentuk awalan untuk system yang bakal dibangunkan juga akan ditentukan dan dinyatakan, antaranya termasuk senibina sistem, rekabentuk antara muka, dan rekabentuk pangkalan data. Sebagai kesimpulannya, kelebihan "*Randomness Fingerprint Authentication with Barcode*" akan ditunjukan dengan kesempurnaan penyiapan tesis ini.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURE

CHAPTER I

INTRODUCTION

1.1 Project Background

The attendance is required in various situations which aim provide convenient to identify individual who attend. The problem that commonly occur in the manual signature attendance system is some individual may fraud or cheat on the attend list. To avoid this problem increase the fingerprint and barcode authentication security biometric technology is proposed add into the attendances system. Biometric technologies now are the most popular recommended methods of recognizing and verify the identity of an individual base on physiological or behavioral characteristics. These biometrics technologies are including fingerprints, iris scanning, handwriting, facial recognition, hand geometry, and voice patterns. Most of the identification method that commonly use is based on "what user know" and "what user have" concept. Biometrics authentication is not base on both concept but is establishing on the third method which is "what user are" concept. By this biometrics authentication technique means the end to using unwieldy password systems.

Through the analysis, corporate IT departments need to spend more than thirty percent of their time to reissuing password. If the user password is their face or finger, the trouble of memories password will be decrease and the user probably never lose their password. Because of these advantages, biometrics is currently becoming more popular for convenient and secure authentication. Fingerprint

authentication method are the best known and universal biometrics method to every human being and unique to each person. The fingerprint biometric has a long history of use and low data collection error rate. In the nineteenth century, Dr. Henry Faulds, a British surgeon superintendent, living in Japan, published a paper about fingerprints in Nature magazine. Since then, fingerprint authentication has been widely used and affordable. Fingerprint is an imprint made by the pattern of ridges on the pad of a human finger. The chance of two people having the same identical fingerprint is never been found, thus fingerprints are widely believed to be unique. The automatic fingerprint identification systems have traditionally been used by law enforcement agencies. Use of the fingerprint identification system is now expanding into various sector and industry such as local or foreign companies, government, financial and banking, and healthcare. These fingerprint technique also gaining popularity for security and access control application.

The topic of this thesis is "Randomness Fingerprint Authentication with Barcode (RFA) system". The core function in RFA system is the combination fingerprint authentication biometric technology and barcode authentication technology system. The fingerprint scanning products are the most common biometrics product type on the market today. But the market of integrated solution between the fingerprint devices with computer usage or other devices is still not mature yet. Research and development in fingerprint identification algorithms and integrated systems still encourage by local or foreign companies and government organizations or different industries. The purpose of this system is research, modified and development in fingerprint identification algorithms and integrated systems between fingerprint devices with others necessary devices. The strength points that focus on this system is randomly fingerprint authentication formula.

1.2 Problem Statements

The problem statement will represent the weakness or some vulnerability scenario that found in the current authentication system. The topic of the project is

produced mainly because of the following existing problem of the current security environment.

a) Attendance system

Nowadays the time and attendance system is still the popular mechanism that use in various sector such as education sector. This attendance system can be the punch card attendance system, student attendance system or others. Same concept with the smart card system, the time and attendances system is base on what use have. The vulnerability that can easier found in this kind of system is card attendance may be used by someone other than the authorized user and easy to lose, inaccurate and the manual signature attendance may be easily fraud by other individual. The weakness of this traditional system is that they allow attendee to clock in or signature for others. This is because the attendance system only verifies the time and attendance card or signature but not the attendee's unique identity. It also can define as the current attendance system unable to identify and verify the correct attendees.

Other weaknesses of these systems are attendance card or list easy to lose, stolen, misread and shared. These vulnerabilities may cause serious problem, for example student will not attended on time and punctuality or direct absence to class but the subject's attendance record still show this student is on working status. This behavior not only leads the management of class out of control and student study attitude also become irresponsible, slothful and inefficient.

