Thesis for the Degree of Master of Engineering

Design and Implementation of Fingerprint Authentication System based on Fuzzy Vault Biometric Cryptosystems

by

Annisa Istiqomah Arrahmah

Department of Information Systems
(Interdisciplinary Program)

The Graduate School

Pukyong National University

February 2017

Design and Implementation of Fingerprint Authentication System based on Fuzzy Vault Biometric Cryptosystems

(퍼지볼트 생체암호에 기반한 지문 인증 시스템의 설계 및 구현)

Advisor: Prof. Kyung-Hyune Rhee

by

Annisa Istiqomah Arrahmah

A thesis submitted in partial fulfillment of the requirements for the degree of

Master of Engineering

in the Department of Information Systems (Interdisciplinary Program),
The Graduate School,
Pukyong National University

February 2017

Design and Implementation of Fingerprint Authentication System based on Fuzzy Vault Biometric Cryptosystems

A dissertation

by

Annisa Istiqomah Arrahmah

Approved by:

(Chairman) *Man Gon Park*

(Member) *Carmadi Machbub*

(Member) *Kyung-Hyune Rhee*

February 24, 2017

Contents

List of Figures

List of Tables

List of Abbreviation

Abbreviation	Name	First usage in page
FIDO	Fast Identity Online	5
ID	Identification	5
BCs	Biometric Cryptosystems	6
CRC	Cyclic Redundant Check	10
FAR	False Acceptance Rate	12
FRR	False Rejection Rate	12
FN	False Negative	12
FP	False Positive	12
GF	Galois Field	25
GAR	Genuine Acceptance Rate	15
UI	User Interface	15
IDE	Integrated Development Environment	19

퍼지볼트 생체암호에 기반한 지문 인증 시스템의 설계 및 구현

안니사 이스티꺼마 아라마

부경대학교 정보시스템학과 (협동과정)

요 약

스마트폰의 사용은 현재 국제적인 트랜드로 자리잡았다. 최근 생체 센서가 부착된 모바일 관련 기술의 발전은 인증 방법의 고도화로 이어지고 있다. 생체 센서의 기술 발전은 기기의 잠금을 해제하는 것만이 아니라 금융 애플리케이션이나 모바일 결제와 같은 중요한 시스템에서 생체 신원으로서 활용되고 있다.

본 논문에서는 안전한 생체 인증 시스템을 제안한다. 사용자의 지문은 생체 정보로서 사용되고 지문으로부터 추출한 지문의 특징은 능선 흐름과 지역 픽셀 분석에 사용된다. 추출한 특징은 암호키와 함께 스마트폰의 데이터베이스에 저장된다. 생체 암호 시스템은 암호키와 생체 정보를 결합하는데 사용된다. 생체 암호 시스템은 퍼지볼트 시스템을 기반으로 한다. 퍼지볼트시스템은 수정된 비임의 채프 지점 생성기와 검증기로, 에러 확인에 대한 새로운 접근 방식으로 사용된다. 이 기법은 기존에 존재하는 퍼지볼트기법에 대해 알려진 부대 공격, 즉, 전수조사 공격, 통계적인 공격과 혼합 대체 공격에 대해 강인하다. 제안한 시스템은 신뢰할 수 있고 효과적인 모바일 애플리케이션으로 개발 및 구현 될 것이다.

키워드: 모바일 애플리케이션, 생체 인증, 생체 암호 시스템, 퍼지볼트, 지문 인식

Chapter 1.
Introduction

1.1 Purpose and Structure of the Thesis

In this thesis, a secure biometric authentication is developed and implemented. This system uses biometric cryptosystem based on fuzzy vault non-random chaff point generator scheme. The main concern of biometric authentication system is to secure biometric templates of the user. In this study, we only consider how to secure the fingerprint information that is used for crucial systems such as financial application or mobile payment system based on user accounts such as PayPal or Google Payment. This system also fast and convenient because it only uses one fingerprint information of the user.

Similarly, with the research to be conducted, it can conclude that this thesis has a focus and objective to develop a reliable, secure and fast mobile payment authentication system that comprises the following aspects such as:

(a). Design product is built to make a secure fingerprint authentication system.

(b). Provide a high privacy of the user biometric information using biometric cryptosystem method.

(c). Provide an easy user interface for enrollment and authentication.

(d). Provide a fast and accurate fingerprint enrollment and authentication process.

Not only contain with focus and objective, there are also several scopes to make the problem is not too extensive, thus some limitations problem to be solved by the application include:

(a). The cryptographic key generation and key distribution are not discussed and implemented in this system. We presume that the key is already given using the common procedure.

(b). Because of the hardware constraint, the input is a fingerprint binary image as a prototype of the fingerprint information of the user.

(c). The input is only one fingerprint image for one person with maximum size 512x512 pixels.

(d). We only make the mobile application for Android and Windows mobile.

The structure of this thesis is divided into six chapters as follows:

(a). ***Chapter 1*** introducing the discussion of the global picture on the background including purpose and structure of the thesis which concluded the thesis objective, scope, and thesis outlines.

(b). ***Chapter 2*** introduces a basic concept of the method and algorithm used with theoretical outlines that support this thesis topic discussion.

(c). ***Chapter 3*** discusses the system requirements and design to discover the analysis of the need to establish a biometric authentication system, system design, system specification, functional requirements and actors involved in the system.

(d). ***Chapter 4*** introduces a system implementation for the application development using MATLAB and C# programming language.

(e). Finally, ***Chapter 5*** concludes this study as the purpose of this thesis including an additional feature that might be required but not yet implement and developed in the thesis.

1.2 Background

Since mobile devices are no longer only used for simple voice or short message communication but are developed with more powerful capacity, memory, and performance, nowadays, most of the people in the world, from teenagers to elders, equip themselves minimal with one mobile device. In 2015, smartphone ownership rates in emerging and developing nations were rising at an extraordinary rate, climbing from a median of 21% in 2013 to 37% in 2015 [1]. Based on the global forecast in Figure 1 (Source: HIS Inc.), an increasing number of smartphones are adopting fingerprint verification as a method to authenticate their users.

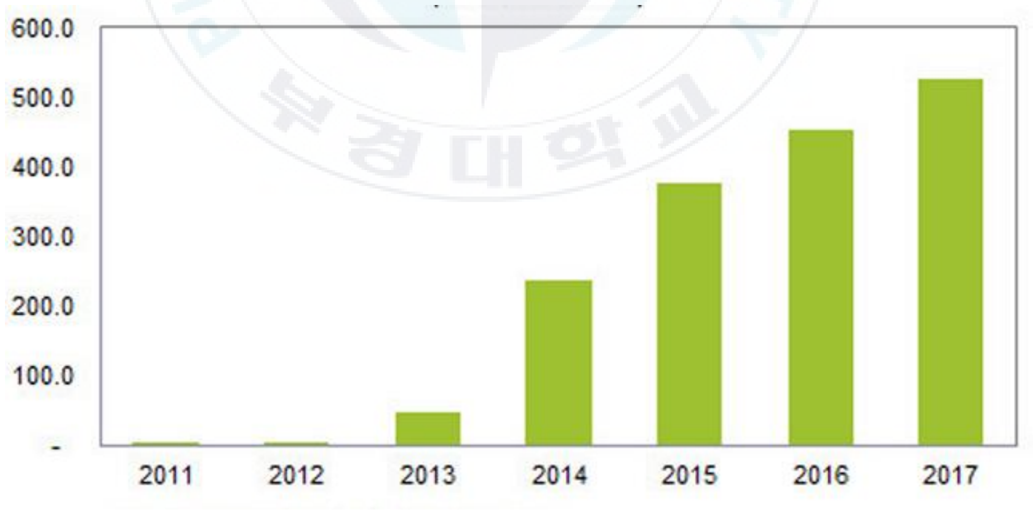


Figure 1. Global Forecast of Cellphones Shipments with Integrated Fingerprint Scanners (Millions of Units), Source: HIS Inc.

Based on a survey by PayPal [2], 53% of smartphones owners would use fingerprints instead of passwords and 46% would be comfortable with retina scans. The biometric authentication is not only used to unlock these smartphones but also used in financial applications such as online payment or mobile payment based on user account. In 2016, FIDO [3] and Google [4] already integrate the fingerprint authentication on their mobile payment system. Both of them have similar mobile payment scenario illustrated in Figure 1. In this scenario, the biometric authentication is made between online payment provider and client's mobile phone. The application uses user ID and user's fingerprint for authentication to the specific account maintained by the Online Payment Provider [5]. If the authentication process is successful, then the next step can be done. There is a countermeasure in the new integration of biometric authentication in the crucial system such as mobile payment system.

Most of the concern in the biometric authentication system is how to secure biometric template of the user. In early 2016, Jo [6] proved that biometric authentication in mobile phones can be compromised. The authors breached the VEGA Secret Note that uses fingerprint for biometric authentication. The authors showed that fingerprint templates of the user can be accessed from the mobile phone system. Because the biometric features are limited, when it is compromised, then the user will not have any substitute for it. To prevent that, a robust security scheme is needed to protect the biometric template in client-server system environments such as financial application and account-based mobile payment application.

