PRIVACY PRESERVING MINUTIA-BASED FINGERPRINT TEMPLATE PROTECTION TECHNIQUES

JIN ZHE

DOCTOR OF PHILOSOPHY IN ENGINEERING

LEE KONG CHIAN FACULTY OF ENGINEERING AND SCIENCE
UNIVERSITI TUNKU ABDUL RAHMAN
DECEMBER 2015

PRIVACY PRESERVING MINUTIA-BASED FINGERPRINT TEMPLATE PROTECTION TECHNIQUES

By

JIN ZHE

A thesis submitted to the Department of Electrical and Electronic Engineering,
Lee Kong Chian Faculty of Engineering and Science,
Universiti Tunku Abdul Rahman,
in partial fulfillment of the requirements for the degree of
Doctor of Philosophy in Engineering
December 2015

To my family – who love and support.

ABSTRACT

PRIVACY PRESERVING MINUTIA-BASED FINGERPRINT TEMPLATE PROTECTION TECHNIQUES

Jin Zhe

Modern cryptosystems rely on password or token to generate keys. This leads to authenticate the *key* instead of the *user*. Biometric technology is likely to provide a new level of security to authenticate the *user* for various applications. Yet if the stored biometric template is compromised, invasion of user privacy is inevitable. For instance, an approximation of fingerprint image can be reconstructed with high accuracy using existing technologies if the corresponding set of fingerprint minutia is revealed to an adversary. Furthermore, since biometric is irreplaceable and irrevocable throughout the individual's lifetime, such an invasion implies a permanent loss of identity. Due to these inextricable mazes, a biometric system with protected template is required immediate attention.

In this doctoral research, a study of biometric template protection has been carried out at two major approaches of biometric template protection, i.e. *cancellable biometric* and *biometric cryptosystems*. To improve the existing cancellable biometrics for fingerprint, two minutiae-based cancellable fingerprint template generation methods, namely 2-dimensional random projected minutiae vicinity decomposition (2D-RP-MVD), randomized graph-based hamming embedding (RGHE) are proposed.

Other than cancellable templates proposed in this thesis, another contribution is dedicated to biometric cryptosystems. Firstly, a complete point-to-string conversion framework is proposed to transform minutiae set to an ordered fixed-length representation that is useful for biometric cryptosystems. As a proof-of-concept, the implementation using the generated binary templates in fuzzy commitment scheme is demonstrated. Secondly, a new biometric key binding construct along with cancellable transforms is proposed without using error correction codes (ECCs). Since ECC is abandoned, the security, privacy threat as well as limitations (e.g. security-performance trade-off) associated with ECC no longer exist.

Another importance of this thesis is devoted to the security and privacy analysis on the proposed methods. For instance, the proposed cancellable templates (i.e. 2D-RP-MVD and RGHE) are analyzed rigorously to justify the feasibility of non-invertibility and cancelability. In the point-to-string conversion framework, the randomness and the correlation between the binary templates generated from the proposed method are examined through the entropy estimation using second-order dependency tree and statistical independence test. While, in the proposed key binding construct, the security-performance trade-off, security and the privacy leakage via some major attacks like Attack via Record Multiplicity (ARM), statistical attack, Surreptitious Key-Inversion Attack (SKI) are analyzed experimentally.

ACKNOWLEDGEMENT

I would like to acknowledge all the people who have assisted me in this Ph.D. study. This journey is long but luckily I was not alone. First, my sincere gratitude goes to Prof. Dr. Goi Bok Min, my supervisor, for his strong support and guidance professionally and personally throughout the study. Besides, I would also like to thank the other equally important member of my supervisory team, Assoc. Prof. Dr. Andrew Beng Jin Teoh and Assoc. Prof. Dr. Tay Yong Haur, for their great encouragement and advice. Particularly, Andrew Teoh, his enthusiasm and wide expertise in the field of research have been my sources of inspiration and driving force. I am also grateful to my friends for their constructive advice and discussion, including Dr. Lim Meng Hui, Dr. Leng Lu, Dr. Tan Syh Yuan, Yap Wun She, Chong Zan Kai. Further, I wish to thank Universiti Tunku Abdul Rahman for offering me the research scholarship scheme (RSS). I would not have pursued my study without such financial support from the university.

Last but not least, my sincere thanks and love to my family members. Father's patience, mother's loves have been the most treasured moment that I enjoyed throughout my research. I am also thankful to my wife and little daughter for their unfailing support, understanding and love. With their constant support, my work on this project has been a truly enjoyable and memorable experience.

APPROVAL SHEET

This dissertation/thesis entitled "**PRIVACY PRESERVING MINUTIA-BASED FINGERPRINT TEMPLATE PROTECTION TECHNIQUES**" was prepared by JIN ZHE and submitted as partial fulfillment of the requirements for the degree of Doctor of Philosophy in Engineering at Universiti Tunku Abdul Rahman.

Approved by:

_____

(Prof. Ir. Dr. GOI BOK MIN) Date:……..
Professor/Supervisor
Department of Electrical and Electronic Engineering
Lee Kong Chian Faculty of Engineering and Science
Universiti Tunku Abdul Rahman

_____

(Prof. Dr. TAY YONG HAUR) Date:……..
Professor/Co-supervisor
Department of Internet Engineering and Computer Science
Lee Kong Chian Faculty of Engineering and Science
Universiti Tunku Abdul Rahman

DECLARATION

I hereby declare that the dissertation is based on my original work except for quotations and citations which have been duly acknowledged. I also declare that it has not been previously or concurrently submitted for any other degree at UTAR or other institutions.

Name _____
(JIN ZHE)

Date _____

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

2D-RP-MVD	Two-Dimensional Random Projected Minutiae Vicinity Decomposition
2P-MCC	Two Factor Protected Minutiae Cylinder-Code
ARM	Attack via Record Multiplicity
AUC	Area Under the Curve
BiPS	Binarized Phase Spectrum
CWS	Chaffing and Winnowing Scheme
CLT	Central Limit Theorem
DITOM	Dense Infinite-To-One Mapping
DQ	Dynamic Quantization
DOF	Degree-Of-Freedom
ECC	Error Correction Code
EER	Equal Error Rate
FAR	False Acceptance Rate
FRR	False Rejection Rate
FC	Fuzzy Commitment
FTCR	Failure-To-Capture-Rate
FV	Fuzzy Vault
FVC	Fingerprint Verification Competition
GAR	Genuine Acceptance rate
GD	Genuine Distribution
ID	Imposter Distribution
ISO	International standard for organization
KPCA	Kernel Principal Component Analysis

KLSH	Kernelized Locality-Sensitive Hashing
KL	Kernel Learning
KRER	Key Release Error Rate
LSH	Locality-Sensitive Hashing
MAC	Message Authentication Code
MCC	Minutiae Cylinder-Code
MLC	Multi-line Code
MTA	Multiple Templates Attack
MVD	Minutiae Vicinity Decomposition
PCA	Principal Component Analysis
PGTQ	Polar Grid-based 3-Tuple Quantization
P-MCC	Protected Minutiae Cylinder-Code
RKHS	Reproducing Kernel Hilbert Space
RP	Random Projection
RGHE	Randomized Graph-based Hamming Embedding
RLRD	Random Local Region Descriptor
ROC	Receiver Operating Characteristic
SKI	Surreptitious Key-Inversion Attack
SPD	Symmetric and Positive Definite

CHAPTER 1

INTRODUCTION

Biometrics has been integrated in large-scale personal identification systems and the rapid proliferation of biometric recognition applications is a foreseeable trend in future. The foreseen pervasiveness of biometric authentication systems speeds up the growing biometric databases. However, if biometric databases breach is occurred, severe influences of biological nature of human are concerns. Particularly, the damage to person's privacy and security is permanent due to the irrevocability and irreplaceability nature of human traits. Therefore, it urgently calls for an efficient and effective mechanism to protect the growing biometric databases. Unfortunately, the traditional data protection mechanism, e.g. encryption/decryption is infeasible indeed, which is attributed to the large variety of biometric samples in each acquisition. The unsuitability of traditional data protection mechanism motivates the creation of a new research area, namely biometric template protection that is devoted to create feasible solutions for protecting data with large variety such as fingerprint data. Although, a variety of techniques have been proposed in literature to address biometric template protection, there is no agree-upon solutions.

In this chapter, an overview of biometrics and fingerprint is first presented in Section 1.1. It covers the backgrounds of biometrics and fingerprint, fingerprint databases, and metrics of performance evaluation for generic biometric systems. The security and privacy of biometric systems is given in Section 1.2. This section includes the vulnerabilities of the biometric system, attackable points over the biometric system and categorization of biometric template protection approaches. In Section 1.3, the problem statements, including generic problems in biometric templates and specific problems in fingerprint minutiae-based templates, are presented. Apart from that, the objectives and contributions of this thesis are provided in Section 1.4, Section 1.5 respectively. Finally, the organization of this thesis is given in Section 1.6.

1.1 Backgrounds of Biometrics and Fingerprints

In modern society, various security-demanded applications require a reliable and accurate identity verification/identification mechanism, such as door access system, country border crossing, e-commerce transactions etc. Traditionally, the knowledge of secrets like password is commonly used to authenticate the identity of a person. However, such authentication mechanism provides inherent and inevitable disadvantages that would potentially breach the security of applications. For instance, password is intended to restrict the use of protected resource. However, password can be easily shared to the unauthorized individuals; thus the intended security is compromised. Furthermore, it is annoying that password can be forgotten by a legitimate user who particularly owns multiple passwords across various applications. This is

also known as “too-many-passwords” issue. To be worse, certain applications enforce the rule that password needs to be changed on a regular basis, which is further inconvenienced users. Moreover, simple password can be fortuitously guessed by an adversary. Splash-Data, a password management company, reported that “password”, “123456”, and “12345678” are the top three most common passwords set by the users in 2012 (SplashData, 2012). Therefore, a dilemma can be observed that simple passwords are easy to be guessed while complex passwords are hard to remember.

1.1.1 Biometrics

Biometric technology gives strong compensations to the knowledge-based authentication. Firstly, biometric identifiers (e.g. fingerprint, iris) are of great convenient to the user as it is always in hand. Secondly, biometric identifiers would never be forgotten or lost by the legitimate user. Thirdly, biometric identifiers are not as easy to be shared or forged as password. In fact, using biometrics as means for identity authentication is a rather nature thought from the point of view of history. In the later nineteenth century, Alphonse Bertillon, a French policeman developed the first set of tools using anatomical traits including head length, head breadth, length of middle finger etc., collectively called Bertillon system, to identify repeat offenders (Bertillonage, 2011). Later, Faulds (1880), Herschel (1880) and Galton (1889) discovered that the ridge pattern in our fingertips is useful for identifying an individual. Based on their discoveries, fingerprint matching systems are developed to replace the inefficient Bertillon system. The fingerprint matching systems initially were manually operated by the experts. Until 1963, Mitchell

Trauring (Trauring, 1963) published the first research paper on *automated* fingerprint matching in journal Nature. Following Trauring's work, other biometric traits are also used for automated matching system outlined on publications, such as voice (Pruzansky, 1963), face (Bledsoe, 1966), signature (Mauceri, 1965), hand geometry (Ernst, 1971), and iris (Daugman, 1993). With the great efforts paid by the aforementioned pioneers, the foundations of biometric recognition[1] systems have been well established and biometric recognition has now become an integral part of many large-scale personal identification systems around the world.

1.1.2 Fingerprints

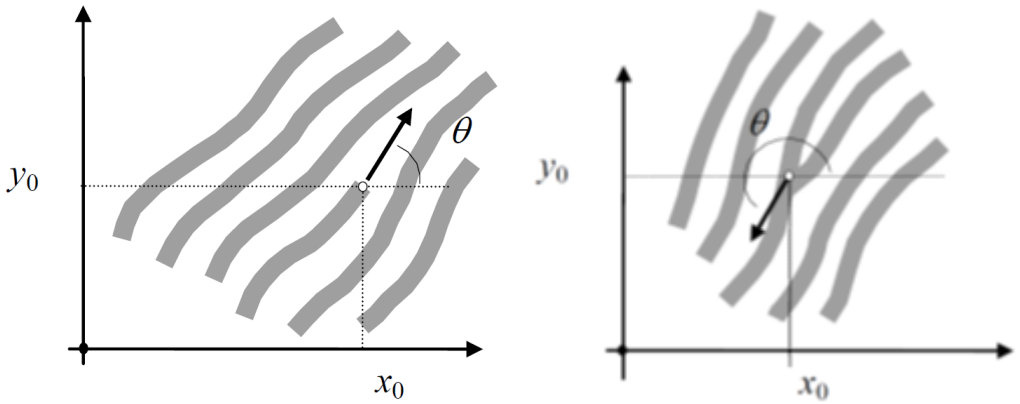
Among the various biometric modalities, fingerprint is probably the most widely used biometric trait for the biometric-based authentication systems (Maltoni et al., 2009). This may be largely attributed to its maturity. Firstly, fingerprint has been used in identifying people for over a century and the validity of fingerprint as means of authentication has been well established (Maltoni et al., 2009). Secondly, fingerprint recognition is one of the leading biometric-based technologies in the current market share. Further, The Wall Street Journal (The Wall Street Journal, 2014) forecasts that fingerprint recognition will continue to dominate the biometric markets in the foreseeable future (Krivokuća, 2014). The work presented in this thesis is based on the fingerprint modality.

[1] Biometric recognition refers to the automated recognition of individuals based on their biological and behavioural characteristics such as fingerprint, face, iris and voice (Jain et al., 2011).

Maltoni et al. (2009) classifies fingerprint features into three levels: namely *level* 1 (i.e. Global level), *level* 2 (i.e. Local level), and *level* 3 (i.e. Very-fine level). The features at the global level are based on the pattern of fingerprint ridge line flow, typically *singular points* (e.g. loop and delta) and *coarse ridge shape* (i.e. Arch, Loop and Whorl). Global level features are useful for fingerprint classification and indexing but less discriminative power for accurate matching (Maltoni et al., 2009). Features at local level are local ridge characteristics, namely *minute details*. There are two most prominent ridge characteristics, called *ridge bifurcations* and *ridge termination*. Generally, fingerprint minutiae are stable and robust to fingerprint impression conditions (Maltoni et al., 2009). Features at very-fine level refer to the intra-ridge details including width, shape, curvature, edge contours of ridges etc. The most significant very-fine level feature is the finger *sweat pores*. However, very-fine level features can only be extracted from high-resolution (e.g. 1000 dpi) fingerprint image with good quality and unavailable to the most practical applications.

Each minutia can be associated with a number of attributes, including location coordinates, orientation, type (e.g. ridge termination or ridge bifurcation), a weight based on the quality of the fingerprint image in the neighbourhood of each minutia, and so on. However, from the common practices, only two attributes are used to represent a minutia: *x*- and *y*-coordinates pertaining to the location of minutia in the fingerprint; the orientation θ of the ridge line to which the minutia is attached (Krivokuća, 2014). Following the common practices, in this thesis, a minutia is represented

as (x, y, θ), i.e. coordinates *x* and *y*, and orientation θ. Fig. 1.1 illustrates the (*x*, *y*) coordinates and the orientation, θ, of a bifurcation and a termination.



(a) (b)

Fig. 1.1: The *x*- and *y*-coordinates and orientation, θ, of (a) a termination, and (b) a bifurcation. (Images obtained from Maltoni et al., 2009).

1.1.3 Fingerprint Recognition System

Fig. 1.2 illustrates the architecture of the generic fingerprint recognition system. A generic fingerprint recognition system consists of four components: fingerprint sensor, feature extraction, storage and matcher. Sensor scans user's fingerprint and passes the acquired fingerprint image to feature extractor. The feature extractor extracts the salient features from the fingerprint image and converts it into pre-defined format, called *template*. Traditionally, the template contains *x*- and *y*-coordinates location and orientation θ of all the minutiae extracted from fingerprint image, represented as $m_i = (x_i, y_i, \theta_i)$, $i = 1,2 \dots, N$, N is the total number of minutia extracted from the fingerprint image.

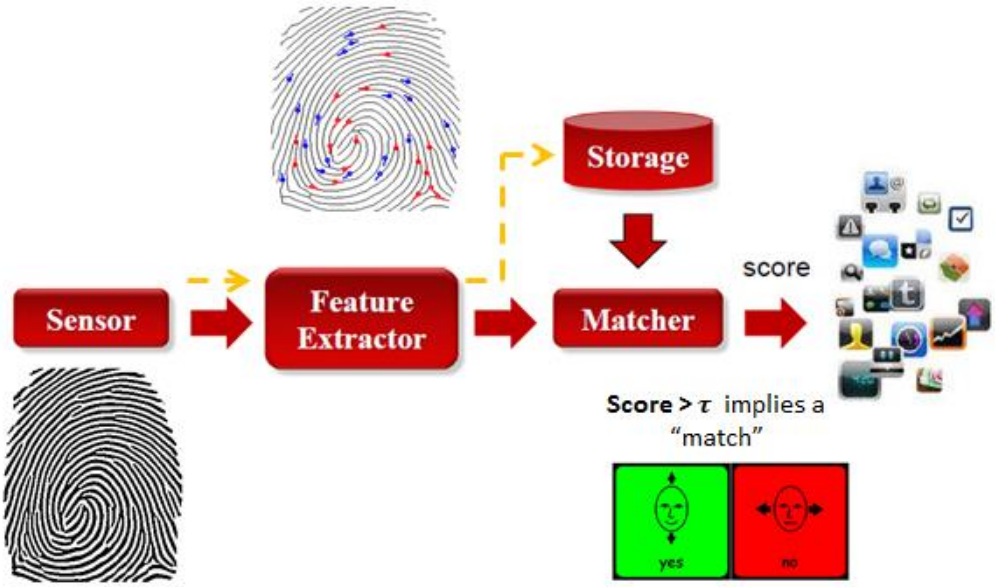


Fig. 1.2: The architecture of the generic fingerprint recognition system.

In the enrolment stage (indicated by the dash orange arrows in Fig. 1.2), user's minutiae are extracted from fingerprint image and stored in the system database. The minutiae template is linked to the user's corresponding identity. On the other hand, at the authentication stage (indicated by the solid red arrows in Fig. 1.2), a user provides a query sample of fingerprint to the sensor and the processes of image acquisition and minutia extraction are carried out. It is noted that the processes of image acquisition and minutia extraction are identical to the processes during the enrolment stage. The matcher then compares the minutiae features extracted from the query image to the minutiae template stored in the database associated with the claimed user identity and computes a numerical matching score. The resultant matching score is matched to the pre-defined threshold for successful authentication based on whether the score is above or below the pre-defined threshold.

1.1.4 Fingerprint Databases

In this thesis, the proposed methods are evaluated using eight well-known fingerprint databases available in public domain, namely FVC2002 ("The Second Fingerprint Verification Competition", 2002), DB1 set A, DB2 set A, DB3 set A, DB4 set A, and FVC2004 ("The Third Fingerprint Verification Competition", 2004), DB1 set A, DB2 set A DB3 set A, DB4 set A. In general, these databases are established as a common benchmark allowing developers to unambiguously compare their algorithms ("The Third Fingerprint Verification Competition", 2004). Each dataset contains 100 users and each user has eight (8) samples, hence there are 800 (100 × 8) fingerprint images in total. Table 1.1 summarizes the characteristics of the eight datasets. Fig. 1.3 illustrates some samples of FVC2002 and FVC2004 fingerprint images. Each row consists of three samples of fingerprint images that belong to the same user.

Table 1.1: Summary of characteristics for FVC2002 and FVC2004 databases.

Databases	**Sensor Type**	**Image Size**	**Amount**	**Resolution**
FVC2002 DB1	Optical Sensor "TouchView II"	388 ×374 (142 Kpixels)	100×8	500 (dpi)
FVC2002 DB2	Optical Sensor "FX2000"	296 ×560 (162 Kpixels)	100×8	569 (dpi)
FVC2002 DB3	Capacitive sensor "100 SC" by Precise Biometrics	300 × 300 (88 Kpixels)	100×8	500 (dpi)
FVC2002	Synthetic	288 × 384	100×8	About 500

DB4	fingerprint generation	(108 Kpixels)		(dpi)
FVC2004 DB1	Optical Sensor “V300”	640 × 480 (307 Kpixels)	100×8	500 (dpi)
FVC2004 DB2	Optical Sensor “U are U 4000”	328 ×364 (119 Kpixels)	100×8	500 (dpi)
FVC2004 DB3	Thermal sweeping Sensor	300 × 480 (144 Kpixels)	100×8	512 (dpi)
FVC2004 DB4	SFinGe v3.0	288 × 384 (108 Kpixels)	100×8	About 500 (dpi)

Fig. 1.3: Samples of fingerprint images in FVC2002 and FVC2004.

1.1.5 Metrics of Performance Evaluation

In a generic biometric system, the most commonly used performance indicators are *False Rejection Rate* (FRR) and *False Acceptance Rate* (FAR). FRR refers to the probability that the system fails to detect a match between the input pattern and a matching template in the database. It measures the percent of valid inputs which are incorrectly rejected (Jain et al., 2011). FRR can be formulated in eq. (1.1). On the other hand, FAR refers to the probability that the system incorrectly matches the input pattern to a non-matching template in the database. It measures the percent of invalid inputs which are incorrectly accepted (Jain et al., 2011). FAR can be calculated using eq. (1.2).

$$FRR = \frac{number\ of\ rejected\ genuine\ users}{total\ number\ of\ genuine\ access} \times 100\% \quad (1.1)$$

$$FAR = \frac{number\ of\ accepted\ imposter}{total\ number\ of\ imposter\ access} \times 100\% \quad (1.2)$$

Besides, there is another performance measurement commonly used, namely *Equal Error Rate* (EER). Equal Error Rate indicates the point at which both accept and reject rate are equal. EER provides a quick way to compare the accuracy between different biometrics systems. In general, the lower EER, the more accurate the system is (Jain et al., 2011).

Apart from FAR, FRR and EER, an overall performance of a biometric system can be demonstrated by using the *Receiver Operating Characteristic* (ROC) curve. ROC is a comprehensive way to analyse the performance of a biometric system. It depicts the dependence of the false acceptance rate with the genuine acceptance rate (GAR) as the system threshold on match score is changed (Jain et al., 2011). Here, *Genuine Acceptance rate* (GAR) is calculated by the formula: GAR = 1 – FRR.

Besides ROC curve, another performance indicator namely genuine-impostor distribution is used to justify the performance of the proposed methods in this thesis. Typically, the genuine-impostor distribution demonstrates two peaks. One peak corresponds to the genuine distribution and the other corresponds to the impostor distribution. A clean separation between

the genuine and impostor distributions indicates better performance while strong overlapping between the genuine and impostor distribution implies poor performance.

1.2 Security and Privacy of Biometric Systems

With the rapid proliferation of biometric systems in both desktop and mobile devices, using biometrics as means of identity verification or identification has raised much public concerns about the security and privacy of biometric data over the last decade. Public worry about violation of user privacy is not uncommon, since the biometric data is inextricably bound to one's identity and a compromise would lead to a permanent loss of their identity. A most recent example of threat reported by FireEye, a security firm, shows that HTC One Max (an Android-based smart phone) stores fingerprint image in unencrypted/unprotected plain text with world readable permission (FireEye report, 2015).

Based on the categorization proposed by Ratha et al. (2001), there are eight levels of attacks that can be launched against a biometric system. In this thesis, the eight levels of attacks are compiled and re-organized into seven attacks. An overview of these seven attack points is demonstrated by the Fig. 1.4.

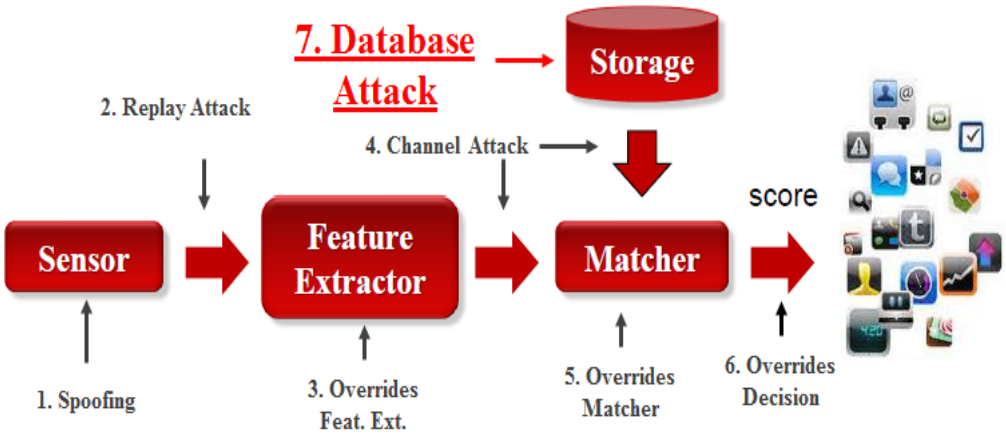


Fig. 1.4: Seven attack points in a biometric system (adopted from Ratha et al., 2001).

1. Spoofing: A fake biometric trait such as latex imitate of a fingerprint may be presented at the sensor.
2. Replay Attack: An illegal data is injected into the channel between sensor and feature extractor and the data may be resubmitted to the system.
3. Overrides Feature Extractor: The feature extraction module may be substituted by a Trojan horse program that generates pre-defined feature sets for matching.
4. Channel Attack: The genuine feature sets may be replaced by the synthetic feature sets during the transmission between feature extractor and matcher; or the data passing between the system database and matcher module may be altered.
5. Overrides Matcher: A Trojan horse program may be injected and replace the matcher to perform the intention of the attack.

6. Overrides Decision: The final decision generated by the matcher may be overridden during the transmission between the matcher module and the application.
7. Database Attack: The original templates stored in the database may be revised or even removed and new templates may be intentionally introduced for intrusion.

In this thesis, the 7th attack (i.e. database attack) mentioned above is addressed and the focus is to design a biometric template protection method. This is due to the fact that database attack is one of the most potentially damaging attacks, which leads to the serious security breaches and privacy threats of biometric templates (Jain et al., 2008). Jain et al. (2008) also highlighted three vulnerabilities on the consequences of biometric template attack: (1) unauthorized access of biometric system by replacing the genuine template with imposter's template; (2) genuine template can be illegally gained to create a physical spoof, thus, compromise both system security and user privacy; (3) stolen template can be involved in various abuse e.g. cross-matching, function creep etc.

For these inextricable mazes, a biometric system with strong template protection needs to be designed urgently. In general, the design criteria for biometric template protection scheme are (Teoh et al., 2006; Jain et al., 2008; Maltoni et al., 2009):

- **Diversity**. Cross-matching between templates from the same user

across different applications must be prevented.

- **Cancelability**. A new template can be reissued once the old template is compromised.
- **Irreversibility/Non-invertibility**. It should be computationally infeasible to derive the original biometric template from the protected template and the helper data.
- **Performance preservation**. The accuracy performance of an unprotected system should be preserved or improved.

Generally, biometric template protection refers a set of techniques that mitigate the aftermaths due to the compromise of biometric templates databases for the purpose of malicious use. Technically, biometric template protection is to design a protect function and apply it into unprotected template to generate protected template as depicted in Fig. 1.5. The template protection methods proposed in literature can be broadly divided into two categories, namely, *feature transformation* approach (or cancellable biometrics) and *biometric cryptosystem* (or helper data methods) (Jain et al., 2008) as shown in Fig. 1.6.

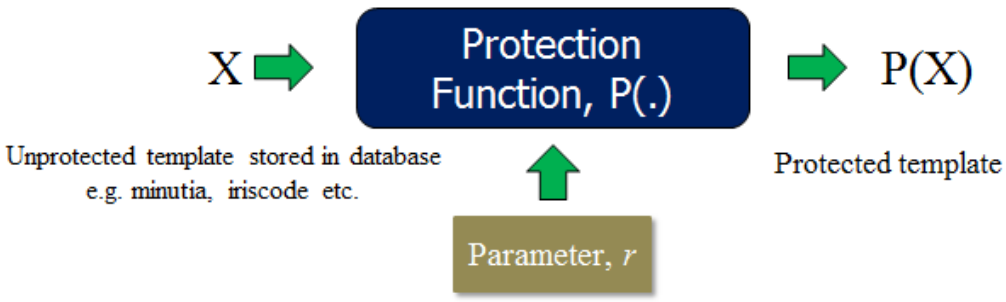


Fig. 1.5: Approach of biometric template protection.

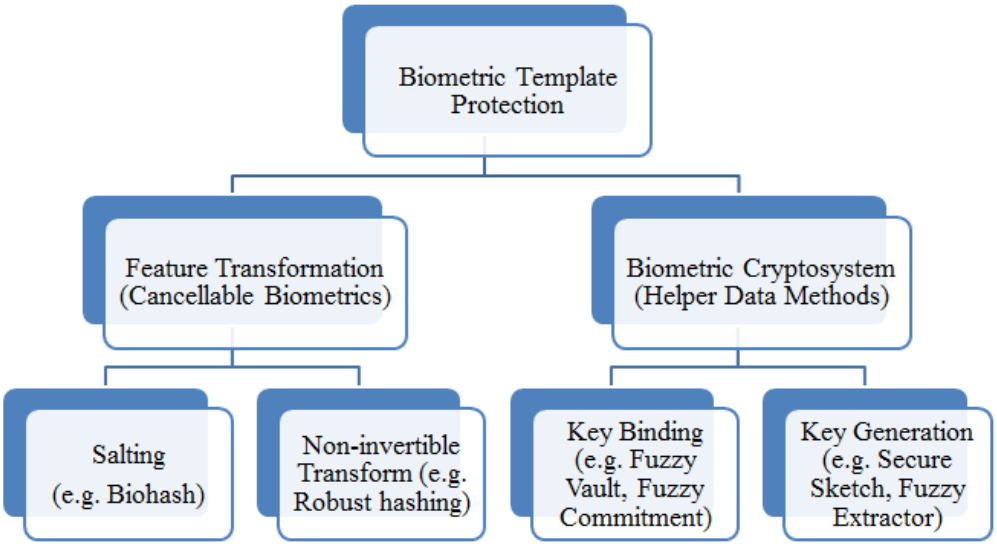


Fig. 1.6: Categorization of Biometric Template Protection Methods (adopted from Jain et al., 2008).

Cancellable biometrics (Ratha et al., 2007; Jain et al., 2008) is truly meant designed for biometric template protection. It refers to the irreversible transform of the biometric template to ensure security and privacy of the actual biometric template. Hence, instead of the original biometric data, only the transformed templates are stored. If a cancellable biometric template is compromised, a new template can be re-generated from the same biometrics. The schemes of cancellable biometrics vary according to different biometric modality and fingerprint minutia oriented template is solely focused in this thesis. Fig. 1.7 illustrates a block diagram of cancellable biometrics.

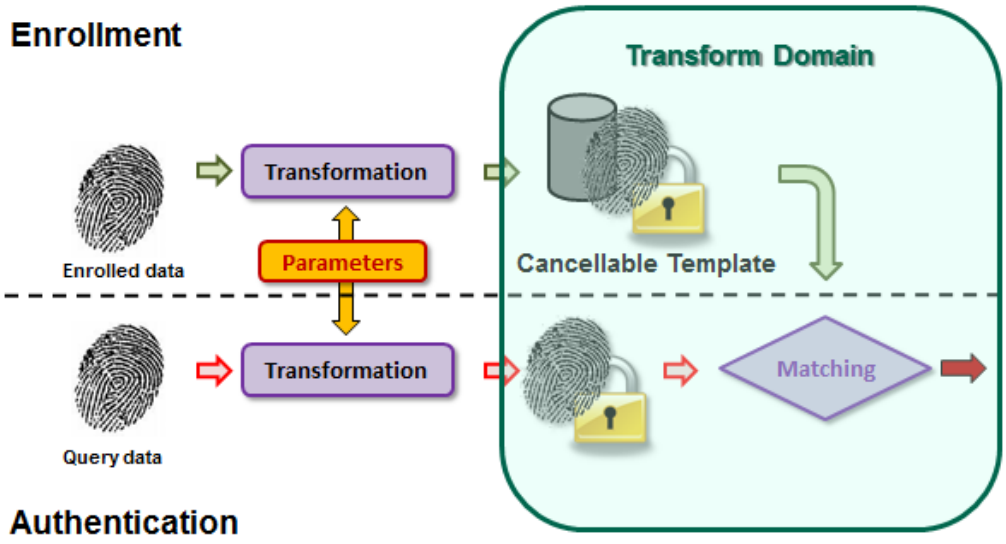


Fig. 1.7: A block diagram of cancellable biometrics.

On the other hand, biometric cryptosystem serves the purpose of either securing the cryptographic key using biometric feature (key binding) or directly generating the cryptographic key from biometric feature (key generation) (Jain et al., 2008). For key binding approach, two well-known instances, fuzzy commitment and fuzzy vault, are proposed by Juels and Wattenberg (1999) and Juels and Sudan (2006) respectively. On the other hand, Dodis et al. (2008) introduced the key generation primitives, known as secure sketch and fuzzy extractor.

1.3 Problem Statements

Along with the benefits of using biometric technologies, the vulnerabilities of security and privacy in biometric systems have been drawn a great attention. The problems, in this thesis, can be categorized into two parts: 1) Problems related to a generic biometric system; 2) Specific problems

associated with fingerprint minutiae. A detailed description of problems related to generic biometric systems is given in the following:

- **Privacy** – Biometric data acquired from human body or activities contain private and sensitive information. For instance, human fingerprint might reveal the sexual orientation of the corresponding identity (Williams et al., 2000) and disease (Weinreb, 1985); the diseases associated with eye, e.g. free-floating iris cyst and diffuse iris melanoma (Zhou, 2012). Such information is strongly associated with human privacy and privacy invasion would be inevitable if biometric data is exposed. Cavoukian et al. (2012) has pointed out that threats to informational privacy rights related to biometric data misuse, function creep and linkage of biometric data in diverse databases makes possible such unintended consequence as surveillance, profiling and discrimination. The global privacy and data protection community therefore have consistently argued against the use of biometrics, especially for centralized database of biometric data (Cavoukian et al., 2012).

- **Irrevocability / non-revocable reference** – Unlike password or token based authentication, biometric data cannot be reset or revoked if they are compromised. More specific, biometric data are permanently associated with an individual and biometric data cannot be re-issued once it is compromised. In the event of compromise, the solution is to either change with another biometric modality or alter the exposed one.

However, neither of two is feasible: (1) human have a limited biometric modalities, e.g. ten fingers, one face, two iris, etc.; (2) an alternation of exposed biometric data such as transplantation, cosmetic surgery is also highly infeasible.

- **Cross-matching** - Multiple applications registered using one identical biometric modality are potentially linked. A biometric identity compromised in on application yields danger in other applications.

- **Trade-off between performance and non-invertibility** – Template protection methods have demonstrated a trade-off between performance and non-invertibility (Nagar et al., 2010c; Wang et al., 2012). This is due to the contradiction where non-invertibility requires to leak as little information about the original template as possible while high accuracy performance is achieved only when retains as much discriminative information from the original template as possible (Nandakumar and Jain, 2015).

- **Security breach and limitations triggered by error correction codes (ECCs)** – Existing biometric key binding scheme, e.g. fuzzy commitment and fuzzy vault relies on error correction code (ECC) to mitigate biometric intra-user variations. Accordingly, those schemes are highly susceptible to a number of security and privacy attacks such as decodability attack (Simoen et al., 2009; Kelkboom et al., 2011), statistical attack (Rathgeb & Uhl, 2011) etc. Further, the employment

of error correction codes in biometric key binding enables a major limitation, namely security–performance tradeoff. That is, the larger key size/higher security results lower Genuine Acceptance Rate (GAR) and vice versa (Nagar, 2012; Kelkboom et al., 2012).

The specific problems associated with fingerprint minutiae are described as follows:

- **Incompatibility between ISO-complaint minutiae template and fuzzy commitment** - ISO/IEC 19794-2 compliant fingerprint minutiae template is an unordered and variable-sized point set data; in contrast, fuzzy commitment only accepts an ordered and fixed-length binary string. Such incompatibility leads that minutia template cannot be adopted in existing fuzzy commitment.

- **Alignment** – In fingerprint minutia-based template protection methods, alignment is often required for accurate matching. However, a stable and reliable registration point e.g. core point and/or delta point for alignment is not always feasible to be extracted in the real world due to the low quality fingerprint images. In literature, fail to extract registration point usually leads to a high failure-to-capture-rate (FTCR) (Nandakumar et al., 2007; Nagar et al., 2008).

1.4 Research Objectives

Based on the problem statements discussed above, the following objectives are formulated in this thesis:

- To design alignment-free template protection methods that generate fingerprint minutiae-based templates with satisfying cancelability, diversity, performance preservation, and irreversibility.

- To propose a point-to-string conversion method that converts the variable-sized minutiae representation into an ordered and fixed-length representation.

- To propose a biometric key binding along with cancellable transform without using error correction code (ECC). Thus, various security attacks and shortages associated with ECC are no longer valid.

1.5 Contributions

The contributions of this thesis are as follows:

- Two alignment-free fingerprint minutiae-based template protection methods, namely 2-Dimensional Random Projected Minutia Vicinity Decomposition (2D-RP-MVD), Randomized Graph-based Hamming Embedding (RGHE) are proposed. Moreover, analysis based on four criteria of biometric template protection, i.e. diversity, cancelability, non-invertibility and performance preservation is carried out to justify

the feasibility of the resultant templates generated from the proposed methods.

- A generic kernel-based point-to-string conversion method is proposed to facilitate the conversion from variable size fingerprint minutiae set to an ordered and fixed-length representation that is useful for conventional cryptography and biometric cryptosystem like fuzzy commitment. Further, the randomness and the correlation between the binary templates generated from the proposed point-to-string conversion method are examined through the entropy estimation using second-order dependency tree and statistical independence test.

- An ECC-free key binding scheme along with cancellable transform for fingerprint minutiae-based biometrics is proposed. Since the ECC is abandoned, the proposed key binding scheme gets rid of the ECC-based attacks (e.g. statistical attack) and shortages (e.g. security-performance trade-off) effectively. Besides, the security and privacy of the proposed key binding scheme is justified by analysing the template non-invertibility, decodability attack, surreptitious key-inversion attack as well as other major attacks occurred in the existing key binding schemes.

1.6 Thesis Organization

The thesis is organized as follows: In chapter 2, a literature review including minutiae-based cancellable fingerprint templates, minutiae-based

point-to-string conversion methods and biometric key binding is presented in detail. Two minutia-based cancellable fingerprint templates, namely Two-Dimensional Random Projected Minutia Vicinity Decomposition (2D-RP-MVD) and Randomized Graph-based Hamming Embedding (RGHE) are proposed in chapter 3. Thereafter, based on kernel learning method, a generic point-to-string conversion framework for fingerprint minutia is proposed in chapter 4. Apart from that, an ECC-free key binding scheme along with cancellable transforms is proposed for minutiae-based fingerprint biometrics presented in chapter 5. Finally, conclusion of this thesis is given in chapter 6.

CHAPTER 2

LITERATURE REVIEW

In this chapter, a literature review on biometric template protection methods is presented. It covers fingerprint minutiae-based cancellable templates, point-to-string conversion methods for fingerprint minutiae (i.e. ordered and fixed-length representation generation), and biometric key binding. Firstly, an overview of fingerprint minutiae-based cancellable templates is presented in Section 2.1. Thereafter, fingerprint minutiae-based point-to-string conversion approaches proposed in the literature is revisited in Section 2.2. Apart from that, an overview of biometric key binding schemes i.e. fuzzy commitment (FC) and fuzzy vault (FV) is provided in Section 2.3. Finally, a summary is given in Section 2.4.

2.1 Overview of Fingerprint Minutia-based Cancellable Templates

In the literature, a number of cancellable biometrics schemes have been proposed. These schemes generally can be categorized into two major approaches, namely Biometric Salting and Non-invertible Transforms (Jain et al., 2008). Resembling password salting in cryptography, Biometric Salting blends user-specific information, such as passwords or token with biometric data to derive a "distorted" version of the biometric template. A popular instance of Biometric Salting is BioHashing (Teoh et al., 2004). Non-invertible Transforms is designed to transform raw biometric data into a new

form that cannot be inverted due to the many-to-one property of the transformation function. A well-known realization of non-inveritible transforms is reported by Ratha et al. (2007).

Fingerprint minutia-based cancellable templates can be broadly divided into two categories: direct minutiae transform and indirect minutiae transform. Direct minutiae transform refers to direct transformation of the original minutiae information, i.e. location and orientation through a function. This approach is speedy since no additional operations are involved. The main disadvantage is the possible revelation of original minutia information if the non-invertible transform function is not properly designed.

To address this issue, instead of using the original minutiae, indirect minutiae transform utilizes certain features that are invariant to translation, rotation and scaling. These features could be the minutia count in the geometrical objects such as triangle, cuboid, local distance and orientation of two minutiae etc. Indirect minutiae transformation approach conceals the original minutiae for improving security at the cost of higher computation time required to convert the minutiae into the invariant features.

1) Direct minutiae transform

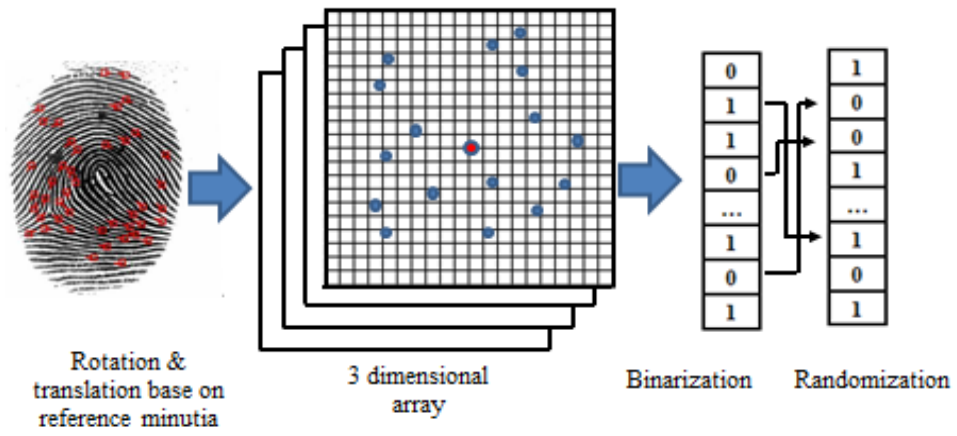
For direct minutiae transform, Ratha et al. (2007) proposed three non-invertible transform functions, namely Cartesian, polar and surface-folding transformation. Although the three transformation functions were claimed to be non-invertible due to the many-to-one mapping property, a scheme by Feng

et al. (2008) reveals that the surface-folding transform can be degenerated when the transformed template and parameters are revealed to the attacker. Meanwhile, Shin et al. (2009) also showed that the surface-folding transform could be inverted if at least two transformed templates originating from the same fingerprint are compromised (a. k. a. Attack via Record Multiplicity).

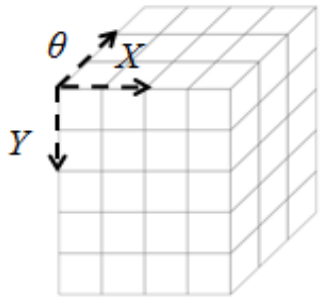
Tulyakov et al. (2005) presented a method to hash fingerprint minutiae and perform fingerprint matching in hashed domain. In their method, a minutia is viewed as a point on a complex plane. Each minutia, along with its two nearest neighbors, is used to select one out of several symmetric functions. The selected function is then evaluated on the three minutiae to obtain the coordinates of the transformed minutia. It is computationally hard to reconstruct the original features with resultant hash values attributed to the one-way transformation characteristic of the hashing function. User can re-enrol with a new hash function to generate new hash values when the old hash values are compromised. Hence, both the non-invertibility and reusability requirements are satisfied. However, performance degradation at 3% of equal error rate (EER) in the best case under FVC 2002 DB1 is unfavorable compare to baseline at EER =1.7%.

Lee & Kim (2010) proposed a cancellable fingerprint template (bit-string) using fingerprint minutiae as shown in Fig. 2.1(a). A 3-dimensional array illustrated in Fig. 2.1(b) is first defined and a number of cells contained in the 3D array are determined by the quantization level. One of the minutiae is then selected as the reference minutiae and the other minutiae are translated

and rotated based on reference minutia. The transformed minutiae fall into each cell according to the *x*-axis, *y*-axis and orientation. Each cell is marked as '1' if it contains more than one minutia and '0' otherwise. Thus, a 1D bit-string is generated by visiting the cells sequentially. It is noted that the bit-string generated thus far is only based on one reference minutia. The processes aforementioned are repeated by using different minutiae as reference minutiae until the entire minutiae set was traversed. The binary template is $n \times l$ matrix, where n and l depict the number of minutiae and the length of 1D bit-string generated based on one minutia respectively. The resultant bits-string is



(a) Overview of the proposed method for bit-string generation



(b) The 3 dimensional array

Fig. 2.1: (a) the block diagram of generating bit-string from fingerprint minutiae proposed by Lee & Kim (2010); (b) demonstrates the 3-dimensional array.

permuted based on a user-specific PIN for revocability purpose. However, in the same PIN scenario, the accuracy performance deteriorated significantly.