On the other hands, attendance system maintenance cost increase also is one of the weaknesses. Easy to lose and susceptible to change effect the sector losing time and resources for manage the attendance list or card replacement and redo attendance record. Electronically attendance signature by using fingerprint authentication is more effective and produces fewer errors when there are larger individual populations. With this biometric technique, the organization or sector can reducing the incidence of fraud and gets rid of manual errors.

b) Unable to authenticated the correct person

Network and application access, confidential data, and employee entrance must be controlled and secured. The current security methods are not only insufficient to provide the stringent logical and physical access required to support organization, but easy to fraud as employees trade cards and/or pin numbers to bypass current security and attendance terminals. These current systems unable to authenticate the correct person therefore unauthorized user can access any time or any where by using other people identity card and pin number which does not belongs to them. Besides, primary reasons exist for inaccurate records may cause duplicate record or similar record. The fingerprint technology is needed to increase site security and guarantees the correct personnel. Duplicate, similar or pretend identity problem will decrease and authentication is more accurate.

b) Vulnerability of smart card or swipe card system

Many highly secure environments have used smart card or card swiping technology for entry access major application or control access to secure location such as rooms and building or can be define as access security. But the reality is utilizing the fingerprint biometric technology for authentication process is more confidential and convenient than these smart card or swipe card authentications system. The smart card seems to be a superior tool for enhancing system security and provides a place for secure storage, the secret of the cryptographic algorithm, the keys stored, and the access control inside the smart card actually become the targets of attackers.

Nowadays many companies and cryptographers claimed to be able to break the smart card and its microcontroller. Some of them perform logical non-invasive attacks; some of them attack the card physically while others just prove their success by mathematical theorems. Logical non-invasive attacks means all the key materials of smart card that stored in the electrically erasable programmable read only memory (EEPROM) can be affected by unusual voltage and temperatures. On the other hands, the vulnerability of smart card security system is easy to damage or sabotage

by invasive physical attacks. These attackers can sabotage the smart card by simply cut away the plastic behind the chip module until the epoxy resin becomes visible.

Security cost increase also is one of the weaknesses of smart card and swipe cards system. Easy to lose, replicated or stolen and susceptible to change will cause the company need to losing time and money for replacement new smart card and redo or manage the identification record. The security cost of fingerprint authentication is lower that smart card authentication because of the security guarantees a positive method of user identification with something that cannot be lost, replicated or stolen.

c) Vulnerability of manual password or pin number

Password mechanism is currently the most popular way to protect data, virtual access or physical access on various industries such as financial and banking, information technology, communication and manufactory. The password mechanism is base on get-and-compare concept. Information theft and unwarranted user have opportunities to access threaten the integrity of entire network if the password or pin number is exposed or know. The password-only solution is not only the weak link in the security solution for company, but expensive to administer. The simple fact is that passwords don't work very well.

This security method is no needing any expensive cost to establish, but organization may lose time and money to maintain the security and network password-administration. The reason is the password or pin number may hard to remember, easy to forget and susceptible to change. The organization administrators or help desk need to spend more than fifty percent time than others security mechanism, for example biometric technique mechanism to solve the problem that related to lost, forgotten password or pin number.

The other vulnerability of password security mechanism is password or pin number is easy to stolen and attack by unauthorized user. This problem may lead to very serious consequences, for example it can be altered or cracked by hackers running a software routine. IT security is a very important and critical issue as more and more mission-critical information resides in electronic form. From financial

records, client records, product designs, business plans, transaction records, network design and account records, access to these electronic resources may have usage or can improve value and productivity for the hacker or attacker. Because of these valuable resources the higher threat to theft and fraud is increase.

While the password and pin numbers are easily defeated using widely available hacker programs and often used in plain sight, they provide weak proof of identity. On the other hands, they are too easy to use and frequently shared to other person, the level of security password mechanism is low. Unauthorized user may use these facilities to access the many highly secure environments or system.