For a client-server system that uses biometric authentication, if the matching process only uses the biometric templates itself, then it is better to store the biometric data in the server side since attacking the server is more difficult than attacking the client (i.e. mobile phone). However, there are some disadvantages if the biometric templates are stored in the server side. First, if an attack occurs, then the possibility of data loss is high. Second, there is no privacy about client's biometric data in the server side. To protect the user’s privacy, it is more convenient to store the biometric data in the client’s mobile phone. To prevent data leakage, the biometric templates must be stored in a secure manner. There are several methods for securing biometric templates [7], one of them is biometric cryptosystems (BCs). BCs require a storage of biometric information to retrieve or generate cryptographic keys, referred as helper data. These helper data are stored as an encrypted form and do not reveal significant information about the biometric templates and the cryptographic keys.

Chapter 2.
Literature Review

2.1 Biometric Authentication

There are three types of authentication method: knowledge-based authentication, possession based authentication and bio-based authentication [8]. The knowledge based and possession based is a traditional authentication method. In knowledge-based, the authenticator relies on their memory such as a password. This type of authentication has weaknesses. It is hard to be managed, especially if we want a strong level security, we have to make a long password. As a result, it is hard to recall. Another problem if we have more than one accounts, we have to remember more than one password for a strong level of security. In possession based, there are cryptographic things such as a token that are owned by the authenticator. This type of authentication also has weaknesses: the token can be lost or stolen. Another authentication method is using biometric information of the authenticator. This kind of authentication uses unique biometrical as physiological or behavioral characteristics for automatic identification in a more trustworthy manner such as fingerprints, retina, iris, palm, keystroke, finger vein, voice, face, ear shape, handwriting, head resonance, etc. Because biometric authentication uses a broad range of characteristics, the requirement for imaging technology in each biometric differ widely. There are five requirements that must be fulfilled for ideal biometric [9]:

(a). Robustness: the individual information remains unchanged over time.

(b). Distinctiveness: the biometric information varies greatly for each individual.

(c). Availability: the biometric information ideally can be measured in multiples for the entire population

(d). Accessibility: the biometric information is easy to collect using electronic sensors.

(e). Acceptability: the measurement process to get the biometric information is accepted widely.

Biometric authentication requires two stage: enrollment stage and authentication stage. In the enrollment stage, the feature data with high quality is extracted and stored in the database as reference data. In the authentication stage, another feature data is extracted as a query data and compared it with the reference data. If the reference data and query data is overlaps one to another, the authentication process is successful.

The personal privacy of the user is another issue in biometric authentication. In general, biometric system, biometric information can be accessed by the government or the authorized group. The main problem in the biometric system is the linkage between a person and their personal data that allow movement tracking. Database of biometric information (i.e. biometric image) is often encrypted to hamper the process of bulk compromise [9].

2.2 Biometric Cryptosystems

Biometric cryptosystem (BCS) are designed to securely bind a digital key to a biometric or generate a digital key from a biometric [10]. This method tries to integrate biometrics with cryptography to protect both the biometric template and cryptographic key stored in the system. This is the solution for biometric dependent key release. Biometric Cryptosystem requires the storage of biometric information, applied to retrieve or generate keys, referred as helper data. This helper data stored as encrypted data and not reveal significant information about the cryptographic key and biometric template. The biometric comparison is performed indirectly by verifying key validities, and the output of the authentication is key release or failure message. Based on how to derive the helper data, Biometric Cryptosystem classified into two types. If the helper data obtained by binding the chosen key with the biometric template, then it called key binding schemes. If the helper data obtained only from the biometric template, then it called key generation schemes. In key binding schemes the cryptographic keys are independent with the biometric template, while in the key generation schemes, the key is dependent from the biometric template because it directly generated from the biometric sample.

2.3 Fuzzy Vault

Fuzzy vault is one of the biometric cryptosystems based on key binding schemes that is introduced by Juels and Sudan in 2002 [11]. Since then, various developments of fuzzy vault have been proposed. The original scheme uses Reed-Solomon code for error-correcting code that can handle noisy data and is designed for an unordered set of data. In recent years, the implementation of Cyclic Redundant Check (CRC) and Lagrange interpolation are introduced to replace Reed-Solomon code. However, CRC-based fuzzy vault scheme still needs some improvements. Recent researches on CRC-based fuzzy vault method focus on preventing attacks such as brute force attack, statistical analysis attack, collusion attack, and blend substitution attack [12].

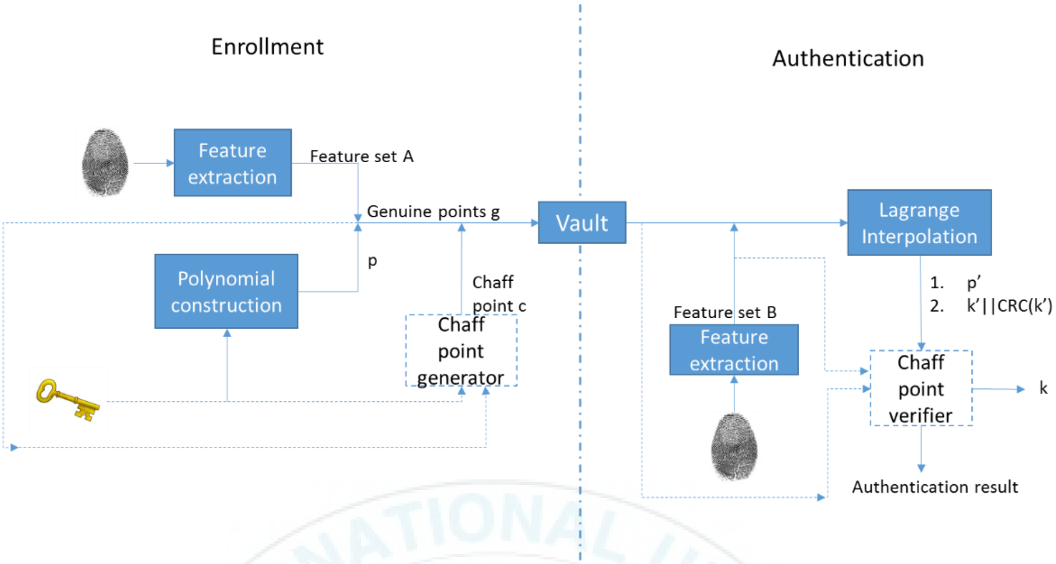


Figure 2. CRC-Based Fuzzy Vault Using Non-Random Chaff Point Generator

Benhammadi [13] proposed a new method using password hardened fuzzy vault based on an improvement of fingerprint feature representation. Khalil-Hani [14] changes the whole scheme by considering non-random chaff point generator which is computationally fast. These two methods only prevent statistical analysis attack. Nguyen [15] proposed a new fuzzy vault method using ridge features. This method resists against advanced brute force attack. Dang [16] proposed a cancellable fuzzy vault. The proposed method performs a periodic transformation on the biometric template. This method is robust against brute force attack. However, this method is possible to be cracked by statistical analysis attack.

Another scheme was proposed by Nguyen [17] in early 2016. This method focuses on preventing the aforementioned attacks, especially blend substitution attack. This scheme introduces a modified chaff point generator and verifier. This non-random chaff point generator and verifier substitute CRC algorithm for error correcting check. The schematic of this method can be seen in Figure 2. Continuous hashing and linear projection are used to generate chaff from the cryptographic key and biometric template in enrollment phase. As a consequence, the same chaff point will be regenerated as a verifier in the authentication phase. In this scheme, chaff point is not a random point but a point that is treated as the signature for the combination of biometric template and a cryptographic key. If there are any modifications in the vault, then this system can detect the modification and the authentication will lead to failure result.

2.4 Fingerprint

Minutiae extraction is one of the feature extraction methods for the fingerprints extraction. Minutiae extraction is widely used and is also one of the old methods in feature extraction field. In the fuzzy vault, feature extraction is a preprocessing step for getting genuine points from the biometric sample. The input for this step is a biometric image from the sensor, and the output is a set of genuine points as the unique identity of the biometric sample. To get a high performance of fuzzy vault system, we have to select an accurate feature extraction. Accurate feature extraction will help in decreasing False Acceptance Rate (FAR) and False Rejection Rate (FRR). An accurate extracting method must have the capability of extracting salient features from the fingerprint in a robust way. The False Negative (FN) rate and False Positive (FP) rate of the extracted genuine points should be the smallest one.

There are many minutiae extraction methods that are introduced by the researchers to get a high-performance fingerprint feature extraction [18]. Distortion issue is a major concern in developing feature extraction method. Distortion in fingerprint comes from variations in skin and impression condition when the user inserts their fingerprint from the sensor.

Minutiae extraction can be done in binarized fingerprint image or grayscale fingerprint image. Binarized fingerprint image can be divided into two types, unthinned binarized images, and thinned binarized images. One of the example methods that uses unthinned binarized images is ridge flow and local pixel analysis. In [19] a method based on ridge flow was used. This proposed method methodically scans the binary images of a fingerprint, identifying localized pixel patterns that indicate the ending or splitting of a ridge. There is pixel pattern as reference. The pattern may represent the end of a black ridge protruding into the pattern. Another example method that uses thinned binarized images is based on Crossing Number. In [20] Wu Zhili uses modified crossing number method to extract minutia point from the fingerprint.