Instead of using equal-size tessellation (Lee & Kim, 2010), Jin et al. (2012) proposed a quantization method using polar-based sector; and the area of each sector differs by the radius. Subsequently, the sectors near the reference minutia have smaller area and otherwise. This leads to the smaller (resp. larger) quantization step around (resp. further away from) the reference minutia to tolerate fingerprint elastic deformation. Experiment shows certain performance improvement under the "stolen token" scenario (a.k.a. same PINs scenario: verification of an imposter's biometric using the stolen token of the target user).

Yang & Busch (2009) proposed another fingerprint template protection method based on minutia vicinity. Given N minutiae $\{m_i \,|i=1, 2,..., N\}$, each minutia m_i with the three nearest neighboring minutiae $\{c_{i1}, c_{i2}$ and $c_{i3}\}$ together form a set of minutia vicinity $V_i = \{m_i, c_{i1}, c_{i2}, c_{i3} | i=1, 2,..., N\}$. Each minutia vicinity comprises 12 orientation vectors: $m_i \rightarrow c_{i1}$, $c_{i2} \rightarrow c_{i3}$, $c_{i3} \rightarrow c_{i1}$, etc. The four coordinate pairs of V_i are then transformed based on the 5 (out of 12) randomly selected orientation vectors in the respective minutia vicinity. Next, the random offsets are added to each V_i in order to conceal the local topological relationship among the minutiae in the vicinity. The transformed minutiae are thus regarded as a protected minutia vicinity with stored random offsets.

However, Simoens et al. (2010) pointed out that the coordinates and orientations of minutiae in Yang & Busch (2009) could inexhaustively be revealed if both random offsets and orientation vectors are disclosed to an adversary. They also showed that the attack complexity is considerably low (e.g., only 2^{17} attempts are required when the random offsets table is known with reference to 2^{120} attempts when the random offsets table is not known). Although Yang et al. (2010) later proposed a dynamic random projection which was originally outlined in Teoh et al. (2006) to alleviate this problem, dynamic random projection incurs substantially increased computation cost than that of random offsets addition in Yang & Busch (2009).

A state-of-the-art fingerprint template representation is recently proposed by Cappelli et al. (2010), namely minutiae cylinder-code (MCC) as depicted in Fig. 2.2. The method shares the same concept of tessellation with Lee & Kim (2010) in quantization. Different from Lee & Kim (2010) that counts the number of minutiae in each cell, MCC considers the probability of finding a minutia within a certain range (fixed radius) around the cell. Compared to nearest-neighbor-based descriptor (Maltoni et al., 2009); fixed radius-based minutia descriptor is not much affected by the presence of missing or spurious minutiae. Thus, this would improve the accuracy performance.

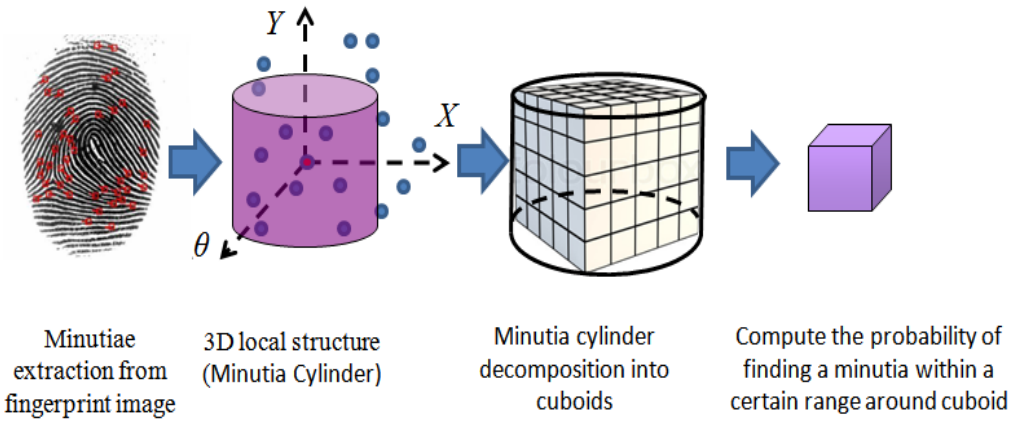


Fig. 2.2: The basic idea of minutiae cylinder-code (MCC) proposed by Cappelli et al. (2010).

However, Ferrara et al. (2012) proposed a recovery algorithm to reveal the original minutiae from the MMC template. A non-invertible scheme is hence proposed, namely protected minutia cylinder-code (P-MCC) by using binary principle component analysis. Although the non-invertibility of P-MCC template has been experimentally justified, it is still unable to fully protect the genuine minutiae points. For instance, it has been reported in Ferrara et al. (2012) that a portion of genuine minutiae (at least 25.4%) could be precisely recovered. Later, a two-factor protection scheme on P-MCC, namely 2P-MCC (Ferrara et al., 2014) is proposed to make the protected MCC template revocable.

In the category of direct minutiae transform, other fingerprint minutia-based cancellable templates proposed in literature can be found as follows: Yang et al. (2010a), Yang et al. (2010b), Yang & Busch (2012), Zhang et al. (2013), Moujahdi et al. (2014).

2) Indirect minutia transform

On the other hand, indirect minutia transform usually offers higher privacy protection than the direct approach as location and orientation of minutiae are not directly revealed. Ang et al. (2005) proposed a key-dependent transformation scheme to produce a cancellable fingerprint template from a set of fingerprint minutiae. In this scheme, the minutia is transformed into a set of invariant feature, such as Euclidean distance between two minutiae, angle between ridges of one minutia with respect to another, number of ridges between two minutiae. The core point is required to be determined in prior, and a line through the core point is then specified. The line orientation, ranging from 0^o to 180^o, is determined by the key transformation function. Different template can be obtained by changing the line orientation.

Lee et al. (2007) proposed a binary cancellable fingerprint template via indirect minutia transformation. Firstly, the translation- and rotation-invariant feature set is extracted using local orientation around each minutia, which was adapted from Tico & Kuosmanen (2003). The feature set is then used as an input to a user-specific transformation function that outputs translational and rotational parameters for minutia transformation. The cancellable templates are generated by transforming each minutia based on the derived parameters. In the case where the template is compromised, a new template can be issued by changing the transformation functions. However, the accuracy performance can be degraded when the quality of the fingerprints is poor due to the strong relation between the invariant feature set and the orientation information around each minutia.

Nagar et al. (2010a, 2010b) described a method of extracting binary code from fingerprint using minutia and fingerprint ridges. For minutia feature, a cuboid-based feature extraction algorithm originally proposed by Sutcu et al. (2008) is adopted to extract the relative features (aggregate wall distance, minutiae average, and minutiae deviation from each randomly-chosen cuboidal regions). This method offers high accuracy performance but it requires the use of the registration points of fingerprint image, which is difficult to detect precisely in poor quality image.

Farooq et al. (2007) presented another method of generating binary fingerprint representation. Their idea is based on the fact that fingerprints can be represented by a set of triangles derived from multiple sets of minutiae triplets. Seven invariant features: length of three sides, three angles between each side and each minutia orientation; and height of the triangle are extracted and quantized into a 2^{24}-bit binary string. However, this method requires exhaustive calculation of invariant features of all possible minutiae triplets, which results in high computational cost. Following the work of Farooq et al. (2007), Jin et al. (2010a, 2010b) attempted to reduce the length of bit-string by using minutiae pairs instead of minutiae triplets. Four invariant features, i.e. Euclidean distance between two minutiae, angular difference between two minutiae, two angles between minutia orientation and the segment connecting two minutiae, are extracted for histogram binning. Consequently, the size of template is reduced to 2^{18} and the performance is enhanced by introducing a majority-voting- based training process.

To address the reversibility of the representation for minutia vicinity presented in Yang & Busch (2009), Jin & Teoh (2011) proposed a minutia vicinity decomposition (MVD) technique to generate a template from a set of geometric invariant features, which conceals the location and orientation of a minutia.

Ahmad et al. (2011a) proposed a pair-polar-coordinate-based fingerprint template protection scheme that explores the relative relationship of minutiae in a rotation and shift-free pair-polar framework. Three invariant features are extracted from a pair of neighbor minutiae, i.e. radial distance, angle between orientation of reference minutia and the connecting edge of a neighbor minutia in the counter-clockwise direction, and angle between orientation of neighbor minutia and the connecting edge of the reference minutia in the counter-clockwise direction. Non-invertibility is achieved due to the many-to-one mapping relation. A random translation parameter is introduced to further distort the minutia distribution.

Wang & Hu (2012) proposed a cancellable fingerprint template based on a dense infinite-to-one mapping (DITOM). By refining the features considered in Jin et al. (2010a, 2010b), the proposed method elaborates three invariant features from a pair of minutiae. The three features are Euclidean distance between two minutiae, angle between the orientation of reference minutia and the direction of the line segment connecting the two minutiae, and angle between the orientation of neighbor minutia and the direction of the line segment connecting the two minutiae. The extracted features are then

quantized, hashed and binarized. Lastly, a complex vector is generated from the resultant bit-string by applying a discrete Fourier transform and the final template is obtained by blending the complex vector with a randomly generated parametric matrix. In addition to DITOM, Wang & Hu (2014) proposed another cancellable fingerprint template based on curtailed circular convolution, which demonstrates an improvement on accuracy and security over DITOM.

Recently, Multi-line Code or MLC proposed by Wong et al. (2013) is a minutia descriptor constructed based on multiple lines centered at a reference minutia. Firstly, a straight line is drawn following the direction of the reference minutiae and constructs a number of overlapped circles with a pre-defined radius. Then the neighbour minutiae are separated into different bins according to their orientation. Compute the mean of the distances between the centre of the circle and the included minutiae for each region. In the binarization stage, two techniques of binarzation methods are used, 1-bit and k-bits binarization. 1-bit binarzation is implemented based on a threshold while gray code is used in k-bits implementation.

In the category of indirect minutiae transform, other instances of cancellable templates for fingerprint minutia proposed in literature can be found as follows: Ahmad & Hu (2010), Ahmad et al. (2011b), Liu et al. (2012), Wang & Hu (2013), Yang et al. (2013).

From the above literature, following observations can be made: (a) Most of the afore-discussed "non-invertible transforms" are in fact susceptible to partial or full inversion (e.g. Ratha et al., 2007; Yang & Busch, 2009); (b) Despite the non-invertibility of the transform (e.g., many-to-one function), most reviewed schemes enjoy strong security while sacrificing the corresponding accuracy performance (Ratha et al., 2007; Tulyakov et al., 2007; Lee & Kim, 2010), thus demonstrating the inevitable security-performance trade-off; (c) Alignment is often required for accurate matching, e.g., Ratha et al. (2007); Ang et al. (2005); Nagar et al. (2010a, 2010b); (d) Most of the methods have yet to catch up the high accuracy compare to pure minutiae matching, e.g., Farooq et al. (2007), Jin et al. (2010), Wang & Hu (2012); (d) Some methods suffer from high computation cost and large storage for template, e.g., Farooq et al. (2007), Jin et al. (2010). All these indicate that fingerprint minutia-based cancellable templates are still immature and there are much room to improve.

2.2 Overview of Fingerprint Minutia-based Point-to-String Conversion Approaches

In this section, point-to-string conversion approaches proposed in the literature are revisited. These methods can be broadly divided into three categories: (1) reference-based approach; (2) histogram-based approach; and (3) spectral transform approach. In reference-based approach, a fixed-size reference, such as circumference of a circle (Sutcu et al., 2007a; Sutcu et al., 2007b), N random cuboids (Sutcu et al., 2008) is defined and then the biometric features are quantized into fixed-length representation. In

histogram-based approach, the fixed-length representation is generated based on the histogram, which is formed based on the tabulated frequencies of extracted features erected over discrete intervals on the extracted feature space. In the spectral transform approach, specific spectral transform technique, such as Fourier transform, is used to transform minutiae to corresponding domain, so that the fixed-length representation can be generated using specific analytical methods in that domain.

1) Reference-based Methods

Sutcu et al. (2007a, 2007b) proposed a geometric transformation to convert fingerprint minutiae into a fixed-length feature vector. This method uses the circumference of a circle as a reference and divides it into *m* equal-width arcs. For every minutia pair, a straight line passing through these two points and mark its intersections onto the circumference of the circle shown in Fig. 2.3. A *m*-dimensional integer feature vector is then constructed by counting the number of projected minutiae in the respective arcs. One limitation of this method is that the transformation is not rotation-invariant, thus the fingerprints have to be aligned before transformation. The additional information such as registration point (e.g. core or delta point) is required for aligning two fingerprint images to be matched. Furthermore, the analysis of minimum entropy on the resultant representation is absent. Thus, the security of the representation under different attack scenarios remains uncertain.

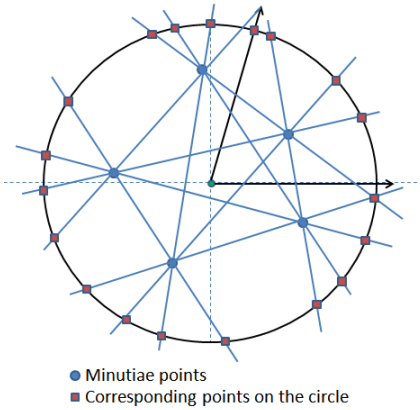


Fig. 2.3: Illustrates the geometric transformation from fingerprint minutiae proposed by Sutcu et al. (2007a, 2007b).

In another instance, namely local point aggregation, Sutcu et al. (2008) define a set of *m* random cuboids as reference on the fingerprint image and construct a *m*-dimensional integer feature vector using the number the minutiae points in each cuboid. The feature vector is then binarized into a bit-string using user-specific thresholds obtained from the median of population minutiae quantity within each cuboid. Yet, this method assumes that all fingerprint images has to be pre-aligned. For accuracy performance, the proposed method achieves a low error rate when the auxiliary information (i.e. the token to generate random cuboids) is stored securely. The overall process is demonstrated in Fig. 2.4. The proposed method achieves a low error rate when the helper data is stored securely. However, the security and privacy is underestimated in the event that helper data is stolen. Apart from this method, Jakubowski & Venkatesan (2007) proposed a randomized radon transform and Jin et al. (2009) proposed a random triangle hashing scheme. Both of these methods adopt a similar strategy in converting the minutiae representation into a discrete feature vector.

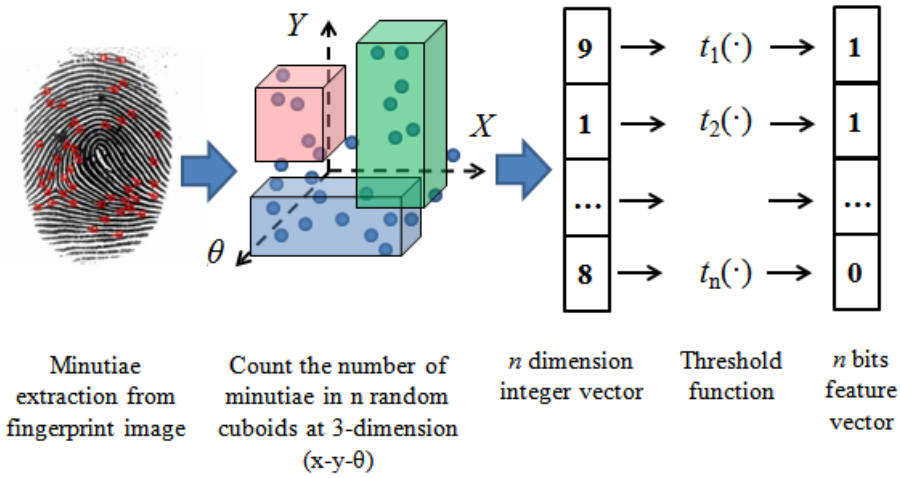


Fig. 2.4: Demonstrating the local point aggregation approach proposed by Sutcu et al. (2008).

Nagar et al. (2010b) consider a more robust set of features than Sutcu's approach (Sutcu et al., 2008) by considering the average minutia coordinate within a cuboid, the standard deviation of the minutiae coordinates, and the aggregate wall distance. This method offers high accuracy performance but it requires registration points (e.g. high curvature points) to align the fingerprint image prior to feature extraction. The detection of registration points can be challenging on poor-quality images.

Bringer & Despiegel (2010) generated a minutiae-vicinity-based binary feature vector, whereby a minutia vicinity is referred to as the neighbourhood structure around a central minutia within a pre-defined radius. This method extracts *N* number representative vicinities as reference using a vicinity selection procedure. With a number of minutia vicinities extracted from each fingerprint, each vicinity of the query template is matched against *N* number of vicinities of the enrolled template to identify the corresponding

enrolled vicinity to each query vicinity. Consequently, the matching score is concatenated to yield a fixed-length real-valued feature vector with N components and then binarized to a bit-string. Fig. 2.5 depicts the mechanism for obtaining a binary vector from a set representative vicinities and query vicinities. It is noted that the resultant bit-string is of around 50,000 bits long, which requires high storage capability.

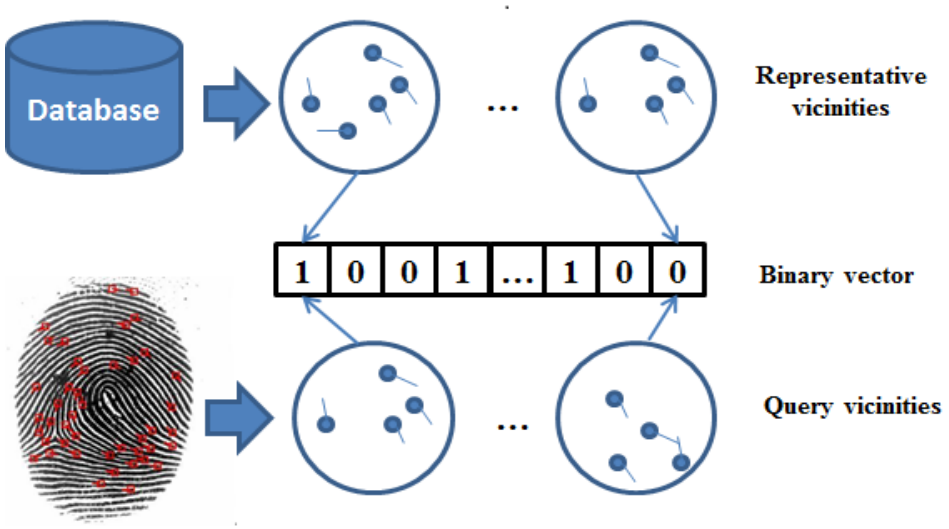


Fig. 2.5: Depicts the vicinity based mechanism proposed by Bringer & Despiegel (2010).

Liu et al. (2012) proposed a fixed-length feature representation by using a minutiae descriptor, namely Random local region descriptor (RLRD). RLRD adopts Tico's sampling structure (Tico & Kuosmanen, 2003) and take it as a reference. The RLRD is an orientation-based local structure, wherein a reference point is generated randomly and a set of uniformly random sampling points are generated along the circumference around the reference point. The order of sampling points is determined via a random seed. The RLRD feature is defined as the angle difference of local ridge direction between the sampling

point and reference point. For each sampling structure, a real-valued fixed-length vector can be generated since the number of sampling points is fixed. The real-valued RLRD feature vector can be further converted into a bit-string for secure sketches measured in the Hamming space. However, the registration point (core or highest curvature point) has to be used to align the enrolled and query images before further processing.

2) Histogram-based Methods

For the histogram approach, Farooq et al. (2007) generated a binary fingerprint representation based on the histograms of triangular features generated from minutiae triplets. Seven invariant features: length of three sides (A1, A2, A3,), three angles between each side and each minutia orientation (S1, S2, S3), and height (H) of the triangle are extracted and quantized into 24 bits, which yields a 2^{24}-bit binary string. Fig. 2.6 shows the main idea of the proposed scheme. However, this method requires high computational cost due to the exhaustive calculation of features for all possible minutiae triplets. Following this work, Jin et al. (2010b) attempted to reduce the length of bit-string by using minutiae pairs instead of minutiae triplets. Four invariant features, i.e. Euclidean distance between two minutiae, angular difference between two minutiae, two angles between minutia orientation and the segment connecting two minutiae, are extracted for histogram binning. Consequently, the size of template is reduced to 2^{18} and the performance is enhanced using a majority-voting-based training process.

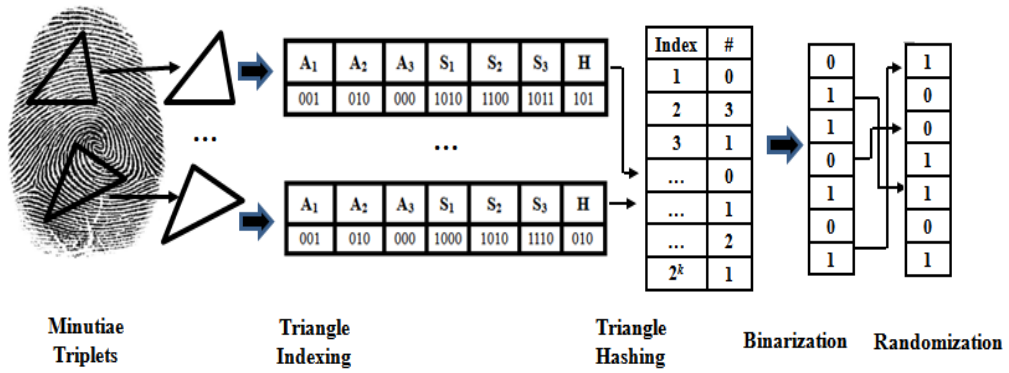


Fig. 2.6: The minutiae triplet based bit-string generation proposed by Farooq et al. (2007).

3) Spectral-Transform-based Methods

Xu et al. (2008) proposed a Spectral Minutiae approach to convert a set of minutiae into a fixed-length feature vector. The proposed approach performs Fourier transform on a minutia set and re-maps the Fourier spectral magnitude onto polar-logarithmic coordinate. By doing so, the spectral minutiae representation is invariant to rotation, shifting and scaling variations. An analytical representation for minutiae is further proposed to minimize error, which can directly be evaluated on polar-logarithmic grids. As the number of grids is fixed, a fixed-length representation can be derived. However, the accuracy of this approach over point-to-point (minutiae) and two-stage procedure matching (minutia descriptor) approaches is inferior.

Instead of using magnitude spectrum in Xu et al. (2008), Nandakumar use phase spectrum of minutiae, namely Binarized Phase Spectrum (BiPS) (Nandakumar, 2010). By incorporating fuzzy commitment and reliable bits selection for binarization techniques, BiPS achieves state-of-the-art accuracy

performance over other biometric cryptosystems. However, BiPS is not rotation-, shifting- and scaling-invariant. Hence, a proper alignment (focal point estimation) is still required.

From the revisit of the point-to-string conversion methods, several concerns can be outlined as follows: (a) Most of the existing point-to-string conversion methods have yet to catch up with the high accuracy of the state-of-the-art minutiae descriptor, i.e. MCC (Cappelli et al., 2010); (b) Most of the afore-discussed well-performed point-to-string conversion methods (Sutcu et al. (2007a, 2007b); Sutcu et al., 2008; Nagar et al., 2010); Liu et al., 2012; Nandakumar, 2010) rely on the pre-alignment or registration, which is not included in ISO minutia template (ISO/IEC 19794-2, 2005); (c) some methods either suffer from high computation cost (Farooq et al. 2007) or consume large storage for template (Bringer & Despiegel, 2010).

Due to the aforementioned concerns in the existing point-to-string conversion methods, it is required to design a high-performing point-to-string conversion method with ISO/ IEC 19794-2 complaint fingerprint minutia template.

2.3 Overview of Biometric Key Binding

In literature, fuzzy commitment (Juels & Wattenberg, 1999) and fuzzy vault (Juels & Sudan, 2006) are the two of most prominent key binding schemes. Fuzzy commitment (Juels & Wattenberg, 1999) is meant to accept input in the binary string form, e.g. iriscode (Daugman, 1999) while fuzzy

vault (Juels & Sudan, 2006) binds the cryptographic key using point-based biometric feature, such as fingerprint minutia.

Fuzzy commitment (Juels & Wattenberg, 1999) is originally designed to protect a cryptographic key and it is later being perceived as a technique for biometric template protection. Assume that the enrolled biometric template $\boldsymbol{B}$ is a *n*-bits binary string, in the enrolment stage (key binding), a codeword *c* is generated from the cryptographic key k_c of length *m* ($m < n$) with error correction code (ECC); the bit-length of *c* is then become identical to $\boldsymbol{B}$; then *c* is bit-wise XORed with $\boldsymbol{B}$ and renders *secure sketch* $y_c = c \oplus \boldsymbol{B}$. The y_c is stored in the database along with $\mathbf{h}(k_c)$, where $\mathbf{h}(.)$ is a hash function. In key release stage, the query biometrics b^q is XORed with y_c to obtain a corrupted codeword, $c^* = y_c \oplus \boldsymbol{B}' = c \oplus (\boldsymbol{B} \oplus \boldsymbol{B}')$. The c^* can be decoded to k^*, if the query bit-string is substantially similar to the enrolled template within the capacity of the ECC. The authentication is deem successful if $\mathbf{h}(k_c) = \mathbf{h}(k^*)$. A block diagram of fuzzy commitment is demonstrated in Fig. 2.7.

It has been pointed out that fuzzy commitment is *information-theoretical* secure only if the bits extracted from biometric features are uniformly and independently distributed (Zhou et al., 2011). Yet, it is hardly to fulfil in practice as biometric data are inherently structured and thus the features remain correlated even after go through feature extractor (Zhou et al., 2011). This will propagate to binary representation if binarization process is not carefully attended. Besides that, privacy leakage is another crisis of fuzzy commitment due to bits redundancy introduced by Error Correction Codes

(ECC) (Zhou et al., 2011; Ignatenko, 2009; Smith, 2004). The aforementioned pitfalls trigger various attacks such as decodability attack (Simoens et al., 2009; Kelkboom et al., 2011), statistical attack (Rathgeb & Uhl, 2011) and attack based on entropy analysis (Zhou et al., 2011).

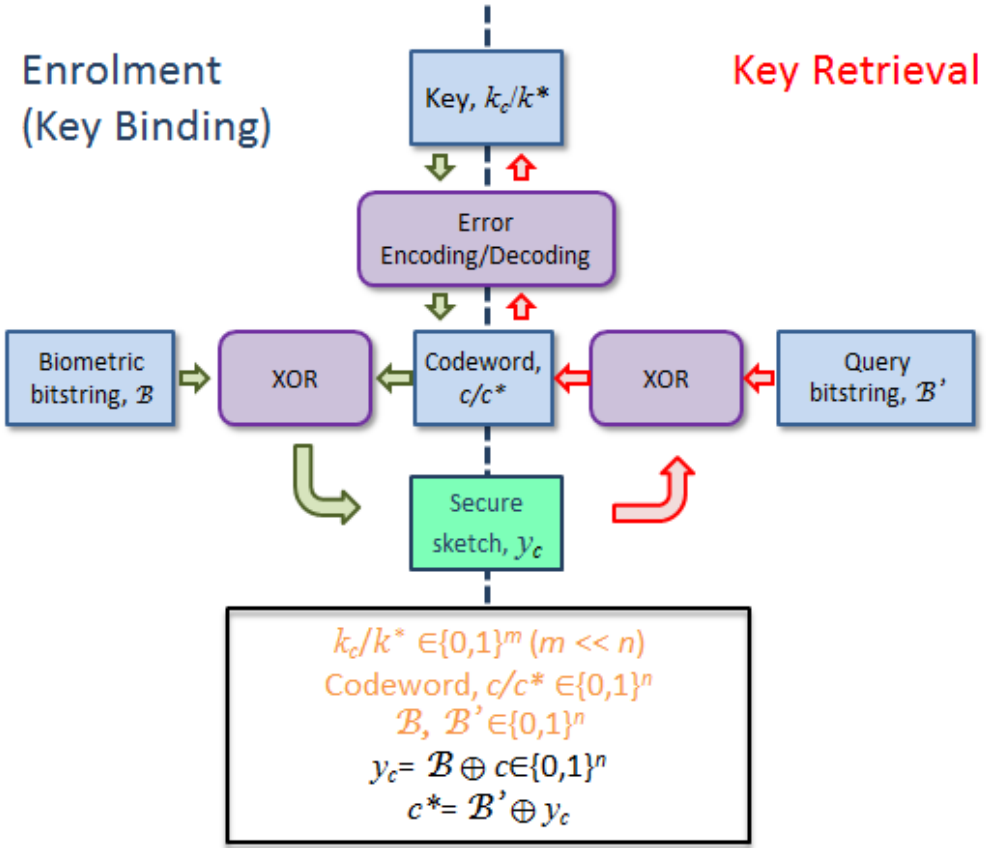


Fig. 2.7: A block diagram of fuzzy commitment.

Simoen et al. (2009) proposed a decodability attack on fuzzy commitment scheme that exploits the correlation of multiple secure sketches that generate from the same subject biometric data. Kelkboom et al. (2011) further analyzed the attack and proposed a bit-permutation mechanism against decodability attack. Assume that biometric features b_1^e, b_2^e are the two references of the same subject across two different applications; c_1 and c_2 are

the corresponding codewords. The secure sketch is obtained as $W_1^e = b_1^e \oplus c_1$ and $W_2^e = b_2^e \oplus c_2$. The attacker can perform $W_1^e \oplus W_2^e = (b_1^e \oplus b_2^e) \oplus (c_1 \oplus c_2) = (b_1^e \oplus b_2^e) \oplus c_3$. Such attack is initiated by the work of Carter & Stoianov (2008) that is to check whether decoding XOR of two secure sketches leads to a valid codeword. If positive, the two secure sketches are most likely derived from the same subject. So, if $b_1^e \oplus b_2^e$ is small (this is usually true if b_1^e, b_2^e are the samples of the same subject), the result of XOR operation will be close to valid codeword. $W_1^e \oplus W_2^e$ is then decodable with high probability. This attack is also known as Attacks via Record Multiplicity (ARM), where specifically outlined by Scheirer & Boult (2007) for fuzzy vault.

Rathgeb & Uhl (2011) proposed a statistical attack based on ECCs that is commonly applied in fuzzy commitment to retrieve the most likely codeword. The attack collects adequate imposter templates b_p and performs XOR successively with the stored secure sketch, $s = b_e \oplus c$ where b_e is the enrolled template and c is codeword, i.e. $b_p \oplus s$. Note that be is segmented into multiple chunks due to the computation speed. The XOR operation is thus on chunk-basis. Thereafter, the codeword of each chunk are collected and a histogram is generated by counting the occurrence frequency of codewords. A bin of histogram corresponding to the histogram maximum is considered as a success, which yields the most likely codeword for this chunk.

Zhou et al. (2011) analyzed the security and privacy leakage of fuzzy commitment thoroughly under the conditions whereby the practical biometric

data are not uniformly and independently distributed. To assess the security and privacy leakage, several evaluation metrics have been proposed: 1) the security can be measured by *average min-entropy, conditional entropy* and *conditional guessing entropy*; 2) privacy protection consists of irreversibility and privacy leakage. Irreversibility can be measured by the same metrics in security assessment while privacy leakage can be measured by *entropy loss* and *mutual information*. With these assessment metrics, Zhou et al. (2011) concludes that the fuzzy commitment is highly vulnerable on security and privacy leakage due to the dependency of biometric features.

Moreover, Scheirer & Boult (2007) introduce an attack, namely Surreptitious Key-Inversion Attack (SKI) on fuzzy vault, which is also an equivalently effective attack against fuzzy commitments. SKI refers to if the cryptographic key is known by an attacker, the biometric string that blended with codeword can be easily recovered through the XOR operation using the compromised cryptographic key and the secure sketch. Thus, the privacy leakage is inevitable.

Apart from that, fuzzy commitment suffers from limitations that associated with ECCs. Firstly, Nagar (2012) and Kelkboom et al. (2012) point out that fuzzy commitments suffers from security (key size) – performance (GAR) trade-off; i.e. the longer key size (higher security) results lower GAR and vice versa. In fuzzy commitments, a codeword is composed of key and redundant bits and it is known that the number of redundant bits is proportional to the error correction capacity. Therefore, the small number of

redundant bits, which implies weaker correction capacity, will lead to the larger key size, which meant better security. This is attributed to the requirement that the codeword size has to be matched to the size of biometric string and hence is fixed. Secondly, Bringer et al. (2008) showed that the maximum key length and the decoding accuracy are upper bounded by the error correction capacity of the chosen ECC.

Another drawback is since fuzzy commitments operates in hamming domain, it has imposed strict requirement on both feature representation (binary biometrics only is allowed) and matcher, i.e. Hamming distance (Dodis et al., 2004). This has severely limited the accuracy performance that can be accomplished as many effective feature extractors and matchers have to be abandoned.

In contrast with binary string used in fuzzy commitment, fuzzy vault (Juels & Sudan, 2006) binds the cryptographic key using points-based biometric feature, such as fingerprint minutia. In the enrolment stage of fuzzy vault, an *n*-order polynomial $P(\omega)$ is selected to encode the key k_c as the coefficients. The polynomial projection is then computed to embed the biometric feature $\boldsymbol{T}$ into a finite field. A large number of randomly generated chaff points *s* that do not lie on the selected polynomial $P(\omega)$ is added to constitute the protected point set. During the key extraction stage, a query unordered set $\boldsymbol{T'}$ is presented in order to retrieve the key k_c. The polynomial $P(\omega)$ can be reconstructed, only if $\boldsymbol{T'}$ overlaps with $\boldsymbol{T}$ substantially. Once the polynomial $P(\omega)$ is successfully reconstructed, secret key k^* can be

degenerated using error-correction coding. The security of fuzzy vault is relied on the hardness of polynomial reconstruction. A block diagram of fuzzy vault is illustrated in Fig. 2.8.

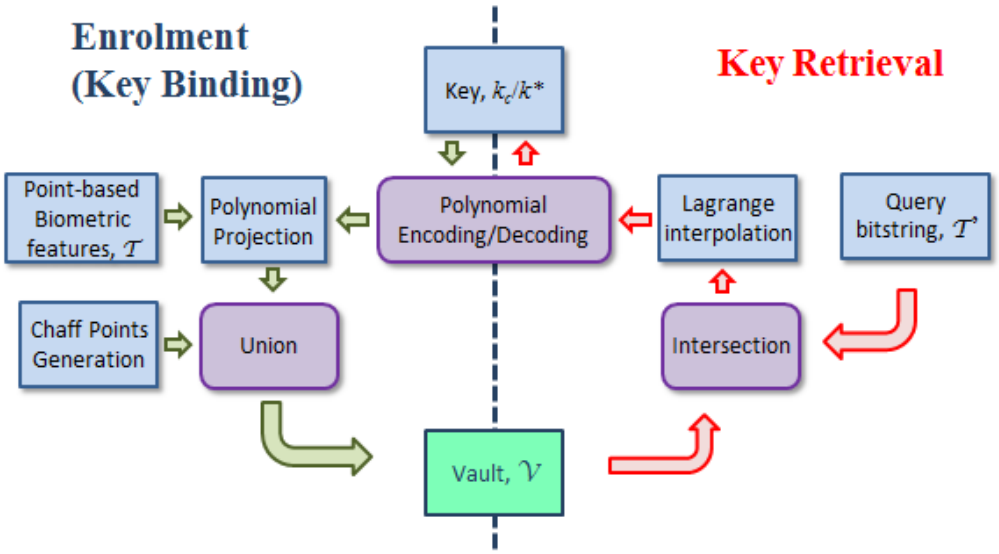


Fig. 2.8: A block diagram of fuzzy vault.

Several attacks against fuzzy vault also have been identified. Scheirer & Boult (2007) introduced three effective classes of attacks against fuzzy vault.

1) Multiple Templates Attack (MTA): Also known as Attacks via Record Multiplicity (ARM). If an attack can harvest multiple secure sketches with same biometric feature locked by different vaults across different applications, it may be possible to correlate the multiple set of vaults and retrieve the genuine minutia set.

2) Surreptitious Key-Inversion Attack (SKI): If the key is known by an attack, the biometric template (e.g. minutia set) that blended with chaff points can be easily identified through the restored polynomial.

3) Heterogeneity Attack: An ideal case is that the genuine and chaff points should be uniformly distributed so that no patterns of genuine and chaff points distribution can be detected. However, such assumption is hardly catered due to the dependency nature of biometric features.

From the aforementioned security and privacy issues of biometric key binding, four substantial observations can be summarized as follows:

(1) Inherent dependency of biometric features. Without considering such constraint, deployment of fuzzy commitment will lead to a significant security reduction and severe privacy leakage.

(2) Potentially poor accuracy performance due to the requirements of binary representation and matcher.

(3) Vulnerabilities that associated to ECCs such as performance-key size trade-off and statistical attack.

(4) Privacy attacks such as Decodability attack (ARM) and SKI attack.

2.4 Summary

In this chapter, literature review covered fingerprint minutia-based cancellable templates, fingerprint minutia-based point-to-string conversion and biometric key binding has been presented in detail. Although, these research topics have been studied extensively, it is observed that a number of

concerns in terms of the accuracy performance, alignment issue, and security, privacy attacks have yet been fully addressed and the overall performance of the existing works is still far from the satisfactory.

For a quick glance on the above literature review, three tables are provided below to summarize the characteristics of the proposed methods in the respective categories. Table 2.1 summarizes the fingerprint minutiae-based cancellable templates available in the literature. While, the characteristics as well as limitations of the state-of-the-arts for the fingerprint minutiae-based point-to-string conversion is given in Table 2.2. Table 2.3 is served as a comparison of the two well-known instances of biometric key binding schemes, i.e. fuzzy commitment and fuzzy vault.

From these enlightening works, the author greatly inspired from it and proposed: (1) two methods to generate the fingerprint minutiae-based cancellable templates presented in the chapter 3; (2) a kernel based point-to-string conversion for fingerprint minutia presented in chapter 4; (3) a new biometric key binding scheme along with cancellable transform presented in chapter 5.

Table 2.1: Summary of published research works on fingerprint minutiae-based cancellable templates.

Methods	**Key Technique**	**Distance**	**Alignment**	**Main drawback**
Direct minutiae transform				
Tulyakov et al. (2005)	Generating hash function	Hamming distance	No	Accuracy degradation

Ratha et al. (2007)	Surface-folding transform	Hamming distance	Yes	Template is invertible (Feng et al., 2008; Shin et al., 2009)
Lee et al. (2010)	Generating 3D array quantization	Normalized Hamming distance	No	Accuracy deteriorate in same PIN scenario
Jin et al. (2010a, 2010b)	Minutia pair histogram	Normalized Hamming distance	No	Accuracy sensitive to low quality image
Jin et al. (2012)	Polar Grid based 3-Tuple Quantization	Normalized Hamming distance	No	Large size of template
Yang & Busch (2009)	Minutia vicinity	Hausdorff distance	No	Attack complexity reduces to 2^{17} if random offsets table is known
Ferrara et al. (2012, 2014)	Protected minutia cylinder-code (P-MCC); two factors P-MCC	Normalized Hamming distance	No	Better hamming-distance preserved matcher is desired
Indirect minutiae transform				
Ang et al. (2005)	Generating random lines	Hamming distance	Yes	Partial minutia information leaked
Lee et al. (2007)	Construct user-specific transformation functions	Normalized set difference	No	Poor accuracy when images quality low
Nagar et al. (2010a, 2010b)	Cuboid-based feature extraction	Normalized Hamming distance	Yes	Requires registration point and ROI information
Farooq et al. (2007)	2^N quantization	Normalized Hamming distance	No	high computation cost and large storage for template
Ahmad et al. (2011a)	Construct pair-polar-coordinate	Normalized set difference	No	Relatively high error rate and vulnerable to ARM
Wang & Hu (2012)	Dense infinite-to-one mapping	Normalized Euclidean distance	No	Large size of user-specific key and vulnerable to ARM
Wong et al. (2013)	Multi-line Code	Dice, NWAZZOO, DWID distances	No	Standalone MLC is not robust for bio-crypto systems

Table 2.2: Various fixed-length minutia-based representations.

Methods	Proposed techniques	Type	Main limitations
Reference-based approach			
Sutcu et al. (2007a, 2007b)	Geometric Transformation	Integer	Require pre-alignment before transformation; Absence of minimum entropy analysis
Sutcu et al. (2008)	Local Point Aggregation	Binary	Requires pre-alignment; Performance in lost auxiliary information case is unknown
Nagar et al. (2010b)	Local Point Aggregation	Binary	Requires pre-alignment and additional information (e.g. boundary of ROI)
Bringer & Despiegel (2010)	Minutia vicinity-based Histogram	Binary	Requires high storage capability for template
Liu et al. (2012)	Random Local Region Descriptor	Real	Requires pre-alignment
Histogram-based approach			
Farooq et al. (2007)	Minutiae Triplet based Histogram	Binary	Requires high storage capability for template and high computational cost
Jin et al. (2010b)	Minutiae Pair based Histogram	Binary	Re-train is required when new user is enrolled
Spectral Transform approach			
Xu et al. (2008)	Spectral Minutiae	Real	Accuracy over classic minutiae matching is unsatisfied
Nandakumar (2010)	Binarized Phase Spectrum (BiPS)	Binary	Requires pre-alignment

Table 2.3: Comparison of fuzzy commitment and fuzzy vault.

Characteristics	Fuzzy Commitment	Fuzzy Vault
Representation	Fixed-length binary string	Varied-size point-based sets
Merits	Intra-users variation tolerance via ECC; Generating compact size of secure sketch;	Intra-users variation tolerance via ECC; Ability to secure point-based features (e.g. fingerprint minutia);
Limitations	Security-GAR trade-off, non-revocable, helper data needs to be carefully designed, difficult to find perfect codes for designed code length	Security-GAR trade-off, non-revocable, helper data needs to be carefully designed, difficulty to generated large number of chaff that are distinguishable to genuine points
Parameters	Key length L, length of codeword N, and error correcting capacity of the code	Polynomial degree (k), size of the template set (r), and number of chaff points (q)
Security-GAR tradeoff	Higher values of (L/N) lead to lower GAR, but higher security and vice versa	Higher values of (k/r) and q lead to lower GAR, but higher security and vice versa
Possible Attacks	Decodability attack (Simoens et al., 2009; Kelkboom et al., 2011), Statistical attack (Rathgeb & Uhl, 2011), Attack on entropy analysis (Zhou et al., 2011), Surreptitious Key-Inversion (SKI) (Scheirer & Boult, 2007)	Attacks via Record Multiplicity (ARM), Surreptitious Key-Inversion (SKI), Blended Substitution Attacks (BSA) (Scheirer & Boult, 2007)
Implementation for Fingerprint	Bringer et al. (2008)	Nandakumar et al. (2007), Yang & Verbauwhede (2005)

CHAPTER 3

MINUTIAE-BASED CANCELLABLE FINGERPRINT TEMPLATES

Cancellable biometrics is truly meant designed for biometric template protection. Following this approach, in this thesis, two methods to generate fingerprint minutiae-based cancellable template, namely two-dimensional random projected minutia vicinity decomposition (2D-RP-MVD) and randomized graph-based hamming embedding (RGHE) are proposed to protect fingerprint minutiae. For the former, 2D-RP-MVD extends the original 1D random projection used in Biohash (Teoh et al., 2004) to a 2D feature representation, dubbed as minutia vicinity decomposition (MVD). MVD represents a set of 2D geometrical invariant features that implies the coordinates and orientation of minutia is concealed. Thus, the problem that minutiae location and orientation can be highly likely exposed from the minutia vicinity construct (Yang & Busch, 2009) is alleviated significantly. For the later, i.e. RGHE, minutia vicinity decomposition (MVD) is also adopted to generate a set of randomized geometrical invariant features using random projection. The randomized MVD is then embedded into a Hamming space by means of Graph-based Hamming Embedding. Due to the highly non-linear equation system provided by RGHE, the generated template can be strongly protected against inversion. The experimental results and security analysis are discussed in depth at the subsequent sections.

3.1 Introduction

Traditionally, reconstructing a fingerprint image from its minutiae set was thought to be infeasible, i.e. minutia is non-invertible to fingerprint image. However, this hypothesis has been overthrown when Hill (2001) demonstrated the first template inversion scheme for fingerprint. Since Hill's attempt, a number of efficient methods have been proposed to reconstruct fingerprint image from minutiae efficiently (Ross et al., 2007; Cappelli et al., 2007; Feng & Jain, 2011). Due to the feasibility of minutia inversion, it is no longer secure to store the original minutiae as a biometric template. As a solution, a layer of protection (non-invertible transform) is applied to convert the original minutiae into a new representation. However, it is noticed that the accuracy performance is generally deteriorated when the non-invertible transform is applied (Ratha et al., 2007; Nagar et al., 2010c; Simoens et al., 2012). Thus, it remains being a challenging task to preserve the accuracy performance when the non-invertible transform is applied.

Cancellable biometrics has been demonstrated as one of the efficient and effective solution for biometric template protection (Ratha et al., 2007; Jain et al., 2008). In this chapter, two methods to generate fingerprint minutiae-based cancellable template, namely two-dimensional random projected minutia vicinity decomposition (2D-RP-MVD) and randomized graph-based hamming embedding (RGHE) are proposed in Section 3.2 and Section 3.3 respectively. Summary is given in Section 3.4.