1.3 Objective

- Guarantees a positive method of user identification with something that cannot be lost, forgotten, misplaced, shared or stolen.
- To be able increase the efficiency of identifying and validating the correct authorized user in electronic attendance signature.
- To be able to enhance current time and attendances system and password mechanism which attendee easy to fraud as authorized user.
- To be able to protect the security, confidentiality and reduce the fraud of electronic information or access.

1.4 Scopes

The target user that proposed to use this Randomness Fingerprint Authentication with Barcode (RFA) System is system administrator, lecturer and student that have opportunities to use the attendance signature technology. This system is a standalone system which using the Microsoft Windows operating system as the most suitable platform for it. The project approach and solution on this system

focus on mortified or develop fingerprint biometrics integrated algorithm. The database security management's policy and private is not concern in this project. It also not covers up the confidentiality service of data. This project will focus on the randomly measurements fingerprint security. However, this Randomness Fingerprint Authentication with Barcode (RFA) systems have its limit and security holes that inevitable in it too. The main issues with fingerprint technology are the technology can not distinguish between the upper skin of a finger (which is almost dead material) and artificially created fake fingers.

1.5 Project Significance

Biometrics has adds a new dimension for identification and authentication of persons. Besides knowledge (e.g. passwords) and possession (e.g. smart cards), biometrics provide new means of security. Although the fingerprint authentication technology is not hundred pèrcent perfect, it still has many security features that other technologies do not provide. It is a strong alternative to passwords and, when used with them as is possible, creates the opportunity for an even stronger security choice. Since passwords do not provide the efficiency and effectiveness of security for an electronically networked society, the need exists for fingerprint authentication method that is easy to use, easy to connect to computer networks and legally accepted is necessary. By implement the fingerprint authentication to replacing passwords and PIN numbers mechanism, it makes the access procedure of corporate information more efficient and secure. It can increase the level of network security while lowering administration costs and time to solve the problem related to lost, stolen, and forgotten password or pin number.

According Robert Pethick, a product marketing manager for Lenel System International Inc. "The most secure form of access control makes access decision based on a combination of three things: something you have (in this case, a photo ID or identity card), something you know (an access pin code or password) and something you are (your unique biometric information)". The Randomness Fingerprint Authentication with Barcode (RFA) system has fulfilled the two

requirement of this concept; one is something user have and something user are. With this two-factor authentication, the Randomness Fingerprint Authentication with Barcode (RFA) system becomes more secure system available today. In addition to authentication of a user via the integrated fingerprint reader, security bar code authentication may also be providing.

But to really increase the safety of using the biometrics systems, Anil Jain- a biometrics expert at Michigan University recommence companies or organization should use multibiometric measurements -- that is, face and fingerprint, or two different fingers. Beside of the two factors that state before, the RFA system support randomness authentication algorithm which makes the system secure than other current authentication system. This measurements although not fulfill the multibiometrics concept- two different fingers but it is similar (different finger is request on each authentication process). The algorithm is set to request the form of fingerprint authentication randomly. Users are encouraged to enroll at least one fingerprint from each hand. After completing registration, these fingerprint patterns will store in database.

When user need to log in, he or she request to provide their valid barcode and fingerprint to the matching algorithm which will looks for the same patterns. The fingerprint request instruction of RFA system is dissimilar with other current authentication system; the system not only simplify request the user to swipe their thumbs but will request to scan other finger depends on the randomness algorithm such as left thumbs finger. Each time user want login to the system the fingerprint requirement will be different. This randomness algorithm of RFA system will be the most attractive and interesting features or function if compare with other authentication system.