2.5 Circle Packing Algorithm

The Euclidian distance calculation is a common way to calculate a distance between two points. The common calculation is shown in expression 1.

$$\sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2} > \delta \qquad (1)$$

There is another method that has a similar purpose, that is circles packing, proposed in [21], a geometrical mathematic to calculate the distance between points. The main idea of this circle packing algorithm is making some circle pack in a defined surface based on a specific condition. Circle with identical radius, non-imbrication circles, square or triangle area as a circle pack, and density pack are the example of a possible condition in circle packing algorithm. The Khalil-Hani algorithm [14] is based on the circle packing solution. The circle problem that is used in Khalil-Hani algorithm is finding the optimal dense packing of the similar square pack which should not overlap with each other in a square surface. This method uses a square boundary surrounded each point in the vault to ensure that the distance between these points is not too close. The boundary that is created by using the method is illustrated in Figure 3. The square boundary is chosen by defining left, right, upper and lower line around each point. The distance between the point and each of these lines is δ.

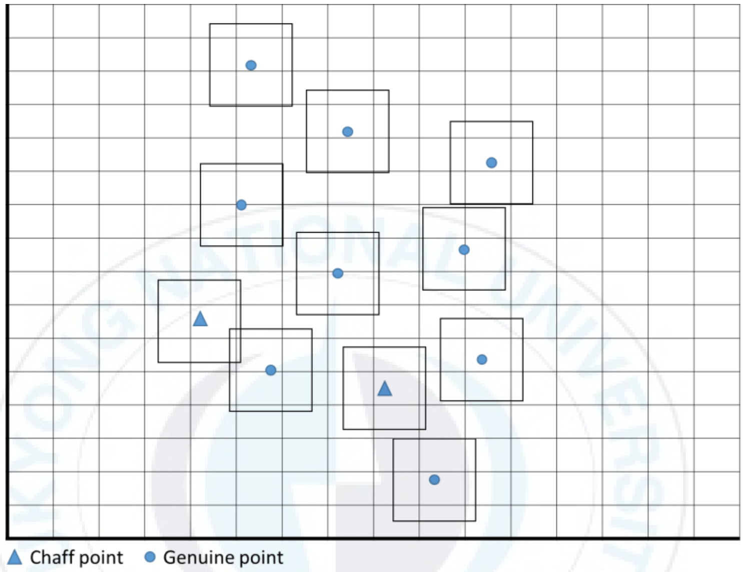


Figure 3. Illustration of Circle Packing Algorithm

Chapter 3.
System Requirements and Design

3.1 Overview of the Application Design System

The design of the system application is intended to identify the problems that will appear later on related aspects such as the availability of reliable and accuracy of performance of applications and data estimates generated within the system. The analysis will be conducted on the topic of discussion as in some of the features such as the Genuine Acceptance Rate (GAR) for the whole system. Time execution also become the measurement metrics, user interface (UI) design is not the subject that included in any analysis features, but it can be seen that the design has been designed properly and adjusted to the features that are built. It is a kind of breakthrough in the field of fingerprint authentication technology that prepared to introduce the system with its both simplicity and security and being a pilot project which was initiated as a solution in the middle of the security problem in the client-server authentication system such as mobile payment.

3.1.1Analysis of User Needs

Overall, the design and implementation of the application are intended to make a secure authentication mechanism for account based mobile payment system using user’s fingerprint information. Also, the privacy of the user’s biometric information must be retained.

3.1.2Analysis System Requirements

The system design must be able to answer the needs of the user. The following are the list of the system requirements that is designed and constructed:

(a). Authenticity: The system can read the fingerprint as the representative of the biometric information of the user. The system must be able to distinguish fingerprint input from the different user. The system also must be able to authenticate different fingerprint input from the same user.

(b). Privacy: The system must not provide any information of the user's biometric information. Any information related to user's fingerprint must be stored as encrypted data.

(c). Non-repudiation: the system should have a mechanism to prove that the authentication request is sent by the corresponding sender.

(d). Ease of use: The user interface for enrollment and authentication process is easy to use, and these process must be fast enough for the user convenience.

3.2 System Architecture

The system contains two main parts. First, the enrollment process for user's fingerprint registration and correlate it with the generated cryptographic key. Second, the authentication process after the registration process is conducted. These authentication and enrollment process uses fuzzy vault biometric cryptosystems [11]. The flow diagram in Figure 4 represents the overall system for the enrollment process. Figure 5 represent the overall system for the authentication process.

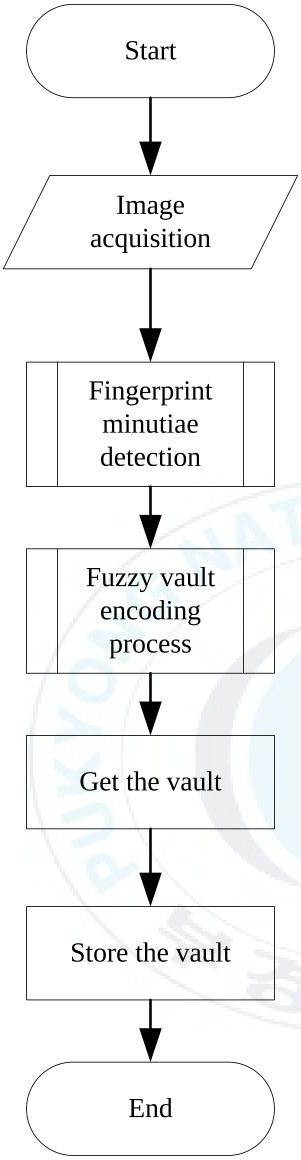


Figure 4. Enrollment Flowchart

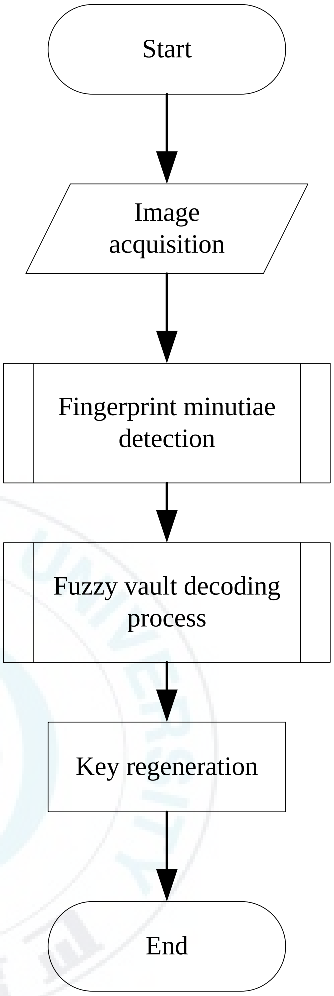


Figure 5. Authentication Flowchart

3.3 System Specification

We use some software for the system development. Some of these are defined in Table 1.

Table 1. Analysis of Software Requirements

No.	Requirements	Specification
1	Operating System	Windows 10 Professional 64-bit
2	Visual Studio IDE	Visual Studio 2015
3	Xamarin: Mobile Application Development	Android and Windows
4	MATLAB	R2016b

3.4 System Design

To implement the enrollment and authentication for the mobile payment system, there are parameters and several key steps that must be done as below.

3.4.1 Fingerprint Minutiae Detection System

Fingerprint minutiae detection system is an important process for both enrollment (encoding) and authentication (decoding). The block diagram of this system can be seen in Figure 6, and the specification can be seen in Table 2. This process produces minutiae points as a feature set. This feature set becomes an input for encoding and decoding process. The input is a grayscale fingerprint image. The example of fingerprint image input is shown in Figure 7. The process includes pre-processing step and feature extraction step as follows and illustrated in Figure 8.

(a). The input image is sent to the pre-alignment module to align the fingerprint image so that the matching process in the authentication process can produce a low false rejection rate. In fingerprint authentication, the query fingerprint image sometimes is a translation, rotation, nonlinear distortion, and noise version of the reference fingerprint. These problems make a large interclass variation in the input. Alignment usually uses the original information of the minutiae template from reference fingerprint and query fingerprint. Because the matching process in the fuzzy vault uses transformed version of minutiae template, it can use another data information extracted from the fingerprint image. This helper data for the pre-alignment process should not give a significant information about the biometric itself. Another alignment method can be used by aligning the feature extraction based on reference points both in reference and query fingerprints.

(b). Feature extraction is a preprocessing step for getting minutiae points from the fingerprint sample. The input for this step is a fingerprint image, and the output is a set of minutiae points as the unique identity of the biometric sample. Minutiae extraction is done by using ridge flow and local pixel analysis with unthinned binarized image [19]. This method methodically scans the binary images of a fingerprint, identifying localized pixel patterns that indicate the ending or splitting of a ridge. There are pixel patterns as a reference, the pattern may represent the end of a black ridge protruding into the pattern. The minutiae points are detected as an x and y coordinate points. The output of this module is illustrated in Figure 9. The blue pattern indicates the minutiae points. The output data of this module is illustrated in Figure 10. The data contain all the decent detected minutiae points.