3.2 Two-Dimensional Random Projected Minutia vicinity Decomposition (2D-RP-MVD)

Yang & Busch (2009) proposed a cancellable fingerprint template based on minutia vicinity. Despite of the protected minutia vicinity representation salted by random offsets are claimed non-invertible, Simoens et al. (2010) pointed out that if an adversary has the knowledge in orientation vectors and random offsets, the coordinates and orientations of minutia in Yang & Busch's proposal (2009) are likely to be revealed. Furthermore, it is computed that only 2^{17} attempts are required for an attack when the random offsets table is known with reference to 2^{120} attempts when the random offsets table is not known (Simoens et al., 2010).

To rectify the highly likely revelation of the minutia location coordinates in Yang & Busch (2009), a two-dimensional random projected minutia vicinity decomposition (2D-RP-MVD) method is proposed to generate fingerprint minutiae-based cancellable template. Fig. 3.1 shows the block diagram of the minutia vicinity decomposition (MVD) with random projection (RP). Firstly, minutia vicinity formed from a set of fingerprint minutiae is decomposed into four minutia triangles. A set of geometric invariant features such as the *length* between two adjacent minutiae, *orientation difference* etc. MVD is then extracted, thus the location and orientation of a minutia is concealed in the stored template. This alleviates the problem of minutia location exposure found in Yang & Busch (2009); and then MVD feature is projected (i.e. inner product) onto a random space with a user-specific token. The 2D random projection provides three advantages:

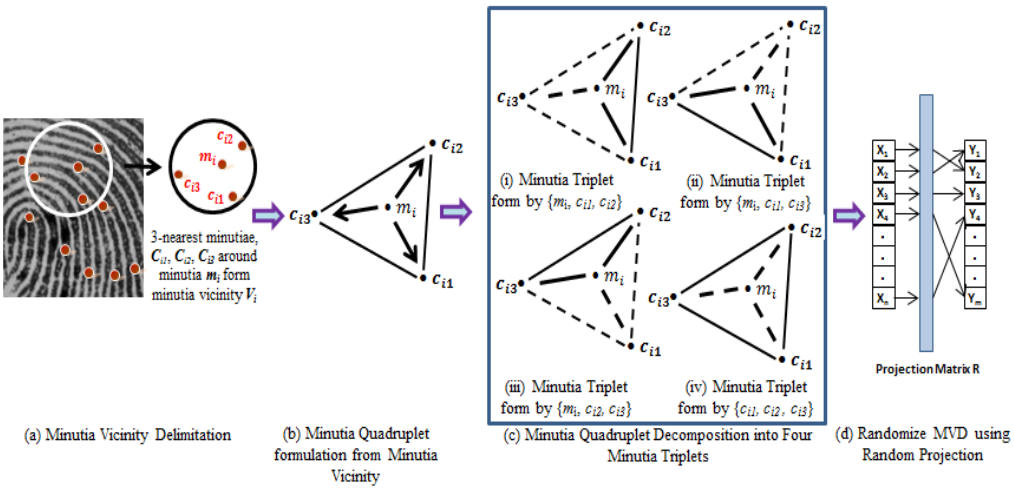


Fig. 3.1: Block diagram of minutia vicinity decomposition (MVD) with random projection (RP).

(1) Cancellability – a new template, in this proposal, can be easily generated by changing an external and independent token.

(2) Enhanced non-invertibility – instead of using minutia information, i.e. location and orientation of minutia, in Yang & Busch (2009), the employment of geometric invariant features increases the difficulty to recover the original minutia significantly.

(3) 2D feature matrix adaption - the original random projection (RP) used in Biohash (Teoh et al., 2004; Teoh et al., 2006) is merely for a one-dimensional fixed length feature vector, which is not applicable for the MVD feature matrix. Note the MVD feature matrix is of varied size, i.e. $N \times 36$ where N denotes the number of minutia vicinity found in fingerprint image. Therefore, a 2-dimensional random projection mechanism is designed as an extension of the original random projection (Teoh et al., 2004; Teoh et al.,

2006). The 2D random projection is well fit for the situation, wherein the feature matrix is size varied and an exhaustive matching procedure is required.

3.2.1 Minutia Vicinity Decomposition (MVD)

Minutia vicinity decomposition (MVD) presented in (Jin & Teoh, 2011) can be described as follows. Given a set of fingerprint minutiae, $\{m_i | i = 1, \ldots, N\}$, a minutia vicinity V_i is defined as m_i together with three (3) nearest neighboring minutiae c_{i1}, c_{i2}, c_{i3} (measured in Euclidean distance), i.e. $V_i=\{m_i,c_{i1},c_{i2},c_{i3}|i=1,\ldots,N\}$. Each minutia vicinity is then decomposed into four minutiae triplets $\{T_{ir}|i=1,\ldots,N, r=1, 2, 3, 4\}$. The nine features, the length of three sides, the three internal angles and the relative orientation between two adjacent minutiae shown in Fig. 3.2 are selected as the invariant features. Hence, a feature vector consists of nine features, which can be described as follows:

$$\boldsymbol{u}_r = (s_1, \alpha_1, \Delta o_1, s_2, \alpha_2, \Delta o_2, s_3, \alpha_3, \Delta o_3) \quad (3.1)$$

$$r=1,\ldots,4$$

where s_1, s_2, and s_3 denote the length of the three sides in pixel; α_1, α_2 and α_3 represent the internal angles measured in degree; $\Delta o_1=|o_1 - o_2|$, $\Delta o_2=|o_2 - o_3|$, and $\Delta o_3=|o_3 - o_1|$ denote the relative orientation between two adjacent minutiae, where o_1, o_2, o_3 are the orientations for minutiae m_1, m_2, m_3, respectively.

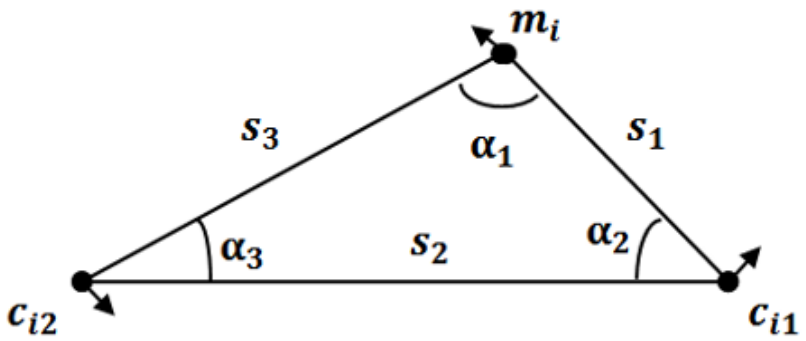


Fig. 3.2: Invariant features extraction from minutia triplet.

Recall the equation in eq. (3.1) that the features extracted from a single minutiae triplet form a 9-dimensional vector $\boldsymbol{u_r}$. By concatenating four 9-dimensional vectors from the four minutiae triples of a minutia vicinity together, a vector $\boldsymbol{u} = [\boldsymbol{u}_1\ \boldsymbol{u}_2\ \boldsymbol{u}_3\ \boldsymbol{u}_4]$ of 36 feature components for a minutia vicinity is obtained.

The above process is repeated for the entire vicinity set (say *N* times) and consequently, the entire MVD features are stored in a matrix, $\boldsymbol{U}$ of size *N* × 36.

However, MVD representation is a set of local features; it is irrevocable in the event of compromise. Therefore, another layer is required to make the MVD feature revocable and diversity. In this thesis, a two-dimensional random projection is devised for such purpose and this is described in the Section 3.2.2.

3.2.2 Randomizing Minutia Vicinity Decomposition (RMVD)

The feature matrix $\boldsymbol{U} \in \mathbb{R}^{N\times 36}$ represents a set of minutia vicinity containing the nearest neighborhood structure and the distance defined in the Euclidean space. $\boldsymbol{U}$ is projected onto a sequence of random subspace determined by an externally-derived pseudorandom sequence. This task can be done via a 3-step algorithm as follows:

- Step (1). Use a token to generate a pseudo random matrix, $\{\boldsymbol{r}_i \in \mathbb{R}^P | i = 1,2,\dots,36\}$ and transform the matrix into an orthonormal matrix $\{\boldsymbol{r}_{\perp i} \in R^P | i = 1,2,\dots,36\}$ by applying the Gram–Schmidt process (Arfken & Weber, 1985). With this, an orthonormal matrix, $\boldsymbol{R} = [\boldsymbol{r}_{\perp 1},\dots,\boldsymbol{r}_{\perp 36}] \in \mathbb{R}^{36\times P}$, $\boldsymbol{P} \leq 36$ can be formed.

- Step (2). Normalize the feature matrix $\boldsymbol{U} \in \mathbb{R}^{N\times 36}$. Let $\boldsymbol{u}^n$ be the *n*-th row of $\boldsymbol{U}$, which represents the 36-dimensional feature vector generated from the *n*-th vicinity (out of *N* vicinities). The normalized feature matrix is denoted as $\bar{\boldsymbol{U}}$, where $\|.\|$ is referred to the Euclidean norm.

$$\overline{\boldsymbol{u}_i^n} = \frac{\boldsymbol{u}_i^n}{\|\boldsymbol{u}^n\|} \tag{3.2}$$

i = 1,…,36 and n = 1,…,N

- Step (3). Compute the randomized feature vector **W** using the following equation:

$$\mathbf{W} = \bar{\boldsymbol{U}}\boldsymbol{R} \in \mathbb{R}^{N\times P} \tag{3.3}$$

where the same $\boldsymbol{R}$ for each user will be used in both enrolment and verification stage. Further, $\boldsymbol{R}$ is determined by a user-specific token that can be either stored in the system or carried by the user depending on the specific applications. It is noted that the user-specific tokens refer to the distinctive tokens assigned to each user, which are used to generate distinctive $\boldsymbol{R}$ to perform random projection described above.

It is noted, since $\boldsymbol{P} \leq 36$, the size of the feature matrix after random projection is less than or equal to the one before random projection. The smaller number of *P*, the more dimensions reduced and vice versa. A low dimension feature vector provides a better irreversibility protection as the less structure information of the feature vector is preserved (Teoh & Chong, 2007; Liu et al., 2006). The performance-irreversibility trade-off on *P* will be presented experimentally in Section 3.2.4.1.

3.2.3 Matching

Matching two randomized minutia vicinity decomposition templates is performed in randomized domain, i.e. randomized MVD representation. The matching process is described as follows: given two randomized MVD templates with different sizes; matching is to search the two most similar randomized minutiae vicinities. Let $\mathbf{W}_e^n = [\boldsymbol{w}_{e1}^n\, \boldsymbol{w}_{e2}^n\, \boldsymbol{w}_{e3}^n \boldsymbol{w}_{e4}^n]$ and $\mathbf{W}_q^m = [\boldsymbol{w}_{q1}^m\, \boldsymbol{w}_{q2}^m\, \boldsymbol{w}_{q3}^m \boldsymbol{w}_{q4}^m]$ be the 36-dimensional (9×4) feature vectors which are generated from *n*-th and *m*-th vicinity respectively. The matched pair scores, p_{ij} of $\mathbf{W}_e^i$ and $\mathbf{W}_q^j$ can be determined using eq. (3.4) and a matrix $\mathbf{P} = [p_{ij}]$ with size $N \times M$ can be formed thereafter.

$$p_{ij} = \min(\left\| \boldsymbol{w}_e^i , \boldsymbol{w}_q^j \right\|) \tag{3.4}$$

$$i = 1,\ldots, N \text{ and } j = 1,\ldots, M$$

where ||.|| denotes the Euclidean distance between $\boldsymbol{w}_e^i$ and $\boldsymbol{w}_q^j$.

Next, we store the *minimum value* for each row in **P**, denoted as a_i.

$$a_i = \min_j(\mathrm{P}_{ij}) \tag{3.5}$$

$$i = 1,\ldots, N \text{ and } j = 1,\ldots, M$$

The score a_i calculated is only the minimum value for each row in P which represents the similarity of the two vicinities. However, the total number of vicinities extracted from different fingerprint images (even from the same finger) may be varied enormously. Thus, the score, a_i may not reflect the truly similarity between two fingerprint templates. Hence, the matching score should be normalized as follows:

$$s = \frac{\sum_{i=1}^{N}(a_i < t)}{\sqrt{N \times M}} \tag{3.6}$$

where *t* is a pre-defined threshold that is empirically established to determine a pair of genuine vicinity. Hence, the score obtained is real where a score is toward '0' indicates a strong mismatch and otherwise. *N* and *M* are the numbers of minutiae found in query and enrolled fingerprint images.

3.2.4 Experiments

The experiments are carried out using two public fingerprint databases: FVC2002 (DB1, DB2, DB3 and DB4) (Fingerprint Verification Competition, 2002) and FVC2004 DB2 (Fingerprint Verification Competition, 2004); each data set contains 100 fingerprints and each fingerprint has 8 different

impressions. Minutiae points used in this experiment are extracted using the commercialized fingerprint recognition software, VeriFinger 7.0 SDK (VeriFinger SDK). Six performance indicators are used to evaluate the proposed method as abbreviated below:

- FAR – False Acceptance Rate
- FRR – False Reject Rate
- EER – Equal Error Rate
- GD – Genuine distribution
- ID – Imposter distribution
- ROC – Receiver Operating Characteristic

Two experimental protocols are applied as follows: (1) 1 vs 1: the first and second impressions of images in the data set are used as gallery and probes respectively. Hence, the matching process yields 5,050 matching scores, which comprises 100 and 4,950 genuine and imposter scores respectively. This strategy provides a benchmark for comparing the proposed method with other methods using the same strategy in literature (Yang & Busch, 2009; Ahmad et al., 2011; Wang & Hu, 2012; Wang & Hu, 2014); (2) FVC: standard experimental protocol for fingerprint verification competition is applied, where each impression is matched against the remaining impressions of the same identity to compute the false reject rate (FRR) while the first impression of each identity is matched against the first impression of the remaining identities to compute false acceptance rate (FAR). This protocol yields 2,800 genuine score and 4,950 imposter scores respectively. Generally this protocol is to evaluate the robustness of the proposed method.

3.2.4.1 Accuracy Performance

For performance evaluation, two scenarios, genuine-token and stolen-token scenario are carried out. For the genuine-token scenario, it is assumed that the secret token is securely stored, so each randomized MVD is salted by a random matrix determined by the user-specific token as shown in eq. (3.3). On the other hand, in the stolen-token scenario, the genuine user lost his/her token; therefore, the randomized MVDs are matched using an identical token.

For genuine-token scenario, the performance results in terms of EER for all datasets are ideal (i.e. the EERs are close to 0). This indicates that all users can be correctly verified and no impostor will be falsely accepted under this scenario given an appropriate threshold for the matching score. Good performance is attributed to the binding of the external token with the biometric features, which increases the dissimilarity between different users tremendously.

Considering stolen-token scenario, a token is generated in advance and this token is assigned to all users. The accuracy performance is computed by comparing the templates from all the 100 users with the same external token.

From the Table 3.1, it can be observed that approximately, the equal error rate of 1.02%, 0.98%, 16.15%, 15.98% and 17.75% for FVC2002 (DB1, DB2, DB3, DB4) and FVC2004 DB2 in 1 vs 1 protocol scenario are achieved while the equal error rate of 6.12%, 5.69%, 29.83%, 16.70% and 20.30% in FVC protocol scenario are obtained approximately. From the Table 3.1, it also can be observed that the performances on FVC2002 DB1 and DB2 are better

than the performance on FVC2002 DB3, DB4 and FVC2004 DB2 in both 1vs1 and FVC protocols. This is due to the relatively good quality of fingerprint image for FVC2002 DB1 and DB2 whereas the quality of image for other fingerprints data sets is poor in terms of large elastic deformation, presence of partial image etc. Further, it is noticed that the performance for 1 vs 1 protocol is better than the performance using FVC protocol. This is expected because the quality of images used in 1 vs 1 protocol (i.e. 1st and 2nd image of each identity) is better compare to the quality of the rest images for the same identity (Ahmad et al., 2011; Wang & Hu, 2012).

Table 3.1: Accuracy Performance in terms of EER (%) for two experiment protocols in stolen-token scenario for FVC2002 and FVC2004.

Experiment Protocols	Equal Error Rate (EER) (%)				
	FVC2002 DB1	FVC2002 DB2	FVC2002 DB3	FVC2002 DB4	FVC2004 DB2
1 vs 1	1.02	0.98	16.15	10.46	17.75
FVC	6.12	5.69	29.83	16.70	20.30

A performance comparison between the proposed method and the existing representative methods is carried out and summarized in Table 3.2. It can be observed that in FVC2002 DB1 and DB2, the proposed method outperforms the existing methods (Tulyakov et al., 2007; Yang & Busch, 2009; Yang et al., 2010; Nagar et al., 2010b; Bringer & Despiegel, 2010; Ahmad et al., 2011; Wang & Hu, 2012; Wang & Hu, 2014). Further, it can be justified that the performance of Yang & Busch (2009) would be deteriorated if the selected direction may be likely based on a spurious minutia and the

further shifting of the rest of minutiae are distorted severely. Therefore, such resultant template reduces the overall performance. However, the performance of the proposed method underperforms Wang & Hu (2012) and Wang & Hu (2014) in FVC2002 DB3. This is because the nearest neighbour structure (i.e. MVD) employed in the proposed method is not robust against missing or spurious minutiae that are occurred in FVC2002 DB3 data set more frequently.

Table 3.2: Performance comparison with state-of-the-arts using 1 vs 1 protocol in stolen-token scenario for FVC2002 DB1 and DB2.

Methods	EER (%)				
	FVC2002 DB1	FVC2002 DB2	FVC2002 DB3	FVC2002 DB4	FVC2004 DB2
***Proposed (2013)**	**1.02**	**0.98**	**16.15**	**10.46**	**17.75**
Tulyakov et al., (2007)	3	-	-	-	-
Yang & Busch (2009)	-	avg. 4.04 (genuine-token)	-	-	-
Yang et al., (2010)	-	Best case: 0.72 Worst case: 2.23	-	-	-
Nagar et al., (2010b)	-	3	-	-	-
Bringer & Despiegel (2010)	-	5.3	-	-	-
Ahmad et al.	9	6	27	-	-

(2011)					
Wang & Hu (2012)	3.5	4	7.5	-	-
Wang & Hu (2014)	2	2.3	6.12	-	-
Before RP	2.13	1.24	12.28	15.05	18.89

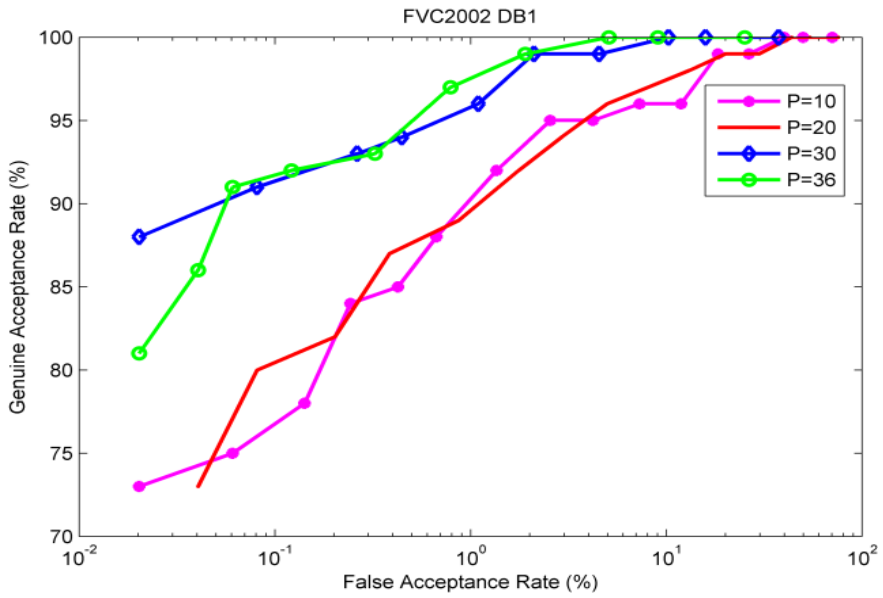
'-' Denoted that results are not reported in the original paper.
'*' EERs are not identical to the paper published in Jin et al., (2014) due to the latest feature extractor used for minutia extraction.

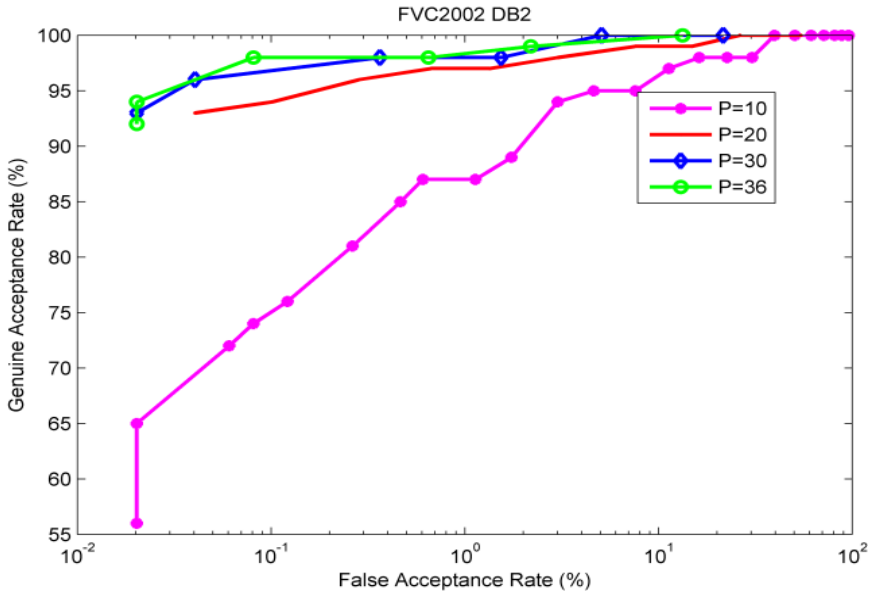
Besides, since the random projection is employed in Wang & Hu (2012) and the proposed method, back projection (Yang et al., 2010) has been demonstrated as a feasible method for template inversion. The analysis of the non-invertibility needs to be carefully justified. The non-invertibility analysis for the proposed method is presented in Section 3.2.4.3.

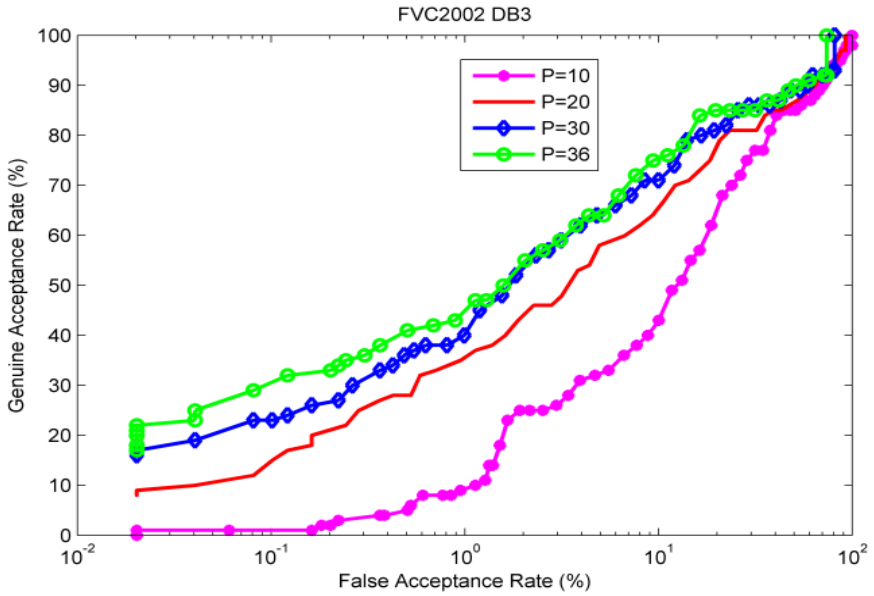
The performance in stolen-token scenario using different dimensions (*P* value) as discussed in Section 3.2.2, varying from 10 to 36, is further investigated. Table 3.3 displays the equal error rate with respect to the different number of *P* (dimensions). It can be observed that with the decrease of dimensions, the performance deteriorates gradually. This can be understood that the more dimensions reduced, the less ability of preserving the structure, which causes the performance degradation. Fig. 3.3 shows the receiver operating characteristics (ROC) curves that serve as a comparison among the performance using different number of dimensions.

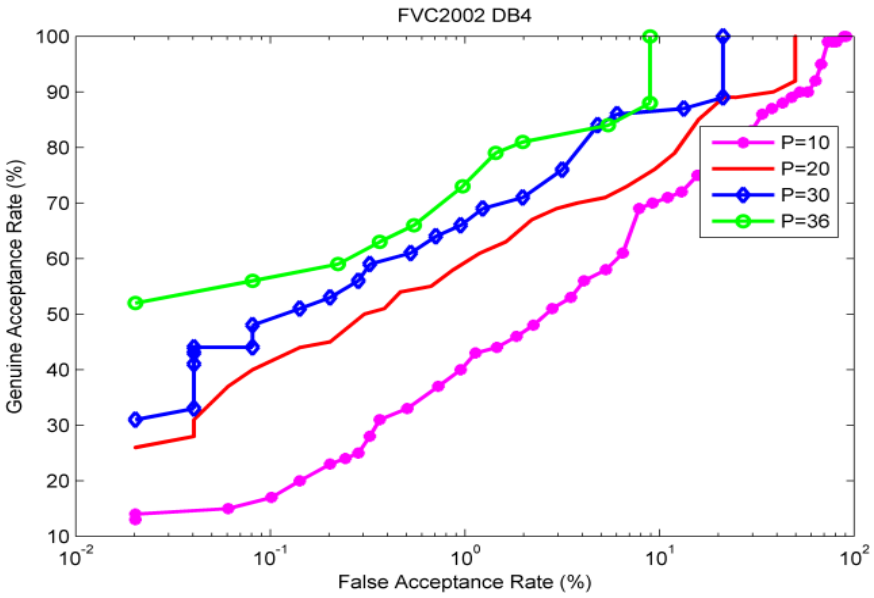
Table 3.3: Display the performance with respect to different dimensions (*P*) for FVC2002 (DB1-DB4) and FVC2004 DB2 databases.

# of Dimensions (*P*)	**36**	**30**	**20**	**10**
EER (%) for FVC2002 DB1	1.02	1.92	3.97	5.02
EER (%) for FVC2002 DB2	0.98	1.77	2.83	4.97
EER (%) for FVC2002 DB3	16.15	19.01	20.99	26.98
EER (%) for FVC2002 DB4	10.46	13.15	15.10	20.09
EER (%) for FVC2004 DB2	17.75	18.99	21.43	24.98




FVC2002 DB2
Genuine Acceptance Rate (%)
False Acceptance Rate (%)
P=10
P=20
P=30
P=36


FVC2002 DB3
Genuine Acceptance Rate (%)
False Acceptance Rate (%)
P=10
P=20
P=30
P=36


FVC2002 DB4
Genuine Acceptance Rate (%)
False Acceptance Rate (%)
P=10
P=20
P=30
P=36

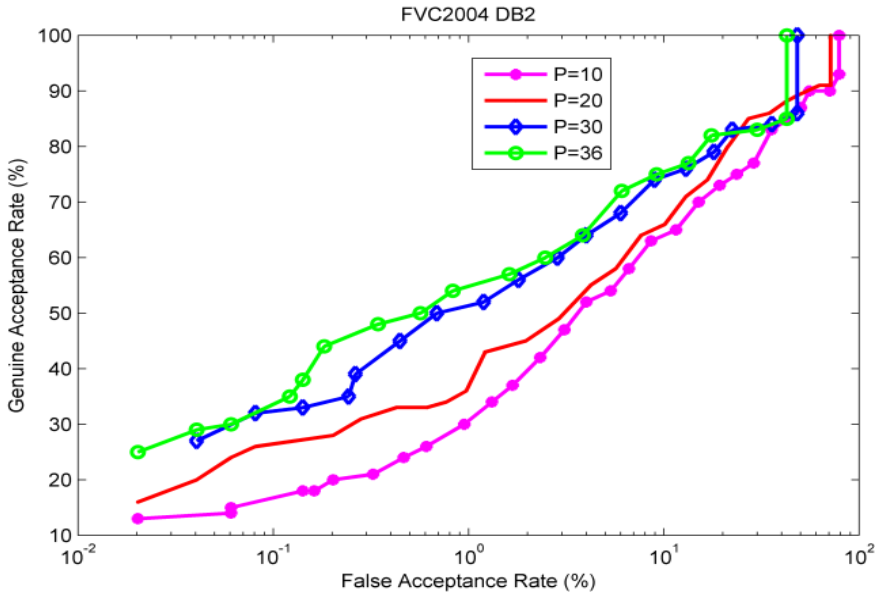
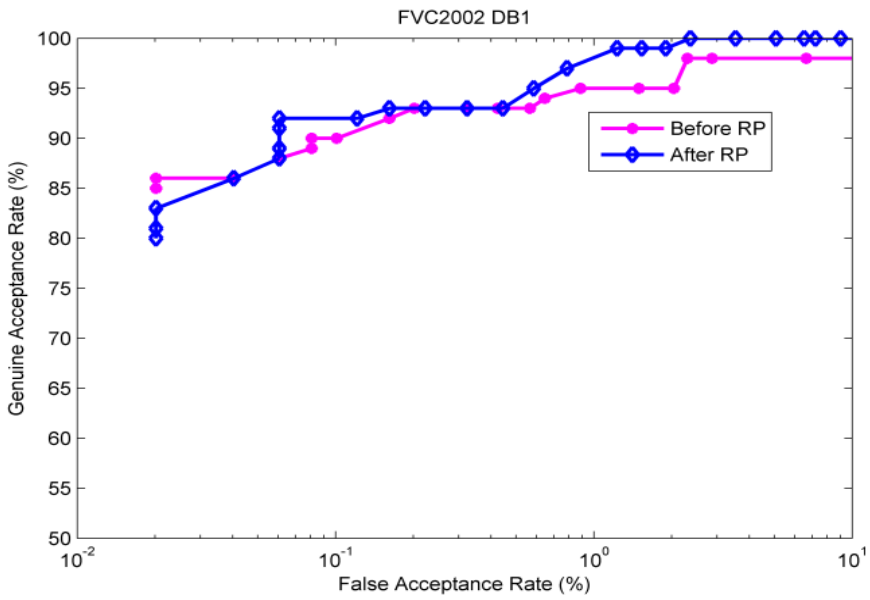
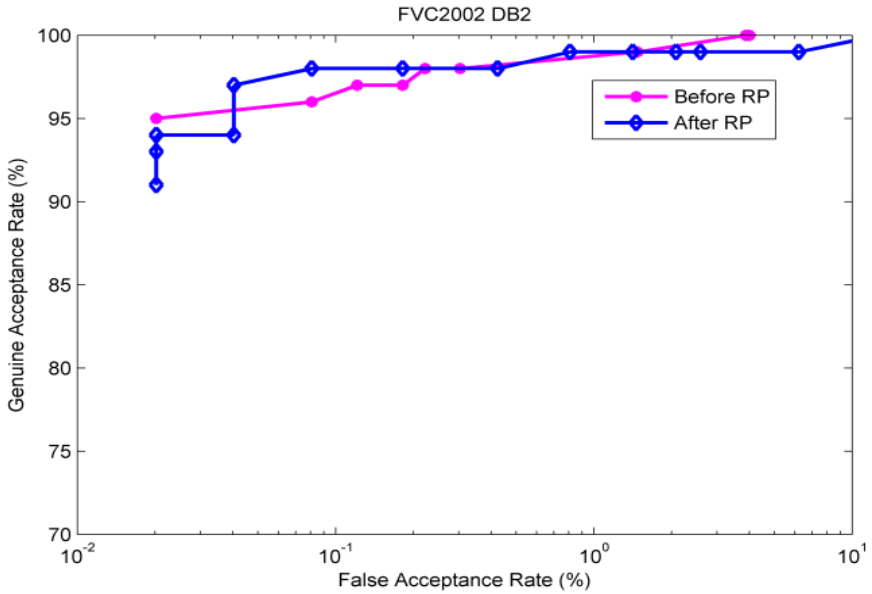


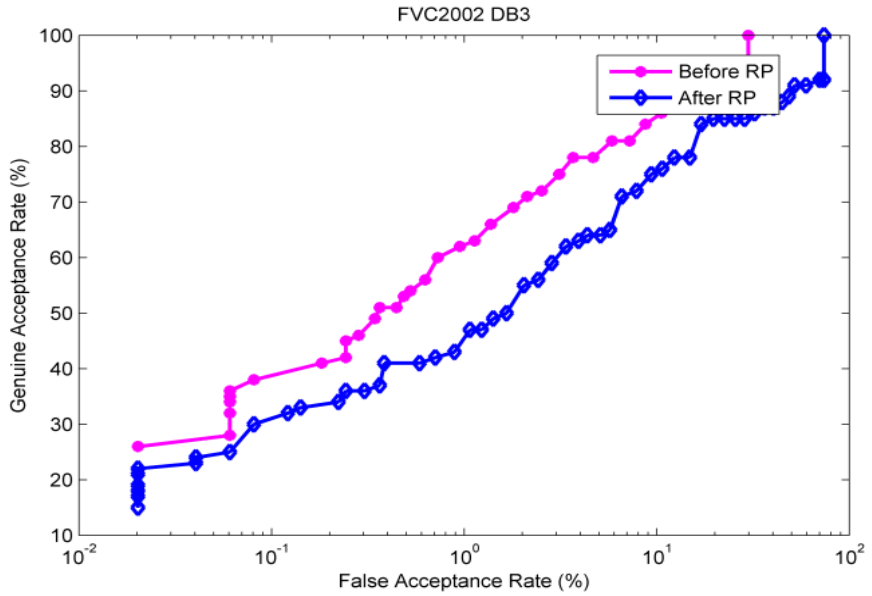
Fig. 3.3: ROC curves serves as a comparison among the performance based on different dimensions *P* using 1 vs 1 protocol in stolen-token scenario.

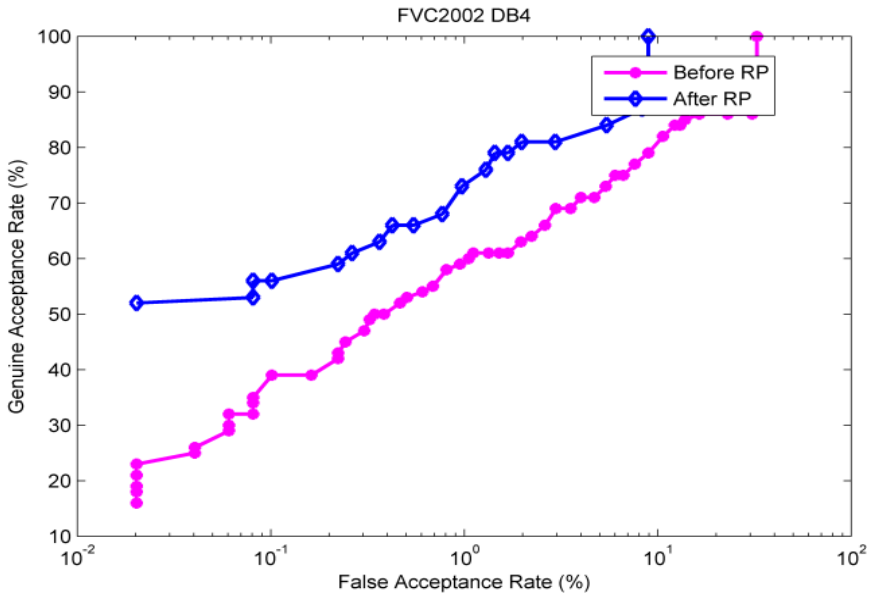
The best performances (1.92%, 1.77%, 19.01%, 13.15% and 18.99% of EER) is achieved when the dimensionality is reduced to 30, which resembles the corresponding performance obtained before random projection (2.13%, 1.24%, 12.28%, 15.05% and 18.89% of EER), very close in DB2 and even better for DB1, thus signifying a good preservation of the actual MVD neighborhood structure after the projection. Fig. 3.4 demonstrates the corresponding ROC curves of before 2D random projection and after random projection at P = 30. In this figure, the good preserving of MVD neighborhood structure by random projection FVC2002 and FVC2004, respectively, can be seen.

Apart from above, the proposed method pays a less storage for the resultant template over the minutia triplet-based instance presented in Farooq et al., (2007). Assume there are N minutiae extracted in a fingerprint image, consequently, the template size of the proposed method is of N×36 (usually N<100) whereas the template with a length of 2^{24} bits is produced by Farooq et al., (2007), which is obviously discouraged. Furthermore, the computational time of the proposed method is also remarkable. This can be observed that there are two major computational overheads: (1) minutia triplet processing time. Assume that the one unit time is used to process one minutia triplet, the total computational time is merely of $4N$ for the proposed method whereas a number of $N!/(N-3)!\,3!$ minutia triplets is required to be processed in Farooq et al., (2007); (2) feature vector projection. With a small size of feature vector (36-dimension), the time consumption of 2D random projection is rather slight.




FVC2002 DB2
Before RP
After RP
Genuine Acceptance Rate (%)
False Acceptance Rate (%)
100
95
90
85
80
75
70
10^{-2}
10^{-1}
10^{0}
10^{1}


FVC2002 DB3
Before RP
After RP
Genuine Acceptance Rate (%)
False Acceptance Rate (%)
100
90
80
70
60
50
40
30
20
10
10^{-2}
10^{-1}
10^{0}
10^{1}
10^{2}


FVC2002 DB4
Before RP
After RP
Genuine Acceptance Rate (%)
False Acceptance Rate (%)
100
90
80
70
60
50
40
30
20
10
10^{-2}
10^{-1}
10^{0}
10^{1}
10^{2}

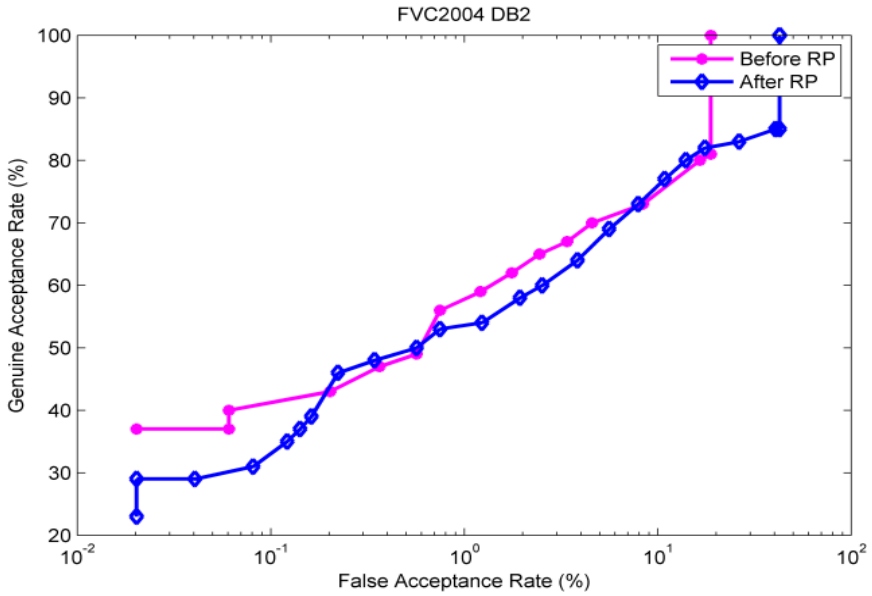


Fig. 3.4: ROC curves demonstrate the good preservation before and after random projection using 1 vs 1 protocol in stolen-token scenario.

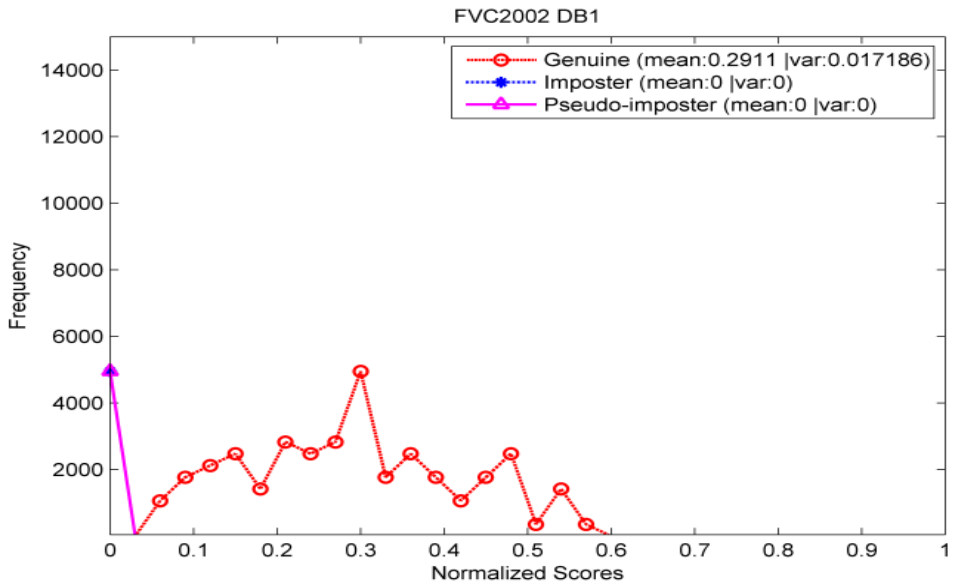
3.2.4.2 Cancellability and Diversity

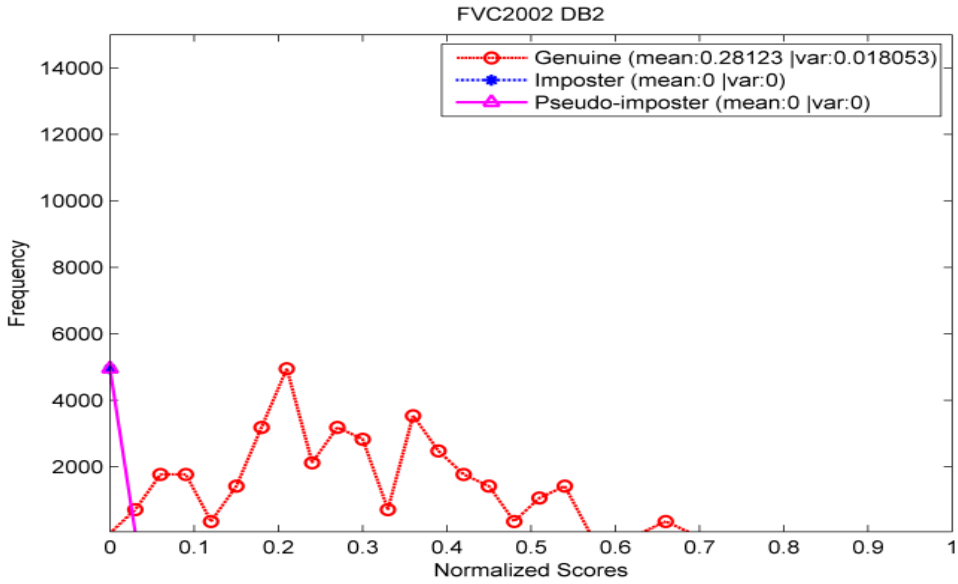
The method introduced by Lee et al. (2010) is adopted to evaluate the cancellability and diversity. In this experiment, 100 templates for each of fingerprint impression by using 100 random factor/external tokens are generated. The templates were matched to each other for generating the so called pseudo-imposter score. In order to be fairly justified, each fingerprint impression used in the experiment takes turns to be the source in generating the cancellable template and the average EER is recorded. Hence, we obtained 80,000 scores from 800 templates.

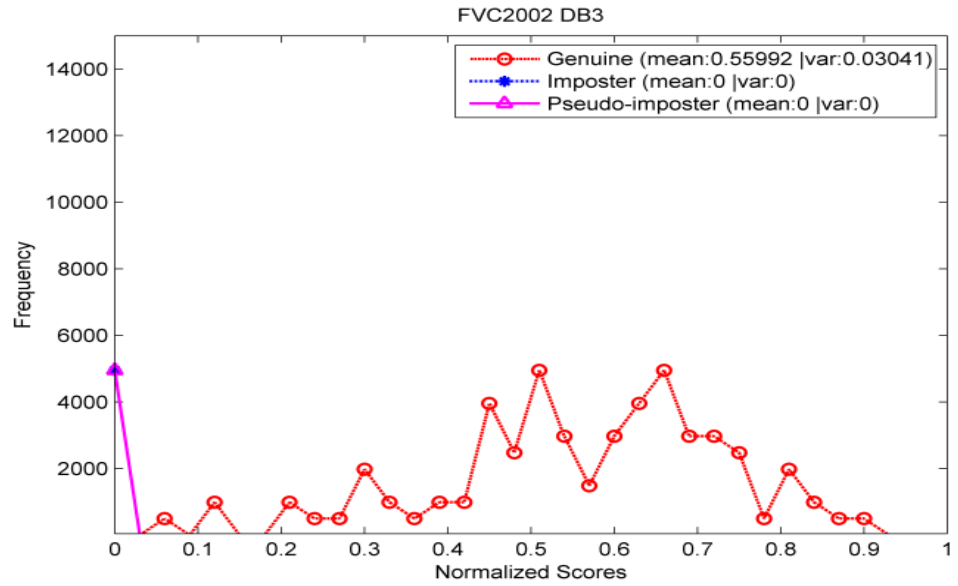
It can be expected, a 0% of average EER is obtained. The genuine distribution, imposter distribution and pseudo-imposter distributions for the cancellability experiments are shown in Fig. 3.5. The impostor distribution

and pseudo-impostor distribution has a strong overlap as shown in Fig. 3.5, which implies that multiple templates generated using different tokens rather resemble a fresh template, even though multiple templates generated from the same image and the performance does not degraded. Therefore, cancellability criterion is satisfied.

