2009 Second International Conference on Computer and Electrical Engineering

Fingerprint Biometrics Authentication on Smart Card

Yuhanim Hani Binti Yahaya
Computer Science Department,
Faculty Of Science and Defence Technology,
National Defence University of Malaysia,
Kem Sungai Besi, 57000
Kuala Lumpur. Malaysia
yuhanim@upnm.edu.my

Mohd Rizal Bin Mohd Isa
Computer Science Department,
Faculty Of Science and Defence Technology,
National Defence University of Malaysia,
Kem Sungai Besi, 57000
Kuala Lumpur. Malaysia
rizal@upnm.edu.my

Mohammad Indera Bin Aziz
Computer Science Department,
Faculty Of Science and Defence Technology,
National Defence University of Malaysia,
Kem Sungai Besi, 57000
Kuala Lumpur. Malaysia
inderaziz@yahoo.com

***Abstract.* Fingerprint matching for user authentication is becoming widely used in many applications. Smart cards are also being used heavily in identification applications. It is now required to combine both technologies so fingerprints can be matched on the smart card. This paper presents combination on two security components which are the fingerprint recognition and smart card. The smart card plays a data storage for storing the cardholder's fingerprint data. The card holder is required to scan his/her fingerprint on a sensor. The scanned fingerprint image is then sent to the card for matching. This research proposes a framework for user identification and authentication using fingerprints and smart cards.**

Keywords: Fingerprint, smart card, card holder, sensor

I. INTRODUCTION

As our life is getting more computerized, security systems are getting more important. The rapid progress in biometrics and smart card technology makes information more susceptible to abuse. Due to the growing importance technology and the necessity of the protection and access restriction, reliable personal identification and authentication is necessary.

Authentication is the process of verifying that the digital identities of people or user are authentic. There three ways to authenticate the identity of a user [1]:

- A user presents something they know, such as password or PIN. This approach is known as *knowledge factors.*
- A user presents something they posses such as card or key. This is known as *possession factors*.
- A user presents a personal physical attribute such as fingerprint or even DNA systems (biometrics). This is known as *being factors*.

Each of these factors has some limitations when used alone. In knowledge factors, user's password is short and easy which makes them easy to guess. Cards can be difficult to manage and can easily be stolen or lost. Biometrics is prone to false rejection of person's physical attribute, even though it is right. Therefore, to achieve a strong identification and authentication process, it is recommended to combine two or more of these factors. In this paper, we propose framework for user identification and authentication using fingerprints and smart cards. The proposed framework will be implemented for entrance system in Military Police Training Centre.

This paper is organized as follows: the next section briefly introduces the concept of smart card technology. Next we describe the technology of fingerprint biometrics. Lastly before conclusion, we proposed the framework for user identification and authentication using fingerprint biometric and smart card.

II. SMART CARD TECHNOLOGY

Smart card has gone several development phases during the years. Today it is a credit-card-sized card equipped with microprocessor and memory. It is a portable and an intelligent device capable of manipulating and storing data.

It is inserted into a reader as part of the authentication process. They often contain a digital certificate and they are usually presented in a combination with a knowledge factor such as password or a personal identification number (PIN).

In biometric process, there are three types of smart card based on their typical technical features and type of authentication they support. The three types of smart card are [2]:

- Template-on-card (TOC)
- Match-on-card (MOC)
- System-on-card (SOC)

In TOC, original identifying biometric template is stored on a smart card. Data acquisition, feature extraction and matching are done on the reader side. During the authentication process, the reading device requests the

978-0-7695-3925-6/09 $26.00 © 2009 IEEE
DOI 10.1109/ICCEE.2009.155

IEEE computer society

identifying template from the smart card and matches it on the reader side with newly scanned template.

In MOC, original template is stored on a smart card. During the authentication process, data acquisition and feature extraction are done at the reader side and the matching is done inside the smart card. The final matching result is computed inside the smart card itself.

In SOC version, smart card incorporates original template, the entire biometric sensor, processor and algorithm. All authentication procedures are done inside the smart card itself.

Adding individuals' unique characteristics into smart card chip, smart card becomes more secure medium, suitable for use in a wide range of applications that support biometric methods of identification [3]. There are numerous ID systems implemented worldwide based on biometric smart card and biometric technology. For example: US Department of Defense Common Access Card, Malaysia's national ID multipurpose card, UK's Asylum Seekers Card – contain photo for visual recognition and fingerprint template stored on smartcard chip for biometric identification [3].

III. FINGERPRINT BIOMETRICS

Biometric authentication uses data taken from measurements of a person’s body, such as fingerprints, faces, irises, retinal patterns, palm prints, voice prints, hand-written signatures and so on, to identify individuals by means of image processing [4]. Such data is unique to the individual and remains throughout one’s life. It is important to have reliable personal identification due to growing importance of information technology. Of all the biometric techniques being used today, fingerprint-based identification is the oldest method, which has been successfully used in numerous applications [4]. Everyone is known to possess a unique fingerprint and it does not change throughout his lifetime and so the fingerprint matching is considered one of the most reliable techniques of people identification.

A fingerprint is formed from an impression of the pattern of ridges on a finger. A ridge is defined as a single curved segment, and a valley is the region between two adjacent ridges. There are two types of fingerprint representations: local and global. Local representations predominantly based on ridge endings or bifurcations (collectively known as minutiae, see figure 1) are the most common. This is due to the following reasons:

- Minutiae capture much of the individual information
- Minutiae-based representations are storage efficient
- Minutiae detection is relatively robust to various sources of fingerprint degradation.