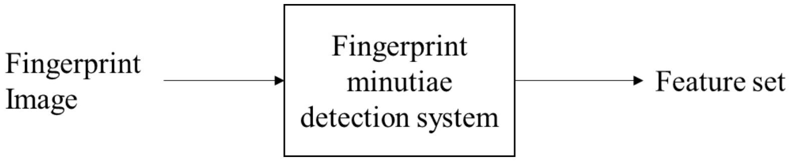
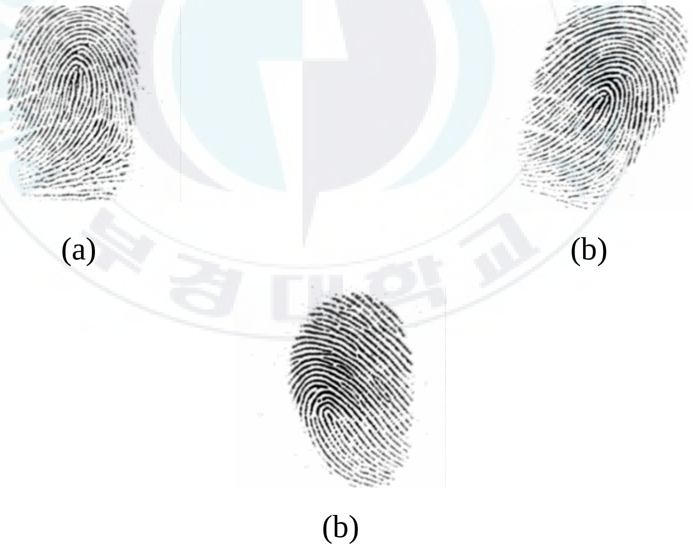


Figure 6. Block Diagram of Fingerprint Minutiae Detection System

Table 2. Specification of Fingerprint Minutiae Detection System

Module	Fingerprint minutiae detection system
Input	Fingerprint image
Output	Feature set
Functionality	Extract minutiae points information from fingerprint image.


(a)

(b)

(b)

Figure 7. Examples: (a) Fingerprint Image of the User; (b) Translation Fingerprint Image of the Same User; (c) Fingerprint Image from Different User

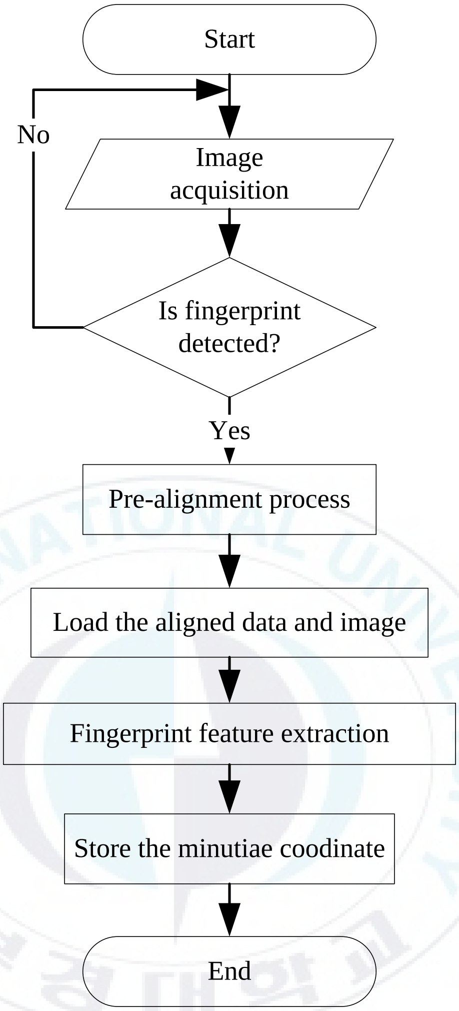

Start
No
Image acquisition
Is fingerprint detected?
Yes
Pre-alignment process
Load the aligned data and image
Fingerprint feature extraction
Store the minutiae coodinate
End

Figure 8. Flow Diagram of Fingerprint Minutiae Detection System

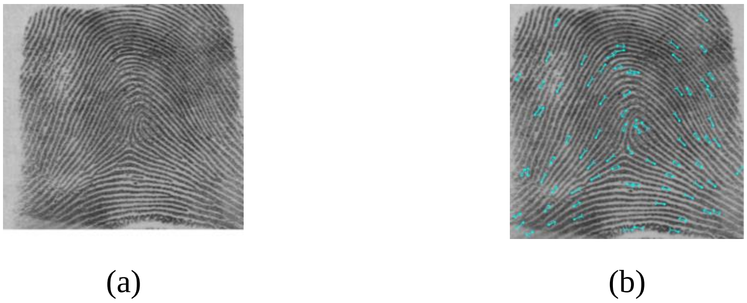
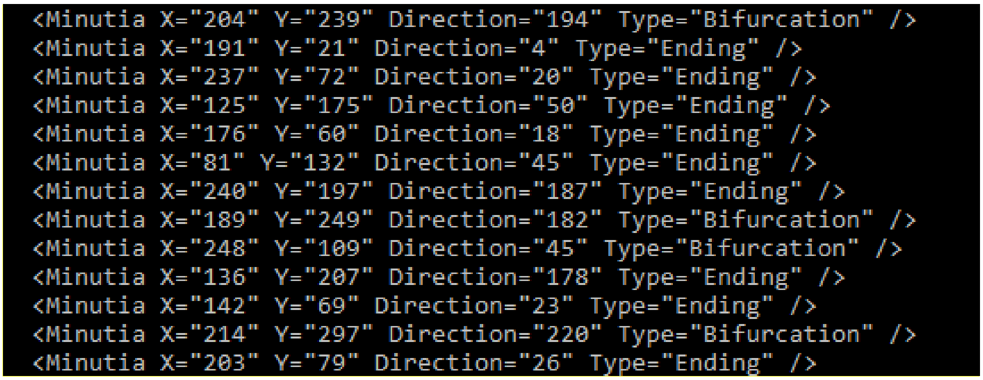


Figure 9. (a) Input Fingerprint Image; (b) Output Fingerprint Image with Minutiae Points Information



```
<Minutia X="204" Y="239" Direction="194" Type="Bifurcation" />
<Minutia X="191" Y="21" Direction="4" Type="Ending" />
<Minutia X="237" Y="72" Direction="20" Type="Ending" />
<Minutia X="125" Y="175" Direction="50" Type="Ending" />
<Minutia X="176" Y="60" Direction="18" Type="Ending" />
<Minutia X="81" Y="132" Direction="45" Type="Ending" />
<Minutia X="240" Y="197" Direction="187" Type="Ending" />
<Minutia X="189" Y="249" Direction="182" Type="Bifurcation" />
<Minutia X="248" Y="109" Direction="45" Type="Bifurcation" />
<Minutia X="136" Y="207" Direction="178" Type="Ending" />
<Minutia X="142" Y="69" Direction="23" Type="Ending" />
<Minutia X="214" Y="297" Direction="220" Type="Bifurcation" />
<Minutia X="203" Y="79" Direction="26" Type="Ending" />
```

Figure 10. Minutiae Point Partial Data for Figure 8(a)

3.4.2 Fuzzy Vault Enrollment (Encoding) System

Enrollment is an important step that must be done before authentication process. The block diagram of this system can be shown in Figure 11, and the specification can be seen in Table 3. This process includes several procedures for the user and main enrollment process that produces vault as encrypted data. This process is illustrated in Figure 12. We divide into several processes as follows.

(a). A random pair of the cryptographic key is selected by the system.

(b). The next step is the main enrollment process. The input is aligned minutiae points as feature set $M = [m_0 \quad m_1 \ \dots \ \mathrm{m}_{\mathrm{n}-1}]^{t}$ as $m_j = [x_{mj} \quad y_{mj}]$, n is the maximum detected minutiae points and private key as secret cryptographic key $S' = [s_{f-1} \quad s_{(f-2)} \cdots \ \mathrm{s}_0]$.

(c). Axis(x-coordinate) of genuine points is obtained by bitwise concatenation for each minutia coordinate. Ordinate(y-coordinate) of genuine points is obtained by plotting the x-coordinate to the polynomial $p(x) = s_{f-1}x^{f-1} + s_{f-2}x^{f-2} + \cdots + s_0$. This process is called polynomial reconstruction and done in Galois field ($GF = 2^{16}$). The output is $V = [v_0 \quad v_1 \ \dots \ \mathrm{v}_{|\mathrm{v}|-1}]^{t}$ with v_j is a tuple of $[x_{vj} \ y_{vj}]$

(d). Chaff points $N = [n_0 \quad n_1 \ \dots \ \mathrm{n}_{\lambda \mathrm{f}-1}]^{t}$ are generated using Chaff Points Generator in [17] illustrated in Figure 13. It uses non-random chaff point generator with feature set and cryptographic key as input. Continuous hashing and linear projection are used to generate chaff points. We modified the Euclidian distance calculation with circle packing algorithm.

(e). Genuine points and chaff points are combined and becoming vault points $V' = [V \quad N]^t = [v_o \quad v_1 \quad \cdots \quad v_{|v|-1} \quad n_0 \quad n_1 \quad \cdots \quad n_{\lambda f-1}]$

(f). These vaults points are stored in the user's mobile phone, for future usage in the authentication phase. The vault data is shown in Figure 14.

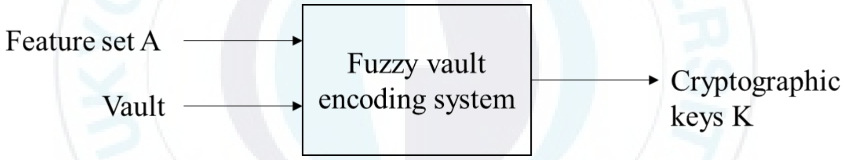


Figure 11. Block Diagram of Fuzzy Vault Encoding System

Table 3. Specification of Fuzzy Vault Encoding System

Module	Fuzzy vault encoding system
Input	• Feature set A • Cryptographic keys K
Output	Vault
Functionality	Generate vault from the feature set and cryptographic keys using fuzzy vault mechanism.