The experiment on evaluating the cancellability conducted above shows the fact that multiple templates generated from a single fingerprint image could be significantly distinguished, thus can be used in different physical applications without cross-matching. Therefore, it can be concluded that the result of the experiment carried out shows both cancellability and diversity can be achieved.




FVC2002 DB2
Genuine (mean:0.28123 |var:0.018053)
Imposter (mean:0 |var:0)
Pseudo-imposter (mean:0 |var:0)
Frequency
Normalized Scores
0
2000
4000
6000
8000
10000
12000
14000
0.1
0.2
0.3
0.4
0.5
0.6
0.7
0.8
0.9
1


FVC2002 DB3
Genuine (mean:0.55992 |var:0.03041)
Imposter (mean:0 |var:0)
Pseudo-imposter (mean:0 |var:0)
Frequency
Normalized Scores
0
2000
4000
6000
8000
10000
12000
14000
0.1
0.2
0.3
0.4
0.5
0.6
0.7
0.8
0.9
1

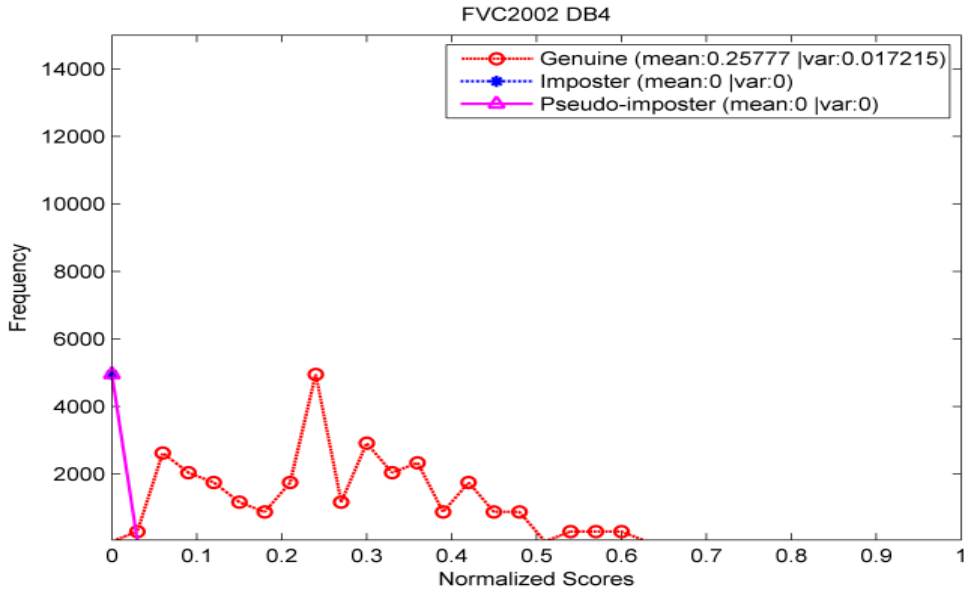


Fig. 3.5: Genuine distribution, impostor distributions for genuine-key scenario and pseudo-impostor distribution for FVC2002.

3.2.4.3 Non-invertibility Analysis

Non-invertibility in this context refers to the computational difficulty in learning the location and orientation of the minutia from the protected template and/or random matrix. This is mainly determined by two assumptions: (1) the secret token is known to an adversary; (2) both secret token and the protected template are revealed to the adversary.

In the first assumption, assume that the random matrix, ***R*** is known by an adversary through the compromised secret token. Yet, according to eq. (3.3), ***R*** is fully uncorrelated with the feature matrix, ***U***; it is rather hard for the adversary to learn any useful information of ***U*** with ***R*** alone.

For the second assumption, we assumed that an adversary has the knowledge of both protected template, $\boldsymbol{W}$ and random matrix, $\boldsymbol{R}$ as well as parameters and algorithm. However, the feature matrix $\boldsymbol{U}$ has been transformed into a random space by using eq. (3.3). Subsequently, in order to obtain the feature matrix $\boldsymbol{U}$, the adversary has to solve an under-determined linear equation system ($\boldsymbol{U = WR^{-1}}$), which is computationally much more difficult compare to Jin & Teoh (2011).

Even though, we assume the adversary can solve eq. (3.3), i.e. $\mathbf{W = UR^{T}}$ partially via pseudo-inverse operation. However, the feature matrix only comprises a set of local features, which do not correlate with location and orientation of minutiae. More specifically, if we assume that a minutia vicinity V_i occupies approximately a 50×50 pixels square in original images that are 388×374, 296×560 pixels respectively. The brute-force attack for guessing the correct x and y of V_i within the fingerprint image requires around (388-50) × (374-50) = 338×324 = 109512 attempts for DB1 and (296-50) × (560-50) = 246×510 = 125460 attempts for DB2. Furthermore, there are 360 possibilities in rotated degrees for V_i, thus the number of attempts increase to 39424320 and 45165600 respectively. Moreover, besides the estimation of minutiae location i.e. x axis and y, the minutia orientation is another factor which should also be taken into account. We noted there are 6 orientation differences, $\pm\Delta o_1$, $\pm\Delta o_2$ and $\pm\Delta o_3$ in total contained in $\boldsymbol{U}$, the total attack complexity for V_i is approximately 39424320×6=236545920≈2^{28} attempts for DB1 and 45165600×6=270993600≈2^{28} attempts for DB2.

Though, the experiment shows that the performance is decreased when a lower dimensions feature matrix applied; however, the lower dimension feature matrix produced by 2D random projection implies that the less structure information of the feature matrix is preserved, thus non-invertible property is enhanced. Hence, it is noted that the dimension of feature matrix is direct proportional to performance while it is inverse proportional to the difficulty of invertible property.

To summarize that the proposed 2D-RP-MVD extended the original 1D random projection used in Biohash (Teoh et al., 2004) to 2D random projection so that it can be applied to protect 2D minutiae-based MVD features. A better accuracy performance over the existing cancellable methods is achieved due to the strong discriminative power offered by the nearest neighborhood structure. More importantly, the properties of template protection, namely cancellability and diversity for 2D features matrix has been well justified, which is the main objective of the proposed 2D-RP-MVD. Although, the invariant features of MVD safeguards the location and orientation of minutiae; however, the security/non-invertibility provided by the 2D random projection has been pointed out to be weak against various attacks, e.g. attack via multiplication (ARM) in literature (Yang et al., 2010; Nagar, 2012). Therefore, stronger irreversible techniques to protect minutiae-based features e.g. RMVD is demanded.

3.3 Randomized Graph-based Hamming Embedding (RGHE)

As discussed in Section 3.2.1, minutia vicinity decomposition (MVD) (Jin & Teoh, 2011) was proposed to conceal the location and orientation of the minutiae. However the MVD features are likely to reveal the minutia vicinity, e.g. four minutiae triangles after decomposition. Furthermore, two dimensional random projection-based MVD features (i.e. 2D-RP-MVD in Section 3.2) is inherited from random projection, which is also possibly invertible by applying back-projection operation (Yang et al., 2009).

To rectify the weak non-invertible issue, a Randomized Graph-based Hamming Embedding (RGHE) technique with strong non-invertibility is proposed to generate a secure cancellable fingerprint template. This technique is able to protect the MVD features and preserve the recognition performance in the original feature space. The Graph-based Hamming Embedding (GHE) is inspired by Weiss's Spectral Hashing (Weiss et al., 2009), which was proposed to solve the big-data nearest-neighbor-search problem. Spectral Hashing searches for a binary mapping function that minimizes the average Hamming distance between the resulting binary codes with respect to the distance measured in the original space. However, original spectral hashing does not address specific cancellable biometric template design criteria such as diversity, non-invertible transformation, accuracy performance retention and "small data" (number of minutiae per template) nature in fingerprint template. Therefore, a substantial alteration has to be made to satisfy these requirements.

In short, RGHE is able to (1) conceal the MVD structure significantly; (2) preserve the actual discriminative power before and after RGHE transformation and alleviates the security-performance trade-off originally caused by the intra-class variation of biometrics; (3) satisfy the cancelability and diversity with Random Projection.

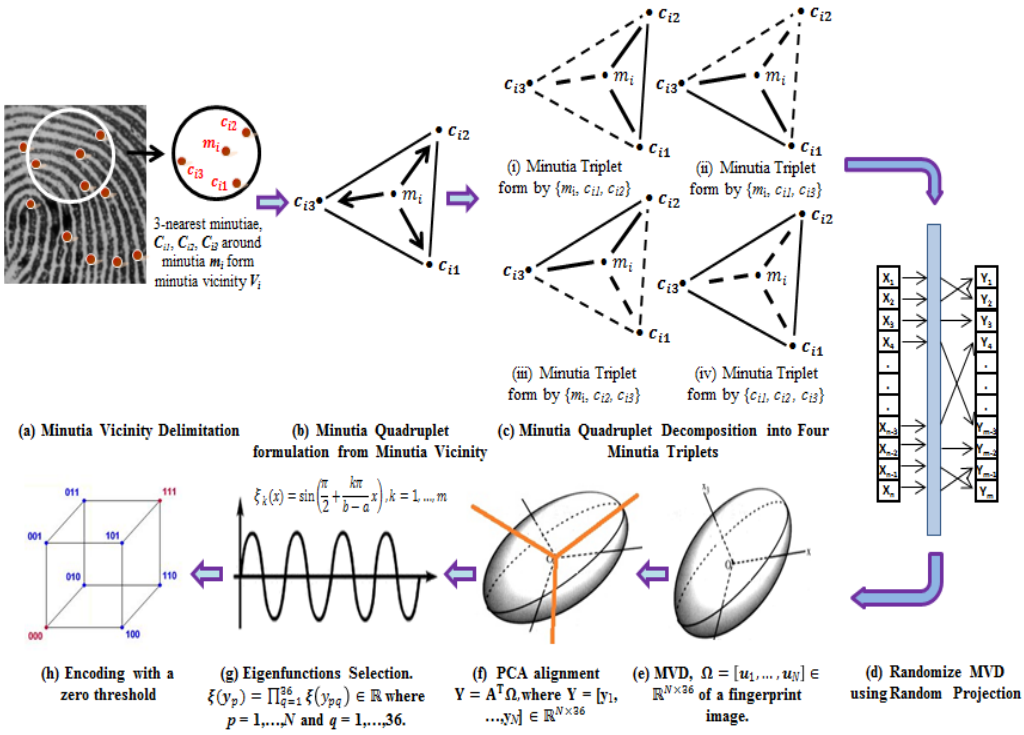


Fig. 3.6: Block diagram of randomized graph hamming embedding (RGHE).

3.3.1 Methodology

The RGHE initially constructs a set of minutia vicinity that describes the nearest neighborhood structure in the Euclidean space. Each minutia vicinity is then decomposed into (4) minutiae triplets, where a set of geometric invariant features is derived from each triplet. Then, the invariant features are projected onto a random subspace determined by an externally-derived pseudorandom sequence. The aforementioned two processes are completely

identical to the Minutia vicinity Decomposition and Two-Dimensional Random Projection, which are presented in Section 3.2. Thereafter, the randomized minutia vicinity decomposition features (RMVD) are transformed using Graph-based Hamming Embedding to preserve the neighborhood structure of RMVD. The block diagram of RGHE is presented in Fig. 3.6.

3.3.1.1 Minutia Vicinity Decomposition (MVD) and Randomizing MVD

These two processes are completely identical to the minutia vicinity decomposition (MVD) and 2-dimensional random projection described in Section 3.2. Hence, the identical processes are not repeated in this section.

3.3.1.2 Graph based Hamming Embedding (GHE)

The trained RMVD $\Omega \in \mathbb{R}^{N\times 36}$ consists of a set of N minutiae vicinities $\boldsymbol{u} \in \mathbb{R}^{36}$ of a fingerprint image in the Euclidean space. Let G={**U**,**W**} be a weighted graph with vertex **U** for |**U**|=N and weight matrix $\mathbf{W} \in \mathbb{R}^{N\times N}$. Each element $\boldsymbol{w}_{ij}$ of **W** denotes the global similarity of vertex pairs ($\mathbf{u}_i$, $\mathbf{u}_j$), which is measured by $\boldsymbol{w}_{ij} = \exp(-\|\mathbf{u}_i - \mathbf{u}_j\|^2 / \sigma^2)$ with σ representing the bandwidth of heat kernel (Belkin & Niyogi, 2003). Our objective is to search a mapping function that preserves the Euclidean distance between the resultant m-components feature with respect to the minutia vicinities in the Euclidean space.

This problem can be formulated by solving the following optimization problem (Weiss et al., 2009):

$$\min_{\varphi} \int \mathbf{W} \| \varphi(\boldsymbol{u_i}) - \varphi(\boldsymbol{u_j}) \|^2 p(\mathbf{u}_i) p(\mathbf{u}_j) d\mathbf{u}_i d\mathbf{u}_j \quad (3.7)$$

subject to

$$\varphi(\mathbf{u}) \in \{-1, 1\}^m$$

$$\int \varphi(\mathbf{u}) p(\mathbf{u}) d\mathbf{u} = 0$$

$$\int \varphi(\mathbf{u}) \varphi(\mathbf{u})^{\mathrm{T}} p(\mathrm{u}) d\mathbf{u} = I$$

where $p(\mathbf{u})$ is the probability distribution of $\mathbf{u}$.

The second constraint $\int \varphi(\mathbf{u}) p(\mathbf{u}) d\mathbf{u} = 0$ requires the flipping probability of each individual bit of the resultant binary code to be 0.5 and the third constraint $\int \varphi(\mathbf{u}) \varphi(\mathbf{u})^{\mathrm{T}} p(\mathrm{u}) d\mathbf{u} = I$ requires the bits to be uncorrelated. Although the optimization problem in (2.7) with the first constraint $\varphi(\mathbf{u}) \in \{-1, 1\}^m$ is NP hard, several analytical solutions are available by applying spectral relaxation, such as *eigenfunctions* of the weighted Laplace-Beltrami operators defined on manifolds (Belkin & Niyogi, 2003).

Specifically, let $\boldsymbol{L_p}$ be a weighted Laplacian operator that maps a function φ to $\psi = L_p \varphi$ by $\psi(\mathbf{u}) / \varphi(\mathbf{u}) = D(\mathbf{u}) \varphi(\mathbf{u}) p(\mathbf{u}) - \int_s \mathbf{W}(\mathbf{s}, \mathbf{u}) \varphi(\mathbf{s}) p(\mathbf{s}) d\mathbf{s}$ with $D(\mathbf{u}) = \int_s \mathbf{W}(\mathbf{u}, \mathbf{s}) p(\mathbf{s}) d\mathbf{s}$. The solution for the minimization problem in eq. (3.7) is therefore eigenfunctions ξ that satisfy $L_p \xi = \beta \xi$ for a real-valued β.

To solve the above problem, two assumptions have to be made: 1) $p(\mathbf{u})$ is a separable distribution; 2) each input feature is drawn from a uniform distribution. It is noted if $p(\mathbf{u})$ is separable, and the similarity between data points is defined by $\boldsymbol{w}_{\mathrm{ij}} = \exp(-\|\mathbf{u}_i - \mathbf{u}_j\|^2 / \sigma^2)$ then the eigenfunctions ξ of the

L_p have an outer product form. The "outer-product" eigenfunctions are merely products of eigenfunctions along different dimensions and their eigenvalue is simply the product of the eigenvalues of these dimensions. Therefore, the first assumption implies that we may construct an eigenfunction $\xi(\mathbf{u})$ of L_p using a product of 36 single-dimensional eigenfunctions, $\xi(\mathbf{u}) = \prod_{i=1}^{36} \xi(u_i)$ corresponding to each feature. The second assumption allows us to select the following eigenfunctions as the single-dimensional eigenfunctions of the single dimensional Laplacian L_p in the small ϵ, which is well studied in mathematics (Weiss et al., 2009):

$$\xi_k(x) = \sin\left(\frac{\pi}{2} + \frac{k\pi}{b-a}x\right) \tag{3.8}$$

$$\beta_k = 1 - e^{-\frac{\epsilon^2}{2}\left|\frac{k\pi}{b-a}\right|} \tag{3.9}$$

where x is a single-dimensional arbitrary real feature uniformly distributed in the range of $[a, b]$; and β_k is the corresponding eigenvalue of $\xi_k(x)$, which serves as an indicator for eigenfunctions selection for the GHE mapping. We notice that the assumption on uniformly distributed data may not fit the case in practice. However, the experimental result illustrates that eq. (3.8) works well on RMVD, although the experimental data might not be uniformly distributed.

From the above description, a two-step algorithm can be derived: 1) Principal Component Analysis (PCA) alignment, 2) Eigenfunctions selection. Here, we take a multi-dimensional Gaussian as the distribution function for $p(\mathbf{u})$ defined in eq. (3.7). This is attributed to the nice property of Gaussian distribution function that can be made separable by simply aligning the data along the axes by rotation, which motivates the use of PCA. It is important to

note that PCA in GHE merely serves the purpose of data alignment but not dimensionality reduction as applied in (Ratha et al., 2007; Ferrara et al., 2012). Therefore, the inversion issue (privacy breach) of back-projection in (Ratha et al., 2007; Ferrara et al., 2012) and the other projection-based techniques (Ratha et al., 2007) would not happen in our case.

The second step is to compute m eigenfunctions using $\xi_i(\mathbf{y}) = \prod_{j=1}^{36} \xi_i(\boldsymbol{y}_j)$ for i=1,…,m according to eq. (3.8), where $\mathbf{y}$ is the 36-dimensional PCA-aligned data. This can be done by evaluating the k eigenvalues for each of the 36 PCA directions using eq. (3.9) and sorting the resultant 36k eigenvalues ascending. After discarding eigenfunctions with zero eigenvalue, we select m eigenfunctions with the m smallest eigenvalues from the remaining eigenfunctions to form a m-components feature vector. The same process is repeated for N minutiae vicinities of an image. Finally, a $N \times m$ real-valued feature matrix is obtained.

The GHE is applied to every individual randomized MVD in both enrollment and verification stages. The parameters required to be stored during the enrollment stage are the range of $\mathbf{Y}$ (a and b) and the projection matrix $\mathbf{R}$ for data alignment.

Note that GHE seeks a m-components feature vector from each 36-dimensional RMVD feature vector of a minutia vicinity. By considering all the minutia vicinities, a GHE-extracted real-valued template of size $N \times m$ can be formed, where N is the number of minutiae. For instance, m can be set to 16,

32, 64, 129 or 256 components and this causes the corresponding real-valued template to take the size of $N \times 16$, $N \times 32$, $N \times 64$, $N \times 128$ or $N \times 256$, respectively. Algorithm 3.1 presents the detailed flow of the proposed GHE method.

Algorithm 3.1. Graph based Hamming Embedding (GHE)

Input: RMVD, $\Omega \in \mathbb{R}^{N\times 36}$ and code length *m*

Step 1: PCA Alignment

1.1: Extracts eigenvectors $\mathbf{\Phi}$ from the covariance matrix, $\mathbf{C}= \mathbf{\Omega\Omega^T}$

1.2: Project $\mathbf{\Omega}$ to eigenspace, i.e. $\mathbf{Y}= \mathbf{\Phi^T\Omega}$, where $\mathbf{Y} = [\mathbf{y}_1, \dots, \mathbf{y}_N] \in \mathbb{R}^{N\times 36}$

1.3: Calculate $a = \min(\mathbf{Y})$ and $b = \max(\mathbf{Y})$ for eq. (3.8) and eq. (3.9).

1.4: Calculate $36k$ eigenvalues from β_k using eq. (3.9) and sort them in ascending order.

Step 2: Eigenfunctions selection

2.1 Compute *m* eigenfunctions according to the *m* smallest eigenvalues from step 1.4, i.e.

For i=1:*m*

Compute $\xi_i(\mathrm{y}) = \prod_{r=1}^{36} \xi_i(y_r) \in \mathbb{R}$ as in eq. (3.8).

End for

2.2 Repeat Step 2.1 for all *N* minutiae vicinities, hence $\xi^{\boldsymbol{n}} = [\xi_{\mathbf{1}}, \dots, \xi_{\boldsymbol{m}}]$, where $n = 1,\dots,N$.

2.3 Form $\mathbf{\Xi} = [\boldsymbol{\xi}^{\mathbf{1}}, \dots, \boldsymbol{\xi}^{\boldsymbol{N}}] \in \mathbb{R}^{N\times m}$

Output: The real-valued template $\mathbf{\Xi}$ for a set of minutia vicinity

3.3.1.3 Matching

The similarity between two distinct fingerprints represented by two resultant binary codes ($\mathbf{\Xi}_i \in \{0,1\}^{N_1\times m}$ and $\mathbf{\Xi}_j \in \{0,1\}^{N_2\times m}$ containing N_1 and N_2 *m*-components templates, respectively) can be measured by the smallest

pairwise Euclidean distance between templates in Ξ_i with respect to those in Ξ_j (measured in Euclidean distance). We devise an exhaustive searching strategy as follows. Let $\Xi_e = [\xi_{e1}, \ldots, \xi_{eN_1}]$ and $\Xi_q = [\xi_{q1}, \ldots, \xi_{qN_2}]$ be the binary vectors of N_1 and N_2 vicinities extracted from an enrolled and a query fingerprint image, respectively. The score of a matched pair p_{ij} in the comparison of Ξ_e and Ξ_q can be computed using eq. (3.10). With this, a score matrix **P** = **[**p_{ij}**]** of size N_1 x N_2 can be formed:

$$p_{ij} = \min(\Xi_e^i, \Xi_q^j) \tag{3.10}$$

where ||.|| denotes the hamming distance between Ξ_e^i and Ξ_q^j.

Next, we store the *minimum value* for each row in **P**, which is denoted as a_i:

$$a_i = \min_j(P_{ij}) \text{ for } i = 1,\ldots, N_1 \text{ and } j = 1,\ldots, N_2 \tag{3.11}$$

The matching score can then be computed by counting the number of a_i that has a less value than the pre-defined threshold *t*. To avoid large variation in the results caused by non-trivial difference in magnitude led by unstable number of minutiae in the query and enrolled images, the matching score can be normalized as follows:

$$s = \frac{\sum_{i=1}^{N_1}(a_i < t)}{\sqrt{N_1 \times N_2}} \tag{3.12}$$

Hence, the score obtained is real where a score is toward '0' indicates a negative match and vice versa.

3.3.2 Experiments

The experiments were conducted on two public fingerprint datasets, namely FVC2002 (Fingerprint Verification Competition, 2002) and FVC2004 (Fingerprint Verification Competition, 2004). Each dataset consists of 100 users, where each user has 8 samples. In total, there are 800 (100×8) fingerprint images. VeriFinger 7.0 SDK (VeriFinger SDK) was used for minutia extraction from the fingerprint images. The performance of the proposed method is evaluated using Equal Error Rate (EER) and receiver operating characteristic (ROC) as well as genuine-imposter distribution.

For the experiments in sequel, two protocols are designed:

(a) 1 vs 1 protocol: The first 100 samples of the same finger in all data sets (FVC2002 DB1, DB2, DB3 and DB4; FVC2004 DB2) are used as gallery and the second 100 samples of the same finger are regarded as probe. Hence, the matching yields 100 genuine scores and 9900 imposter scores. Note that this is a popular experimental setup, since the same setup has been employed by many existing methods (Yang & Busch, 2009; Ahmed et al., 2011; Wang & Hu, 2012; Wang & Hu, 2014).

(b) FVC protocol: Fingerprint Verification Competition (FVC) protocol is applied, where each sample is matched against the remaining samples of the same finger to compute the False Rejection Rate (FRR) while the first sample of each finger is matched against the first sample of the remaining fingers to compute the False Acceptance Rate (FAR). This protocol results 2800 genuine scores and 4950 imposter scores respectively.

3.3.2.1 Accuracy Performances

The performances in two scenarios, namely genuine-token and stolen-token scenarios, are evaluated. For genuine-token, each individual is assigned a random matrix, which is used to mix with feature matrix as shown in eq. (3.3) and this random matrix is user specific. On the other hand, verification in the stolen-token scenario is the scenario where an impostor has stolen the token of the target user and uses the random matrix of the target user to perform verification. This is also known as the *Lost Token Attack*.

Table 3.4: Accuracy Performance in terms of EER (%) for two experiment protocols in stolen-token scenario for FVC2002 and FVC2004.

Experiment Protocols	Equal Error Rate (EER) (%)				
	FVC2002 DB1	FVC2002 DB2	FVC2002 DB3	FVC2002 DB4	FVC2004 DB2
1 vs 1	2.07	0.90	10.28	10.44	15.80
FVC	6.71	6.30	16.95	11.35	18.96

For genuine-token scenario, the performance results in terms of EER for all datasets are ideal (the EERs are close to 0). This is due to the binding of the external token with the biometric features, which increases the dissimilarity between different users tremendously.

In stolen-token scenario, a token is generated in advance and this token is assigned to all users. The accuracy performance is computed by comparing the templates from all the 100 users with the same external token.

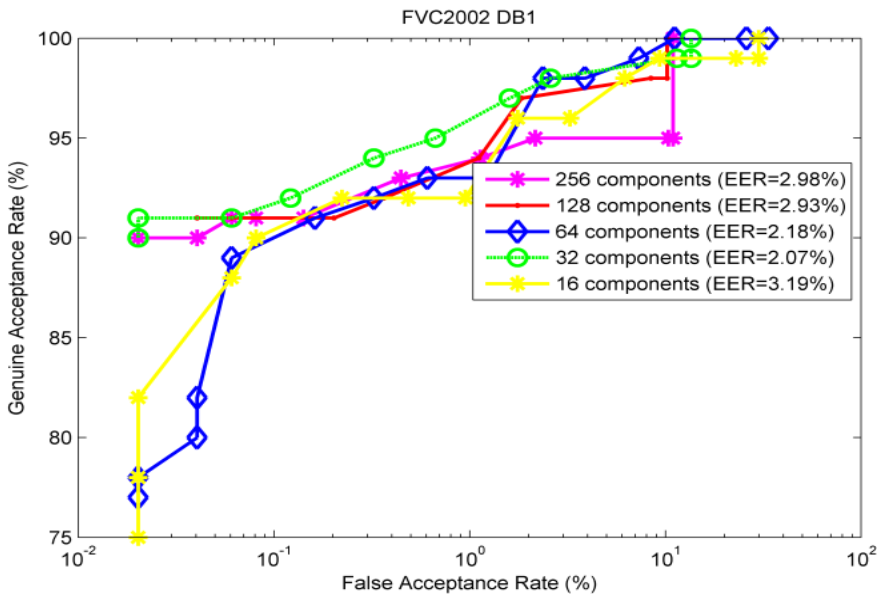
From the Table 3.4, it can be observed that approximately, the equal error rate of 2.07%, 0.90%, 10.28%, 10.44% and 15.80% for FVC2002 (DB1, DB2, DB3, DB4) and FVC2004 DB2 in 1 vs 1 protocol scenario are achieved while the equal error rate of 6.71%, 6.30%, 16.%, 11.35% and 18.96% in FVC protocol scenario are obtained approximately. It also can be observed that: (1) the accuracy performances of FVC2002 DB1 and FVC2002 DB2 are better than the rest of data sets (i.e. FVC2002 DB3, DB4 and FVC2004 DB2); (2) the performance for 1 vs 1 protocol is better than the performance using FVC protocol. These observations are identical to the experiment observations in the proposed 2D-MVD-RP method. Thus, the justification in Section 3.2.4.1 can be confirmed.

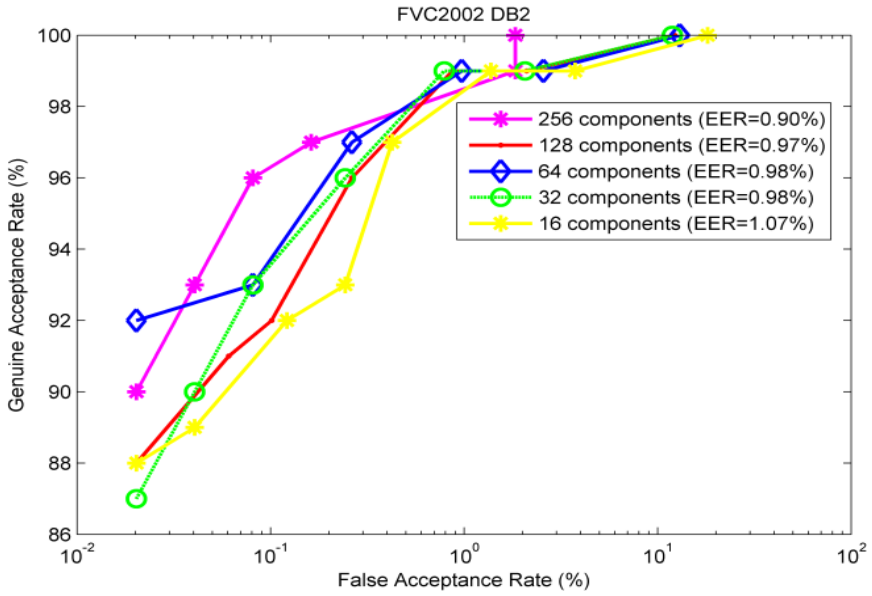
The performance of RGHE for different number of components *m* is then investigated, where *m* ranges from 16 to 256. Table 3.5 illustrates the EER of RGHE with respect to different *m*. It is observed that the performance of RGHE improves as *m* increases for FVC2002 DB2. When *m* = 256, RGHE performs the best where the corresponding EER = 0.90%. While, the performances of RGHE demonstrates bell-shape-liked curve as *m* increases for other data sets. The lowest EERs achieved are 2.07% for FVC2002 DB1, 10.28% for FVC2002 DB3, 10.44% FVC2002 DB4 and 15.80% FVC2004 DB2 respectively where the corresponding *m* are16 for FVC2002 DB1 and 64 for FVC2002 DB3, DB4 and FVC2004 DB2. The best accuracy from FVC2002 DB2 is somehow expected, since the features (minutia vicinity) extracted from other data sets are generally less discriminative than FVC2002 DB2. It is noticed that the recognition performance deterioration occurs as *m*

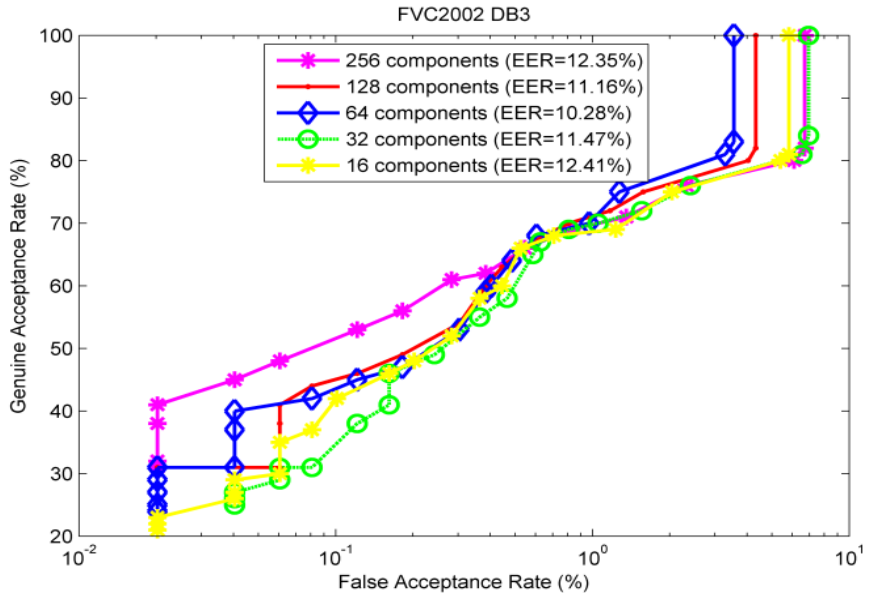
increases in all the data set except FVC2002 DB2. This is due to the fact that RGHE does not converge to a deterministic functional form and this eventually brings down the performance when *m* increases (Raginksi & Lazebnik, 2009). Therefore, the selection of *m* for optimal performance is database-dependent. Fig. 3.7 demonstrates the corresponding ROC curves of GHE based on different values of *m*.

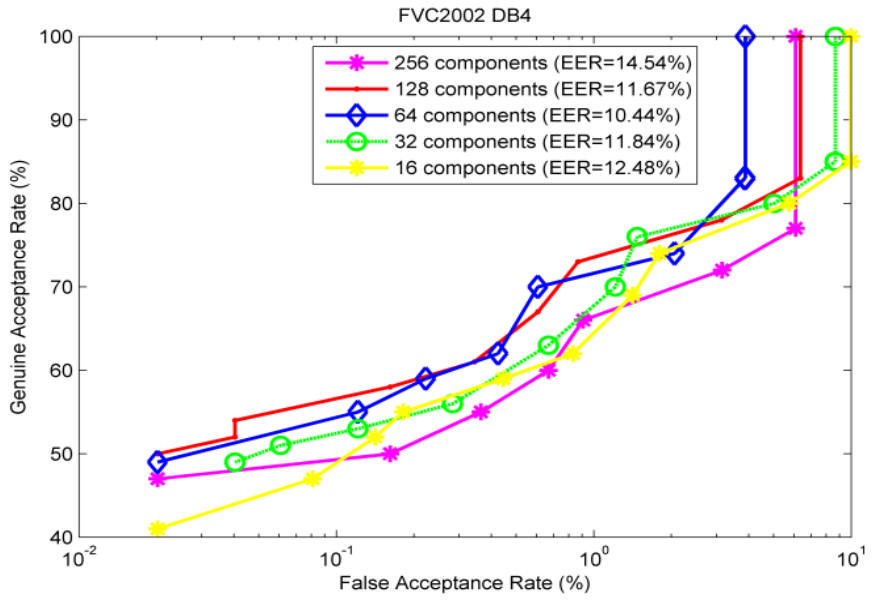
Table 3.5: EER performance of the RGHE for different number of components *m* (EER obtained in stolen-token case with 1 vs 1 protocol).

# of components, *m*	FVC2002 DB1	FVC2002 DB2	FVC2002 DB3	FVC2002 DB4	FVC2004 DB2
16	3.19%	1.07%	12.41%	12.48%	17.40%
32	2.07%	0.98%	11.47%	11.84%	17.24%
64	2.18%	0.98%	10.28%	10.44%	15.80%
128	2.93%	0.97%	11.16%	11.67%	16.93%
256	2.98%	0.90%	11.73%	14.54%	17.28%




FVC2002 DB2
Genuine Acceptance Rate (%)
False Acceptance Rate (%)
256 components (EER=0.90%)
128 components (EER=0.97%)
64 components (EER=0.98%)
32 components (EER=0.98%)
16 components (EER=1.07%)


FVC2002 DB3
Genuine Acceptance Rate (%)
False Acceptance Rate (%)
256 components (EER=12.35%)
128 components (EER=11.16%)
64 components (EER=10.28%)
32 components (EER=11.47%)
16 components (EER=12.41%)


FVC2002 DB4
Genuine Acceptance Rate (%)
False Acceptance Rate (%)
256 components (EER=14.54%)
128 components (EER=11.67%)
64 components (EER=10.44%)
32 components (EER=11.84%)
16 components (EER=12.48%)

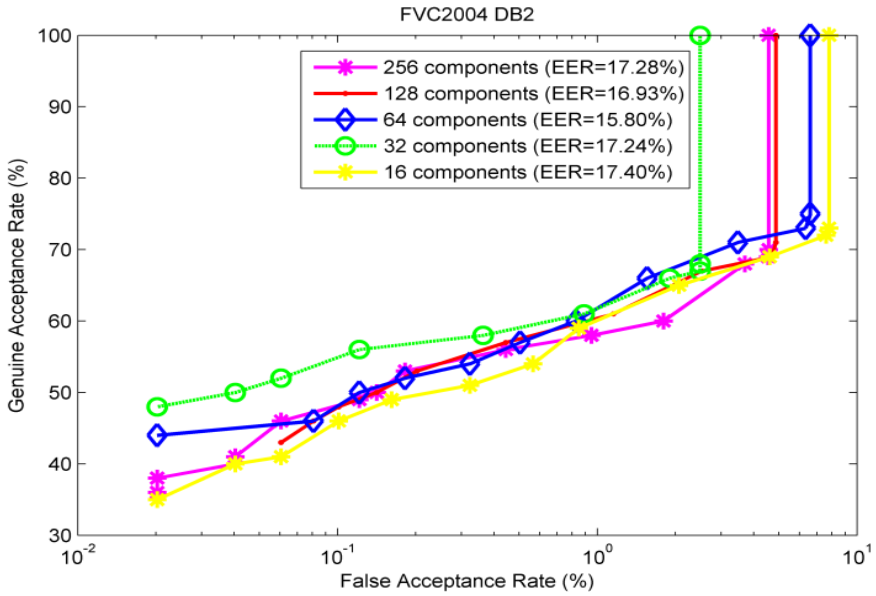


Fig. 3.7: Demonstrates the corresponding ROC curves of RGHE based on different values of *m* for the FVC2002 and FVC2004.

Table 3.6 shows the EERs performance comparisons between the proposed method and the other methods in the literature using 1 vs 1 protocol. The proposed method achieves better performance than the most of the state-of-the-arts (Tulyakov et al., 2007; Yang & Busch, 2009; Nagar et al., 2010b; Bringer & Despiegel, 2010; Ahmed et al., 2011; Wang & Hu, 2012, Wang & Hu, 2014) in FVC2002 DB2 whereas the proposed method underperforms Wang et al.'s method (Wang & Hu, 2012) in FVC2002 DB3 and Wang et al.'s method (Wang & Hu, 2014) FVC2002 DB1 and DB3. However, those methods are to be vulnerable to attack via record multiplicity (ARM) (Li and Hu, 2014).

Table 3.6: Performance accuracy of the proposed method in comparison with several state-of-the-art methods using 1 vs 1 protocol.

Methods	**EER (%) in stolen-token scenario**				
	FVC2002 DB1	FVC2002 DB2	FVC2004 DB3	FVC2002 DB4	FVC2004 DB2
Proposed	2.07	0.90	10.28	10.44	15.80
Ahmad et al., (2011)	9	6	27	-	-
Wang & Hu (2012)	3.5	4	7.5	-	-
Wang & Hu (2014)	2	2.3	6.12	-	-
Tulyakov et al., (2007)	3	-	-	-	-
Yang & Busch (2009)	-	Avg. 4.04	-	-	-
Yang et al., (2010)	-	Best case: 0.72 Worst case: 2.23	-	-	-
Nagar et al., (2010b)	-	3	-	-	-
Bringer & Despiegel (2010)	-	5.3	-	-	-

'-' Denoted that results are not reported in the original paper.

3.3.2.2 Preservation of the Performance

Apart from the above, we also investigate the recognition performance before and after RGHE. It is noted that the performance deterioration caused by GHE is rather insignificant. Among the five data sets, the accuracy deterioration only occurs in FVC2002 DB1 (from 1.02% to 2.07%). By contrast, the accuracy performances have been improved for FVC2002 DB2,

FVC2002 DB3, FVC2002 DB4 and FVC2004 DB2, as shown in Table 3.7, thus signifying a good preservation of the actual MVD neighborhood structure in the Euclidean space.

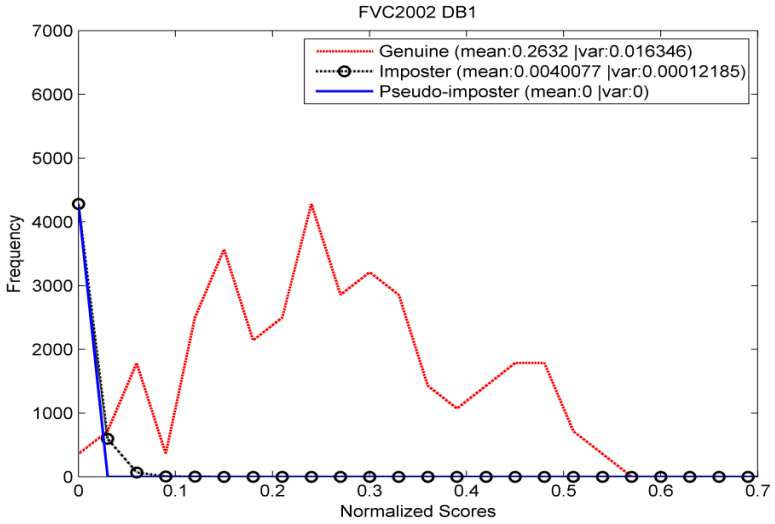
Table 3.7: Accuracy comparison (EER %) in before and after RGHE transform using FVC protocol.

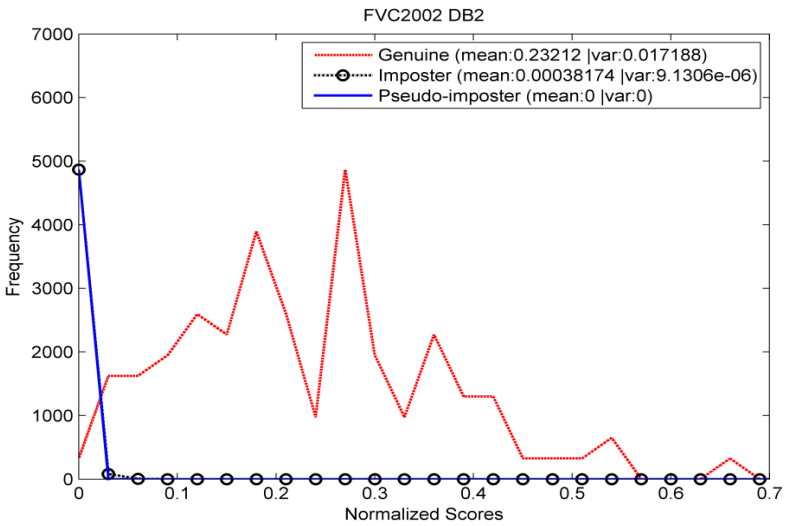
	FVC2002 DB1	**FVC2002 DB2**	**FVC2002 DB3**	**FVC2002 DB4**	**FVC2004 DB2**
Before RGHE Transform	1.02	0.98	16.15	10.46	17.75
After RGHE Transform	2.07	0.90	10.28	10.44	15.80

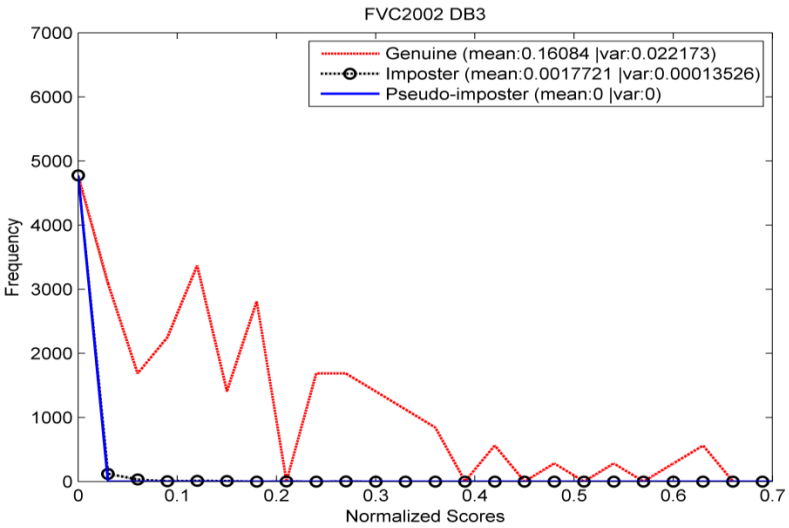
3.3.2.3 Revocability

To evaluate this criterion, 100 sets of random matrices are first generated. Subsequently, 100 different templates are generated from a single fingerprint image based on these different random matrices. The 100 templates are compared with the genuine template and the resulting distances (scores) are used to generate a distribution called the *pseudo-impostor distribution*. The genuine-imposter and pseudo-imposter distributions for the revocability experiments are shown in Fig. 3.8. It can be observed that there is a strong overlap between the impostor distribution and pseudo-impostor distribution. This implies that the templates generated using different tokens and the same biometrics is no different to templates generated from biometric data belonging to a different identity. Therefore, the claim of revocability is

vindicated.