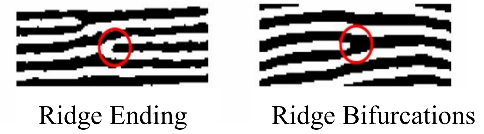

Figure 1. The ridge ending and ridge bifurcations.

There are three main methods to capture fingerprint images, which are optical, applicative and thermo conductive [5]. The optical method is implemented with a small camera and light source to capture an image of a fingerprint. The capacitive method makes full use of the human body’s natural electrical charge to measure the differences in capacitance value between ridges and valley in a fingerprint and certain algorithms are used to construct an image from the capacitance values. The last method, which is the thermo conductive method, is done by measuring the human tissue’s then a conductivity characteristic difference between the ridges and valleys of a fingerprint. In other words, the ridges and valleys conduct heat at different rates and these minute differences can be registered. This research will use the capacitive method provided by AET63 USB Biotrustkey.

IV. PROPOSED AUTHENTICATION AND IDENTIFICATION FRAMEWORK

Fingerprint is chosen as it is more mature in terms of the algorithm availability while other biometrics such as face recognition may not be well suited to an ordinary smart card processor. Fingerprint identification is suitable as a method to authenticate users to use a smart card [6]. This can elaborate by using two factors [6]: space complexity and time complexity. A common available smart card has approximately 8K to 16K of non-volatile memory. The current state-of-art fingerprint technology [7] shows that the minimum size of a fingerprint template adequate for comparison can be as small as several hundreds of bytes. So space complexity is not a major problem as the smart card can store the entire fingerprint template. For time complexity, it refers to whether the in-card processor is capable to accomplish the entire fingerprint matching calculation in real time [6].

Figure 2 shows our proposed authentication and identification framework. The fingerprint sensor is used to capture fingerprints. The fingerprint is processed by comparing the captured image and the present image provided by the user. Before comparing process can occur, the images need to be reduced to their key features called minutiae points. The fingerprint template having the minutiae information is transferred smart card through the smart card reader. The authentication algorithm for this framework involves:

- Minutiae extraction extracts features of the fingerprint image called minutiae. Minutiae generally refer to the ridge ends and branches that constitute a fingerprint pattern.

- Minutiae matching conducted on the smart card compares the minutiae in the master fingerprint template saved in the smart card and those scanned fingerprint (live scanned). If the fingerprint matches then a user will be recognized as the valid cardholder.

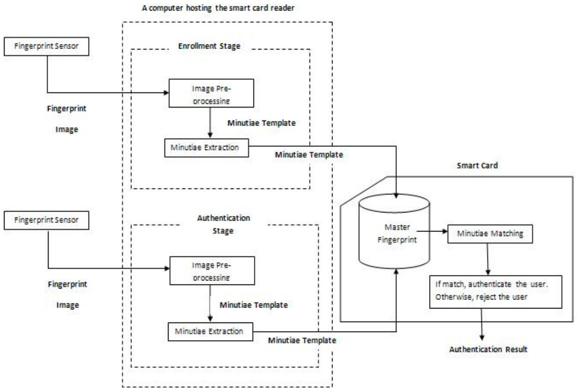

Figure 2. Proposed Authentication and Identification Framework

The following are the general steps in this fingerprint matching technique:

- Image Pre-Processing

  This refers to the refinement of the original fingerprint image against image distortion produced from the fingerprint scanner.

- Minutiae Extraction

  This refers to the fingerprint feature extraction. The following algorithm based on the techniques from several research papers [7], [8], [9] will be used for future work.

- Minutiae Matching

  When we get the user fingerprint image from the sensor, we can then use the image processing techniques before turning the image into a skeleton image. Based on the points in the template file, we compare the input image minutiae points.

V. CONCLUSION

Biometric identification are becoming widely accepted and are slowly replacing traditional identification the methods of which identification using password is still most widely spread. The aim of this research is to point out the basic characteristics and possibilities of combining smart card and fingerprint biometrics in authentication and identification processes. This research has proposed a framework for authentication and identification using these two technologies. As a challenge for future research work, we will develop the fingerprint matching algorithm and evaluate the accuracy of the matching algorithm.

REFERENCES

[1] Smart Cards and Biometrics: Your Key to PKI, http://www.linuxjournal.com/article/3013.

[2] An Introduction to Biometric Match-On-Card, http://www.itsc.org.sg

[3] Hi-Tech Security Solutions: The Industry Journal for Security & Business Professional, http://www.securitysa.com

[4] Jain A.K. et al.: BIOMETRICS: Personal Identification in Networked Society, Kluwer Academic Publishers.(1999)

[5] Jain, A.K., et al.: Matching and Classification: A Case Study in Fingerprint Domain. Proceeding of Indian National Science Academy (INSA-A). vol.67, no.2, pp.67-85. (2001)

[6] Moon, Y.S. et al.: A Secure Card System with Biometrics Capability. Proceeding of IEEE Canadian Conference on Electrical and Engineering, May 9-12, Alberta, Canada. 261-266. (1999)

[7] Maio, D., Maltoni, D.:Direct Gray-Scale Minutiae Detection in Fingerprints. IEEE Transactions on Pattern Analysis Machine Intelligence, vol. 19, no. 1, pp.25-29.(1997)

[8] Maio, D., et al.: An Efficient Approach to On-Line Fingerprint Verification. Proceeding VIII Int. Symp. On Artificial Intelligence, Mexico, October.(1995)

[9] Bergengruen,O.: Matching Minutiae of Fingerprint Images, pp.5-7.(1994)