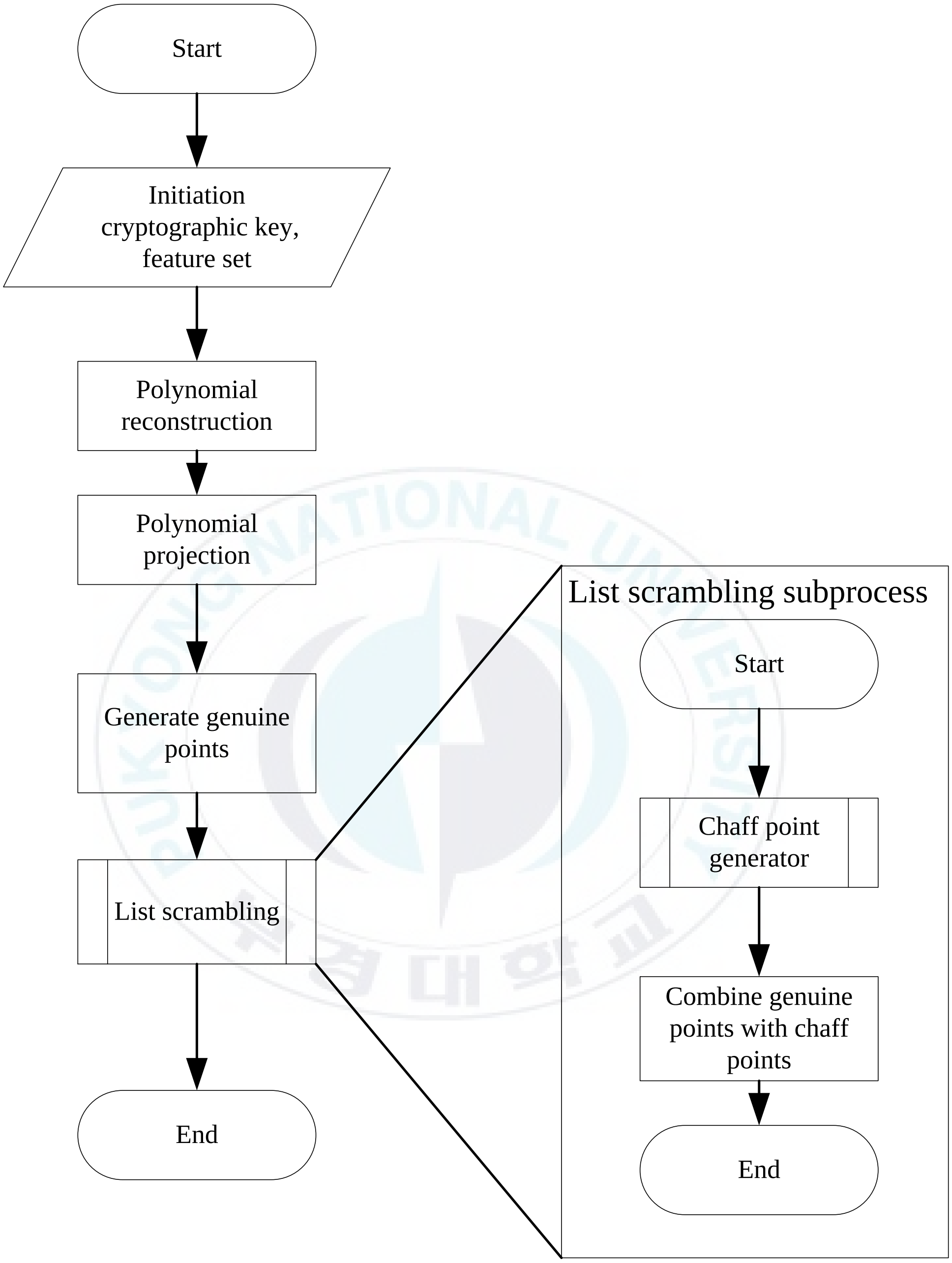

Start
Initiation cryptographic key, feature set
Polynomial reconstruction
Polynomial projection
Generate genuine points
List scrambling
End
List scrambling subprocess
Start
Chaff point generator
Combine genuine points with chaff points
End

Figure 12. Flow Diagram of Encoding System

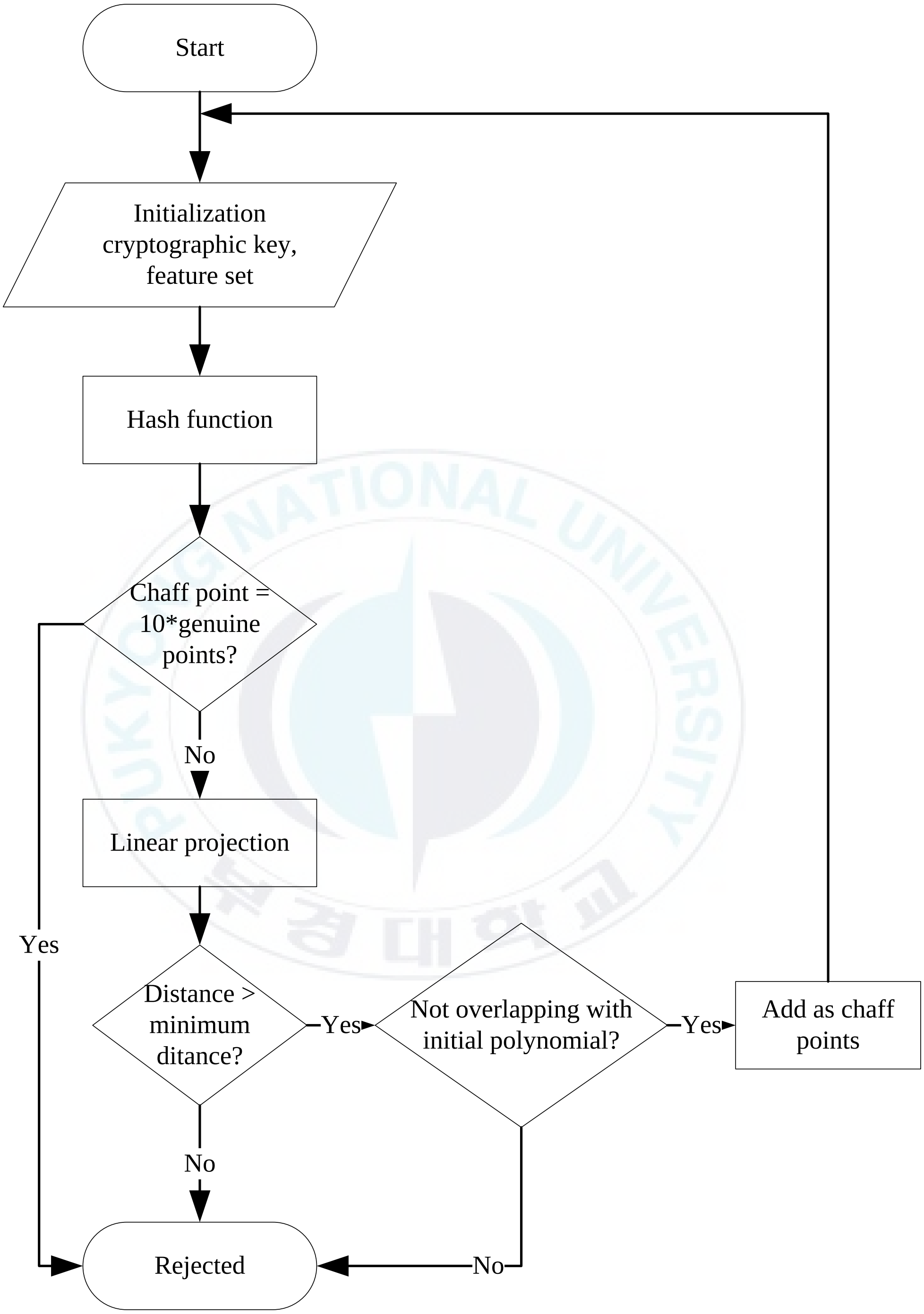
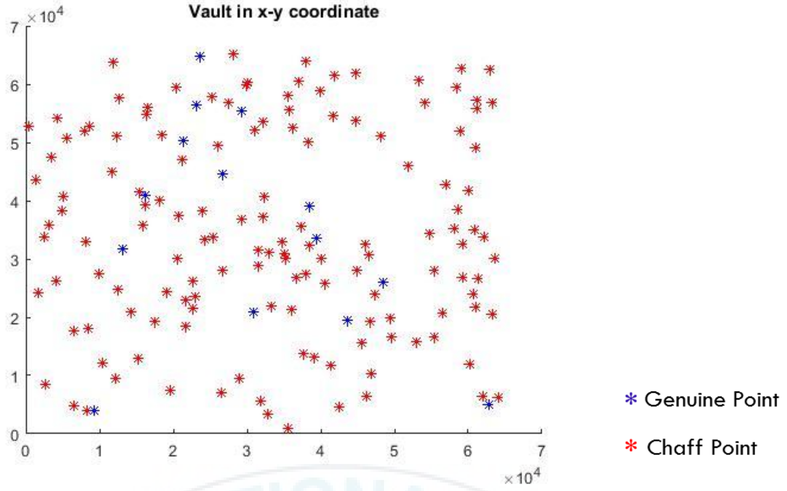
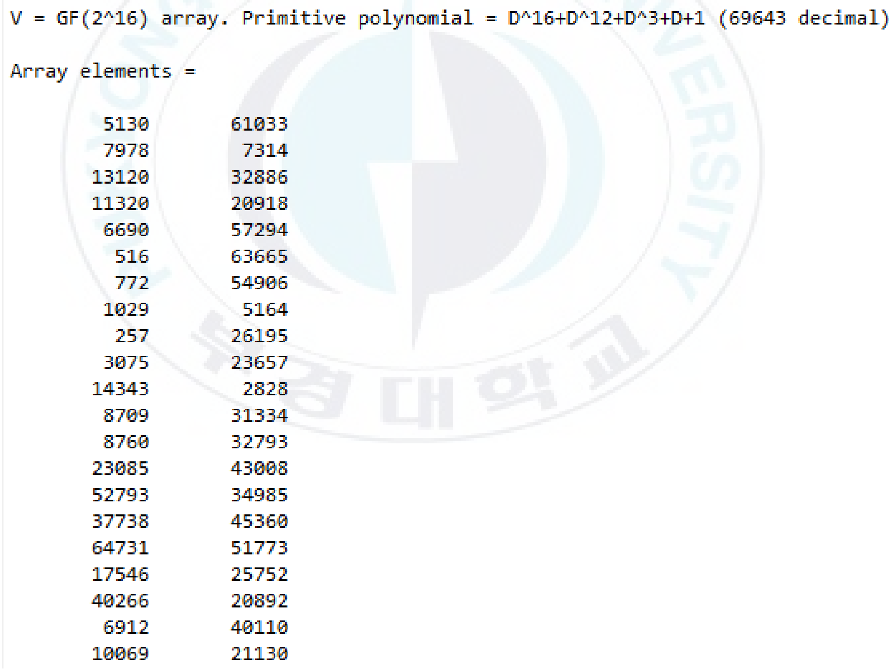