FVC2002 DB1
Genuine (mean:0.2632 |var:0.016346)
Imposter (mean:0.0040077 |var:0.00012185)
Pseudo-imposter (mean:0 |var:0)
Frequency
Normalized Scores


FVC2002 DB2
Genuine (mean:0.23212 |var:0.017188)
Imposter (mean:0.00038174 |var:9.1306e-06)
Pseudo-imposter (mean:0 |var:0)
Frequency
Normalized Scores


FVC2002 DB3
Genuine (mean:0.16084 |var:0.022173)
Imposter (mean:0.0017721 |var:0.00013526)
Pseudo-imposter (mean:0 |var:0)
Frequency
Normalized Scores

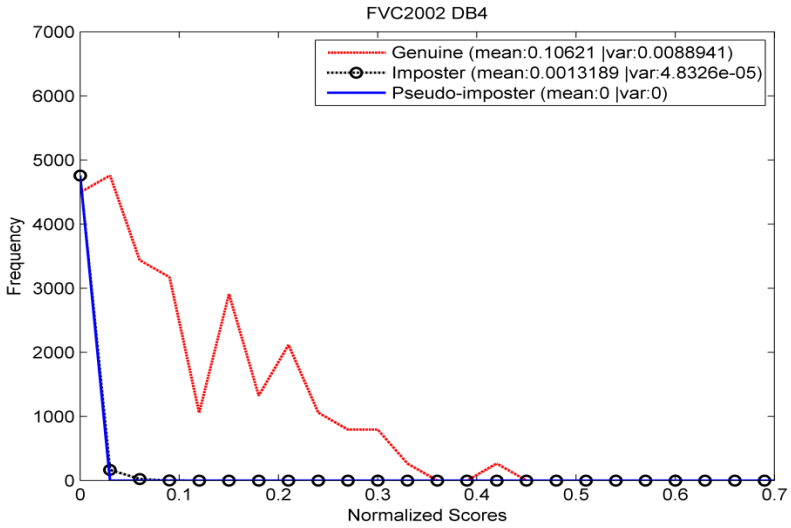


Fig. 3.8: Shows the genuine-imposter and pseudo-imposter distributions for the FVC2002 database.

3.3.2.4 Diversity

The experiment conducted in section 3.3.2.3 shows that even though the 100 different templates are generated from a single fingerprint image, they can still significantly be distinguished from the original template. That means individual can enrol different templates using the same finger at different physical applications without cross-matching. Therefore, the experiments conducted do not only vindicate the claim of revocability but also to validate the property of diversity.

3.3.3 Non-invertibility and Computation Complexity Analysis

In this section, the non-invertibility of RGHE is evaluated through (1) small range of shifting/small angle approximation analysis based on the study of two existing methods (Ratha et al., 2007); (2) evaluation of invertibility complexity. The computational complexity of RGHE is also provided in this section. In our context, non-invertibility refers to the computational hardness

in recovering the *fingerprint minutia* from the generated bit-string and/or helper data.

1) Small range of shifting/small angle approximation analysis. To analyze the non-invertibility property of cancellable biometrics, many-to-one property of the transformation methods have always been taken as a main criterion for evaluation; yet, the poor design of many-to-one transformation function would always weaken or even compromise the non-invertibilitiy of transformation function (Nagar et al., 2010c; Feng et al., 2008). We reveal that small range of shifting/small angle approximation can weaken the many-to-one property of the non-linear functions, which is less studied in the literature.

A well-known instance proposed in literature is Ratha's surface folding scheme (Ratha et al., 2007); it is shown that inappropriate parameters selected for minutia transformation leads to small range of shifting for the transformed minutiae. In fact, such transformation de-generates the many-to-one surface folding function to a linear function. Therefore, non-invertibility can be compromised via restoring the small shifted minutiae. Similar analysis is also applicable to another realization, namely, BioPharsor (Teoh & Ngo, 2006). Generally, BioPhasor can be formulated as follow:

$$a_j = \frac{1}{n}\sum_{i=1}^{n} \tan^{-1}\left(\frac{x_i}{r_{ij}}\right), j = 1, \dots m, m < n \text{ and } r \neq 0 \qquad (3.13)$$

where x_i and r_i represent an ordered fixed-length feature vector $x_i \in \mathbb{R}^n$ and a set of random numbers respectively; and *n* and *m* denote the length of x_i and α_j respectively.

If $\theta = \left(\frac{x_i}{r_{ij}}\right) < 0.176$ rad, then $\tan^{-1}\left(\frac{x_i}{r_{ij}}\right) \approx \frac{x_i}{r_{ij}}$. This small angle approximation can be observed in Fig. 3.13(a). Hence, we analyze two cases separately, i.e. i) $\theta < 0.176$; ii) $\theta \geq 0.176$.

(1) For < 0.176 , the BioPhasor degenerates to:

$$a_j = \frac{1}{n}\sum_{i=1}^{n}\left(\frac{x_i}{r_{ij}}\right) = \sum_{i=1}^{n}\left(\frac{1}{nr_{ij}}x_i\right) \tag{3.14}$$

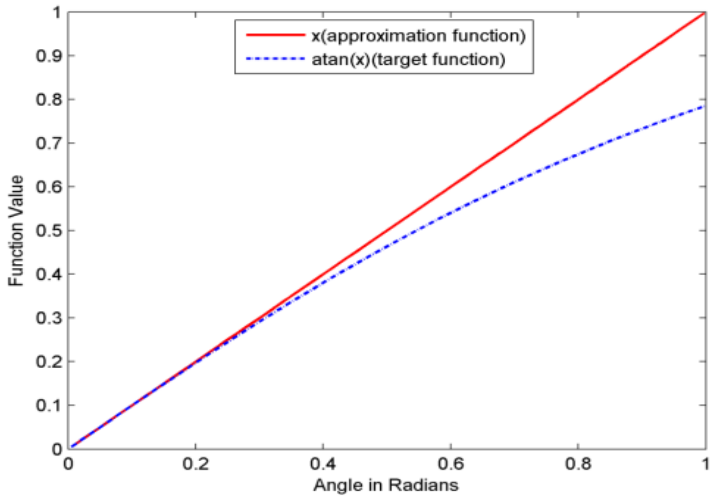
or if

$$\begin{aligned} R_{ij} &= \frac{1}{nr_{ij}} \\ a_j &= \sum_{i=1}^{n} R_{ij}x_i \end{aligned} \tag{3.15}$$

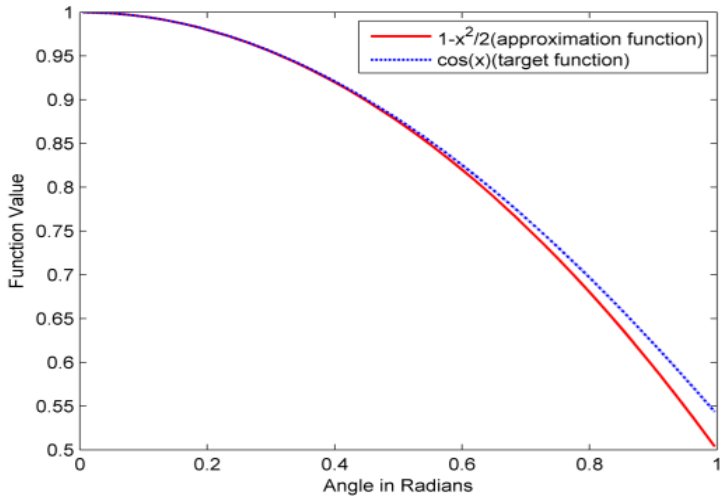
(2) If $\theta \geq 0.176$, the inverse tangent function can be approximated using infinite series.

$$\tan^{-1}\left(\frac{x_i}{r_{ij}}\right) = \frac{x_i}{r_{ij}} - \frac{1}{3}\left(\frac{x_i}{r_{ij}}\right)^3 + \frac{1}{5}\left(\frac{x_i}{r_{ij}}\right)^5 - \frac{1}{7}\left(\frac{x_i}{r_{ij}}\right)^7 + \cdots \tag{3.16}$$

As a result, we reveal that 1) if $\theta < 0.176$, BioPhasor in eq. (3.15) is degenerated to a random projection. Thus, the accuracy performance can be preserved due to Johnson–Lindenstrauss lemma but the non-invertibility could be compromised if a pseudo-inverse is applied (Ferrara et al., 2012). On the other hand, when the angle is large, the non-linearity of BioPhasor becomes prominent but the preservation of accuracy performance could be traded off.



(a)



(b)

Fig. 3.9: The approximations of (a) the inverse tangent function by a linear function and (b) cosine function by the function $1-\frac{x^2}{2}$. The approximation is more precise as the angle approaches 0.

In the proposed RGHE, the sinus function in eq. (3.8) offers a many-to-one mapping to ensure its non-invertitibility. Now, we carry out an analysis to investigate the small angle approximation issue. Firstly, we make the following manipulation:

$$\xi_i = \prod_{r=1}^{36} \sin\left(\frac{\pi}{2} + \frac{i\pi}{b-a} y_r\right) = \prod_{r=1}^{36} \cos\left(\frac{i\pi}{b-a} y_r\right) \tag{3.17}$$

Let $\theta = \frac{i\pi}{b-a} y_r$,

$$\prod_{r=1}^{36} \cos\left(\frac{i\pi}{b-a} y_r\right) = \prod_{r=1}^{36} \cos(\theta) \tag{3.18}$$

Small angle approximation for cosine function ($\cos(\theta) \approx 1 - \frac{\theta^2}{2}$) is valid when $\theta < 0.664$ rad, as shown in Fig. 3.9(b). In this case, the "many(outputs)-to-one(input)" of cosine function has been reduced to a "two-to-one" quadratic function, thus weakening the non-invertibility of the function.

$$\xi_i = \prod_{r=1}^{36} \cos(\theta) \approx \prod_{r=1}^{36} \left[1 - \frac{1}{2}\left(\frac{i\pi}{b-a} y_r\right)^2\right] \tag{3.19}$$

Therefore, it is worthwhile to investigate whether θ computed by RMVD template is in the range of small angle approximation attack. As such, we design an experiment as follows:

1. Compute the mean and standard deviation of the angle from all the minutia vicinity decomposition in one RMVD template;
2. Since there are 800 RMVD templates derived from each dataset, we further compute the average mean and average standard deviation from the 800 RMVD templates.

The results presented in Table 3.8 show that the angle (in rad) is much larger than 0.664 rad, thus invalidating the small angle approximation analysis. Furthermore, the many-to-one property of RGHE is effective as the

mean and the range of angle shown in Table 3.8 indicate that multiple solutions exist (i.e. θ exceeds 2π). To provide a clearer demonstration on the range of angle, histograms that are plotted for a few samples are shown in Fig. 3.10.

Table 3.8: Mean and standard deviation for θ in Radian.

Measurements	**FVC2002 DB1**	**FVC2002DB2**
Average Mean of angle (rad)	11.6851	13.0572
Average S.T.D of angle (rad)	8.7962	10.6427
Range of angle (rad)	≈ 1.57 to 48.69	≈ 1.57 to 67.54
Maximum number of possible inputs corresponding to an output of a single-dimensional eigenfunction	8	10

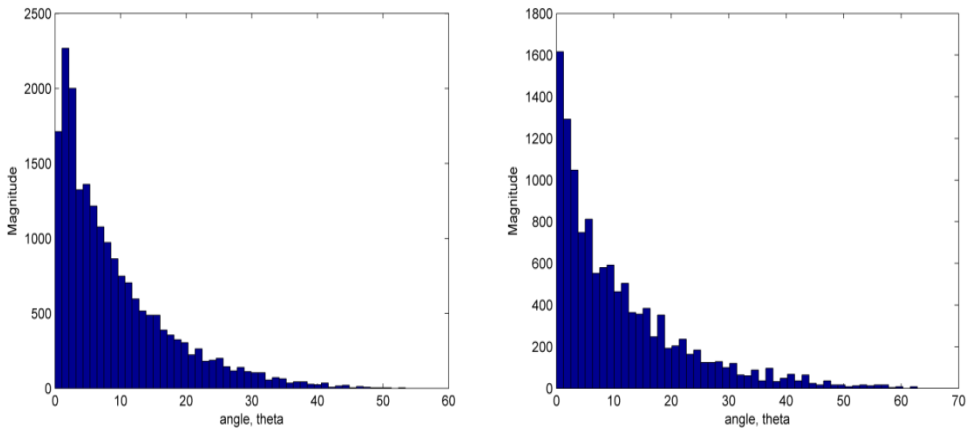


Fig. 3.10: Samples of the distribution of angle θ.

2) Evaluation of invertibility complexity. To evaluate the invertibility of the 36 dimensional eigenfunctions $\xi_i = \prod_{r=1}^{36} \sin\left(\frac{\pi}{2} + \frac{i\pi}{b-a} y_r\right)$ in step 2.1

of algorithm 3.1, it is common to assume that ξ_i is known in this invertibility analysis (e.g., after database is compromised). The hardness of inverting ξ_i lies in the associated number of input possibilities. In table 3.8, it is known that there are 8 and 10 possible inputs associated with ξ_i for FVC2002 DB1 and DB2, respectively. Hence, for FVC2002 DB1 and DB2, the invertibility complexity for single minutia vector decomposition is upper bounded by $8^{36} \approx 2^{118}$ and $10^{36} \approx 2^{129}$, yielding 118 and 129 bits entropy, respectively. To invert N number of vicinities (all elements in Ξ in Step 2.3 of algorithm 3.1), the total invertibility complexity is therefore upper bounded by $8^{36}N \approx 2^{118}N$ and $10^{36}N \approx 2^{129}N$, yielding $118+\log_2(N)$ and $129+\log_2(N)$ bits entropy for FVC2002 DB1 and DB2, respectively.

3.4 Summary

In this chapter, two techniques, namely Two-Dimensional Random Projected Minutia Vicinity Decomposition (2D-RP-MVD) and Randomized Graph-based Hamming Embedding (RGHE), are proposed to generate cancellable fingerprint templates. More precisely, 2D-RP-MVD is designed for 2-dimensional feature matrix (e.g. MVD) and considered as an extension of the 1-diemensional random projection (RP) used in Biohash (Teoh et al., 2004). Besides, 2D-RP-MVD utilizes geometrical invariant features as the source of template; thus, the original minutia coordinates and orientation is well concealed. As the main intention of 2D-RP-MVD, cancelability and non-invertibility can be easily achieved by replacing the external assigned tokens. However, it has been found that random projection is possibly invertible by applying back-projection operation. It requires an additional layer to shield the

biometric templates. RGHE is therefore proposed to serve such purpose. Besides the strong non-invertibility provided by RGHE, it also preserves the accuracy performance compare to the original representation (e.g. minutiae descriptor). Thus, alleviate the security-performance trade-off.

CHAPTER 4

POINT-TO-STRING CONVERSION: FINGERPRINT MINUTIA TO FIXED-LENGTH REPRESENTATIONS USING KERNEL METHODS

ISO/IEC 19794-2 compliant fingerprint minutiae template is an unordered and variable-sized point set data. Such characteristic leads to the restriction for the applications that can only operate on fixed length binary data, such as cryptographic applications and certain biometric cryptosystems e.g. fuzzy commitment. In this chapter, a generic point-to-string conversion framework for fingerprint minutia is proposed based on kernel learning method to generate discriminative fixed length binary string that enables rapid matching. The proposed framework consists of four stages: minutiae descriptor extraction; kernel transformation method that is composed of Kernel Principal Component Analysis or Kernelized Locality-Sensitive Hashing for fixed length vector generation; dynamic feature binarization and matching. The promising experimental results on six datasets from FVC2002 and FVC2004 justify the feasibility of the proposed framework in terms of matching accuracy, efficiency and template randomness.

4.1 Introduction

Fingerprint minutia is certainly the most widely-used fingerprint feature for fingerprint recognition (Maltoni et al., 2009). This is attributed to the observations: (1) minutia are generally reliable and robust to the image noise (Maltoni et al., 2009); (2) unlike global features such as singular point and coarse ridge line shape, minutia provide sufficient distinctiveness for matching (Maltoni et al., 2009). However, minutiae representation defined in ISO/IEC 19794-2 (ISO/IEC 19794-2, 2005) is unordered and variable in size. This is because the number of minutia extracted from multiple impressions of a finger can largely vary due to inherent variations like rotation, translation, and skin elastic deformation. Fig. 4.1 shows two different impressions of the same finger with very different number of detected minutiae.

Fig. 4.1: Two different impressions of the same finger from FVC2004 DB1. There are 12 extracted minutiae in the left image while 27 minutiae in the right, where the circle and square markers represent minutia and core point, respectively.

Traditionally, minutiae-based fingerprint matching is viewed as a 2D point pattern matching in the search of optimal minutiae pairs. Solving this matching problem with Hough transform for instance is computationally expensive and less effective due to its low robustness against non-linear fingerprint elastic deformation (Cappelli et al., 2010). In the past decade, a popular representation, *minutiae descriptor*, was introduced for fingerprint indexing by Hrechak & McHugh (1990) and was later extended for fingerprint recognition by Wahab et al., (1998). A minutiae descriptor characterizes information (e.g. intensity of image, ridge frequency, etc.) in a local neighborhood of a minutia. Generally, the minutiae descriptor can be divided into three categories depending on the feature type (Nagar, 2012): (1) image feature descriptor; (2) minutiae feature descriptor; and (3) texture feature descriptor. The image feature descriptor extracts image intensity information of the local region around a central minutia. The minutiae feature descriptor describes information about a set of neighbor minutiae around a central minutia. The texture feature descriptor captures texture information such as ridge orientation and ridge frequency around a central minutia. In this thesis, the minutiae feature descriptor is mainly focused on.

Minutiae feature descriptor allows *local minutiae* matching, i.e. matching two fingerprints according to the local minutiae structure (Cappelli et al., 2010) due to the rotation, translation, and scaling invariant properties of minutiae descriptor. This alleviates the need of manual fingerprint alignment during fingerprint registration. Thus, a high matching accuracy can be anticipated. To date, a state-of-the-art minutia feature descriptor, namely

Minutiae Cylinder Code (MCC) was reported by Cappelli et al. (2010). Other minutiae feature descriptors can be found as follows: Wahab et al. (1998); Jiang & Yau, (2000); Tico & Kuosmanen, (2003); Jea, & Govindaraju, (2005).

A well-known standard to compare two sets of minutiae descriptors is to carry out a two-stage procedure (Jiang & Yau, 2000): local descriptor matching and global template matching. In the former stage, the similarity values between all local descriptors extracted from the query and template are calculated. In the latter stage, the ratio of the matched descriptor pairs (determined by the threshold) over all the descriptor pairs is computed based on the similarity values as the final matching score between two fingerprints. The two-stage matching procedure has shown better robustness to spurious and missing minutia than the traditional minutiae point-to-point matching (Maltoni et al., 2009; Nagar, 2012; Jiang & Yau, 2000).

Although having such advantages, the minutiae feature descriptor and the minutiae template are: (1) computational expensive in matching due to exhaustive search of corresponding descriptor/minutiae pairs; (2) unordered and variable in size, which leads to inapplicable to certain biometric cryptographic applications, e.g., fuzzy identity based identification (FIBI) (Tan et al., 2012), Fuzzy commitment (Juels & Wattenberg, 1999). Therefore, it would be useful to convert minutiae to *ordered and fixed-length representation* that can be used in biometric cryptographic applications and allow fast matching due to the pure involvement of bitwise operations.

In literature, a number of works for *point-to-string conversion* was reported, such as geometric transformation (Sutcu et al., 2007a; Sutcu et al., 2007b), local point aggregation approach (Sutcu et al., 2008; Nagar et al., 2010b), triplet histogram (Farooq et al., 2007), and spectral minutiae (Xu et al., 2008). However, the accuracy performance deteriorates usually when such a conversion was done (Farooq et al., 2007; Xu et al., 2008), which implies a drop in discriminability. This suggests that the point-to-string conversion and accuracy performance are in disagreement if the algorithm is not carefully designed.

4.1.1 Motivations and Contributions

The primary motivations to construct a bit-string from sole minutiae feature descriptors are described as follows:

❖ *High-performing representation* – From the literature review in Chapter 2 Section 2.2, it is observed that: (1) most of the algorithms reported in FVC2002 and FVC2004 employ a combined features set such as local ridge frequency and ridge counts, which are excluded in the ISO/IEC minutiae template; (2) the existing well-performed point-to-string conversion methods requires registration point, such as core point or delta point (Sutcu et al., 2007a; Sutcu et al., 2007b; Sutcu et al., 2008; Nagar et al., 2010b; Liu et al., 2012; Nandakumar, 2010), which is omitted in ISO/IEC minutiae template as well. Since minutiae template has been standardized by ISO/IEC 19794-2 worldwide, an accurate representation of *minutiae-only* template that is compliant to the standard minutiae format (i.e. ISO/IEC 19794-2) is preferred.

❖ *Demand for fast matching* – Sole minutia and minutiae descriptor set are computational expensive in matching as discussed in Section 4.1. To alleviate the problem of high matching cost, converting minutiae template into binary representation and matching in the Hamming domain is a feasible solution due to the pure involvement of bit-wise operations. Furthermore, binary representation could facilitate 1: N identification schemes.

❖ *Usage in bio-crypto-key generation schemes* – Most of the biometric cryptosystems such as fuzzy commitment (Juels & Wattenberg, 1999) and fuzzy identity-based identification schemes (Tan et al., 2012) necessitate the biometric data to be availed in the fixed-length ordered integer or bit-string form. However, the incompatibility problem exists for fingerprint minutia as it is unordered and variable in size. Hence, the research on point-to-string conversion methods is non-trivial.

In this thesis, a novel usage of kernel learning (KL) method is demonstrate to construct a fixed-length ordered binary vector from unordered variable-size minutiae descriptor via a projection matrix. The KL was originally meant to map the input data to Reproducing Kernel Hilbert Space (RKHS) via the Mercer's kernel function to harness a richer representation of the data distribution (Shawe-Taylor & Cristianini, 2004). However, instead of considering a direct point-to-string conversion problem, an unconventional treatment of using KL method to convert the *fixed-size training samples to fixed-length vector* is explored. In this regard, an admissible kernel function for this purpose is designed. According to Mercer's theorem, only symmetric and positive definite (SPD) kernels would delineate valid RKHS (Shawe-

Taylor & Cristianini, 2004). Unfortunately, such a SPD kernel is inadmissible in this problem when the non-metric dissimilarity measure is applied to compute the distance of a pair of unordered variable-size fingerprint templates. Hence it is a challenge to address this problem in this work.

In the proposed framework, a minutiae descriptor known as Polar Grid-based 3-Tuple Quantization (PGTQ) proposed in (Jin et al., 2012) is adopted. However, the original PGTQ is simplified for kernel transformation purpose while preserving its alignment-free property. Two kernel methods, namely Kernel Principal Component Analysis (KPCA) and Kernelized Locality-Sensitive Hashing (KLSH) are explored to generate ordered and fixed-length feature vector. Then a dynamic feature binarization technique (Lim et al., 2012) is incorporated to convert the resulting transformed vector to bit-string. The main contributions of this work are as follows:

- A generic point-to-string conversion framework via kernel-learning method is proposed.
- A modified PGTQ minutia descriptor is proposed, which is alignment-free and computationally efficient for kernel transformation.
- A novel SPD kernel function based on a non-metric dissimilarity measure of a pair of unordered variable-size fingerprint templates is proposed.
- It validates that the symmetric and positive definite property of a kernel function is essential for gaining good performance.

- ❖ Performance justifications for kernel PCA and kernel LSH on six benchmark databases and an effect analysis is provided when dynamic quantization is incorporated.
- ❖ Entropy estimation via second-order dependency tree as well as statistical independence test to examine the randomness and the correlation between the binary templates of different identities are performed.

The rest of this chapter is organized as follows: the preliminaries of kernel LSH, kernel PCA are introduced in Section 4.2. Details about the modified PGTQ descriptor, kernel-based transformation and template matching are described in Section 4.3. The experimental results and performance analysis are provided in Section 4.4. The entropy estimation of the resulted bit string is demonstrated in Section 4.5. The implementation of fuzzy commitment using proposed bit string is given in Section 4.6. Finally, discussion and conclusion are presented in Section 4.7.

4.2 Preliminaries

4.2.1 Kernel Principal Component Analysis

Principal component analysis (PCA) is an orthogonal transformation that converts a set of correlated data into a set of linearly uncorrelated data, called principal component (Schölkopf et al., 1998). Let a set of data $\mathbf{x}_j$, $j = 1, \dots, \ell$, $\mathbf{x}_j \in \mathbb{R}$, $\sum_{j=1}^{\ell} \mathbf{x}_j = 0$, the covariance matrix of $\mathbf{x}_j$ can be defined as:

$$\boldsymbol{C} = \frac{1}{\ell}\sum_{j=1}^{\ell} \mathbf{x}_j \mathbf{x}_j^{\mathrm{T}} \tag{4.1}$$

Then the eigen-decomposition of the covariance matrix $\boldsymbol{C}$ can be solved by

$$\lambda \mathbf{v} = \boldsymbol{C}\mathbf{v} \tag{4.2}$$

where $\mathbf{v}$ and λ represent the eigenvectors and eigenvalues, respectively.

To project a test feature, $\mathbf{x}_{test}$ the projected feature vectors $\mathbf{Y}$ is computed by projecting $\mathbf{x}_{test}$ onto principle component $\mathbf{v}_{\boldsymbol{pc}} \subset \mathbf{v}$ as shown in eq. (4.3)

$$\mathbf{Y} = \mathbf{v}_{\boldsymbol{pc}}^{\mathrm{T}} \mathbf{x}_{test} \tag{4.3}$$

However, it is noted that PCA holds an improbable assumption that the data are multivariate Gaussian distributed. This limitation motivates the introduction of kernel PCA (Schölkopf et al., 1998). The basic idea of kernel PCA is to apply a nonlinear function $\Phi(\cdot)$ to a set of data $\mathbf{x}_j$ on the kernel space. Let the data $\mathbf{x}_j$ to be mapped onto a feature space, $\Phi(\mathbf{x}_1), \ldots, \Phi(\mathbf{x}_\ell)$, where $\sum_{j=1}^{\ell} \Phi(\mathbf{x}_j) = 0$. The covariance matrix is computed by

$$\overline{\boldsymbol{C}} = \frac{1}{\ell}\sum_{j=1}^{\ell} \Phi(\mathbf{x}_j)\Phi(\mathbf{x}_j)^{\mathrm{T}} \tag{4.4}$$

Similar to eq. (4.2), it is required to find eigenvalues $\bar{\lambda}$ and eigenvectors $\bar{\mathbf{v}}$ satisfying eq. (4.5) in the feature space

$$\bar{\lambda}\bar{\mathbf{v}} = \overline{\boldsymbol{C}}\bar{\mathbf{v}} \tag{4.5}$$

By substituting eq. (4.4) into eq. (4.5), the eigenvectors can be expressed in terms of coefficients $a_1,\ldots,a_\ell$ and derived into eq. (4.6) (Schölkopf et al., 1999)

$$\bar{\mathbf{v}} = \sum_{i=1}^{\ell} a_i \Phi(\mathbf{x}_i) \tag{4.6}$$

By defining a $\ell \times \ell$ kernel matrix **K**, such that

$$\mathbf{K} = k(x,y) = \langle \Phi(x) \cdot \Phi(y) \rangle = \Phi(x)^T \Phi(y) \tag{4.7}$$

Substituting eq. (4.4), eq. (4.6), and eq. (4.7) into $\bar{\lambda}\bar{\mathbf{v}} = \bar{\boldsymbol{C}}\bar{\mathbf{v}}$ yield

$$\ell\tilde{\boldsymbol{\lambda}}\boldsymbol{\alpha} = \mathbf{K}\boldsymbol{\alpha} \tag{4.8}$$

where $\boldsymbol{\alpha}$ and $\tilde{\boldsymbol{\lambda}}$ are the eigenvectors and eigenvalues of **K**. Then the eigenvectors is normalized using $(\boldsymbol{a}_i)^{\mathrm{T}}\boldsymbol{a}_i = 1$.

The testing feature $\mathbf{x}_{test}$ is projected onto the principle component as shown in eq. (4.9) by substituting eq. (4.6), eq. (4.7), where $\bar{\mathbf{v}}_{pc} \subset \bar{\mathbf{v}}$ and $\bar{\boldsymbol{\alpha}} \subset \boldsymbol{\alpha}$. Some Mercer's admissible kernels are Linear Kernel $k(x,y) = x^{\mathrm{T}}y + c$, Polynomial Kernel $k(x,y) = (ax^{\mathrm{T}}y + c)^d$, and Gaussian Kernel $k(x,y) = \exp(-\|x-y\|^2/2\sigma^2)$.

$$\bar{\mathbf{Y}} = \bar{\mathbf{v}}_{pc}{}^{\mathrm{T}}\Phi(\mathbf{x}_{test}) = \sum_{i=1}^{\ell} \bar{\boldsymbol{\alpha}}_i \Phi(\mathbf{x}_i)^{\mathrm{T}}\Phi(\mathbf{x}_{test}) = \sum_{i=1}^{\ell} \bar{\boldsymbol{\alpha}}_i k(\mathbf{x}_i, \mathbf{x}_{test}) \tag{4.9}$$

4.2.2 Kernelized Locality-Sensitive Hashing

Locality-Sensitive Hashing (LSH) (Gionis et al., 1999; Charikar 2002) is an algorithm that searches approximate nearest neighbors that preserves the property: $\Pr\big[h(x_i) = h\big(x_j\big)\big] = sim(x_i, x_j)$, where h is the hash function and

$sim(x_i, x_j) \in [0,1]$, is the similarity function. Charikar et al., (2002) proposed a hash function $h_c(x)$ for inner product similarity: $sim(x_i, x_j) = x_i^T x_j$ based on rounding the output of a product with a random hyperplane:

$$h_c(x) = \begin{cases} 1 & w_c^T x > 0 \\ 0 & \text{otherwise} \end{cases} \tag{4.10}$$

where $w_c = [w_{c1}, w_{c2}, \dots, w_{cd}]^T$ is a random hyperplane from a zero-mean multivariate Gaussian $N(0,1)$ of dimension *d*. It is noted that based on the random projection, the performance of LSH is provable due to the Johnson-Lindenstrauss lemma (Johnson & Lindenstrauss, 1984).

However, considering the case that the feature space embedding is unknown or computationally infeasible, it is therefore impossible to apply the original LSH in this case. Kulis and Grauman (2012) proposed the Kernelized Locality-Sensitive Hashing (KLSH) based on central limit theorem (CLT) (Rice, 2001), which allows approximation of a random vector using a set of training data. KLSH can be summarized in the following four steps:

- Select *p* data points and form a kernel matrix **K** over this data.
- Centralize the kernel matrix.
- Form the hash table over database items: For each hash function $h(\phi(x))$, form $\boldsymbol{e}_s$by selecting *n* indices at random from $[1, \dots, p]$, then form weighted matrix $w = \mathbf{K}^{-1/2}\boldsymbol{e}_s$, and assign bits according to $h(\phi(x)) = \text{sign}(\sum_i w(i)k(x, x_i))$. Note that $\boldsymbol{e}_s$ is a vector with ones in the entries corresponding to the indices of dataset *S*.

❖ For each query, form a hash key using these hash functions and employ existing LSH methods to find the approximate nearest neighbors.

4.3 Proposed Framework

The proposed kernel learning-based framework for point-to-string conversion is shown in Fig. 4.2. Generally, this framework consists of four main components: minutiae descriptor extraction, kernel learning based transformation, feature binarization and matching.

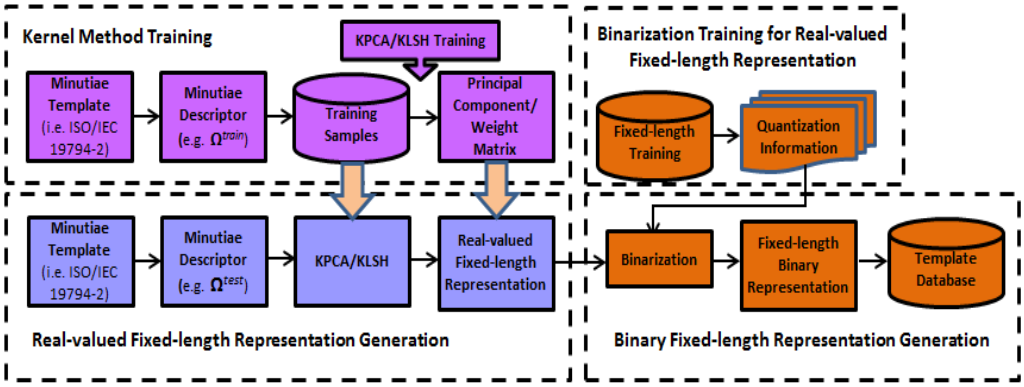


Fig. 4.2: Overall block diagram of the transformation for fixed-length representation, where $\boldsymbol{\Omega}^{train}$ and $\boldsymbol{\Omega}^{test}$ represent the training and testing samples of PGTQ-based minutiae descriptor, respectively.

4.3.1 Polar Grid based 3-Tuple Quantization (PGTQ)

PGTQ (Jin et al., 2012) is an alignment-free minutiae descriptor that utilizes the variable-size tessellated quantization in polar coordinate. The sectors near the reference minutia have smaller area and vice versa. This leads to a smaller (resp. larger) quantization step surrounding (resp. further away from) the reference minutia to tolerate fingerprint elastic deformation. In the

original PGTQ-based descriptor, polar coordinate covers the entire image and produce lengthy bit-string, which leads to the computational infeasibility of kernel-based transformation in Section 4.3.2. As a solution, it considers the polar coordinate that only covers a partial image limited by the radius *R*. Thus, the bit-length of the resultant bit-string can be significantly reduced. The details of the modified PGTQ-based descriptor are described as follows:

1. Let $m_r = \{x_r, y_r, \theta_r\}$ be the reference minutiae. The neighboring minutiae within a radius *R* in Euclidean distance are rotated and translated based on the reference minutiae using eq. (4.11) and eq. (4.12). The transformed minutiae are represented as, $m^t = \{x_i^t, y_i^t, \theta_i^t | i = 1, \dots N_R - 1\}$ where N_R is the total number of minutiae within a pre-defined radius *R*.

$$\begin{bmatrix} x_i^t \\ y_i^t \end{bmatrix} = \begin{bmatrix} \cos\theta_r & -\sin\theta_r \\ \sin\theta_r & \cos\theta_r \end{bmatrix} \begin{bmatrix} x_i - x_r \\ -(y_i - y_r) \end{bmatrix} \tag{4.11}$$

$$\theta_i^t = \begin{Bmatrix} \theta_i - \theta_r; & \theta_i \geq \theta_r \\ 360 + \theta_i - \theta_r; & \theta_i < \theta_r \end{Bmatrix} \tag{4.12}$$

2. The translated and rotated minutiae are then converted into polar coordinates using eq. (4.13) and eq. (4.14). ρ_i and α_i indicate the radial distance (in pixels) and the radial angle of the *i*-th minutia in Polar coordinates ($\alpha_i \in (0, 360]$), respectively.

$$\rho_i = \sqrt{(x_i^t)^2 + (y_i^t)^2} \tag{4.13}$$

$$\alpha_i = \arctan(\frac{y_i^t}{x_i^t}) \tag{4.14}$$

3. 3-Tuple based Quantization. The 3-tuple based quantization is a sector-based quantization for all minutiae. Each quantized minutia can be represented as a vector, $\omega = \{\rho^q, \alpha^q, \theta^q\}$, such that

$$\rho_i^q = \lfloor \rho_i / x \rfloor \tag{4.15}$$

$$\alpha_i^q = \lfloor \alpha_i / y \rfloor \tag{4.16}$$

$$\theta_i^q = \lfloor \theta_i / z \rfloor \tag{4.17}$$

where '/' denotes quotient; *x*, *y* and *z* indicate the radius of the polar grid segment (in pixels), radial angle for tolerance ($y \in (0, 360]$) and orientation angle to be tolerated $z \in (0, 360]$, respectively. The quantization level is hence determined by *x*, *y* and *z*.

4. Binarization. After quantization, polar grids can be binarized using the quantized feature vector. A simple rule is defined to generate binary string that if a polar grid contains two and above minutia (represented in $\omega = \{\rho^q, \alpha^q, \theta^q\}$) then it is marked as 1 otherwise 0. The length of the resultant bit-string is $l = (R/x) \times (360/y) \times (360/z)$, which is equivalent to the total number of polar grids.

The above steps are repeated for the remaining minutiae to generate the full binary PGTQ minutiae descriptor. This template, denoted as $\mathbf{\Omega} \in \{0,1\}^{N_m \times l}$ is variable in size because the total minutiae number (N_m) extracted from each fingerprint image is different.

5. Matching. Due to variable-size of PGTQ-based minutiae descriptor, the typical two-stage matching strategy: local descriptor matching and

global matching is adopted. The local descriptor matching searches for the intersections between two binary strings in which the PGTQ-based descriptor is represented.

Let $\boldsymbol{\Omega}^e = [\boldsymbol{b}_1^e; \boldsymbol{b}_2^e, \dots, \boldsymbol{b}_{n^e}^e]$ and $\boldsymbol{\Omega}^q = [\boldsymbol{b}_1^q; \boldsymbol{b}_2^q, \dots, \boldsymbol{b}_{n^q}^q]$ be the enrolled and query PGTQ-based minutiae descriptor sets that consist of n^e and n^q *l-bit* binary strings, respectively. From here onwards, we slightly abuse the notation of $\boldsymbol{b}$, where $\boldsymbol{b}_{i,k}$ represents the *k*-th bit for *i*-th binary string where $1 \leq k \leq l$ and $1 \leq i \leq n^e$ or n^q. To take into account the difference of minutiae quantity in the enrolled and query image, the similarity scores between two local descriptors $\boldsymbol{\Omega}^e$ and $\boldsymbol{\Omega}^q$ is normalized as follows:

$$S_{ij}^b = \frac{(N_j^q + N_i^e)\sum_{k=1}^{l}(\boldsymbol{b}_{j,k}^q \bullet \boldsymbol{b}_{i,k}^e)}{(N_j^q)^2 + (N_i^e)^2} \tag{4.18}$$

where S^b denotes matching score between two binary strings and • represents the bitwise AND operator, $N_i^e = \sum_{k=1}^{l}(\boldsymbol{b}_{i,k}^e)$ and $N_j^q = \sum_{k=1}^{l}(\boldsymbol{b}_{j,k}^q)$ denote the total number of 1's of the enrolled and query bit-strings, respectively. The $\sum_{k=1}^{l}(\boldsymbol{b}_{j,k}^q \bullet \boldsymbol{b}_{i,k}^e)$ term in (4.18) sums the bit positions that have value '1' in both the query and enrolled bit-strings. The scores $S^b \in \mathbb{R}^{n^q \times n^e}$ range from 0 to 1 where '1' indicates a perfect match and vice versa.

Once the similarity score matrix S^b is calculated from the local descriptor matching; a global matching process is carried out. Given the score matrix $S^b = \{s_{ij}^b\}$, the final score can be calculated as:

$$S_{PGTQ} = \max\{\frac{1}{m}\sum_{j} s_{j(max)}, \frac{1}{n}\sum_{i} s_{i(max)}\} \tag{4.19}$$

where $s_{j(max)} = \max_i\{s_{ij}^b\}$ and $s_{i(max)} = \max_j\{s_{ij}^b\}$ represent the maximum score component of *i*-th column and *j*-th row, respectively. The detailed matching process is illustrated in Algorithm 4.1.

Algorithm 4.1: Matching Two PGTQ-based Minutiae Descriptors (variable-size)

Input $\mathbf{\Omega}^e$, $\mathbf{\Omega}^q$, n^q and n^e

Function Prototype: $sim(\mathbf{\Omega}^e, \mathbf{\Omega}^q)$

$n^e \leftarrow \text{size}(\mathbf{\Omega}^e)$

$n^q \leftarrow \text{size}(\mathbf{\Omega}^q)$

For $i = 1: n^e$

$B_i^e = \mathbf{\Omega}^e(i)$

For $j = 1: n^q$

$B_j^q = \mathbf{\Omega}^q(j)$

Calculate similarity score s_{ij}^b between $\boldsymbol{b}_i^e$ and $\boldsymbol{b}_j^q$ using eq. (4.18)

End for

End for

$S^b = \{s_{ij}^b\}$

$s_{j(max)} = \max_i\{s_{ij}^b\}$

$s_{i(max)} = \max_j\{s_{ij}^b\}$

$$S_{PGTQ} = \max\{\frac{1}{m}\sum_j s_{j(max)}, \frac{1}{n}\sum_i s_{i(max)}\}$$

Output The matching score, S_{PGTQ} between $\mathbf{\Omega}^e$ and $\mathbf{\Omega}^q$.

4.3.2 Kernel Method based Fixed-length Transformation

In the proposed framework, the fixed-length representation is induced by the fixed number of training samples and the projection matrix produced by the kernel methods. The procedure of the kernel learning-based point-to-string conversion can be described as follows:

1. *Kernel matrix computation*. Let $\mathbf{\Omega} = \{\mathbf{\Omega}^{train}(i) | i = 1: N_{train}\}$ be a set of training samples for PGTQ-based minutiae descriptor and N_{train}

denotes the total number of $\boldsymbol{\Omega}^{train}$. A kernel matrix $\boldsymbol{K} \in \mathbb{R}^{N_{train} \times N_{train}}$ can be constructed by using the following kernel function:

$$\begin{aligned} \boldsymbol{K}(i,j) &= k\left(\boldsymbol{\Omega}^{train}(i), \boldsymbol{\Omega}^{train}(j)\right) \\ &= \exp(-\left(1 - S_{PGTQ}(i,j)\right)^2 / 2\sigma^2) \end{aligned} \tag{4.20}$$

where $S_{PGTQ} \in [0,1]$ is the dissimilarity measure that described in eq. (4.18) and eq. (4.19).

Unlike Mercer's kernel matrix that admits metrics such as inner product or Euclidean distance, the kernel matrix computed with sole $S_{PGTQ}(i,j)$ is indeed non-SPD, in the sense that it is neither symmetric nor positive definite. This may potentially deteriorate the accuracy performance of Kernel based methods (Wu et al., 2005; Pękalska & Haasdonk, 2009). In order to rectify this problem, we follow Jayasumana et al. (2013) by applying a heat kernel function shown in eq. (4.20) to induce a SPD kernel function subject to specific range of spread factor, σ. The feasible range of σ that enables SPD property will be shown experimentally in Section 4.4.2. Experiment results show that SPD property is an essential factor for accuracy performance, which will be justified in Section 4.4.2 too.

2. With the computed $\boldsymbol{K}$, the projection matrix $\widetilde{\boldsymbol{\alpha}}$ (i.e. eigenvectors of KPCA or weighted matrix of KLSH) can be obtained by eq. (4.8), $\overline{\boldsymbol{\alpha}} \in \mathbb{R}^{N_{train} \times N_{dim}}$, where N_{dim} denotes the number of desired output dimension.

3. *Transformation of variable-size PGTQ-based descriptor to fixed-length real-valued representation.* Let $\mathbf{\Omega}^{test} = \{\mathbf{\Omega}^{test}(i) | i = 1: N_{test}\}$ be a set testing samples of PGTQ-based descriptor.

Step 1) $\mathbf{\Omega}^{test}$ is first matched with all training samples $\mathbf{\Omega}^{train}(i)$ for $1 \leq i \leq N_{train}$. Subsequently, a fixed vector $\mathbf{v}^{fl} \in \mathbb{R}^{1 \times N_{train}}$ is formed by concatenating N_{train} matching scores.

$$\mathbf{v}_i^{fl} \leftarrow sim(\mathbf{\Omega}^{test}, \mathbf{\Omega}^{train}(i)) \tag{4.21}$$

Step 2) $\mathbf{v}_i^{fl}$ is then transformed into the kernel space using the kernel function defined in eq. (4.20), in which the transformed feature vector $\bar{\mathbf{v}}^{fl}$ can be described by

$$\bar{\mathbf{v}}^{fl} = \exp(-(1 - \mathbf{v}^{fl})^2 / 2\sigma^2) \tag{4.22}$$

Step 3) The fixed-length ordered real-valued vector can be generated by projecting the $\bar{\mathbf{v}}^{fl}$ using the projection matrix $\bar{\boldsymbol{\alpha}}$.

$$T^{fl} = \bar{\mathbf{v}}^{fl} \bar{\boldsymbol{\alpha}} \tag{4.23}$$

where $\bar{\mathbf{v}}^{fl} \in \mathbb{R}^{1 \times N_{train}}$ and $\bar{\boldsymbol{\alpha}} \in \mathbb{R}^{N_{train} \times N_{dim}}$. Thus, the length of T^{fl} is N_{dim}. Algorithm 4.2 presents the pseudo-code of kernel-method-based transformation.