1.6 Expected Output

This RFA system is used as a time recorder, attendance recorder, or access control system. In order to ensure the performance of a Randomness Fingerprint

Authentication with Barcode system will be robust with respect to the quality of fingerprint image, it is essential to incorporate a fingerprint enhancement algorithm in the fingerprint device. The RFA system that proposed first will verify the user identity with gather the security bar code on id cards which given to the particular person by using barcode scanner. The system will start identifies and verifies the user identity by matching with the existing authorization user database.

Users that want to access through this RFA system is encouraged to enroll security bar code on ID card and at ten fingerprints from each hand. The enroll process is only proceed by system administrator. That means user or employee can not register themselves by using the RFA system because the system is not support overt registry. The system administrator will begins the enrollment process by scanning the security bar code and swiping user's fingers to register one or more prints. The security bar code and fingerprint templates are stored in the system in such a way that they are associated with the same active user ID and access password. All of these security bar code and fingerprints template will be used to match the ID card and finger in the future. Combination of fingerprint verifying and bar code card mechanism can improves the effectively identification of the particular person.

The computer will have another integrated system with the fingerprint sensor and the randomly fingerprint placement instruction will launch. User can start scan the fingerprint image by follow the instruction. The instruction of request fingerprint will be loaded randomly and different while user login. The finger image will be verify and identify by matching it with existing fingerprint images database that store at host computer. Users will successful signature the attendance if the authentication result is positive. The positive authentication result is means the fingerprint pattern is valid and assists. If the user has not enrolled the security bar code on the ID card and fingerprint pattern, he or she is not allowing to signature the attendance. System will denial the access while the user not follows the fingerprint request instruction or shows the security bar code that not belongs to him or her.

1.7 Conclusion

The main issue that lead the development of this RFA system is the weaknesses and inefficiency of some current attendance system which can not provide the secure and confident protection, example password security mechanism. Many companies and organization worried about the authentication, privacy, and integrity of the electronic information and access.

Fingerprint is a unique feature to each individual. It stays with a person throughout his or her life. This makes the fingerprint the most reliable kind of personal identification because it cannot be forgotten, misplaced, or stolen. Fingerprint authorization is potentially the most effective and convenient method of verifying a person's identity. Therefore, the scope of this project will focus on the randomly measurements fingerprint security. By combine the security bar code authentication and randomly measurements fingerprint security, it hope that the level of security and protection of RFA system higher than current authentication system.

The objectives of this project are to enhance the security measures of the student attendance system especially using manual signature. Another objective of the project is to present the wellness of combinability of fingerprint technology with other security method such as bar code card. The fingerprint security mechanism can guarantees a positive method of user identification with something that cannot be lost, forgotten, misplaced, shared or stolen.

To be able increase the efficiency of identifying and validating the correct authorized user and able to protect the security, confidentiality and reduce the fraud of electronic information or access are another two objective that proposed in this RFA system. Finally, it is hoped that with the completion of this project, the RFA system with integrated fingerprint and barcode readers make an excellent choice for those looking to protect the information or control access to secure location.

CHAPTER II

LITERATURE REVIEW AND PROJECT METHODOLOGY

2.1 Introduction

The detail description of literature review and project methodology will be show in this chapter. Literature review means searching, collecting, analyzing, studying and write conclusion from all debates and issues raised in relevant body of literature. In Randomness Fingerprint Authentication with Barcode (RFA) system, the literature review will focuses on the research of various theory and basic network knowledge that related with fingerprint authentication mechanism and barcode authentication mechanism which is the main feature of system. Through the literature review, chance to investigate and explore areas that reader may not know about before and read around. Reader can get the summarize view which is derived from the study and analysis on the current issues revolving the topic of the project and also the comments and opinion of the author.

The project methodology is an important part that needs to involve in each project. The function of project methodology is to collect, analyses, and distribute responsibility and estimate outcomes. The project management methodology may be more elaborate in complex projects to assist in each of the project management tasks. In small projects, the implemented project management methodology may be considerably simpler. Prototyping model have selected as the project management methodology of Randomness Fingerprint Authentication with Barcode (RFA)