Start
Initialization cryptographic key, feature set
Hash function
Chaff point = 10*genuine points?
No
Yes
Linear projection
Distance > minimum ditance?
Yes
Not overlapping with initial polynomial?
Yes
Add as chaff points
No
No
Rejected

Figure 13. Flow Diagram of Chaff Point Generator



(a)



```
V = GF(2^16) array. Primitive polynomial = D^16+D^12+D^3+D+1 (69643 decimal)

Array elements =

        5130       61033
        7978        7314
       13120       32886
       11320       20918
        6690       57294
         516       63665
         772       54906
        1029        5164
         257       26195
        3075       23657
       14343        2828
        8709       31334
        8760       32793
       23085       43008
       52793       34985
       37738       45360
       64731       51773
       17546       25752
       40266       20892
        6912       40110
       10069       21130
```

(b)

Figure 14. (a) Simulation Results of Generated Vault in Graphic; (b) Simulation Result of Vault Points in MATLAB

3.4.3 Fuzzy Vault Authentication (Decoding) System

Authentication (decoding) process is done between query fingerprint image and vault that is stored as an encrypted representative of reference fingerprint image. The block diagram of this system can be seen in Figure 15, and the specification can be seen in Table 4. This process is a matching process based on fuzzy vault biometric cryptosystems scheme. During this phase, the vault is unlocked using the query fingerprint template to get the cryptographic key as the authentication result. The whole process is illustrated in Figure 16. We divide the system into several processes as follows.

(a). A fingerprint image is inserted as a query input and extracted using fingerprint minutiae detection system. The vault template that is stored in the mobile phone also become the input of the system. The query feature set $\mu = [\mu_0 \quad \mu_1 \ \ldots \ \mu_{|\mu|-1}]$ is obtained.

(b). A matching process is conducted by finding the nearest matching member of the member of the query feature set. We initialize the constant δ as the maximum allowable distance between the two points for positive matching. A new dataset as selected genuine points $\eta = [\eta_0 \quad \eta_1 \ \ldots \ \eta_{|\eta|-1}]$ is obtained. With η_{n_x} is the x-coordinate of matching vault and η_{n_y} is the y-coordinate of the corresponding matching vault.

(c). A polynomial reconstruction is done to the selected genuine points using Lagrange Interpolation with the degrees of the polynomial is already known. At least f sets of the polynomial are constructed. The candidate coefficient becomes the candidate cryptographic key.

(d). Some genuine points are filtered from the vault that is corresponded with the reconstructed polynomial. These genuine candidate points become an input for Chaff Point Verifier.

(e). A verification function is done using Chaff Point Verifier that utilizes chaff point generator module. This verification function is performed to each of polynomial candidate. If the generated vault from Chaff Point Verifier is same with the stored vault, then the cryptographic key is obtained, and the authentication is successful.

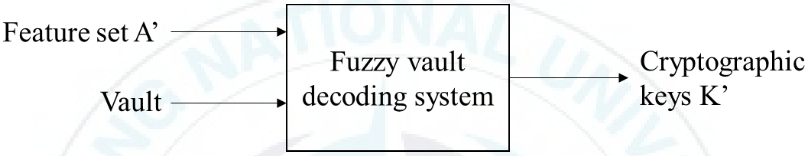


Figure 15. Block Diagram of Fuzzy Vault Decoding System

Table 4. Specification of Fuzzy Vault Decoding System

Module	Fuzzy vault decoding system
Input	• Feature set A' • Vault
Output	Cryptographic keys K'
Functionality	Reconstruct the cryptographic keys K' from feature set A' and vault.

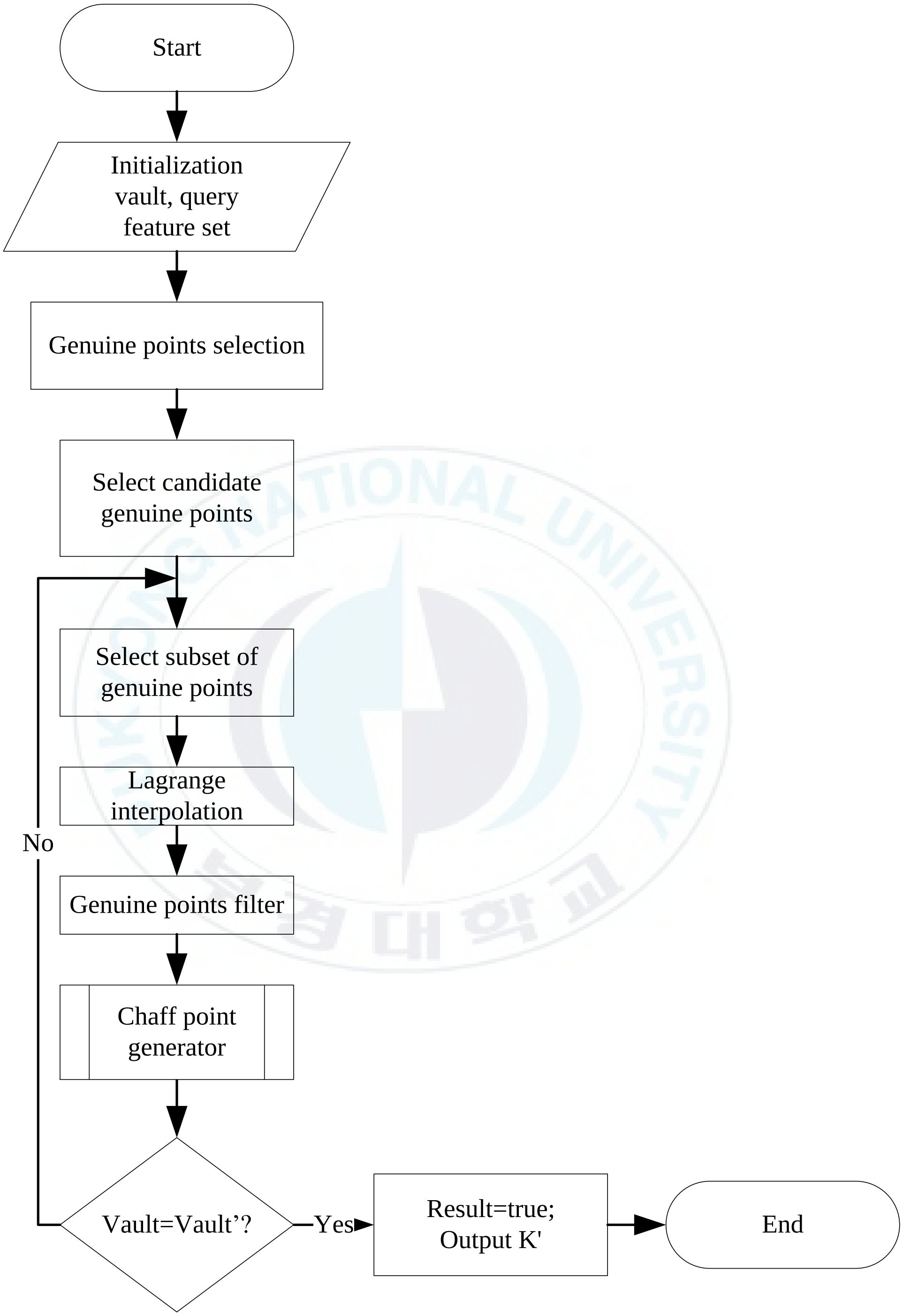


Figure 16. Flow Diagram of Decoding System

3.5 System Functional Requirement

The functional requirements described in this thesis to determine the possible effect of the system or what the system must accomplish. Based on several studies in the literature review, the functionalities that are needed for the application can be determined as follows.