Algorithm 4.2: Kernel Method based Fixed-length Transformation

Input $\mathbf{\Omega}^{train}$, $\mathbf{\Omega}^{test}$, N_{dim} and σ

Stage 1: Kernel Matrix Computation

1.1: $N_{train} = \text{length}(\mathbf{\Omega}^{train})$

1.2: Initialize $\boldsymbol{K}(i, j) = 1,\ 1 \leq i, j \leq N_{train}$

1.3: *For* i = 1: N_{train}

For j = 1:i

$\boldsymbol{K}(i,j) = sim(\boldsymbol{\Omega}^{train}(i), \boldsymbol{\Omega}^{train}(j))$

$\boldsymbol{K}(i,j) = \exp(-\left(1 - k(i,j)\right)^2 / 2\sigma^2)$

End for

End for

1.4: Make $\boldsymbol{K}$ symmetric

Stage 2: Compute The Projection Matrix $\bar{\boldsymbol{\alpha}}$

2.1(a): $\bar{\boldsymbol{\alpha}} \leftarrow$ KPCA($\boldsymbol{K}$) or

2.1(b): $\bar{\boldsymbol{\alpha}} \leftarrow$ KLSH($\boldsymbol{K}$), $\bar{\boldsymbol{\alpha}} \in \mathbb{R}^{N_{train} \times N_{dim}}$

Stage 3: Transform variable-size PGTQ to fixed-length vector

3.1: Initialize $\mathbf{v}^{fl}(i)$, $\bar{\mathbf{v}}^{fl}(i) = 1$; $1 \leq i \leq N_{train}$

For i=1: N_{train}

$\mathbf{v}^{fl}(i) \leftarrow sim(\boldsymbol{\Omega}^{test}, \boldsymbol{\Omega}^{train}(i))$

$\bar{\mathbf{v}}^{fl}(i) = \exp(-\left(1 - \mathbf{v}^{fl}(i)\right)^2 / 2\sigma^2)$

End for

3.2: $T^{fl} = \bar{\mathbf{v}}^{fl}\bar{\boldsymbol{\alpha}}$

3.3: Save T^{fl}

Output The real-valued fixed-length representation T^{fl}

In our treatment, the training data (i.e. PGTQ descriptor) are required to be stored for fixed-length representations generation. However, if the training data stored in database is compromised, the security and privacy of the system is highly vulnerable to template replay, spoof construction and targeted false accepts (Nagar, 2012). To alleviate this problem, we adopted a random bits-toggling process presented in (Farooq et al., 2007). This process is to randomly select a fraction of bits and set 0 bit to 1 bit and vice-versa. Such a process resembles to adding noises with the intention to distort the training data. Since PGTQ descriptor is a feature matrix; the bits-toggling process is applied in row-wise basis. Further, techniques such as incremental KPCA (Chin & Suter, 2007) can be adapted to avoid re-training of new afresh projection matrix when a new user is enrolled to the system.

4.3.3 Feature Vector Binarization

Biometric feature binarization is the process of converting real-valued biometric features into a binary string. Generally, two approaches, namely static and dynamic binarization techniques, are widely used based on the fixed or varied number of intervals defined in each feature space (Lim & Teoh, 2012; Lim & Teoh, 2013). More specifically, biometric binarization can be decomposed into two essential components: biometric quantization and feature encoding. These components may be governed by a static or dynamic bit allocation algorithm, determining whether the quantity of binary bits allocated to every feature dimension is fixed or varied respectively. In this chapter, two different binarization methods, zero-thresholding quantization and reliability-based dynamic quantization method (Lim et al., 2012) are investigated.

- Zero-thresholding quantization. Each feature space is partitioned into two quantization intervals based on a global threshold (zero) and a single-bit encoding scheme with two binary labels ('0' and '1') is employed. Zero-thresholding quantization is a special case of static quantization, wherein the threshold is zero. This quantization technique can be formulated by using a simple rule shown in eq. (4.24)

$$b_i = \begin{cases} 1 & \text{if } T_i^{fl} \geq 0 \\ 0 & \text{if } T_i^{fl} < 0 \end{cases} \tag{4.24}$$

where T_i^{fl} denotes the *i*-th elements of the PGTQ-based template T^{fl} and b_i represents the *i*-th binary value corresponding to the *i*-th elements of T^{fl}.

❖ Reliability-based dynamic quantization. In contract to static approach, dynamic quantization approach assigns a varied number of allocated bits to each feature component according to the distinct discriminability of user-specific feature. In this chapter, an instance of dynamic quantization, namely reliability-based dynamic quantization proposed by Lim et al. (2012) is adopted. I briefly describe the procedure of this method as follows:

1. Statistical analysis

Let *I* be the number of users participated the training process and N^t be the number of training samples for each user. T^{fl} denotes the real-valued fixed-length representation.

Step 1.1 Compute the mean feature vector μ_i^{fm} of user *i*, and the grand mean vector μ^g.

$$\mu_{id}^{fm} = \frac{1}{N^t}\sum_{j=1}^{N^t} T_{ijd}^{fl} \qquad (4.25)$$
$$\mu_i^{fm} = [\mu_{i1}^{fm} \dots \mu_{iN_{dim}}^{fm}]$$

$$\mu_d^g = \frac{1}{I \cdot N^t}\sum_{j=1}^{N^t}\sum_{i=1}^{I} T_{ijd}^{fl} \qquad (4.26)$$
$$\mu^g = [\mu_1^g \dots \mu_{N_{dim}}^g]$$

where *j* and *d* denotes *j*-th sample of user *i* and *d*-th dimension of T^{fl} respectively.

Step 1.2 Compute the within-class variance vector v_i^{wc} of *i*-th user and the between-class variance vector v^{bc}.

$$v_{id}^{wc} = \frac{1}{N^t}\sum_{j=1}^{N^t}(T_{ijd}^{fl} - \mu_{id}^{fm})^2 \tag{4.27}$$
$$v_i^{wc} = [v_{i1}^{wc} \dots v_{iN_{dim}}^{wc}]$$

$$v_d^{bc} = \frac{1}{I}\sum_{i=1}^{I}(\mu_{id}^{fm} - \mu_d^g)^2 \tag{4.28}$$
$$v^{bc} = [v_1^{bc} \dots v_{N_{dim}}^{bc}]$$

Step 1.3 Calculate the signal-to-noise ratio vector ε_i of *i*-th user.

$$\varepsilon_i = [\varepsilon_{i1} \dots \varepsilon_{iN_{dim}}] = \left[\frac{v_1^{bc}}{v_{i1}^{wc}} \dots \frac{v_{N_{dim}}^{bc}}{v_{iN_{dim}}^{wc}}\right] \tag{4.29}$$

2. Reliability weight computation

According to equal background probability mass of normal distribution, feature space is quantized into 2^n intervals. Each interval is labeled with a *n*-bit gray code. With the fixed-length representation T^{fl} obtained from Section 4.3.2, following conversion is performed.

Step 2.1 Each real-valued component of T^{fl} is mapped to a *n*-bit gray code segment according to the interval labels.

$$GC(T_{ijd}^{fl}) = [b_{ijd}^1 \dots b_{ijd}^n] \tag{4.30}$$

where b_{ijd}^xdenotes the *x*-th bit allocated to *d*-th feature component for *j*-th samples of *i*-th user.

Step 2.2 Compute the reliability weight vector w_d for each binarized feature component by counting the agreeing bits at very bit position and dividing each summation.

$$w_d = \{w_{d1}, w_{d2}, \dots, w_{dn}\} = \left\{\sum_{i=1}^{I} b_{id1}/I, \sum_{i=1}^{I} b_{id2}/I, \dots, \sum_{i=1}^{I} b_{idn}/I,\right\} \quad (4.31)$$

Step 2.3 Repeat step 2.1 and 2.2 for all $d \in [1, N_{dim}]$. Then concatenate the all w_d to obtain a user-specific reliability weight vector.

3. Bit allocation based on weighted reliability and sorted feature

Step 3.1 Sort the feature vector in descending order according to the signal-to-noise ratio ε_i obtained in step 1.3. The sorted indices of the feature components are stored as

$$[s_i(1), s_i(2), \dots, s_i(N_{dim})] \leftarrow sort_{desc}(\varepsilon_i) \quad (4.32)$$

Step 3.2 In order for selecting most reliable M_{rb}bits from extracted N_{dim} bits string, a reliability weight threshold τ_{rw} is defined as

$$\tau_{rw} = 1 - N_{step} \quad (4.33)$$

where N_{step} denoting an incremental variable range from 0 to 0.5 with a sorting step of $N_{step} = \frac{1}{N^t}$. The bit allocation process is described as follow: start from the first sorted feature component; if the *j*-th bit is satisfied with threshold τ_{rw}, this bit is selected and proceed to the $(j+1)$ bits; otherwise, the *j*-th bit is ignored and the following $(j+1)$ bits are evaluated consecutively. Let M_{bit} be the number of bits for the binarized representation of T^{fl}; consider that the total number of selected bits is less than M_{bit} after the selection process travelled the

entire sorted feature components; the same process repeats with a step down reliability weight threshold.

Step 3.3 Once the most M_{rb} discriminable and reliable bits have been selected, the sort is terminated. The number of bits selected for *d*-th feature components of the user, $m_{id}^{b} \in \{1, \dots, n\}$.

$$M_{rb} = \sum_{i=1}^{N_{dim}} m_{id}^{b} \tag{4.34}$$

It can be observed that the quantization intervals are varied for different feature component. For every dimension *d*, the cutpoints of $2^{m_{id}^{b}}$ intervals and all m_{id}^{b} values are stored as helper data.

4.3.4 Matching Two Fixed-length Representations

It considers two types of representation for fixed-length matching: real-valued and binary.

- [Real-valued]: Let $T_k^{flr,e}$ and $T_k^{flr,q}$ be two fixed-length real-valued representations. The matching score is

$$S_r^{fl} = \frac{\sum_{k=1}^{N_{dim}} (T_k^{flr,e} * T_k^{flr,q})}{\sum_{k=1}^{N_{dim}} (T_k^{flr,e})^2 + \sum_{k=1}^{N_{dim}} (T_k^{flr,q})^2} \tag{4.35}$$

where $*$represents an element-wise multiplication operator; $\sum_{k=1}^{N_{dim}} (T_k^{flr,e})^2$and $\sum_{k=1}^{N_{dim}} (T_k^{flr,q})^2$ denote the summation of squared element of $T_k^{flr,e}$ and $T_k^{flr,q}$ respectively.

- [Binary]: Let $T_k^{flr,e}$ and $T_k^{flr,q}$ be the two fixed-length binary representations. The matching score is

$$S_b^{fl} = 1 - \frac{\sum_{k=1}^{M_{bit}} (T_k^{flr,e} \oplus T_k^{flr,q})}{M_{bit}} \quad (4.36)$$

where $\oplus$ represents a bit-wise XOR operator; M_{bit}denotes the bit-length of the binary representation $T_k^{flr,e}$and $T_k^{flr,q}$.

4.4 Experiment Analysis

The experiments were conducted on six public fingerprint datasets, FVC2002 (DB1, DB2, DB3) and FVC2004 (DB1, DB2, DB3). Each dataset consists of 100 users with 8 samples per user. In total, there are 800 (100×8) fingerprint images for each dataset. VeriFinger 7 SDK was used for minutia extraction. The minutiae template is extracted according to ISO-complaint format for evaluation, i.e. (x, y, θ). The performance of the proposed framework is evaluated using Equal Error Rate (EER), Area under the curve (AUC) and receiver operating characteristic (ROC) as well as genuine-imposter distribution. In addition, the degree-of-freedom (DOF) and entropy (bits)/information rate are used in the statistical independence test and for entropy estimation, respectively.

4.4.1 Experiment Settings

Various representations involved in this chapter are abbreviated as follows:

- VSB – variable-sized binary PGTQ-based template;
- TKLSH – kernel LSH based fixed-length real-valued template;
- TKPCA – kernel PCA based fixed-length real-valued template;

- ❖ TKLSH-ZT – kernel LSH based fixed-length binary template with zero-thresholding method;
- ❖ TKPCA-ZT – kernel PCA based fixed-length binary template with zero-thresholding method;
- ❖ TKLSH-DQ – kernel LSH based fixed-length binary template with dynamic quantization method;
- ❖ TKPCA-DQ – kernel PCA based fixed-length binary template with dynamic quantization method;

For matching, the matching technique described in algorithm 4.1 is used for VSB; eq. (4.35) is applied for fixed-length real-valued templates in TKLSH and TKPCA; and eq. (4.36) is used for matching fixed-length binary templates i.e. TKLSH-ZT, TKLSH-DQ, TKPCA-ZT and TKPCA-DQ).

For VSB matching, the first sample (gallery) of every identity in each dataset is matched against the remaining samples (probe) of every identity for false rejection rate (FRR) calculation. On the other hand, the first sample of each identity is matched against the first sample of the remaining identities for false acceptance rate (FAR) calculation. This matching method yields 700 genuine scores and 4950 imposter scores for each dataset. When matching the real-valued fixed-length representations, the first three samples of every identity are used for training and the remaining five are used for testing, yielding 400 genuine scores and 4950 imposter scores for each dataset. When matching fixed-length binary template, we consider the scenario where if user A is matched against user B, user A has to use user B's helper data to generate

binary template and compare to user B's binary template generated using its own helper data (i.e. user B's helper data). This results 400 genuine scores and 9900 imposter scores for each dataset.

As discussed in Section 4.3.2, the bits-toggling process is applied to distort the training samples. However, Farooq et al. (2007) reveals that large number of randomly toggling bits deteriorate accuracy performance; anyhow, by carefully selecting a portion of bits for flipping, the error rate does not increase significantly (Farooq et al., 2007). In our experiment, a 5-bits toggling is set, which approximately is 50% (10 bits) of total number of 1s in each bit-string averagely. This indicates that a significant portion of noise (50%) has been added while accuracy does not decrease significantly as shown in Table 4.4.

Table 4.1 tabulates various parameter settings used in the experiments. All parameter values in Table 4.1 are commonly applied to all six data sets, except the N_{dim}, M_{bit} and kernel width σ in eq. (4.20) because these are dataset-specific parameters that requires tuning.

Table 4.1: Parameters used in the experiments.

Symbol(s)	Description	Value
R	Radius for polar coordinates (in pixel)	70
x	Radius of polar grid segment (in pixel)	10
Y	Radial angle of polar grid segment (in degree)	20
Z	Minutiae orientation angle (in degree)	30
N_{train}	Training samples of PGTQ-based minutiae	300

	descriptor (for kernel matrix computation) (100 identities and 3samples for each identity)	
σ	Sigma used in the kernel function in eq. (4.20) (see Table 4.2)	vary for different data sets
K	The size of kernel matrix $\boldsymbol{K} \in \mathbb{R}^{N_{train} \times N_{train}}$	300×300
N_{dim}	Number of desired dimension/length for real valued fixed-length representation (applied for both KLSH and KPCA)	vary for different data sets
N^t	Training samples of each user for dynamic quantization	3
I	Training number of user for dynamic quantization	100
g	Number of Gaussian approximation elements for KLSH	30
M_{bit}	Number of bits for the fix-length binary representation (applied for both KLSH and KPCA)	vary for different data sets

4.4.2 Feasible Range of σ for Kernel Function

As elaborated in Section 4.3.2, the SPD property of the kernel function defined in eq. (4.20) is valid only for certain feasible range. It can be observed that σ yielding positive definiteness (sole non-negative eigenvalues of kernel matrix) in the six data sets consistently ranges from 0.002 to 0.46, as shown in Table 4.2.

Table 4.2: The range of σ yielding positive definite kernel on the FVC2002 and FVC2004 databases.

σ represents the width of Gaussian kernel in eq. (4.20)	FVC2002			FVC2004		
	DB1	DB2	DB3	DB1	DB2	DB3
Range to be positive definite	0.002-0.47	0.003-0.44	0.005-0.41	0.004-0.35	0.005-0.40	0.004-0.46

We then conducted another set of experiments to observe whether SPD kernel can outperform non-SPD kernel. We examined this observation by comparing two experimental results: with heat kernel function (SPD) and without heat kernel function (non-SPD). From Table 4.3, it can be observed that, for both kernel PCA and kernelized LSH transformed binary template, the experimental results with heat kernel function consistently outperformed those without heat kernel function significantly throughout six FVC databases. Although, SPD is asserted not a definite factor to yield the best performance (Harandi et al., 2012), our experiments conversely substantiate that a SPD kernel function is indeed essential in our proposed construction.

Table 4.3: Performance comparison between with and without heat function for real-valued templates: TKPCA and TKLSH.

Heat Kernel	FVC2002 (EER %)			FVC2004 (EER %)		
	DB1	DB2	DB3	DB1	DB2	DB3
KLSH						
With Heat Kernel	3.22 @σ=0.34	3.84 @σ=0.33	8.92 @σ=0.33	17.28 @σ=0.27	11.60 @σ=0.33	12.67 @σ=0.25
Without Heat Kernel	5.95	6.27	14.49	19.85	19.22	16.71

KPCA						
With Heat Kernel	3.34 @σ=0.29	3.71 @σ=0.35	8.19 @σ=0.37	17.17 @σ=0.29	10.78 @σ=0.35	12.29 @σ=0.23
Without Heat Kernel	6.64	6.84	15.57	21.16	19.93	15.21

4.4.3 Performance Evaluation

Table 4.4 reports the equal error rate (EER) performance over six data sets. The corresponding receiver operating characteristic (ROC) curves and the area under curve (AUC) values are shown in Fig. 4.3. For EER performance, the smaller the better; while for AUC values, the larger the better. From these results, our observations are as follows:

(1) The real-valued fixed-length representations (TKLSH and TKPCA) generated using kernel methods generally preserve the performance with respect to VSB template though they also shown outperformed VSB in some databases. The experimental result justified our analysis in Section 4.2, whereby KPCA extracts the maximum variance that is presented by a set of linearly uncorrelated variables - principal components and thus preserving discrimination power; while random hyperplane and central limit theory ensure the preservation of neighboring structure in KLSH.

(2) The performance deteriorates drastically when zero-thresholding method (TKLSH-ZT and TKPCA-ZT) is used for binarization. This is expected because this naive direct binarization ignores information from user feature distribution; and consequently losing discriminative power after binarization.

(3) When TKLSH and TKPCA are binarized with dynamic quantization (DQ), the performance of TKLSH-DQ and TKPCA-DQ are preserved over the other representations. For some datasets such as FVC2004 DB2 and DB3, the performances are slightly better than VSB. This result is expected because DQ is user-specific (Lim et al., 2012; Lim & Teoh, 2012; Lim & Teoh, 2013). The experimental results reported in Table 4.4 confirmed the preserved performance of dynamic quantization on fixed-length kernelized feature representation.

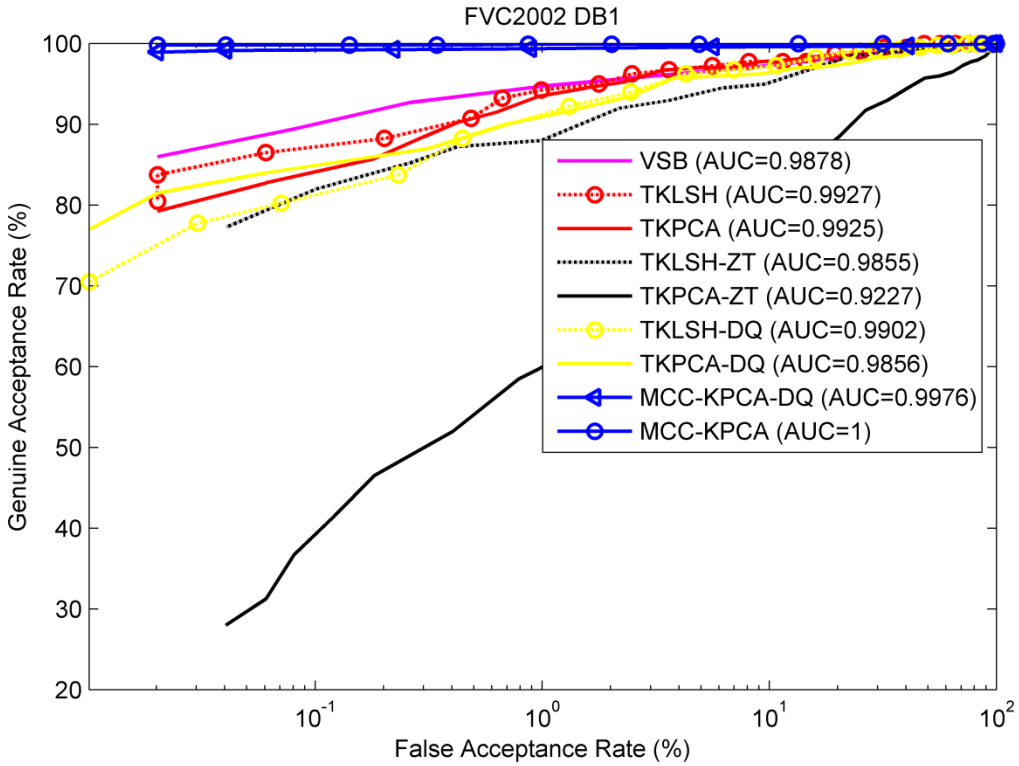
More importantly, other minutiae descriptors can be flexibly replaced and integrated into the proposed framework. To further demonstrate the feasibility of the proposed method, Minutia Cylinder-Code (MCC)[2], a state-of-the-art minutiae descriptor, is considered. Abbreviation of MCC, MCC-KPCA and MCC-KPCA-DQ shown in Table 4.4 denote the MCC descriptor, real and binary fixed-length representations generated from MCC respectively. The accuracy performance of MCC-KPCA and MCC-KPCA-DQ shown in Table 4.4 re-confirms the proposed method can preserve the performance after transformation. However, MCC is unprotected and hence MCC-KPCA and MCC-KPCA-DQ could be vulnerable to some security and privacy attacks as mentioned in Chapter 2 Section 2.2. In this circumstance, P-MCC (Ferrar et al., 2012), which is a protected version of MCC, can be applied.

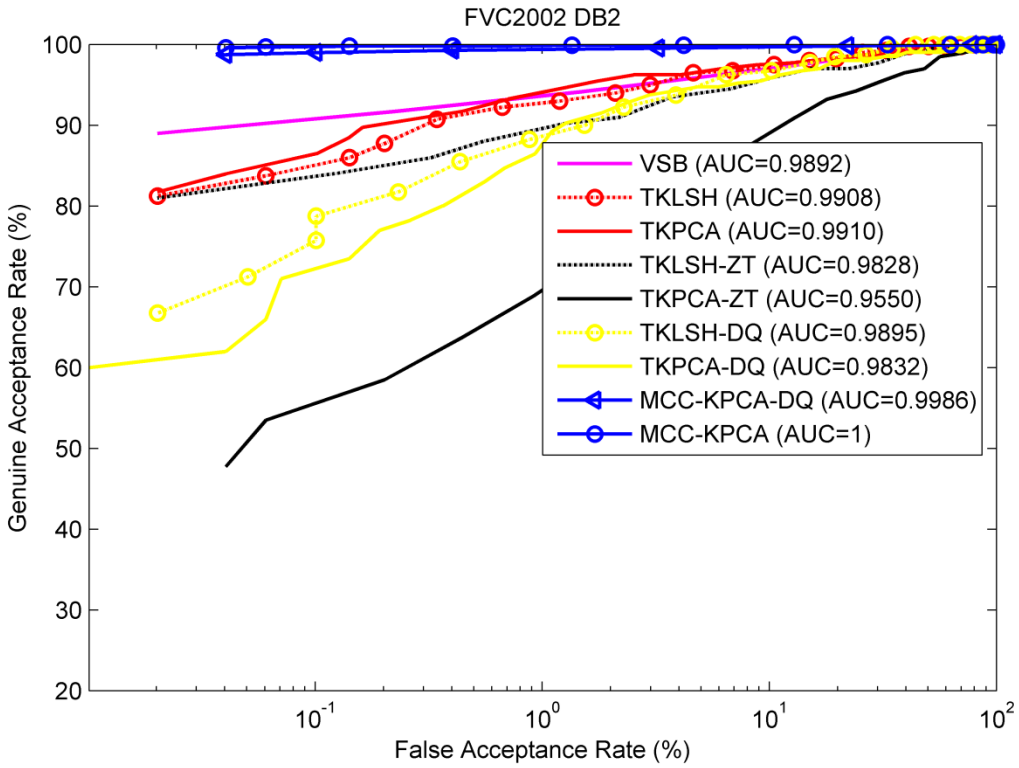
[2]MCC templates are generated using MCC SDK (Minutia Cylinder-Code SDK 2.0, 2015)

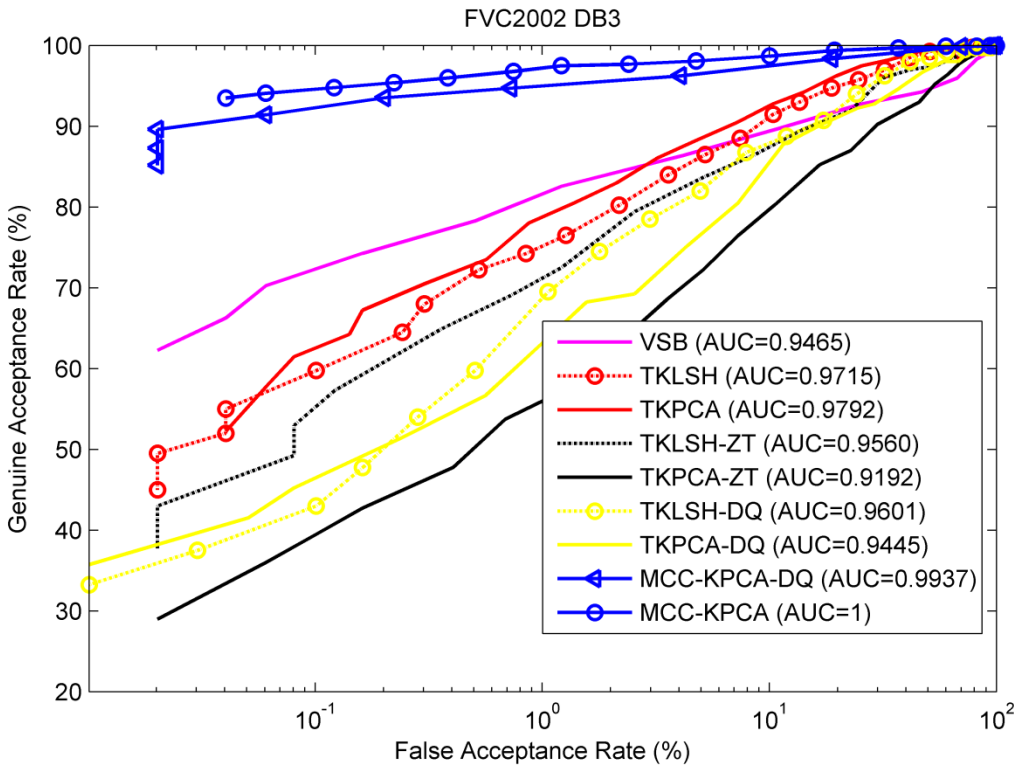
Table 4.4: Performance accuracy on FVC2002 and FVC2004 databases.

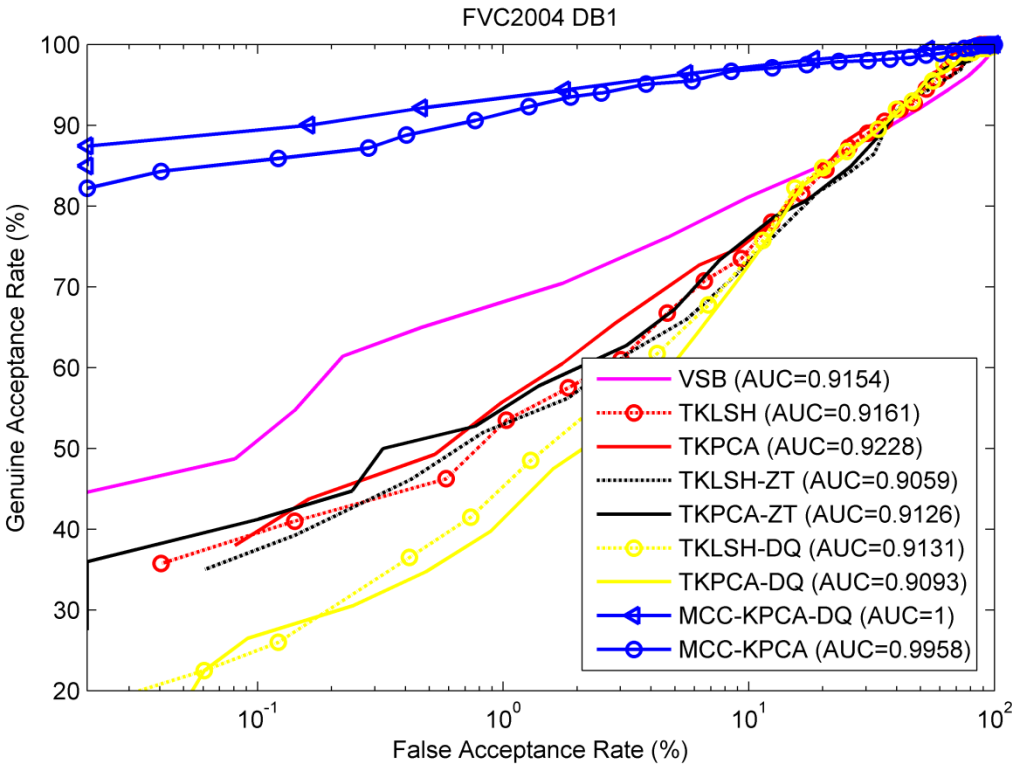
Methods	EER (%) for FVC2002			EER (%) for FVC2004		
	DB1	DB2	DB3	DB1	DB2	DB3
VSB	3.86	4.24	10.49	16.31	13.36	14.78
TKLSH	3.71	3.92	9.09	17.72	13.33	12.74
TKLSH with toggling bits	3.22	3.84	8.92	17.28	11.60	12.67
TKPCA	3.60	3.51	8.81	17.57	10.47	10.72
TKPCA with toggling bits	3.34	3.71	8.19	17.17	10.78	12.29
TKLSH-ZT	5.35	5.78	11.39	18.67	13.40	15.19
TKPCA-ZT	14.87	10.78	15.44	18.27	16.71	17.49
TKLSH-DQ	4.35 (280bits)	4.76 (280bits)	11.49 (280bits)	17.36 (256bits)	12.72 (256bits)	12.43 (280bits)
TKLSH-DQ with toggling bits	3.76 (280bits)	4.84 (280bits)	11.58 (280bits)	17.11 (256bits)	12.49 (256bits)	14.50 (256bits)
TKPCA-DQ	4.95 (192bits)	5.05 (186bits)	12.23 (182bits)	17.34 (235bits)	12.37 (195bits)	12.25 (195bits)
TKPCA-DQ with toggling	4.03 (190bits)	5.04 (185bits)	11.86 (184bits)	17.39 (206bits)	10.95 (220bits)	13.49 (221bits)

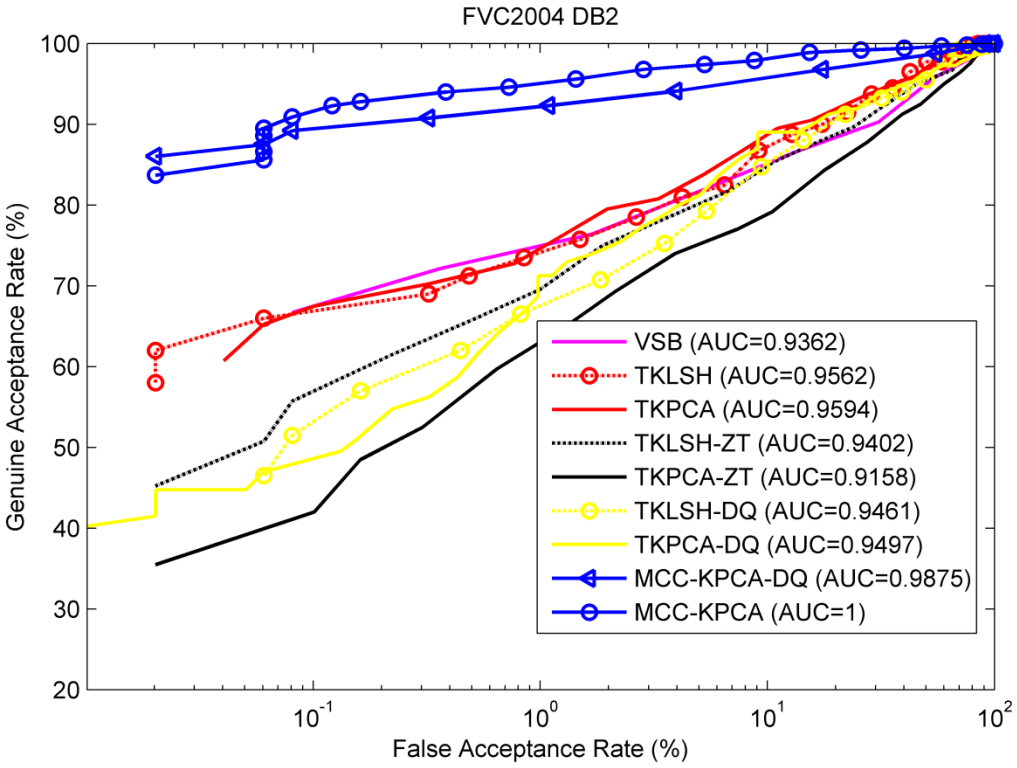
bits						
MCC	0.60	0.59	3.91	3.97	5.22	3.82
MCC-KPCA	0.20	0.19	2.30	4.70	3.13	2.80
MCC-KPCA-DQ	0.44 (256bits)	0.33 (200bits)	4.17 (256bit)	4.56 (256bits)	5.28 (300bits)	4.43 (256bits)




FVC2002 DB2
Genuine Acceptance Rate (%)
False Acceptance Rate (%)
VSB (AUC=0.9892)
TKLSH (AUC=0.9908)
TKPCA (AUC=0.9910)
TKLSH-ZT (AUC=0.9828)
TKPCA-ZT (AUC=0.9550)
TKLSH-DQ (AUC=0.9895)
TKPCA-DQ (AUC=0.9832)
MCC-KPCA-DQ (AUC=0.9986)
MCC-KPCA (AUC=1)


FVC2002 DB3
Genuine Acceptance Rate (%)
False Acceptance Rate (%)
VSB (AUC=0.9465)
TKLSH (AUC=0.9715)
TKPCA (AUC=0.9792)
TKLSH-ZT (AUC=0.9560)
TKPCA-ZT (AUC=0.9192)
TKLSH-DQ (AUC=0.9601)
TKPCA-DQ (AUC=0.9445)
MCC-KPCA-DQ (AUC=0.9937)
MCC-KPCA (AUC=1)


FVC2004 DB1
Genuine Acceptance Rate (%)
False Acceptance Rate (%)
VSB (AUC=0.9154)
TKLSH (AUC=0.9161)
TKPCA (AUC=0.9228)
TKLSH-ZT (AUC=0.9059)
TKPCA-ZT (AUC=0.9126)
TKLSH-DQ (AUC=0.9131)
TKPCA-DQ (AUC=0.9093)
MCC-KPCA-DQ (AUC=1)
MCC-KPCA (AUC=0.9958)


FVC2004 DB2
Genuine Acceptance Rate (%)
False Acceptance Rate (%)
VSB (AUC=0.9362)
TKLSH (AUC=0.9562)
TKPCA (AUC=0.9594)
TKLSH-ZT (AUC=0.9402)
TKPCA-ZT (AUC=0.9158)
TKLSH-DQ (AUC=0.9461)
TKPCA-DQ (AUC=0.9497)
MCC-KPCA-DQ (AUC=0.9875)
MCC-KPCA (AUC=1)

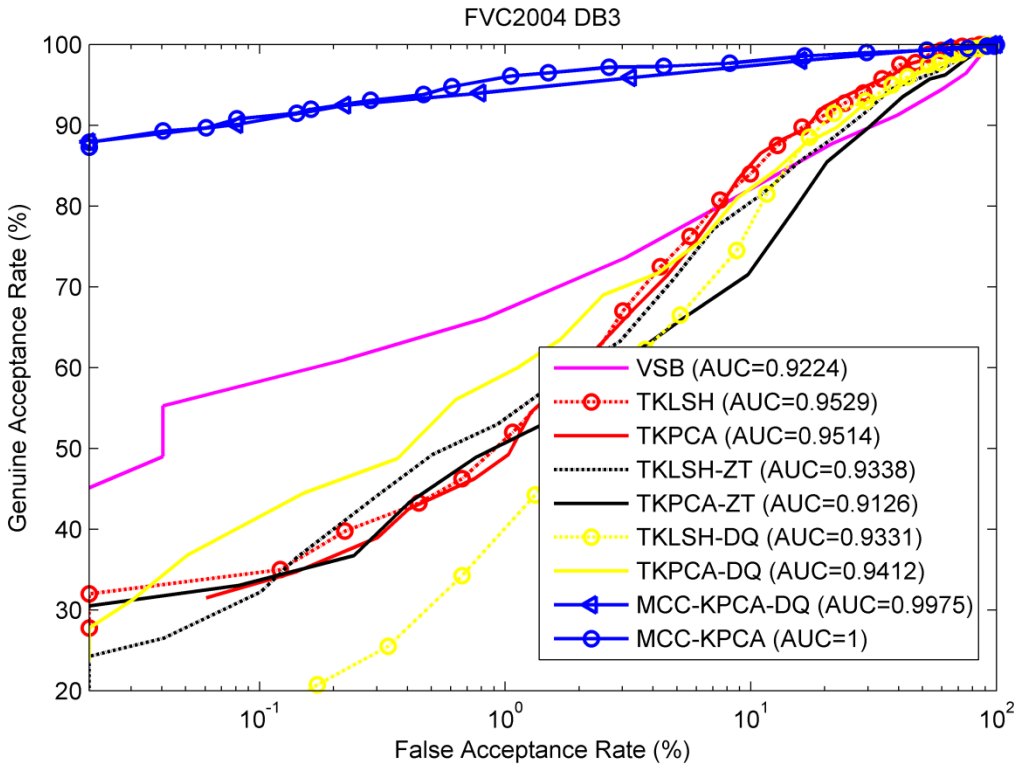


Fig. 4.3: ROC curves on FVC2002 and FVC2004 databases.

Apart from the above, an accuracy comparison is conducted between the proposed methods with the state-of-the-arts (Nagar et al., 2010; Bringer & Despiegel, 2010; Farooq et al., 2007; Xu et al., 2009; Nandakumar, 2010) that generate fixed-length templates and the results are shown in Table 4.5. From the table, the performance of the proposed TKPCA-DQ and TKLSH-DQ is not better than (Nagar et al., 2010; Farooq et al., 2007; Xu et al., 2009; Nandakumar, 2010). However, we point out that: (1) in Nagar et al. (2010) only the first and last impression of each user is used for enrolment and testing respectively while only four samples 1,2,7,8 in Xu et al. (2009) are used for experiment. In contrast, all eight samples are used in our experiments (samples 1th-3rd for training and samples 4th-8th for testing): (2) the database used in Farooq et al. (2007) is not publicly available and alignment is mandatary in

(Nagar et al., 2010; Nandakumar, 2010) (e.g. high curvature point) while our method is alignment-free. Nevertheless, when a superior minutiae descriptor such as MCC is incorporated, MCC-KPCA-DQ outperforms all the existing fixed length representation methods as shown in Table 4.5.

Table 4.5: Accuracy comparison with the state-of-the-arts on FVC2002 and FVC2004 databases.

Methods	EER (%) for FVC2002			EER (%) for FVC2004		
	DB1	DB2	DB3	DB1	DB2	DB3
Nagar et al., (2010)	-	3.00	-	-	-	-
Bringer & Despiegel, (2010)	-	5.30	-	-	-	-
Farooq et al., (2007)	1.59 * (private database used)					
Xu et al., (2009)	-	3.86	-	-	-	-
Nandakumar, (2010)	2.10	1.70	-	-	-	-
Proposed TKLSH-DQ	3.76	4.84	11.58	17.11	12.49	14.50
Proposed TKPCA-DQ	4.03	5.04	11.86	17.39	10.95	13.49
MCC-KPCA-DQ	0.44	0.33	4.17	4.56	5.28	4.43

The time efficiency on various phases of the entire framework is also investigated and the results are shown in Table 4.6. The average time is captured by the experimental machine with Intel i7 (3.4GHz) CPU and 4GB RAM.

The matching efficiency on the fixed-length representation (t_{MFLR} and t_{MFLB}) is much higher than that of the variable-size representation t_{MPMD} because a two-stage matching algorithm has to be performed for variable-size representation. Particularly, for the binary fixed-length representation t_{MFLB}, the average matching time has met the expectation for an efficient matching requirement compared to FVC2002 and FVC2004 (light category[3]). Furthermore, it is also observed that the operation on creating kernel matrix consumes the most time t_{CKM}during the training stage. However, this would not compromise the feasibility of the method in *real time* scenario because of two reasons: (1) kernel matrix creation is a one-time-operation (during the system setup); (2) kernel matrix creation is performed offline and it is not performed in the matching process.

Table 4.6: Average time processed in different phases of the framework (in second).

Different Phases	**Average Time (Seconds) for FVC2002**			**Average Time (Seconds) for FVC2004**		
	DB1	**DB2**	**DB3**	**DB1**	**DB2**	**DB3**
Training Stage						
Create PGTQ-base Minutiae Descriptor (t_{CPMD})	0.0043	0.0057	0.0022	0.0052	0.0041	0.0070
Generate Fixed-length	3.8191	5.8023	1.8623	5.2117	3.4975	6.6996

[3] The light category is intended for algorithms conceived for light architectures and therefore characterized by low computation cost, in limited memory storage and small template size (from FVC 2002, and FVC2004).

Representation (t_{GFLR})						
Create Kernel Matrix with size of (300×300) (t_{CKM})	610.9821	937.6017	260.3855	626.9327	487.7635	910.9222
Matching Stage						
Matching in PGTQ-base Minutiae Descriptor (t_{MPMD})	0.0131	0.0214	0.0057	0.0142	0.0125	0.0226
Matching in Real Fixed-length Representation (t_{MFLR})	7.8238e-006	8.2109e-006	9.8168e-006	7.8208e-006	7.9370e-006	8.0894e-006
Matching in Binary Fixed-length Representation (t_{MFLB})	4.4567e-006	4.5556e-006	5.1510e-006	3.1784e-006	4.0160e-006	4.6129e-006

4.5 Quantitative analysis on correlation of bit-strings

4.5.1 The test of statistical independence

One common observation in biometric systems is that the security and accuracy is a trade-off. A binary biometric representation with good accuracy performance can be highly correlated (i.e. low entropy) and is easier to guess, thus heightening the possibility of a system-security violation. Hence, it is important for a practical system to maintain a good balance between accuracy performance and security. With our promising accuracy performance justified in the previous section, we now investigate the correlation of bit-strings (i.e. TKLSH-DQ and TKPCA-DQ) between different identities.

The experiments are carried out by adopting a test that was proposed by Daugman (2003). This test is virtually guaranteed to pass when the bit-strings from different identities are compared, but failed when the bit-string of an identity is compared with another version of itself. More specifically, if binary templates of different users are independent among each other, the ideal expected proportion of agreeing bits between the binary strings for different identities, i.e. imposter distribution is 0.5. However, practically, it is impossible to expect that the bit-strings among different identities are perfectly uncorrelated due to the inevitable inherent correlation of the extracted features (Zhou et al., 2012).

Considering that each comparison between two bits of binary template belonging to different identities is essentially a Bernoulli trial, the imposter distribution with mean μ and standard deviation σ corresponds to a binomial distribution having expectation of degree-of-freedom DOF. The DOF can be formulated as:

$$\mathrm{DOF} = \frac{\mu(1-\mu)}{\sigma^2} \tag{4.37}$$

If the binary templates are completely uncorrelated, the DOF is then equal to the length of the binary templates, which yields a perfect binomial distribution with mean μ=0.5 and variance $\sigma^2 = \frac{\mu(1-\mu)}{\mathrm{DOF}} = 9.7656 \times 10^{-4}$. Generally, the stronger the correlation of the bit-strings is, the smaller the degree-of-freedom will be. It is observed in Table 4.7 that the mean and standard deviation/variance of the empirical imposter distribution deviates

from the ideal distribution, thus resulting in a lower DOF. This deviation is mainly caused by the bit dependency in the binary templates (Lim et al., 2013). In fact, such deviation is expected, because the dynamic binarization scheme is designed based on the assumption of independence among individual feature dimensions, which may not be true in practice.

Moreover, we notice that in kernel PCA, the generated feature vectors are linearly uncorrelated (see eq. 4.9); while feature vectors in kernelized LSH are not necessarily uncorrelated. In the event where other factors are identical, i.e. same input (PGTQ-based descriptors) and same dynamic quantization, we can reason that the bit-strings TKLSH-DQ exhibits higher correlativeness over TKPCA-DQ. Such reasoning can be confirmed from Table 4.7, where lower DOFs of TKLSH-DQ bit strings are observed.

Table 4.7: DOFs for bit-string TKPCA-DQ and TKLSH-DQ on FVC2002 and FVC2004 databases.

DOF	FVC2002			FVC2004		
	DB1	DB2	DB3	DB1	DB2	DB3
TKPCA-DQ	143 (192bits)	96 (186bits)	123 (182bits)	121 (235bits)	115 (195bits)	68 (195bits)
TKLSH-DQ	140 (280bits)	155 (280bits)	130 (280bits)	131 (256bits)	138 (256bits)	97 (280bits)

4.5.2 Entropy Estimation

This section evaluates the randomness (entropy) of the binary templates generated from TKPCA-DQ and TKLSH-DQ. Zhou's entropy

estimation method (Zhou et al., 2011) that is based on a second-order dependency tree proposed by Chow & Liu (1968) is adopted. Let $P(X)$ be the joint probability of feature $X = [x_1, x_2, \dots, x_l]$. The second-order dependency tree can be described as $\hat{P}(X) = \prod_{i=1}^{l} P\left(x_{u_i} \middle| x_{u_{j(i)}}\right), 0 \le j(i) \le i$ where $[u_1, u_2, \dots, u_l]$ is a permutation of index $[1,2, \dots, l]$ and $P\left(x_{u_1} \middle| x_{u_{j(1)}}\right) = P(x_{u_1})$. To reduce the computational load, only bit pair formed by each bit with one of its prior bits is used for mutual information calculation $I(x_i, x_{i'})$ in the entropy estimation, $x_i, x_{i'} \in [1,2, \dots, l]$ and $x_i \neq x_{i'}$. If x_i and $x_{i'}$ are independent, $I(x_i, x_{i'}) = 0$. If completely dependent, $I(x_i, x_{i'}) = H(x_i) = H(x_{i'})$. Chow & Liu (1968) optimized the estimation of Kullback-Leibler distance between the real distribution of *X* and the second-order dependency tree and indicated that Kullback-Leibler distance is dependent on variables: $D(P(X)|\left|\hat{P}(X)\right) = \sum_{i=1}^{l} H\left(x_{u_i}\right) - H(X) - \sum_{i=2}^{l} I(x_{u_i}, x_{u_{j(i)}})$, where $H(X)$ and $\sum_{i=1}^{l} H\left(x_{u_i}\right)$ represent entropy of feature *X* and the entropy sum of individual bits, respectively. Because minimizing the estimation error for Kullback-Leibler distance is equivalent to maximizing $\sum_{i=2}^{l} I(x_{u_i}, x_{u_{j(i)}})$, the best estimated entropy of *X* is $\hat{H}(X) = \sum_{i=1}^{l} H\left(x_{u_i}\right) - \max_{[u_1, u_2 \dots, u_l]}\{\sum_{i=1}^{l} I(x_{u_i}, x_{u_{j(i)}})\}$.

In the ideal case, i.e. feature *X* is uniformly and independently distributed; its entropy is identical to the feature bit-length, and the information rate equals to 1. Note that the information rate is described as average entropy per symbol, which can be computed as the ratio of the estimated entropy with respect to the feature bit-length. It ranges from 0 to 1

with the value 1 indicates the highest information rate. However, obtaining ideal information rate is nearly impossible in practice due to the inevitable dependency caused by the biometric feature extraction. Table 4.8 shows the estimated entropy in bits and information rate for FVC2002 and FVC2004 databases. From Table 4.8, it can be observed that the maximum and minimum entropies obtained by the proposed schemes are 256 bits over 280 bit-length string (FVC2002 DB2 for TKLSH-DQ) and 171 bits over 185 bit-length string (FVC2004 DB2 for TKPCA-DQ), respectively. The information rates achieved by the proposed schemes are approximately from 0.9 to 0.94. These results have demonstrated the significant randomness of the binary templates compared to the results from (Zhou et al., 2011).

Table 4.8: Estimated entropy in bits and information rate on FVC2002 and FVC2004 databases.

Entropy & Information Rate	FVC2002			FVC2004		
	DB1	DB2	DB3	DB1	DB2	DB3
TKPCA-DQ	178/0.94 (190bits)	171/0.92 (185bits)	172/0.93 (184bits)	192/0.93 (206bits)	205/0.93 (220bits)	206/0.93 (221bits)
TKLSH-DQ	249/0.89 (280bits)	254/0.91 (280bits)	248/0.89 (280bits)	234/0.92 (256bits)	231/0.90 (256bits)	256/0.92 (280bits)

4.6 Implementation of Fuzzy Commitment

In this section, fuzzy commitment scheme is implemented to observe the feasibility of the binary representations generated by the proposed methods. There is almost none of the works reported for fuzzy commitment scheme based on transformed minutiae bit string except Nandakumar (2010),

thus we compare our method with Nandakumar (2010) on FVC2002 DB1 and DB2. In this implementation, BCH error correction code is applied and TKLSH-DQ is used for demonstration. TKLSH-DQ is 280-bits representation for FVC2002.Yet, the length of the codeword for BCH is set to 511. So zero padding on TKLSH-DQ is required in order to perform XOR operation. Table 4.9 shows the FAR/FRR of this implementation as well as comparison with Nandakumar (2010). Although, the results are poorer than Nandakumar's work (2010), it can be justified that the proposed method is *solely based on minutiae information* while Nandakumar (2010) requires minutiae alignment (e.g. high curvature points), which is not ISO compliant. Thus the performance of the proposed method is comparable to state-of-the-art.

Table 4.9: FAR/FRR of fuzzy commitment implementation using proposed TKLSH-DQ as well as comparison with Nandakumar (2010).

Databases	**FMR/FNMR Nandakumar (2010)**	**FAR/FRR (%)**		
		BCH (*n*, *k*) (511, 40)	**BCH (*n*, *k*)** (511, 58)	**BCH (*n*, *k*)** (511, 67)
FVC2002 DB1	(0.1)/(12.5)	(9.41)/(4)	(4.18)/(6)	(1.61)/(8.5)
FVC2002 DB2	(0.1)/(8.9)	(7.71)/(5.75)	(3.05)/(9.5)	(1.07)/(13.75)

4.7 Discussion and Summary

Several points regarding the usability of the proposed framework are further highlighted: (1) other than the modified PGTQ-based minutiae descriptor used in this implementation, various binary or real-valued minutiae descriptors, e.g. Minutiae Cylinder Code (MCC) (Cappelli et al., 2010) can be

flexibly replaced and integrated into the proposed framework. This is because the proposed framework only converts the matching score of the minutiae descriptors from a variable-size descriptor to a fixed-length representation; (2) the matching algorithm between minutiae descriptors has to be carefully designed because the matching scores are used to form the kernel matrix, which is sensitive to the performance; (3) besides the stability-dependence dynamic quantization methods, other feature binarization methods such as DROBA (Chen et al., 2009) can also be applied.

Finally, it is concluded that, in this chapter, a generic framework is proposed to convert variable-size minutiae descriptor into a fixed-length representation. The framework is comprised of four main components: minutiae descriptor extraction, fixed-length feature generation by kernel methods, feature binarization and matching. The experiment shows that the performance of the proposed TKPCA-DQ and TKLSH-DQ is comparable to the-state-of-the-arts for the fixed-length representations. Besides the feasible accuracy performance, high matching efficiency is also achieved. Furthermore, the framework provides good adaptability: The minutiae descriptor, kernel, and feature binarization components used in this implementation can easily be replaced with better state-of-the-art components. Additionally, the randomness and the correlation between the binary templates of different identities are extensively examined using entropy estimation with second order dependency tree and statistical independence test. In conclusion, all these advantages justify the feasibility of the proposed framework in applications.

CHAPTER 5

BIOMETRIC CRYPTOSYSTEM: A NEW BIOMETRIC KEY BINDING AND ITS IMPLEMENTATION FOR FINGERPRINT MINUTIAE-BASED REPRESENTATION

Despite Fuzzy Commitment (FC) is a theoretically sound biometric-key binding scheme, it relies on error correction code (ECC) completely to mitigate biometric intra-user variations. Accordingly, FC suffers from the security–performance trade-off. That is, the larger key size/higher security always trades with poor key release success rate and vice versa. Additionally, the FC is highly susceptible to a number of security and privacy attacks. Furthermore, FC is limited to simple distance metrics such as Hamming distance to measure the dissimilarity of biometric features. This implies many efficient matching algorithms are to be abandoned. In this chapter, an ECC-free key binding scheme along with cancellable transforms is proposed for minutiae-based fingerprint biometrics. Apart from that, the minutiae information is well protected with a strong non-invertible cancellable transform, which is crucial to prevent a number of security and privacy attacks. The scheme is not limited to binary biometrics as in FC but instead can be applied to various types of biometric features and hence a more effective matcher can be applied. Experiments conducted on FVC2002 and FVC2004 show that the accuracy performance is comparable to state-of-the-

arts. It is further demonstrated that the proposed scheme is robust against several major security and privacy attacks.

5.1 Introduction

Biometric technology is likely to provide a heightened security level for identity verification and identification. Yet, the invasion of identity privacy is inevitable if the stored template is compromised. On the other hand, in cryptography, key management is mandatory for key storage, exchange and transaction, which remains a challenge task (Adam & Lloyd, 1999). The idea of using biometrics to lock and unlock a cryptography key is thus attractive since biometric trait is admissibly unique (Jain, 2013). In fact, the study of binding biometrics with cryptography key has been carried out in the past decade as a plausible solution for key management as well as for biometric template protection (Juels & Wattenberg, 1999; Juels & Sudan, 2006). As a result, biometric cryptosystem was born to respond to the needs of either securing the cryptographic key using biometrics (key binding) or generating cryptographic key from biometrics (key generation) (Jain et al., 2008).

Despite key generation is an attractive proposition, it is difficult to be realized due to intra-user variability of biometrics that leads to a contradiction for achieving high key entropy and stability simultaneously (Jain et al., 2008). Furthermore, the original idea of key generation scheme is not designed for providing cancelability and non-linkability. The representative instances of key generation schemes can be found in (Vielhauer et al., 2002; Chang et al.,

2004; Dodis et al., 2008). It is noted that due to the nature of biometric variability, key generation is less popular than that of the key binding scheme.

For key binding approach, the basic idea is to embed the cryptographic key using biometric data. The cryptographic key is completely independent to the biometrics. A key is released only if the query instance with sufficient similarity to the template is supplied during the decoding stage. Error correction code (ECC) is employed to manage the variations of biometric data. The well-known instances of key binding approach are fuzzy commitment (Juels & Wattenberg, 1999) and fuzzy vault (Juels & Sudan, 2006). Despite effective, several vulnerabilities and drawbacks were recognized. This hinders the proliferation of key binding schemes. The details of vulnerabilities and drawbacks in key binding schemes have been discussed in Chapter 2 Section 2.3.

On the other hand, cancellable biometrics (Ratha et al., 2007) is a method for biometric template protection. It refers to the irreversible transform of the biometric data to ensure security and privacy of the biometric template can be protected. Hence, instead of the original biometric data, the transformed templates are stored. If a cancellable biometric template is compromised, a new template can be regenerated from the original biometric data.

In a nutshell, while both biometric cryptosystems and cancellable biometrics serve to protect biometric template, the former is also meant to

protect key in cryptographic applications. However, both approaches are also suffered from accuracy performance, security and privacy issues. In this chapter, a new biometric key binding scheme is put forward by bridging the biometric cryptosystem and cancellable biometrics. In some sense, the proposed scheme achieves a middle-ground between the two main approaches but overcoming the limitations of both. It can thus be better served for both cryptographic key and biometric template protection.

The organization of this chapter is as follow: Motivation and contribution are given in Section 5.2. The proposed key binding scheme and its implementation are presented in Section 5.3 and 5.4 respectively. The experimental results are provided in Section 5.5. In Section 5.6, security and privacy analysis are given. Finally, conclusion is followed by Section 5.7.

5.2 Motivations and Contributions

The limitations of both biometric cryptosystems (i.e. fuzzy commitment and fuzzy vault) and cancellable biometrics have been summarized in Chapter 2. It is indeed challenging to resolve all these problems in their own regime. However, it is believable that the assimilation of both approaches would be a plausible response to this open problem.

In this chapter, an ECC-free key binding scheme along with cancellable transforms is proposed for minutiae-based fingerprint biometrics in place of fuzzy commitments. This idea is inspired from *chaffing and winnowing scheme*, which was conceived by Ron Rivest (Rivest, 1998). The

goal of chaffing and winnowing is to achieve confidentiality without using encryption when sending data over an insecure channel. However, the scheme that often used in conventional cryptography context cannot be applied directly to biometrics due to the stochastic nature of biometric data as well as various unique design criteria as aforementioned. Therefore, a major alteration to the original scheme has to be carried out.

In this realization, the previous proposed alignment-free minutia descriptor, namely Minutia Vicinity Decomposition (MVD) (Jin & Teoh, 2011) and a modified non-invertible transform, called Graph-based Hamming Embedding (GHE) are adopted to construct an adoptive cancellable transform that facilitates the binding of cryptographic key with fingerprint biometrics. The main contributions of this work are as follows:

- A new ECC-free biometric key binding scheme and the realization in fingerprint biometrics are proposed. Since ECC is abandoned, the issues that associate with ECC such as security-performance trade-off and statistical attack are no longer exist.

- A modified randomized GHE in constructing the cancellable transform is proposed. Therefore, cancelability criterion for template protection is satisfied.

- ❖ Several security and privacy analysis for the proposed scheme are performed; particularly focus on the major privacy attacks, such as ARM and SKI.

- ❖ The proposed scheme is not limited to the binary feature representation and the matcher, but it can be applied to variety of biometric feature representations.

5.3 Proposed Biometric Key Binding Scheme

5.3.1 Methodology

In this section, the conventional chaffing and winnowing scheme (CWS) (Rivest, 1998) is first reviewed, which is the primary source that inspired this work. The CWS comprises of two stages: 1) adding the fake packets (chaffs) and bogus message authentication code (MACs) based on a sequence of number and message, i.e. chaffing; 2) discarding packets with bogus MACs at receiver, i.e. winnowing. In this regard, an eavesdropper is clueless to identify which package is real or bogus without secret key information that is only shared by the genuine sender and receivers. An example of CWS is demonstrated in Fig. 5.1. Unfortunately, conventional CWS is not directly transferrable to the biometric-key binding scheme due to the fuzziness of biometric data as well as various unique design criteria as presented in Chapter 2.

The proposed biometric-key binding scheme is illustrated in Fig. 5.2. For key binding, given a binary key *k*, encode 1s in *k* with true templates while

encode 0s with synthetic templates. The encoding process is to apply cancellable transform to both true and synthetic biometric templates with *different* transformation seed, in order to produce a series of cancellable templates. It is noted that for *m*-bits key, *m* cancellable transforms are required to encode the key entirely. This process corresponds to "chaffing" in CWS.

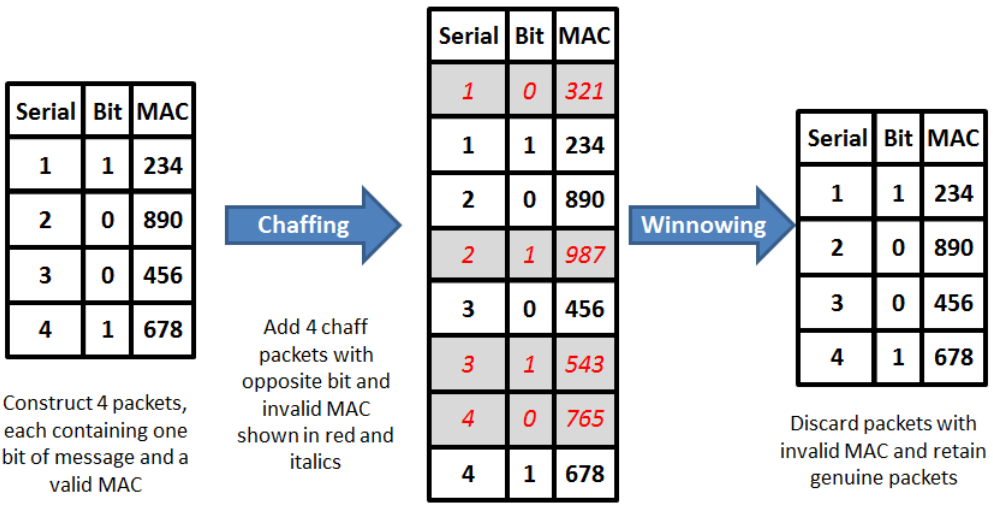


Fig. 5.1: An example of chaffing and winnowing scheme adopted from (Wikipedia, 2015).

On the other hand, the key release consists of a two-steps procedure: 1) apply *m* cancellable transforms to the query data yield *m* cancellable query instances; 2) match the cancellable query instances with the stored cancellable templates and compare the matching score with respect to a pre-defined threshold τ. If the matching score $s \geq \tau$, release 1; otherwise 0. This corresponds to "winnowing" in CWS.

The detailed algorithms for key binding and key release are presented in Algorithm 5.1 and 5.2 as follows:

Algorithm 5.1. Key Binding (Enrollment)

Input: True template $\mathbf{\Omega}^e$, synthetic template $\mathbf{\Omega}^s$, *m*-bits key $k \in \{0,1\}$, *m* cancellable transforms $C_{i=1}^{m}$

Encode *m*-bits key *k* using *m* cancellable transforms
For *i*=1:*m*
  if $k_i = 1$
    $\Xi_i^c = C_i(\mathbf{\Omega}^e)$
  else
    $\Xi_i^c = C_i(\mathbf{\Omega}^s)$
End for

Output: A set of cancellable templates $\Xi_{i=1\ldots m}^{c}$

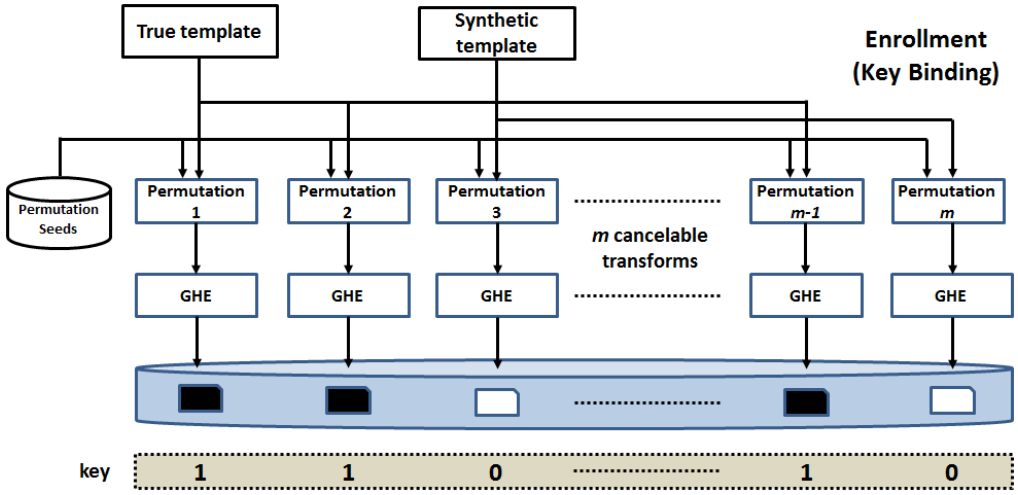
Algorithm 5.2. Key Extraction (Authentication)

Input: A set of cancellable templates Ξ^c obtained in Algorithm 1, matching threshold τ, query biometric $\mathbf{\Omega}^q$, *m* cancellable transforms $C_{i=1}^{m}$ used in Algorithm 1.

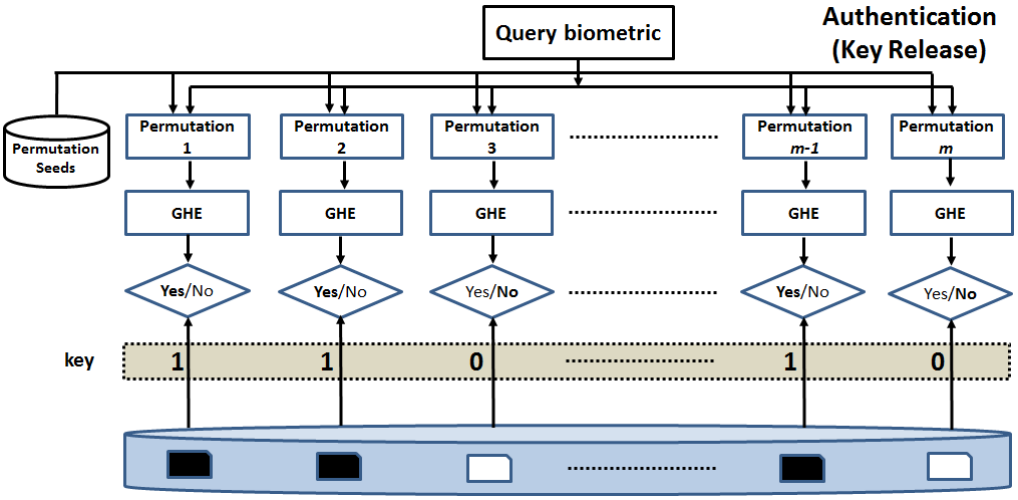
Step 1: Applying *m* cancellable transforms on query biometric.
For *i*=1:*m*
  $\Xi_i^q = C_i(\mathbf{\Omega}^q)$
End for

Step 2: Match the enrolled cancellable templates Ξ^c with query cancellable templates Ξ^q computed in step 1 and release 1 or 0 based on similarity score. sim(.) denotes the similarity measure function.
For *i*=1:*m*
  sim(Ξ_i^q, Ξ_i^c) = *s*
  if $s \geq \tau$
    $\bar{k}_i = 1$
  else
    $\bar{k}_i = 0$
End for

Output: Released *m*-bits key $\bar{k}$.



(a) Key Binding



(b) Key Release

Fig. 5.2: Diagrams for the proposed key binding scheme: (a) demonstrates the key binding with biometrics data that comprises of true template and synthetic template; (b) depicts the key release by presenting a query biometric template.

5.3.2 Synthetic Templates Generation

For key binding purpose, the proposed method employs both true and synthetic templates to generate a set of cancellable templates. Several options to create synthetic templates are suggested: 1) use different biometric

modalities: for instance, fingerprint template for true template and palm print template for synthetic template etc.; 2) use two different feature extraction algorithms on the same biometric data to generate true and synthetic templates; 3) use imposter template as synthetic template.

However, an inconsiderate design of synthetic templates may leads to the revelation of the cryptography key easily. For instance, if the sizes of synthetic and true template differ and propagate to the cancellable template stage, the key can be easily determined. This is commonly found in fingerprint minutia as they are point set variable in size. Furthermore, the cancellable synthetic template should not be statistically differentiable to the cancellable true templates. For instance, the elements in a cancellable synthetic template are ranged from 0 to 1 while the range of cancellable true template is -1 to 0.

To take into account the above cautions in generating synthetic template, random permuted version of true templates is used to generate the synthetic templates in this implementation. Such synthetic templates are: 1) of same length with true templates; 2) a randomized version of the true templates after cancellable transform. Hence it is highly unlikely to distinguish the true templates and synthetic templates statistically. The synthetic templates generation can be expressed as follows:

$$\boldsymbol{\Omega_i^s} = \mathrm{Perm}(\boldsymbol{\Omega_i^e}) \quad (i = 1, \dots, N) \tag{5.1}$$

where $\boldsymbol{\Omega}^s$ and $\boldsymbol{\Omega}^e$ represent the synthetic and true templates, respectively and $\mathrm{Perm}(.)$ denotes the random permutation function. $\boldsymbol{\Omega}_i$ refers to the *i*-th row of minutia vicinity decomposition (MVD) (Jin & Teoh, 2011) and *N* is the total

number of vicinities extracted from minutia set. The permutation seed is discarded after the process of synthetic template generation is completed.

5.3.3 Cancellable Templates Generation

With the synthetic and true templates, the cryptography key can be encoded via a set of cancellable templates. The cancellable templates generation essentially consists of a two-steps procedure: 1) random permutation; 2) applying non-invertible feature transform. The steps are described as follows:

1) ***Random permutation***. In order to bind an *m*-bits key, *m* random permutations are required to generate *m* cancellable templates so that each cancellable template is used to encode the each bit of cryptography key. In the stage of key binding, random permutation with different seed is again applied to both true and synthetic templates subject to the specific bit in the key as expressed in eq. (5.2), while in the stage of key release, random permutation is applied to query template as expressed in eq. (5.3).

$$\boldsymbol{\Omega}_{j,i} = \begin{cases} \mathrm{Perm}(\boldsymbol{\Omega}_{\boldsymbol{i}}^{\boldsymbol{e}}) & if\ k_j = 1 \\ \mathrm{Perm}(\boldsymbol{\Omega}_{\boldsymbol{i}}^{\boldsymbol{s}}) & if\ k_j = 0 \end{cases} (j = 1, \dots, m), (i = 1, \dots, N) \tag{5.2}$$

$$\boldsymbol{\Omega}_{j,i} = \mathrm{Perm}(\boldsymbol{\Omega}_{\boldsymbol{i}}^{\boldsymbol{q}}) \quad (j = 1, \dots, m), (i = 1, \dots, N) \tag{5.3}$$

where $\boldsymbol{\Omega}^{s}$ and $\boldsymbol{\Omega}^{e}$ represent the synthetic and true templates, respectively and $\mathrm{Perm}(.)$ denotes the random permutation function. $\boldsymbol{\Omega}_{j,i}$ refers to the *i*-th row of minutia vicinity decomposition (MVD) for

the j-th random permutations and N is the total number of vicinities extracted from minutia set.

The permutation seeds applied on key binding are kept, which are used in key release stage in the identical order. Note that permutation in eq. (5.2) and eq. (5.3) is different from eq. (5.1) as the latter is meant for generating synthetic template and the seed will be discarded right after used.

2) ***Non-invertible feature transform***. The non-invertible transform is to ensure: (1) the key is strictly concealed; (2) the restoration of biometric features (e.g. minutiae) is computationally hard. For (1), the transformed template $\boldsymbol{\Xi}$ should be difficult to be recovered in order to prevent the leakage of the key. If $\boldsymbol{\Xi}$ is inverted and parameters of permutation function are learned by the adversary, the original features $\boldsymbol{\Omega}$ can be restored thereafter. Once the entire set of $\boldsymbol{\Xi}$ is restored, the complexity of key retrieval reduces to 2^1 because only two sources (i.e. true template and synthetic template) are used to encode the key. For (2), the raw biometric data (e.g. fingerprint minutiae) should not be recovered from $\boldsymbol{\Xi}$. For instance, fingerprint minutia should not be learned from a compromised $\boldsymbol{\Xi}$. This is identical to the requirement of non-inveritiblity for template protection. Therefore, non-invertible transform is a critical construct for the proposed key binding scheme.

5.4 Implementation

5.4.1 MVD and RGHE

In the implementation, a modified randomized graph-based hamming embedding transform (RGHE) is used to transform the fingerprint minutia vicinity decomposition (MVD) features into a non-invertible form. The propositions of MVD and RGHE have been described in Chapter 3 Section 3.2 and 3.3 respectively. Hence, the identical processes are not repeated in this section.

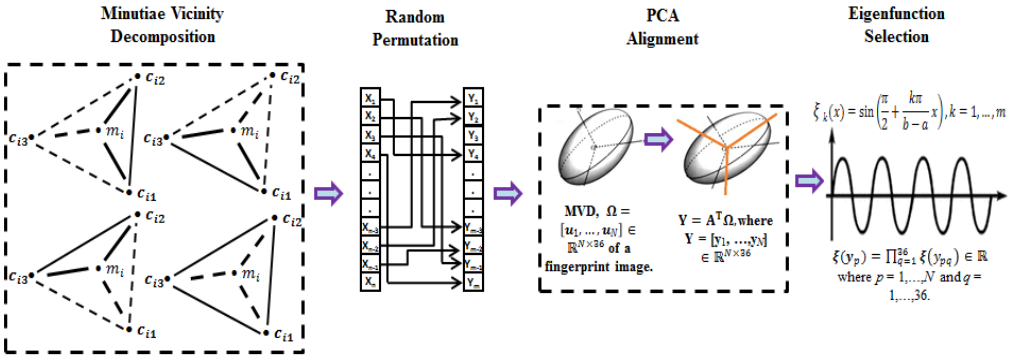


Fig. 5.3: Diagram of the modified randomized graph based hamming embedding (RGHE).

5.4.2 Modified RGHE

It is noted that the original Randomized GHE described in Chapter 3 (Section 3.3), which consists of a combination of random projection and GHE, is for cancellable biometric template construction with strong non-invertible property. Yet, it is not meant for key binding scheme that required addressing different set of design requirements. In this thesis, the Randomized GHE is modified as shown in Fig. 5.3 for the proposed key binding scheme. The modifications are described as follows:

a. Instead of using random projection on MVD (Jin & Teoh, 2011), the minutia vicinity vectors within MVD matrix is first randomly permuted. The reason is that the range values of these vectors are non-uniform since they are extracted from triangles (*length* of three sides, three internal *angles* and *orientation* difference). Therefore, random permutation is done by row-wise basis, $\widehat{\boldsymbol{\Omega}}_{\boldsymbol{i}} = \mathrm{Perm}(\boldsymbol{\Omega}_{\boldsymbol{i}}), i = 1, \dots, N$, which can preserve the characteristics of different features. $\boldsymbol{\Omega}_{\boldsymbol{i}}$ and $\widehat{\boldsymbol{\Omega}}_{\boldsymbol{i}}$ represent the original and the permuted template respectively; N is the total number of vicinities extracted from minutia set.

b. Note that the original RGHE discussed in Chapter 3 Section 3.3 applied a single-bit quantization scheme to covert the real-valued features to binary bits for speedy matching purpose. However, single-bit quantization cannot preserve the Euclidean neighborhood structure effectively after mapping to Hamming space. In this construct, quantization step is omitted and found that accuracy performance can be gained, yet it wouldn't compromise the non-invertible property significantly. This will be justified in Section 5.6. The details for the modified RGHE are given in Algorithm 5.3.

Algorithm 5.3. Modified Randomize Graph based Hamming Embedding

Input Minutia vicinity Decomposition (MVD), $\boldsymbol{\Omega} \in \mathbb{R}^{N\times 36}$ and code length $\widehat{m}$

Step 1: Random Permutation

1.1: $\widehat{\boldsymbol{\Omega}} = \mathbf{Perm}(\boldsymbol{\Omega}) \in \mathbb{R}^{N\times 36}$, **Perm**(.) denotes permutation function.

Step 2: PCA Alignment

2.1: Extracts eigenvectors $\boldsymbol{\Phi}$ from the covariance matrix, $\mathbf{C}= \widehat{\boldsymbol{\Omega}}\widehat{\boldsymbol{\Omega}}^{\mathbf{T}}$

2.2: Project $\widehat{\boldsymbol{\Omega}}$ to eigenspace, i.e. $\mathbf{Y}=\boldsymbol{\Phi}^{\mathbf{T}}\widehat{\boldsymbol{\Omega}}$, where $\mathbf{Y} = [\mathbf{y}_1, \dots, \mathbf{y}_N] \in \mathbb{R}^{N\times 36}$

2.3: Calculate a = min(**Y**) and b = max(**Y**) for eq. (5.4) and eq. (5.5).

2.4: Calculate 36k eigenvalues from β_k using eq. (5.4) and sort them in

ascending order.

Step 3: Eigenfunctions selection
3.1 Compute $\hat{m}$ eigenfunctions according to the $\hat{m}$ smallest eigenvalues from step 2.4, i.e.
For i=1:$\hat{m}$
Compute $\xi_i(\mathbf{y}) = \prod_{r=1}^{36} \xi_i(y_r) \in \mathbb{R}$ as in eq. (5.4).
End for
3.2 Repeat Step 3.1 for all *N* minutiae vicinities, hence $\boldsymbol{\xi^n} = [\boldsymbol{\xi_1}, \ldots, \boldsymbol{\xi}_{\hat{m}}]$, where $n = 1,\ldots,N$.

Output Resulting template $\boldsymbol{\Xi} = [\boldsymbol{\xi^1}, \ldots, \boldsymbol{\xi^N}] \in \mathbb{R}^{N \times \hat{m}}$

* The equations (5.4) and (5.5) used in algorithm 5.3 are displayed below. The two equations have been described in Chapter3 Section 3.3.1.2. The readers may refer that for more details.

$$\xi_k(x) = \sin\left(\frac{\pi}{2} + \frac{k\pi}{b-a}x\right) \tag{5.4}$$

$$\beta_k = 1 - e^{-\frac{\epsilon^2}{2}\left|\frac{k\pi}{b-a}\right|^2} \tag{5.5}$$

5.4.3 Matching

After executed algorithm 5.3, a template, $\boldsymbol{\Xi}$ with size $N \times \hat{m}$ can be formed, where *N* is the number of minutia vicinity. The dissimilarity of enrolled and query templates, $\boldsymbol{\Xi}_e = [\boldsymbol{\xi}_{e1}, \ldots, \boldsymbol{\xi}_{eN_1}] \in \mathbb{R}^{N_1 \times \hat{m}}$ and $\boldsymbol{\Xi}_q = [\boldsymbol{\xi}_{q1}, \ldots, \boldsymbol{\xi}_{qN_2}] \in \mathbb{R}^{N_2 \times \hat{m}}$ can be computed by the smallest pairwise Euclidean distance between templates $\boldsymbol{\Xi}_e$ and $\boldsymbol{\Xi}_q$, where N_1 and N_2 are the number of vicinities extracted from an enrolled and a query fingerprint image. The score of a matched pair p_{ij} in the comparison of $\boldsymbol{\Xi}_e$ and $\boldsymbol{\Xi}_q$ can be computed using eq. (5.6). With this, a score matrix **P = [p_{ij}]** of size N_1 x N_2 can be formed:

$$p_{ij} = \min(\|\boldsymbol{\Xi}_e, \boldsymbol{\Xi}_q\|) \tag{5.6}$$

where ||.|| denotes the Euclidean distance between $\boldsymbol{\Xi}_e$ and $\boldsymbol{\Xi}_q$.

Next, the *minimum value* is stored for each row in **P**, which is denoted as a_i:

$$a_i = \min_j(\mathrm{P}_{ij}) \text{ for } i = 1,\ldots, N_1 \text{ and } j = 1,\ldots, N_2 \quad (5.7)$$

The matching score can then be computed by counting the number of a_i that has a greater value than the pre-defined threshold *t*. To avoid large variation in the results caused by non-trivial difference in magnitude led by unstable number of minutiae in the query and enrolled images, the matching score can be normalized as follows:

$$s = \frac{\sum_{i=1}^{N_1}(a_i < t)}{\sqrt{N_1 \times N_2}} \quad (5.8)$$

Hence, the score obtained is the real-valued score and the value '0' indicates a strong negative match and vice versa.

5.5 Experimental Results

The experiments are conducted on five public fingerprint datasets, FVC2002 (DB1, DB2, DB3 and DB4) (FVC2002, 2002) and FVC2004 DB2 (FVC2004, 2004). Each dataset consists of 100 users with 8 samples per user. In total, there are 800 (100×8) fingerprint images for each dataset. VeriFinger 7 SDK (Verifinger, 2015) was used for minutia extraction. The minutiae template is extracted according to ISO-complaint format for evaluation, i.e. (x, y, θ). The accuracy performance is evaluated using False Acceptance Rate (FAR), False Reject Rate (FRR), Genuine Acceptance Rate (GAR) as well as the receiver operating characteristic (ROC) curves.

In this experiment, two testing protocols are adopted: 1) *1vs1 protocol*: the first and second impressions of each subject are used as gallery and probe respectively. Due to the relatively good in image quality, this protocol is widely used for the experiments in biometric cryptosystems (Nagar et al., 2008; Nagar et al., 2010b; Li et al., 2010; Yang et al., 2013; Yang et al., 2014a; Yang et al., 2014b). More precisely, such experimental setting can be justified that in biometric cryptosystems, the users are cooperative and willing to provide good quality biometric data to retrieve their cryptographic keys (Nandakumar et al., 2007; Xu et al., 2009). Hence, the matching yields 100 genuine scores and 4950 imposter scores. Note that this is a popular experimental setup in fingerprint key binding scheme, since the same setup has been employed by state-of-arts (Nandakumar et al., 2007; Nagar et al., 2008); 2) *1-8 protocol*: the first impression of each subject is used as gallery and the rest of eight impressions of each subject are of probe. This protocol is to examine the robustness of the proposed method. Yet, it is noted that a poorer performance is anticipated via 1-8 protocol as the performance gap between the biometric cryptosystems and conventional biometric recognition systems has been acknowledged in Chapter 2 Section 2.3. This protocol results 700 genuine scores and 4950 imposter scores.

5.5.1 Accuracy Performance of the Modified RGHE

The accuracy performance of the original RGHE and the modified RGHE is first investigated. Fig. 5.4 shows the receiver operating characteristic (ROC) curves of the original RGHE and the modified RGHE. It can be observed that the accuracy performance of the latter is improved over the

former. This experiment confirms the justification given in Section 5.4.2, where the accuracy improvement is attributed by the removal of quantization in RGHE.

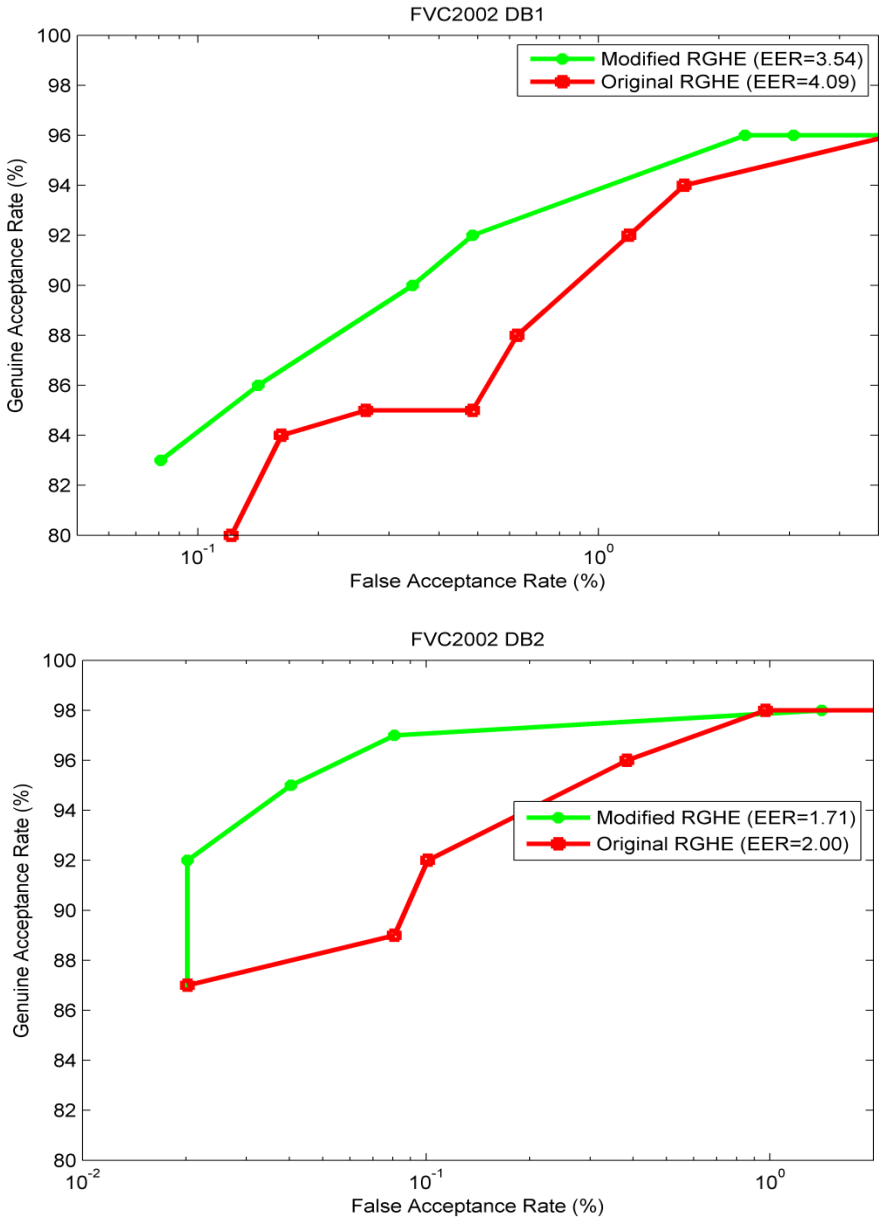


Fig. 5.4: ROC curves are served as comparison of the accuracy performance of the original RGHE and the modified RGHE for FVC2002 DB1 and DB2.

5.5.2 The Key Release Error Rate (KRER) of the Proposed Key Binding Scheme

As discussed in Chapter 2 Section 2.3, one of the main limitations of existing key binding is the security-performance trade-off. However, such a trade-off is eliminated in the proposed scheme. In this thesis, the performance of key release is evaluated by a metric, namely key release error rate (KRER) that comprises of two common indicators, false acceptance rate (FAR) and false rejection rate (FRR). From Table 5.1, it is interesting to note that the KRER remains the same for key size *m* from 1, 16, 32, 64 to 128 bits. This surprising fact is attributed to the RGHE mechanism and two-stage matcher that applied in this scheme. First, row-wise permutation of MVD vectors within the MVD, described in eq. (5.2) and eq. (5.3) is invariant with respect to the two-stage matcher (Section 5.4.3). Recall in two-stage matcher, the pairwise distances of row minutia vicinity vectors are first exhaustively computed and the minimum value is taken for verification with respect to a chosen threshold value. Therefore, permutation would not alter the resulting KRER. This characteristic is propagated to matching of two cancellable templates if the non-invertible transformation adopted in this scheme, i.e. RGHE, could preserve the pairwise relative distances of row minutia vicinity vector of a MVD after transformation. From the experiments results, it is noticed that this assumption is hold for RGHE (performance preservation before and after transformation). Since all *m* distance scores are computed from the matching of *m permuted* cancellable templates and query input pair and all of them render *identical* distance scores, this implies that the KRER remains the same regardless *m.*

To better illustrate this observation, let Ξ_1^e and Ξ_1^q be the 1st cancellable templates for enrolled and query pair and s_1 be the distance of Ξ_1^e and Ξ_1^q. Similarly, Ξ_2^e and Ξ_2^q be the 2nd permuted cancellable templates for enrolled and query pair and s_2 be the distance score of Ξ_2^e and Ξ_2^q. According to RGHE and two-stage matcher properties, it is known that Ξ_1^e and Ξ_2^e (also for Ξ_1^q and Ξ_2^q) are invariant with respect to the two-stage matcher, hence $s_1 = s_2$. By increasing the number of bits to *m*, the distance s_m of Ξ_m^e and Ξ_m^q is also identical to s_1 and s_2, i.e. $s_1 = s_2 = \cdots s_m$. Since m distances among the cancellable templates $\Xi^e$and Ξ^q are identical, the key release operation just resembles a-single matching that repeated for *m* times. Thus, this explains why KRER remain the same regardless *m*.

To further verify this observation, random projection (Johnson & Lindenstrauss, 1984) as a means of permutation function alternative, along with GHE is also examined and the KRERs are shown in Table 5.1. It can be observed that the KRERs for different *m* are no longer identical but slightly fluctuated. This is due to the row vectors in MVD after random projection is not exactly invariant to two-stage matcher despite the GHE still preserve the MVD structure.

Table 5.1: Key release error rate for the proposed key binding scheme when the key length is increased.

Databases	Key-length (bits)	Random Permutation + GHE		Random Projection + GHE	
		1vs1 protocol (1st & 2nd images)	1-8 protocol (1st to 8th images)	1vs1 protocol (1st & 2nd images)	1-8 protocol (1st to 8th images)

		FAR (%)	FRR (%)	FAR (%)	FRR (%)	FAR (%)	FRR (%)	FAR (%)	FRR (%)
FVC2002 DB1	1	0.16	11	0.12	26.57	0.18	11	0.26	23.71
	16	0.16	11	0.12	26.57	0.1	11	0.55	23.14
	32	0.16	11	0.12	26.57	0.1	11	0.30	25.14
	64	0.16	11	0.12	26.57	0.02	11	0.12	25.71
	128	0.16	11	0.12	26.57	0.02	12	0.10	27.86
FVC2002 DB2	1	0.061	3	0.12	13.14	0.16	2	0.34	13.29
	16	0.061	3	0.12	13.14	0.04	2	0.10	13.29
	32	0.061	3	0.12	13.14	0.02	3	0.20	13.14
	64	0.061	3	0.12	13.14	0.04	2	0.12	14.86
	128	0.061	3	0.12	13.14	0.02	2	0.10	15.29
FVC2002 DB3	1	1.25	25	3.45	27.14	0.71	33	0.99	41.43
	16	1.25	25	3.45	27.14	0.54	32	0.77	42.43
	32	1.25	25	3.45	27.14	0.48	33	0.79	41.71
	64	1.25	25	3.45	27.14	0.44	35	0.75	43.86
	128	1.25	25	3.45	27.14	0.40	35	0.77	44.71
FVC2002 DB4	1	1.49	21	3.47	21.86	0.57	38	0.97	33
	16	1.49	21	3.47	21.86	0.36	38	0.79	30.43
	32	1.49	21	3.47	21.86	0.26	38	0.79	29.14
	64	1.49	21	3.47	21.86	0.20	38	0.63	31.29
	128	1.49	21	3.47	21.86	0.14	38	0.55	32.43
FVC2004 DB2	1	1.89	45	3.07	45.86	1.73	45	1.27	50
	16	1.89	45	3.07	45.86	1.39	39	0.77	43.71
	32	1.89	45	3.07	45.86	0.93	39	0.77	44.29
	64	1.89	45	3.07	45.86	0.59	43	0.77	45.29
	128	1.89	45	3.07	45.86	0.42	45	0.69	51

Apart from the above, an accuracy comparison experiment has been conducted between the proposed scheme with state-of-the-arts (Nandakumar et al., 2007; Nagar et al., 2008; Nagar et al., 2010b; Nandakumar, 2010; Li et al., 2010; Li et al., 2012; Hartloff et al., 2013; Yang et al., 2013; Yang et al.,

2014a; Yang et al., 2014b) in fingerprint modality. Note that only FVC2002 DB1, DB2 and 1vs1 protocol are used for comparison as most of the literature (Nandakumar et al., 2007; Nagar et al., 2008; Nagar et al., 2010b; Nandakumar, 2010; Li et al., 2010; Li et al., 2012; Hartloff et al., 2013; Yang et al., 2013; Yang et al., 2014a; Yang et al., 2014b) follows this protocol. The state-of-the-arts of key binding schemes are partitioned into three groups: i.e. fuzzy vault, fuzzy commitment and other alignment-free bio-cryptosystems. From the results shown in Table 5.2, the observations are summarized as follows:

- For fuzzy vault, the accuracy of the proposed scheme is better than the works (Nandakumar et al., 2007; Nagar et al., 2008; Li et al., 2010; Yang et al., 2013). Besides, there are two additional advantages provided by the proposed scheme: a) it is solely based on the minutiae information while the works (Nandakumar et al., 2007) requires minutiae alignment based on the high curvature points and additional information such as ridge orientation, frequency required by (Nagar et al., 2008;); b) a 2% of failure-to-capture rate (FTCR) in Nandakumar et al. (2007) and Nagar et al. (2008) is observed (e.g. failure for high curvature point extraction) while there is no failure-to-capture rate in the proposed method since no additional information is utilized for performance improvement.