- Generate and view the result of fingerprint authentication.
- Generate and view the result of fingerprint enrollment.

Chapter 4.
System Implementation, Testing, and Analysis

4.1 System Implementation

After determining the design and conduct the system requirement, the next stage is doing the implementation. The components that have been addressed in the design will be implemented in the form of prototype software products into a system of mutually integrated. The implementation is applied to the mobile phone as explain in the first chapter. There is a specification and limitation of the input while doing the implementation. One of the main limitation is fingerprint image that already registered because of hardware constraint.

For method review, we divide into several parts. Before authentication, first, the reference image of the user fingerprint is inserted into the system, and a cryptographic key is selected. After enrollment, if the user wants to authenticate, they insert the query fingerprint image to the system. After that, the application will perform local biometric authentication and produce the corresponding cryptographic key.

4.2 Experimental Design

In this part, an experiment design is created to get the data for analyzing. The input data that is used for testing the system is fingerprint NIST Special Database 04 (SD04). The original SD04 data is an ANSI/NIST format (AN2) file. This database contains 8-bit grayscale images of randomly selected fingerprints. This file contains 4000 (2000 pairs) fingerprint stored in PNG (image) files format and

TXT (data) files with information extracted from the AN2 file. Each print is 512×512 pixels with 32 rows of white space at the bottom of the print. The fingerprint are classified into one of five categories (L = left loop, W = whirl, R = right loop, T = tented arch, and A = arch). For this implementation, the database from figs_0 is used. The record file holds the image for the subject and some information about the image in a text file. The experiment is conducted in MATLAB and Visual Studio with Xamarin.

4.3 Results

4.3.1 Accuracy Test

In this section, a statistical method is used to analyze the accuracy performance of the matching process in the authentication system. The analysis of the results based on Genuine Acceptance Rate (GAR). GAR describes the number of successful authentication of non-authorized users. For this calculation, we only inspect 50 fingerprint images. The experiment is conducted using program prototype in MATLAB. The accuracy calculation is done using expression 2.

$$\text{Accuracy} = \frac{\text{Number of successful authentication}}{\text{Number of use}} \times 100\% \qquad (2)$$

For the experiment, we use several data analyses. We change a number of genuine points and chaff points that is used in the fuzzy vault to see their influence on accuracy. From the Table 5 and Figure 17 we can see that the higher the number of Genuine Points used in the fuzzy vault, the better the value of accuracy. This because the number of possibilities that is used for the matching process will be higher for a higher amount of genuine points. But, after we increase the number of genuine points, the accuracy tends to be constant.

Table 5. Accuracy Results

Values		**GAR (%)**
Genuine Points	**Chaff Points**	
14	140	66%
16	160	68%
18	180	74%
20	200	76%
25	250	84%
30	300	92%
40	400	92%

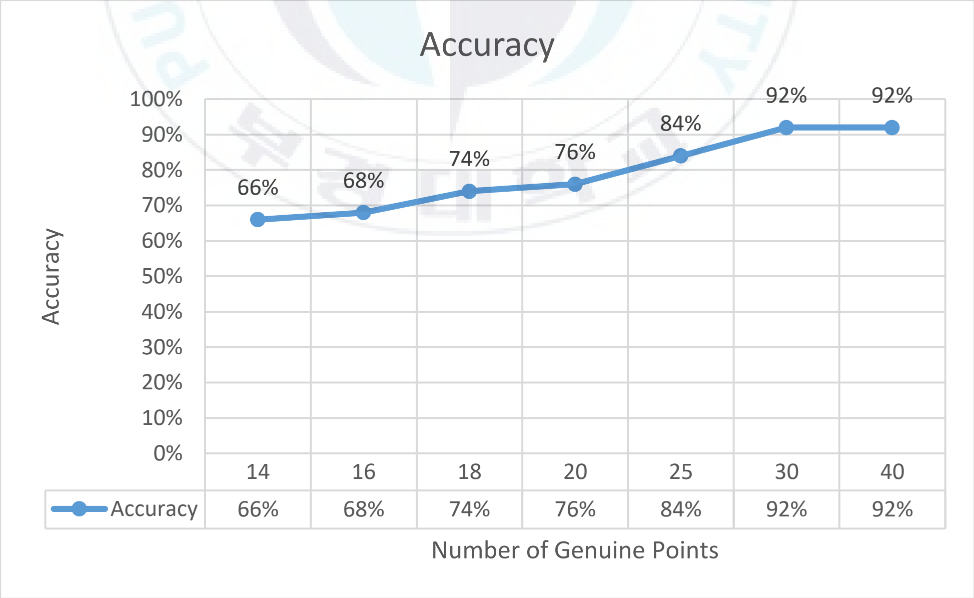
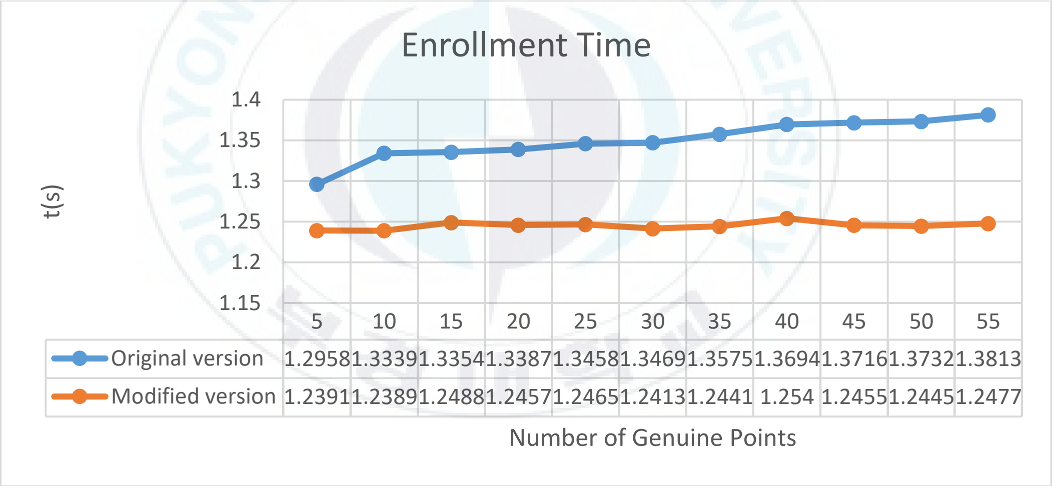


Figure 17. Graphic of Accuracy

4.3.2 Execution Time Test

In this section, we analyze the execution time of the system. We compare the previous system that uses Euclidian distance in the non-random chaff point generator with the modified system that uses circle packing algorithm. We can see that the execution time of the modified version is lower than the original version for enrollment (Figure 18) and authentication (Figure 19). The execution time of the original version become longer if we make the number of genuine points higher. In the modified version, the execution time is independent of the number of genuine points.



	5	10	15	20	25	30	35	40	45	50	55
Original version	1.2958	1.3339	1.3354	1.3387	1.3458	1.3469	1.3575	1.3694	1.3716	1.3732	1.3813
Modified version	1.2391	1.2389	1.2488	1.2457	1.2465	1.2413	1.2441	1.254	1.2455	1.2445	1.2477

Figure 18. Graphic of Enrollment Execution Time

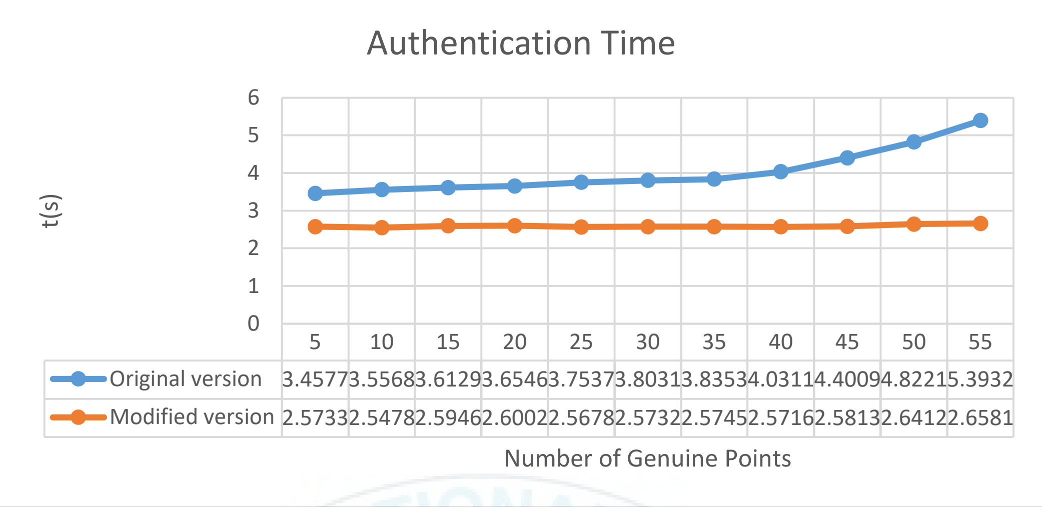


Figure 19. Graphic of Authentication Execution Time

4.4 Functionality and Objective Analysis

Testing of system functionality based on the functions was performed by the system. From the Table 6, it can conclude that the functionality of the main goal of the application was successfully implemented. There are several points that being an approach as the main goal which is explained in below table.

Table 6. Functionality Assessment of the Applications

In Term of Connection with the User		
No	**Functionality Testing**	**Result Conclusion**
1	Perform biometric enrollment process to create the vault with the corresponding ID	Succeed
2	Perform biometric authentication process using query fingerprint image	Succeed

Chapter 5.
Conclusions and Future Studies

In this thesis, a method is proposed and implemented to enhance the security of biometric authentication. This system uses fuzzy vault biometric cryptography. Biometric cryptography (BCs) is a good solution to secure biometric template that is stored locally. By using BCs, the biometric template is stored as encrypted data. Fuzzy vault BCs key binding techniques is a right solution for a system that has an independent relation between biometric template and cryptographic key such as mobile payment with the account based remotely scenario. In this thesis, fuzzy vault BCs non-random chaff point generator fuzzy vault is an improved method of the original fuzzy vault. This method is based on non-random chaff point generator. We modified it using circle packing algorithm. This method tries to solve the previous flaw on preventing attacks especially original attack or blend substitution attack which is harmful to the user if the vault is stolen from the mobile phone.

This system consists of three main parts. First, the fingerprint minutiae detection system. Second, the enrollment process for user’s fingerprint registration and correlate it with the generated cryptographic key. Last, the authentication process after the registration process is conducted. These authentication and enrollment process uses fuzzy vault biometric cryptosystems. Fingerprint minutiae detection system is an important process for both enrollment (encoding) and authentication (decoding). This process produces minutiae points as a feature set. This feature set becomes an input for encoding and decoding process. The input is a grayscale fingerprint image. This process includes pre-processing step and feature extraction step. Enrollment is an important step that must be done before authentication process. This process includes several procedures for the user and main enrollment process that produces vault as encrypted data. Authentication (decoding) process is done between query fingerprint image and vault that is stored as an encrypted representative of reference fingerprint image.This process is a matching process based on fuzzy vault biometric cryptosystems scheme. During this phase, the vault is unlocked using the query fingerprint template to get the cryptographic key as the authentication result.

There are several limitations that we define in this thesis. The cryptographic key generation and key distribution are not discussed and implemented in this system. We presume that the key is already given using the common procedure. Because of the hardware constraint, the input is a fingerprint binary image as a prototype of the fingerprint information of the user. The input is only one fingerprint image for one person with maximum size 512x512 pixels.

From the experimental results, we got two main results. First, the execution time of the modified version is lower than the original version both in enrollment and authentication. The execution time of the original version become longer if we make the number of genuine points higher. In the modified version, the execution time is independent with the number of genuine points. Second, the higher the number of genuine points used in the fuzzy vault, the better the value of accuracy. This because the number of possibilities that is used for the matching process will be higher for a higher amount of genuine points. But, after we increase the number of genuine points, the accuracy tend to be constant. For the final result, this method has 92% accuracy.

In the future studies, hopefully, it can be developed by using another biometric information such as finger vein, 2D face, or iris based on the sensor that already integrated in the future mobile phone. We can use another biometric information using this scheme by changing the fingerprint minutiae detection process with another feature extraction process based on the selected biometric information.

References

[1] PewResearchCenter, "Smartphone Ownership and Internet Usage Contues to Climb in Emerging Economies."
Retrieved on 10th October 2016 from http://www.pewglobal.org/.

[2] J. Egan, "Will voice recognition replace passwords on smartphone?"
Retrieved on 14th November 2016 from http://www.bankrate.com/.

[3] R. Lindemann, D. Baghdasaryan and E. Tiffany, "FIDO Alliance."
Retrieved on 29th October 2016 from https://fidoalliance.org/.

[4] Google Developer," Android Pay API."
Retrieved on 10th November 2016 from
https://developers.google.com/android-pay/tutorial.

[5] J. T. Isaac and S. Zeadally, "Secure Mobile Payment Systems," *IT Professional*, Vol. 16, No. 3, pp. 36-43, 2014.

[6] Y.-H. Jo, S.-Y. Jeon, J.-H. Im and M.-K. Lee, "Security Analysis and Improvement of Fingerprint Authentication for Smartphones," *Mobile Information Systems,* pp. 11-17, 2016.

[7] S. Rane, Y. Wang, S. C. Draper et.al., "Secure Biometrics: Concepts, Authentication Architectures & Challenges," *IEEE Signal Processing Magazine,* pp. 51-64, 19 August 2013.

[8] H. Kim, J. Park, J. Lee et. al., "Biometric Authentication Technology Trends in Smart Device Environment," *Mobile and Wireless Technology*, 2016.

[9] J. Wayman, A. Jain, D. Maltoni et.al., *Biometric Systems*. Springer, New York, 2005.

[10] C. Rathgeb and A. Uhl, "A Survey in Biometric Cryptosystems and Cancelable Biometrics," *EURASIP Journal on Information Security 2011.1,* Vol. 1, pp. 1-25, 2011.

[11] A. Juels and M. Sudan, "A Fuzzy Vault Scheme," *Designs, Codes and Cryptography*, Vol. 38, No. 2, pp. 237-257, 2006.

[12] W. J. Scheirer and T. E. Boult, "Cracking Fuzzy Vaults and Biometric Encryption," *IEEE Biometrics Symposium*, 2007.

[13] F. Benhammadi and K. B. Bey, "Password Hardened Fuzzy Vault for Fingerprint Authentication System," *Image and Vision Computing,* Vol. 32, No. 8, pp. 487-496, 2014.

[14] K.-H. Mohamed, M. N. Marsono and R. Bakhteri, "Biometric Encryption Based on a Fuzzy Vault Scheme with a Fast Chaff Generation Algorithm," *Future Generation Computer Systems,* Vol. 29, No. 3, pp. 800-810, 2013.

[15] N. H. Thi, Y. Wang, Y. Ha et.al., "Performance and security-enhanced fuzzy vault scheme based on ridge features for distorted fingerprints," *IET Biometrics,* Vol. 4, No. 1, pp. 29-39, 2015.

[16] T. K. Dang, Q. C. Truong, T. T. B. Le et.al., "Cancellable fuzzy vault with periodic transformation for biometric template protection," *IET Biometrics,* 2016.

[17] T. N. Minh, Q. T. Truong and T. K. Dang, "Enhance fuzzy vault security using nonrandom chaff point generator," *Information Processing Letters,* Vol. 116, No. 1, pp. 53-64, 2016.

[18] R. Bansal, P. Sehgal and P. Bedi, "Minutiae Extraction from Fingerprint Imaages – a Review," *International Journal of Computer Science Issues,* Vol. 8, No. 5, 2011.

[19] C. I. Watson, M. D. Garris, E. Tabassi, et.al., *User's Guide to NIST Biometric Image Software*. NIST, Gaithersburg, 2007.

[20] W. Zhili. *Fingerprint Recognition*. Department of Computer Science, Hong Kong Baptist University, Hongkong, 2002.

[21] C. Collins and K. Stephensen, "A circle packing algorithm," *Computational Geometry,* pp. 233-256, 2003.

Acknowledgements

In the name of Allah, the Beneficent, The Merciful.

Praise be to Allah (The Almighty) for the blessing given to me, so that, I can finally complete this thesis. Peace and Blessing be upon the lovely prophet Mohammed; Peace be upon Him.

I would like to express my gratitude to all those who supported me and helped while I was writing this thesis.

1. My first and foremost gratitude go to my advisor, Prof. Kyung-Hyune Rhee, Pukyong National University, for supervising my research and giving me important comments and guidance along the way in Korea, with his patience and encouragement. He is an outstanding mentor through his invaluable academic and professional guidance, remarkable dedication to me, and exceptional insight into research.
2. Second, I would like to thank my advisor in Indonesia, Ir. Yudi Satria Gondokaryono, MSEE, Ph.D., for his guidance in Indonesia. His comment and advice is an important start for me to select the topic of the thesis.
3. I also would like to express my sincere gratitude to Prof. Man Gon Park for his support during the hard time. He always gives me strength. I believe him as my second father in Korea.
4. My gratitude also goes to Prof. Chang Soo Kim, and Prof. Bong Ki Shin for their help and assistance during this whole year.
5. My sincere gratitude also goes Dr.Ir. Hilwadi Hindersah, M.Sc., Prof. Dr. Ir. Charmadi Machbub and Ir. Arief Syaichu Rohman, MEngSc, Ph.D. for the continuous support in the dual degree program, partnership between PKNU and ITB.

6. I also owe a debt of gratitude to all the members of the LISIA members: Dr. Park Yongho, Noh Siwan, Mas Bayu, Lewis, Kim Mideum, Vincentius and Aditya for their unfailing academic or non-academic helpfulness during the research study.
7. My sincere thanks go to my colleagues in the DPP PKNU-ITB Batch 2 program who have supported me in many different aspects. We fight together from the beginning, and I hope we success together until the end.
8. Last, I want to thank with eternally grateful to my family: my parents, my sisters and my brothers for all of the spiritual and materials support they give me, especially during my difficult and fragile time. Without their support, this master thesis would not have been possible