- For fuzzy commitment, it is observed that the KRER of the proposed scheme is comparable to the works Nagar et al. (2010b), Nandakumar,

(2010), Li et al. (2012) and Hartloff et al. (2013). Just to point out that for Nagar et al. (2010b) and Nandakumar, (2010), additional information such as focal point of high curvature regions is mandatory for minutiae alignment.

❖ For minutiae-based alignment-free bio-cryptosystems, the proposed scheme outperforms Yang et al. (2014b) as observed in Table 5.2. Although a bio-cryptosystems recently reported by Yang et al. (2014a) shows an improvement both in security and accuracy performance. It is noticed that a helper data is exploited to reject the low quality query sample for decoding. However, the failure-to-decode rate is not reported so that the comparison cannot be fairly justified without such information.

Table 5.2: Accuracy comparison between the proposed key binding scheme with the state-of-the-arts using 1 vs 1 protocol.

Methods	**FVC2002 DB1**	**FVC2002 DB2**
Proposed	FRR=11 (GAR=89); FAR=0.16 (Security - identical to key length)	FRR=3 (GAR=97); FAR=0.061 (Security - identical to key length)
Fuzzy Vault for fingerprint		
Nandakumar et al. (2007)	-	GAR=91; FAR=0.01; failure-to-capture rate (FTCR)=2
Nagar et al. (2008)	-	GAR=95; FAR=0.01; failure-to-capture rate (FTCR)=2
Yang et al.	FRR=19; FAR=0.38	FRR=17; FAR=0.09

(2013)	(14 bits security)	(25 bits security)
Li et al. (2010)	GAR=85; FAR=0.00 (29 bits security)	GAR=93; FAR=0.00 (32 bits security)
Fuzzy Commitment for fingerprint		
Nandakumar, (2010)	FNMR=12.5; FMR=0.1 (Approx. 43 bits security)	FNMR=8.9; FMR=0.1 (Approx. 43 bits security)
Nagar et al. (2010b)	-	GAR=85; FAR=0.13 (Approx. 45 bits security)
Hartloff et al. (2013)	FRR=36.54; FAR=0.29 (Approx. 143.2 bits security)	FRR=26.48; FAR=0.23 (Approx. 203.3 bits security)
Li et al. (2012)	FRR=18.6; FAR=0 (39 bits security)	FRR=8.03; FAR=0 (45 bits security)
Minutiae-based alignment-free bio-cryptosystems		
Yang et al. (2014b)	FRR=8; FAR=0.59 (Null)	FRR=6; FAR=0.02 (112 bits security)
Yang et al. (2014a)	FRR=4; FAR=0 (Approx. 33 bits security)	FRR=2; FAR=0 (Approx. 37 bits security)

It is further pointed out that the main objective of this work is to demonstrate the feasibility of the proposed key binding scheme using cancellable transforms with comparable accuracy performance. Nevertheless, the performance could be enhanced by using more effective minutiae descriptor derived from sole minutiae set. As a proof-of-concept, 2P-MCC (Ferrara et al., 2014), a cancellable and strong non-invertible representation derived from the state-of-the-art minutia descriptor, MCC (Cappelli et al., 2010), is adopted in the proposed key binding scheme. Table 5.3 demonstrates that the proposed key binding scheme outperforms all the existing key binding schemes when 2P-MCC is incorporated. Such outstanding performance gained

is attributed to the capability of adopting high discriminative but non-restricted biometric representation and sophisticated matcher.

Table 5.3: Key release error rate of the proposed key binding scheme by incorporating 2P-MCC using 1 vs 8 protocol.

Key-length (bits)	Key release error rate (FAR/FRR)(%)				
	FVC2002 DB1	FVC2002 DB2	FVC2002 DB3	FVC2004 DB1	FVC2004 DB2
1	0.06/3.29	0.06/2.57	0.83/16.71	0.99/17	0.73/16.43
16	0/2.29	0/1.57	0/10.57	0/15.71	0/16.29
32	0/2.43	0/1.57	0/11.71	0/16.14	0/14.42
64	0/2.43	0/1.71	0/12	0/16.86	0/15.14
128	0/2.43	0/1.86	0/13.29	0/17.29	0/16.86

5.5.3 Cancelability

Cancelability in this work refers to two scenarios: 1) if the cryptographic key is compromised, a new key can be re-issued and the KRER should be preserved; 2) if the random permutation seeds for cancellable templates generation are compromised, a set of new seeds is issued to generate cancellable templates and the decoding accuracy should be preserved as well. Several experiments have been designed to evaluate the cancelability under these two scenarios.

A) Cancelability in Cryptographic Key Compromise Scenario

To do this, 100 sets of key randomly are generated; each set consists of four keys with 16, 32, 64 and 128 bit-length respectively. The same

experimental protocol described in Section 5.5 is applied to evaluate the KRER by changing the keys repeatedly. It is observed that the KRER is identical to what it has presented in Section 5.5.2. This is expected, in fact, whether a key can be released correctly is subjected to the matching result of two cancellable templates as shown in Fig. 5.2. Key changing would not affect the KRER as they are completely independent.

B) Cancelability in Permutation Seed Compromise Scenario

On the other hand, to assess the cancelability in permutation seed compromise scenario, we also randomly generated 100 sets of random permutation seeds and perform the experiment described in Section 5.5 by changing the permutation seeds. Note that 100 sets of random permutation seeds produce 100 sets of cancellable template to bind and release the cryptographic key. As expected, the KRER is identical to the accuracy presented in Section 5.5.2. The accuracy preservation is due to the RGHE mechanism and two-stage matcher as discussed before. Row-wise permutation in MVD by changing the seeds is invariant to the two-stage matcher and thus the distance between two MVD is identical. Further, it has been shown that the characteristics of GHE (i.e. structure preservation of MVD before and after transformation) could preserve the relative distances propagated from MVD features. This is to prove the cancellable property in permutation seed compromise scenario is indeed achievable.

5.5.4 Complexity Analysis

The time complexity on encoding and decoding are also investigated and the results are shown in Table 5.4. The average time is captured by the experimental machine with Intel i7 (3.4GHz) CPU and 4GB RAM. It can be observed from Table 5.4 that the average time of encoding and decoding is proportional to the bit-length of cryptographic key, which is straightforward due to the fact that more bits of the key requires more time to encode and decode it. In general, the time efficiency for the proposed key binding method is feasible for deployment.

Table 5.4: Average time of encoding and decoding for the proposed key binding method in different bit-length.

Databases		Encoding **(Seconds)**	Decoding **(Seconds)**
FVC2002 DB1	16bits	0.1183	0.1042
	32bits	0.2509	0.2231
	64bits	0.4932	0.4360
	128bits	1.0013	0.8601
FVC2002 DB2	16bits	0.1477	0.1385
	32bits	0.2896	0.2672
	64bits	0.5744	0.5417
	128bits	1.1522	1.0757

5.6 Security and Privacy Analysis

In this section, the security and privacy of the implementation for the proposed key binding scheme is investigated. More precisely, the terms of

privacy in this context refer to non-invertibility, non-linkability respectively while security refers the attacks for illegitimate access. As such, the analysis on the non-invertibility of the modified RGHE, Attacks via record multiplicity (ARM), Surreptitious Key-Inversion Attack (SKI) and statistical attack are given.

5.6.1 Non-invertibility of the Modified RGHE

The non-invertibility in this context refers that the cancellable templates generated by RGHE is computationally difficult to be reverted into minutia vicinity decomposition (MVD) features. This is to ensure that the original minutiae are securely protected (privacy preserving) and the spoofed impersonation derived from MVD is infeasible (security).

The non-invertibility of the modified RGHE is imposed by two ingredients: 1) the sinus function in eq. (5.4) offers many-to-one mapping; 2) 36 eigenfunctions product using $\xi(\mathbf{u}) = \prod_{i=1}^{36} \xi(u_i)$ where $\xi_i(x) = \sin\left(\frac{\pi}{2} + \frac{k\pi}{b-a}x\right)$ in eq. (5.4). The θ of the sinus function in eq. (5.4) is first investigated. Because the many-to-one property is functioned, only when the θ of sinus function is greater than 2π and the larger θ the stronger non-invertibility. To do this, the following experiments are conducted: a) compute the mean and standard deviation of the angle θ from each MVD feature matrix; b) Since there are 800 MVD feature matrices derived from each dataset, we further compute the average mean and average standard deviation from the 800 MVD feature matrices. The results presented in Table 5.5 show that the angle (in rad) is invalid for the small angle approximation analysis

while the many-to-one property of RGHE is effective as the mean and the range of angle indicate that multiple solutions exist (i.e. θ exceeds 2π).

Secondly, to evaluate the invertibility of the 36 dimensional eigenfunctions $\xi_i = \prod_{r=1}^{36} \sin(\frac{\pi}{2} + \frac{i\pi}{b-a} y_r)$, it is common to assume that ξ_i is known in the analysis (e.g., after database is compromised). The hardness of inverting ξ_i lies in the associated number of input possibilities. In Table 5.5, it is known that there are 8 and 10 possible inputs associated with ξ_i for FVC2002 DB1 and DB2, respectively. Hence, for FVC2002 DB1 and DB2, the invertibility complexity for single minutia vector decomposition is upper bounded by $8^{36} \approx 2^{118}$ and $10^{36} \approx 2^{129}$, yielding 118 and 129 bits entropy, respectively. To invert N number of vicinities, the total invertibility complexity is therefore upper bounded by $8^{36}N \approx 2^{118}N$ and $10^{36}N \approx 2^{129}N$, yielding $118+\log_2(N)$ and $129+\log_2(N)$ bits entropy for FVC2002 DB1 and DB2, respectively.

Table 5.5: Mean and standard deviation for θ in Radian.

Measurements	**FVC2002 DB1**	**FVC2002DB2**
Average Mean of angle (rad)	11.6851	13.0572
Average S.T.D of angle (rad)	8.7962	10.6427
Range of angle (rad)	≈ 1.57 to 48.69	≈ 1.57 to 67.54
Maximum number of possible inputs corresponding to an output of a single-dimensional eigenfunction	8	10

Additionally, the user privacy in this context is highly concerned due to the fact that minutiae points can be used to reconstruct the fingerprint image easily (Hill, 2001). To prevent the privacy leakage, the fingerprint minutiae points have to be protected securely. To do this, the MVD features reversal from the stored cancellable templates must be strictly prevented. This is equivalent to non-invertiblity problem of RGHE reasoned above. It has been demonstrated that such reversal is indeed infeasible due to computational hardness. Even in the event that MVD features are disclosed, converting the minutiae descriptor with invariant features into the absolute location and orientation of a minutia are rather challenging based on the existing techniques (e.g. Hill climbing). For example, a hill climbing approach may generate many spurious minutiae outside the region of interests (ROI) of the fingerprint image. Such reconstructed minutiae points may not lead to a high match score with another impression of the same finger (Nagar, 2012).

5.6.2 Surreptitious Key-Inversion Attack (SKI)

As discussed in Section 5.3.3, the key can be retrieved only if the entire set of cancellable templates is successfully reversed to the true and synthetic templates. The effort to recover the MVD features from a single cancellable template requires 118 and 129 bits entropy respectively (see Section 5.6.1). Therefore, the full recovery for a single key with length m requires 118^m and 129^m ($m \geq 128$) trials respectively. Therefore, the SKI attack is computationally infeasible.

5.6.3 ECC-based Attacks

A. Attacks via record multiplicity (ARM)

ARM in fuzzy commitment refers the decodability attack that has been discussed in Chapter 2 Section 2.3. In principle, ARM is feasible with high possibility due to the limitations of error correction codes employed. However, ARM is not possible in the proposed method as no ECC is employed.

It is further pointed out that, without the knowledge of key, the adversary is still difficult to distinguish the cancellable templates generated from true template or synthetic template. Thus, the correlation analysis among the cancellable templates generated from true templates cannot be performed. As such, it can be reasoned that ARM on the set of cancellable templates is indeed infeasible.

B. Statistical attack

Similarly, statistical attack discussed in Chapter 2 Section 2.3 is also an ECC triggered attack. However, this attack is absent in the proposed key binding scheme due to the abandon of ECC. Further, statistical analysis on cancellable templates is hardly feasible due to: 1) without cryptographic key, no clue of cancellable templates generated from true or synthetic template; 2) cancellable templates produced by RGHE are statistical indistinctive as discussed in Section 5.3.3.

5.7 Discussion and Summary

In this chapter, an ECC-free key binding scheme along with cancellable transforms is proposed for minutiae-based fingerprint biometrics in place of fuzzy commitments. The key binding process is accomplished by employing a series adoptive cancellable transforms and thresholding mechanism, which enjoys several merits. Firstly, the security-performance trade-off that attributed by ECC is resolved in the proposed key binding scheme. This is confirmed by the extensive experiments where the accuracy performances remain stagnant regardless increment of key size. Secondly, unlike fuzzy commitment, the scheme does not impose any restriction to the representation form of biometrics and hence matchers. A great flexibility of adopting effective feature extractors and robust matchers can be attained. Thirdly, the security and privacy of the proposed key binding construct that associated to non-invertibility and non-linkability criteria are justified. While ECC-free key binding scheme is still a new direction to study, we believe the proposed scheme has wide room to improve in security, privacy and recognition performance aspects in the future. We hope this work can provoke thoughts and discussions in this area.

CHAPTER 6

CONCLUSION AND FUTURE WORKS

In this thesis, a study towards minutia-based fingerprint template protection was carried out. As results of the study, four unique proposals have been presented, which cover the major approaches (cancellable biometrics and biometric cryptosystems) of biometric templates protection. Among the four proposals, two distinct cancellable fingerprint template generation methods, i.e. 2D-RP-MVD and RGHE, are dedicated to the biometric salting and non-invertible transform (two sub-classes of cancellable biometrics) respectively. While, the rest of two proposals, i.e. point-to-string conversion and fingerprint key binding, are mainly devoted to biometric key binding (a sub-class of biometric cryptosystems). Each proposed method was elaborated and evaluated chapter-by-chapter throughout the thesis. As a final remark, this chapter summarizes the importance of this doctoral work and avenues the future works not only from the extension of this study but also other research opportunities in relevant realms.

6.1 Summary of Thesis Chapters

An extensive literature review has been done in Chapter 2. It includes three aspects of study: 1) fingerprint minutia-based cancellable templates, 2) point-to-string conversion for fingerprint minutiae and 3) biometric key binding. Firstly, a categorization method for fingerprint minutia-based

cancellable templates was introduced, i.e. *direct minutiae transform* and *indirect minutiae transform*. The former approach is efficient in processing speed, but is of risk to minutiae revelation while the latter approach is just opposite to the former approach. At the end of this study, we revealed that the original random projection (RP) used in literature is merely for a 1D fixed length feature vector, which is not applicable for the 2D minutia-based feature representation. Further, the cancellable templates are weak against inversion due to the careless design of non-invertible functions. Apart from that, most of the proposed security-oriented cancellable templates trade with poor accuracy performance, thus demonstrating security-performance trade-off. Secondly, in the study of point-to-string conversion, a classification based on how a set of points is converted into ordered and fixed-length bit-string was introduced, i.e. *reference-based approach*, *histogram-based approach*, and *spectral transform approach*. We learned that the existing point-to-string conversion methods hardly compete with the state-of-the-art minutiae descriptor in performance accuracy thus far. Thirdly, in the study of biometric key binding, we found out that the existing ECC-enabled biometric key binding schemes suffers from security and privacy leakage via a number of attacks, e.g. Decodability attack (ARM), SKI attack and statistical attack etc.

Based on the findings from the study of fingerprint minutia-based cancellable templates, two distinct fingerprint minutia-based cancellable template generation methods were proposed in Chapter 3, i.e. two-dimensional random projected minutia vicinity decomposition (2D-RP-MVD) and randomized graph-based hamming embedding (RGHE). 2D-RP-MVD is

designed to extend the random projection used for 1D feature vector to 2D feature representation with the intention of adapting 2D minutiae-based feature representation, i.e. MVD. With 2D-RP-MVD, the objective of generating cancellable fingerprint templates is accomplished. Further, the utilized descriptor, i.e. MVD generates the geometrical invariant features that conceal the original minutia coordinates and orientations. This provides the additional protection over the original minutia vicinity construct wherein the original minutia coordinates and orientations are stored. Though, 2D-RP-MVD excels in performance-preservation, it is vulnerable to reverse attack when the user-specific key is stolen by the adversary. This motivates us to design a transformation function with strong non-invertible property. RGHE was then presented. Essentially, RGHE offers a highly non-linear equation system involving multiple products of 36 sinus functions (a non-linear many-to-one function), which makes MVD extremely hard to be retrieved through inverting this equation system even when the helper data is known by the adversary. The cancellability of RGHE can be achieved by amalgamating 2D-RP-MVD.

Experimental results showed that both 2D-RP-MVD and RGHE manage to maintain the performance accuracy over the minutia descriptor (MVD). The overall performance accuracies in terms of EER for 2D-RP-MVD and RGHE are better than the existing methods. In addition, the security and privacy of the two distinct cancellable template generation methods were analysed. 2D-RP-MVD is effective in generating cancellable template for 2D feature representation, but provides weak privacy. It was also shown that

RGHE, on the contrary, offers strong irreversibility against inversion due to the non-linear equation system. Furthermore, the irreversible strength of angle-based many-to-one (non-linear) function is addressed via the small angle approximation analysis.

Minutiae template (e.g. ISO-compliant format) extracted from a fingerprint image in each time may vary in terms of the amount, coordinates and orientation. The variability of minutia amount can be propagated to the minutiae descriptors (e.g. MCC) that are variable in size and unordered. Such characteristic of templates hinders the applications that only operate on ordered fixed-length representation, such as fuzzy commitment, dynamic quantization for template binarization, fingerprint indexing etc. Therefore, in Chapter 4, a complete point-to-string conversion framework based on kernel transformation method was proposed to convert the minutiae template into an ordered and fixed-length representation. In the proposed framework, two distinct branches of kernel transformation method were introduced, i.e. KPCA and KLSH. On top of that, the matching function of minutiae descriptor yields a non-SPD kernel matrix, thus a Gaussian-like kernel function is specially designed to induce SPD that is an essential factor for accuracy performance. The objective of point-to-string conversion is not accomplished without feature binarization. Thus, the real-valued fixed-length representation generated from kernel transformation methods is binarized into bit-string. The bit-string refers to one dimensional fixed-length binary vector. Two binarization techniques, static quantization (or precisely zero-thresholding) and dynamic quantization, were used to binarize the said representations for

comparison in this thesis. As a finishing touch, the implementation using the generated binary templates in fuzzy commitment scheme is also demonstrated.

The experiment conducted for point-to-string conversion framework showed that the accuracy performance is admissibly preserved among the minutiae descriptor (VSB), real-valued fixed-length representations (TKPCA and TKLSH) and binary fixed-length representations (TKPCA-DQ and TKLSH-DQ). Furthermore, the accuracy performance of DQ-based binarization outperforms the zero-thresholding based binarization in a significant extend. This is because DQ-based binarization utilizes the information of feature distribution for bits allocation while the zero-thresholding based binarization totally ignores such information. In the aspect of computation complexity, the most of the time-consuming operations are executed off-line. The on-line runtime does not compromise the real time scenario considering the current computation technology.

The existing biometric key binding schemes utilize error correction codes (ECC) to mitigate the variability of biometric data. The security breaches and limitations associated with ECCs are therefore inevitable. In the Chapter 5 of this thesis, an ECC-free biometric key binding construct was proposed and implemented for fingerprint minutiae. The key binding and release is accomplished with the thresholding mechanism and cancellable transforms, but without ECCs. Apparently, ECC associated security breaches and limitations no longer exist as ECC has been abandoned. As a fresh point of view, amalgamating cancellable biometrics for biometric key binding

creates a tangible solution with the intention of overcoming the security breach and limitations in a significant extend. Experimental results showed that the accuracy performances remain stagnant regardless increment of key size. Furthermore, the proposed key binding construct is immune to several major security and privacy attacks. Another merit is that more effective minutiae descriptor and matchers can be flexibly integrated as the proposed scheme does not impose any restriction to biometric representation and matchers.

6.2 Future Works

In this section, some possible future works are briefly discussed. A straightforward one is to improve the proposed methods, for instance, algorithm modifications, processing flow optimization. On top of that, the potential works extended from this study would not be limited in inciting the practical usage of the proposed methods but discovering the new research opportunities in relevant realms.

Currently, biometrics is rapidly being adopted by mobile devices, such as Apple’s iPhone and Samsung's Galaxy series. The home button in the phone is also functioned as a fingerprint scanner used to unlock the phone. Since mobile devices are easy to be lost or stolen, the fingerprint data stored in the devices is highly vulnerable to privacy invasion. However, due to the technologies of small fingerprint sensor used in mobile devices, the fingerprint template protection methods for traditional (large) fingerprint sensors might not be adopted directly. As the proliferation of the fingerprint recognition in

mobile devices is foreseeable, it is necessary to modify the fingerprint template protection techniques to adopt the small-size fingerprint sensor in mobile environment.

As a practical application, a new user should be allowed to enrol to the application after it is set up. Yet, some algorithms (e.g. KPCA, KLSH and DQ for binarization) used in this thesis require a training procedure to compute the helper data during the application's start-up. This implies that re-training becomes inevitably when a new user is enrolled to the system, which is impractical for real world applications. Literature suggested that incremental KPCA could be the decent solution to resolve the re-training issue. Nonetheless, the study on the optimized incremental algorithms to update the pre-trained helper data is still a future research direction.

In this thesis, there are four methods proposed with the intention of protecting fingerprint minutiae. Although the prototypes are evaluated via publicly available databases, transforming lab prototypes to real world applications requires solving a number of practical issues involving optimization in programming languages, study of software engineering. To the best of our knowledge, there is currently no fingerprint recognition system with practically template protection functionality. Thus, study the realization for the proposed methods or at least implementing partial functionality e.g. non-invertibility is one of the promising future works.

REFERENCE

Adams, C. and Lloyd, S., 1999. *Understanding public-key infrastructure: concepts, standards, and deployment considerations*. Sams Publishing.

Ahmad, T., & Hu, J., 2010. Generating cancelable biometrie templates using a projection line. *Proceedings of 11th International Conference on Control Automation Robotics & Vision*, 7 - 10 December 2010 Singapore, pp. 7-12.

Ahmad, T., Hu, J. and Wang, S., 2011a. Pair-polar coordinate based cancellable fingerprint templates. *Pattern Recognition*, 44(10), pp. 2555-2564.

Ahmad, T., Hu, J. and Wang, S., 2011b. String-based cancelable fingerprint templates. *Proceedings of 6th IEEE Conference on Industrial Electronics and Applications (ICIEA)*, 21 - 23 June 2011 Beijing, pp. 1028-1033.

Ang, R., Rei, S., N. and McAven, L., 2005. Cancelable Key-Based Fingerprint Templates. *Proceedings of the Information Security and Privacy: 10th Australasian Conference*, 4 - 6 July 2011 Brisbane, pp. 242-252.

Arfken, G., 1985. Gram-schmidt orthogonalization. *Mathematical methods for physicists*, 3, Orlando, FL: Academic Press, pp. 516-520.

Bertillonage, 2011. *Bertillonage*. [Online]. Available at: http://www.nleomf.org/museum/news/newsletters/online-insider/November-2011/bertillon-system-criminal-identification.html/ [Accessed: 10 July 2015].

BIOIDENTIFICATION, 2012. *How is the probability distribution function measured for a biometric system's authorized and unauthorized users?* [Online]. Available at: http://www.bromba.com/faq/biofaqe.htm [Accessed: 25 July 2015].

Bledsoe, W. W., 1966. Man-machine facial recognition. *Rep. PRi*, 22.

Bringer, J., Chabanne, H., Cohen, G., Kindarji, B. and Zémor, G., 2008. Theoretical and practical boundaries of binary secure sketches. *IEEE Transactions on Information Forensics and Security*, 3(4), pp. 673-683.

Bringer J. and Despiegel. V., 2010. Binary feature vector fingerprint representation from minutiae vicinities. *Proceedings of the Fourth IEEE International conference on Biometrics: Theory Applications and Systems*, 27 - 29 September 2010 Washington DC, pp. 1–6.

Belkin, M. and Niyogi. P., 2003. Laplacian Eigenmaps for Dimensionality Reduction and Data Representation. *Neural Computation*, 15(6), pp. 1373–1396.

Cappelli, R., Lumini, A., Maio, D. and Maltoni, D., 2007. Fingerprint image reconstruction from standard templates. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 29(9), pp. 1489–1503.

Cappelli, R., Ferrara, M. & Maltoni, D., 2010. Minutia Cylinder-Code: a new representation and matching technique for fingerprint recognition. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 32(12), pp. 2128 – 2141.

Cappelli, R., Ferrara, M., & Maio, D. (2012). A fast and accurate palmprint recognition system based on minutiae. *IEEE Transactions on Systems, Man, and Cybernetics, Part B: Cybernetics*, 42(3), pp. 956-962.

Cappelli, R., & Ferrara, M., 2012. A fingerprint retrieval system based on level-1 and level-2 features. *Expert Systems with Applications*, 39(12), pp. 10465-10478.

Carter, F. and Stoianov, A., 2008. Implications of biometric encryption on wide spread use of biometrics. *EBF Biometric Encryption Seminar*.

Cavoukian, A., Chibba, M. and Stoianov, A., 2012. Advances in Biometric Encryption: Taking Privacy by Design from Academic Research to Deployment. *Review of Policy Research*, 29(1), pp. 37-61.

Chang, Y. J., Zhang, W. and Chen, T., 2004. Biometrics-based cryptographic key generation. *Proceedings of IEEE International Conference on Multimedia and Expo*, 27-30 June 2004 Taipei, pp. 2203-2206.

Charikar, M., 2002. Similarity Estimation Techniques from Rounding Algorithms. *Proceedings of the thirty-fourth annual ACM Symposium on Theory of Computing*, 19 – 21 May 2002 Montreal, pp.380-388.

Chen, C., Veldhuis, R. N. J., Kevenaar, T. A. M. and Akkermans, A. H. M., 2009. Biometric quantization through detection rate optimized bit allocation. *EURASIP Journal on Advances in Signal Processing*, 29, pp. 1–16.

Chow C. and Liu, C., 1968. Approximating discrete probability distributions with dependence trees. *IEEE Transactions on Information Theory*, 14(3), pp. 462-467.

Daugman, J. G., 1993. High confidence visual recognition of persons by a test of statistical independence. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 15(11), pp. 1148-1161.

Dodis, Y., Ostrovsky, R., Reyzin, L. and Smith, A., 2008. Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data. *SIAM Journal on Computing*, 38(1), pp. 97-139.

EER, *The Free Encyclopedia* [Online]. Available at: http://en.wikipedia.org/wiki/Biometrics#cite_note-2 [Accessed: 28 June 2015].

Ernst, R. H., 1971. Hand ID System" United States patent number US 3576537.

FAR, *The Free Encyclopedia* [Online]. Available at: http://en.wikipedia.org/wiki/Biometrics#cite_note-2 [Accessed: 28 June 2015].

Farooq, F., Bolle, R. M., Jea, T. Y. and Ratha, N. K., 2007. Anonymous and Revocable Fingerprint Recognition. *Proceedings of the International Conference on Computer Vision and Pattern Recognition*, 18-23 June 2007 Minneapolis Minnesota, pp.1-7.

Faulds, H., 1880. On the skin-furrows of the hand. *Nature*, 22, pp. 605.

Feng, J., & Jain, A. K., 2009. FMmodel based fingerprint reconstruction from minutiae template. *Proceeding of the International Conference on Biometrics*, 2-5 June 2009 Alghero, pp. 544-553.

Feng, J. and Jain, A.K., 2011. Fingerprint reconstruction: From minutiae to phase. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 33(2), pp. 209–223.

Feng, Q., Su, F., Cai, A. and Zhao, F. F., 2008. Cracking Cancelable Fingerprint Template of Ratha. *Proceedings of the International Symposium on Computer Science and Computational Technology*, pp. 572-575.

Ferrara, M., Maltoni, D. and Cappelli, R., 2012. Noninvertible Minutia Cylinder-Code Representation. *IEEE Transactions on Information Forensics and Security*, 7(6), pp. 1727-1737.

Ferrara, M., Maltoni, D. and Cappelli, R., 2014. A two-factor protection scheme for MCC fingerprint templates, *Proceedings of the 2014 International*

Conference of the Biometrics Special Interest Group (BIOSIG), 10 – 12 September Darmstadt, pp. 1–8.

FRR, *The Free Encyclopedia* [Online]. Available at: http://en.wikipedia.org/wiki/Biometrics#cite_note-2 [Accessed: 28 June 2015].

FVC2002. *In Second International Fingerprint Verification Competition* [Online]. Available at: http://bias.csr.unibo.it/fvc2002/ [Accessed: 15 May 2015].

FVC2004. *In Third International Fingerprint Verification Competition*. [Online]. Available at: http://bias.csr.unibo.it/fvc2004/ [Accessed: 15 May 2015].

Galton, F., 1889. Personal identification and description. *Nature*, 38, pp. 201-202.

Gionis, A., Indyk, P. and Motwani, R., 1999. Similarity Search in High Dimensions via Hashing. *Proceedings of 25th International Conference on Very Large Data Bases*, 7-10 September 1999 Edinburgh, pp. 518-529.

Harandi, M. T., Sanderson, C., Wiliem, A. and Lovell, B. C., 2012. Kernel analysis over Riemannian manifolds for visual recognition of actions, pedestrians and textures. *Proceedings of IEEE Workshop on Applications of Computer Vision*, 9 – 11 January 2012 Breckenridge, Colorado, pp. 433–439.

Hartloff, J., Dobler, J., Tulyakov, S., Rudra, A. and Govindaraju, V., 2013. Towards fingerprints as strings: Secure indexing for fingerprint matching. *Proceedings of International Conference on Biometrics (ICB)*. 4 - 7 June 2013 Madrid, pp. 1-6.

Herschel, W. J., 1880. Skin furrows of the hand. *Nature*, 23, pp. 76.

Hill, C., 2001. *Risk of masquerade arising from the storage of biometrics*. Master thesis, Australian National University, Australia.

Hrechak, A. K. and McHugh, J.A., 1990. Automated Fingerprint Recognition Using Structural Matching. *Pattern Recognition*, 23(8), pp. 893-904.

Ignatenko, T., 2009. *Secret-Key Rates and Privacy Leakage in Biometric Systems*. PhD thesis, Eindhoven University of Technology, Netherlands.

ISO/IEC 19794-2:2005, Information Technology—Biometric Data Interchange Formats—Part 2: Finger Minutiae Data, 2005.

Jain, A. K., Nandakumar, K. and Nagar, A., 2008. Biometric Template Security. *EURASIP Journal on Advances in Signal Processing*, pp. 113.

Jain, A. K., Ross, A. A. & Nandakumar, K., 2011. Introduction to biometrics. *Springer Science & Business Media*.

Jain, A. K., 2013. 50 Years of Biometric Research: The (Almost) Solved, The Unsolved, and The Unexplored, *Keynotes of 5th International Conference on Biometrics*, Madrid, Spain, 2013.

Jakubowski, M. H. and Venkatesan, R., 2007. Randomized radon transforms for biometric authentication via fingerprint hashing. *Proceedings of the ACM workshop on Digital Rights Management*, 29 October Alexandria, pp. 90-94.

Jayasumana, S. Hartley, R. Salzmann, M. Li, H. and Harandi, M., 2013. Kernel methods on the riemannian manifold of symmetric positive definite matrices. *Proceedings of IEEE Conference on Computer Vision and Pattern Recognition*, 25 -27 June 2013 Columbus, Ohio, pp. 73-80.

Jiang, X. and Yau, W. Y., 2000. Fingerprint Minutiae Matching Based on the Local and Global Structures. *Proceedings International Conference on Pattern Recognition*, 3-8 September 2000 Barcelona, pp. 6038-6041.

Jin, Z., Teoh, A. B. J., Ong, T. S., & Tee, C., 2009. Secure Minutiae-based Fingerprint Templates Using Random Triangle Hashing. *Proceeding of the 1st International Visual Informatics Conference*, 13-15 November 2013 Kuala Lumpur pp. 521-531.

Jin, Z., Teoh, A. B. J., Ong, T. S. and Tee, C., 2010a. Generating Revocable Fingerprint Template Using Minutiae Pair Representation. *Proceeding of the 2nd International Conference on Education Technology and Computer*, 22 - 24 June 2010 Shanghai, pp. 251-255.

Jin, Z., Teoh, A. B. J., Ong, T. S. and Tee, C., 2010b. A Revocable Fingerprint Template for Security and Privacy Preserving. *KSII Transactions on Internet and Information Systems*, 4(6), pp. 1327-1342.

Jin, Z. and Teoh, A. B. J., 2011. Fingerprint Template Protection with Minutia Vicinity Decomposition. *Proceeding of the International Joint Conference on Biometrics*, 11 – 13 October 2011 Washington DC, pp. 1-7.

Jin, Z., Teoh, A. B. J., Ong, T. S. and Tee, C., 2012. Fingerprint Template Protection with Minutiae based Bit-string for Security and Privacy Preserving. *Expert Systems with Applications*, 39(6), pp. 6157–6167.

Jin, Z., Goi, B.M., Teoh, A. B. J. and Tay, Y.H., 2014. A two-dimensional random projected minutiae vicinity decomposition-based cancellable fingerprint template. *Security and Communication Networks*, 5(12), pp. 1312-1324.

Jin, Z., Lim, M.H., Teoh, A. B. J. and Goi, B.M., 2014. A non-invertible Randomized Graph-based Hamming Embedding for generating cancelable fingerprint template. *Pattern Recognition Letters*, 42, pp. 137-147.

Johnson W. B. and Lindenstrauss, J., 1984. Extensions of Lipschitz mappings into a Hilbert space. *Contemporary Mathematics*, 26(189-206), pp. 1.

Juels, A. and Sudan, M., 2006. A Fuzzy Vault Scheme. *Designs, Codes and Cryptography*, 38(2), pp. 237-257.

Juels, A. and Wattenberg, M., 1999. A Fuzzy Commitment Scheme. *Proceeding of the Sixth ACM Conference on Computer and Communications Security*, 1 – 4 November 1999 Singapore, pp. 28-36.

Kelkboom, E. J., Breebaart, J., Kevenaar, T. A., Buhan, I. and Veldhuis, R. N., 2011. Preventing the decodability attack based cross-matching in a fuzzy commitment scheme. *IEEE Transactions on Information Forensics and Security*, 6(1), pp. 107-121.

Kelkboom, E. J., Breebaart, J., Buhan, I. and Veldhuis, R., 2012. Maximum Key Size and Classification Performance of Fuzzy Commitment for Gaussian Modeled Biometric Sources. *IEEE Transactions on Information Forensics and Security*, 7(4), pp.1225-1241.

Kulis, B. & Grauman, K., 2012. Kernelized locality-sensitive hashing. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 34(6), pp. 1092-1104.

Lee, C. H., Choi, C.Y. and Toh, K.A., 2007. Alignment-Free Cancelable Fingerprint Templates Based on Local Minutia Information. *IEEE Transactions on Systems, Man and Cybernetics, Part B*, 37(4), 980-992.

Lee, C. H. and Kim, J., 2010. *Cancelable* fingerprint templates using minutiae-based bit-strings. *Journal of Network and Computer Applications*, 33(3), pp. 236–246.

Li, C. and Hu, J., 2014. Attacks via record multiplicity on cancelable biometrics templates. *Concurrency and Computation: Practice and Experience*, 26(8), pp. 1593-1605.

Lim, M.-H. Teoh, A. B. J. and Toh, K.-A., 2012. An efficient dynamic reliability-dependent bit allocation for biometric discretization. *Pattern Recognition*, 45(5), pp. 1960–1971.

Lim, M. H. and Teoh, A. B. J., 2012. An analytic performance estimation framework for multibit biometric discretization based on equal-probable quantization and linearly separable subcode encoding. *IEEE Transactions on Information Forensics and Security*, 7(4), pp. 1242-1254.

Lim, M. H. and Teoh, A. B. J., 2013. A Novel Encoding Scheme for Effective Biometric Discretization: Linearly Separable Subcode. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 35(2), pp. 300-313.

Lim, M. H., Teoh, A. B. J. and Toh, K. A., 2013. Dynamic Detection-Rate-Based Bit Allocation With Genuine Interval Concealment for Binary Biometric Representation. *IEEE Transactions on Cybernetics*, 43(3), pp. 843-857.

Liu, E. Zhao, H. Liang, J. Pang, L. Chen, H. and Tian, J., 2012. Random local region descriptor (RLRD): A new method for fixed-length feature representation of fingerprint image and its application to template protection. *Future Generation Computer Systems*, 28(1), pp. 236–243.

Liu, K. Kargupta, H. and Ryan, J., 2006. Random projection-based multiplicative data perturbation for privacy preserving distributed data mining, *IEEE Transactions Knowledge and Data Engineering*, 18(1), pp. 92–106.

Maltoni, D., Maio, D., Jain. A. K. and Prabhakar, S., 2009. *Handbook of Fingerprint Recognition*. 2nd ed., New York: Springer-Verlag.

Mauceri, A. J., 1965. Feasibility Study of Personal Identification by Signature Verification. *North American Aviation*, Technical Report SID65-24.

Minutia Cylinder-Code SDK v2.0, *Minutia Cylinder-Code SDK* [Online]. Available at: http://biolab.csr.unibo.it/researchPages/download/MCCSdkv2.0.zip. [Accessed: 30 July 2015]

Moujahdi, C., Bebis, G., Ghouzali, S. and Rziza, M., 2014. Fingerprint shell: Secure representation of fingerprint template. *Pattern Recognition Letters*, 45, pp. 189-196.

Nagar, A., 2012. *Biometric Template Security*. Ph.D. Michigan State University, US.

Nagar, A. and Chaudhury, S., 2006. Biometrics based Asymmetric Cryptosystem Design Using Modified Fuzzy Vault Scheme. *Proceedings of IEEE International Conference Pattern Recognition*, 20 – 24 August 2006 Hong Kong, (4), pp. 537–540.

Nagar, A., Nandakumar, K., and Jain, A.K., 2008. Securing fingerprint template: Fuzzy vault with minutiae descriptors. *Proceedings of International Conference on Pattern Recognition*, 8-11 December 2008 Tampa Florida, pp. 1-4.

Nagar, A., Rane, S. and Vetro, A., 2010a. Alignment and Bit Extraction for Secure Fingerprint Biometrics. *IS&T/SPIE Electronic Imaging*, pp. 75410N-75410N.

Nagar, A., Rane, S. and Vetro, A., 2010b. Privacy and security of features extracted from Minutiae Aggregates. *Proceedings of IEEE International Conference on Acoustics Speech and Signal Processing*, 14-19 March 2010 Dallas, pp. 524–531.

Nagar, A., Nandakumar, K. and Jain, A. K., 2010c. Biometric template transformation: a security analysis. In *IS&T/SPIE Electronic Imaging* (pp. 75410O-75410O). International Society for Optics and Photonics.

Nandakumar, K., Jain, A. K. and Pankanti, S., 2007. Fingerprint-based fuzzy vault: Implementation and performance. *IEEE Transactions on Information Forensics and Security*, 2(4), pp. 744-757.

Nandakumar, K., 2010. A fingerprint cryptosystem based on minutiae phase spectrum. *Proceedings of IEEE International Workshop on Information Forensics and Security*, 12-15 December 2010 Seattle, pp. 1-6.

Nandakumar, K. and Jain, A. K., 2015. Biometric Template Protection Schemes: Bridging the Performance Gap Between Theory and Practice, *IEEE Signal Processing Magazine,* (To Appear).

Parziale, G., & Niel, A., 2004. A fingerprint matching using minutiae triangulation. *Proceedings of Proceedings of International Conference on Biometric Authentication*, vol. 3072, pp. 241-248.

Pękalska E. and Haasdonk, B., 2009. Kernel Discriminant Analysis for Positive Definite and Indefinite Kernels. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 31(6), pp. 1017–1032.

Prabhakar, S., Pankanti, S., & Jain, A. K., 2003. Biometric recognition: Security and privacy and privacy concerns. *IEEE Security and Privacy Magazine*, (2), pp. 33-42.

Pruzansky, S., 1963. Pattern-Matching Procedure for Automatic Talker Recognition. *The Journal of the Acoustical Society of America*, 35(3), pp. 354-358.

Raginksi, M. and Lazebnik, S., 2009. Locality-sensitive binary codes from shift-invariant kernels. *Advances in neural information processing systems*, pp. 1509-1517.

Ratha, N. K., Connell, J. H. and Bolle, R. M., 2001. Enhancing security and privacy in biometrics-based authentication systems. *IBM systems Journal*, 40(3), pp. 614-634.

Ratha, N.K., Chikkerur, S., Connell, J.H. and Bolle, R.M., 2007. Generating Cancelable Fingerprint Templates. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 29(4), pp. 561-572.

Rathgeb, C. and Uhl, A., 2011. Statistical attack against iris-biometric fuzzy commitment schemes. *Proceedings of Computer Vision and Pattern Recognition Workshops (CVPRW)*, 20-25 June 2011 Colorado Springs pp. 23-30.

Rice, J., 2001. Mathematical Statistics and Data Analysis. *Duxbury Press.*

Rivest, R. L., 1998. Chaffing and winnowing: Confidentiality without encryption. *CryptoBytes* (RSA laboratories) [Online]. 4(1), 12-17. Available at: http://people.csail.mit.edu/rivest/pubs/Riv98a.pdf.

ROC. *Scholarpedia, the peer-reviewed open-access encyclopedia* [Online]. Available at: http://www.scholarpedia.org/article/Biometric_authentication [Accessed: 28 June 2015]

Ross, A. K., Shah, J. and Jain, A. K., 2007. From Template to Image: Reconstructing Fingerprints From Minutiae Points. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 29(4), pp. 544–560.

Scheirer, W. J. and Boult, T. E., 2007. Cracking fuzzy vaults and biometric encryption. *Proceedings of Biometrics Symposium*, 11 – 13 September 2007 Baltimore, pp. 1-6.

Schölkopf, B., Smola, A. and Müller, K. R., 1998. Nonlinear Component Analysis as a Kernel Eigenvalue Problem. *Neural Computation*, 10(5), pp. 1299-1319.

Schölkopf, B., Smola, A. and Müller, K. R., 1999. Kernel principal component analysis. *In: Advances in Kernel Methods—Support Vector Learning, (Ed)* B Schölkopf and CJC Burges and AJ Smola, MIT Press, Cambridge, MA, 327-352.

Shawe-Taylor, J. and Cristianini, N., 2004. Kernel methods for pattern analysis. *Cambridge university press.*

Simoens, K., Tuyls, P., and Preneel, B., 2009. Privacy weaknesses in biometric sketches, *Proceedings of the IEEE Symposium on Security and Privacy*, 17 – 20 May 2009 Oakland, California, pp. 188-203.

Simoens, K., Chang, C. M. and Preneel, B., 2010. Reversing Protected Minutiae Vicinities. *Proceedings of the IEEE 4th International Conference on Biometrics: Theory, Applications and Systems*, 27-29 September 2010 Washington DC, pp. 1-8.

Simoens, K., Yang, B., Zhou, X., Beato, F., Busch, C., Newton, E. and Preneel, B., 2012. Criteria Towards Metrics for Benchmarking Template

Protection Algorithms. *Proceedings of the 5th IAPR International Conference on Biometrics,* 29 March – 1 April 2012 New Delhi, India, pp. 498-505.

Shin, S.W., Lee, M. K., Moon, D.S. and Moon, K.Y., 2009. Dictionary Attack on Functional Transform-Based Cancelable Fingerprint Templates. *ETRI Journal*, 31(5), pp. 628-630.

Smith, A. D., 2004. *Maintaining Secrecy when Information Leakage is Unavoidable*. PhD thesis, Massachusetts Institute of Technology, US.

SplashData, 2012. *Worst Passwords of 2012 and How to Fix Them* [Online]. Available at: http://splashdata.com/press/PR121023.htm. [Accessed: 3 August 2015]

Sutcu, Y., Li, Q. and Memon, N., 2007a. Protecting Biometric Templates with Sketch: Theory and Practice. *Proceedings of IEEE Transactions on Information Forensics and Security*, 2(3), pp. 503–512.

Sutcu, Y. Sencar, H. T. and Memon, N., 2007b. A geometric transformation to protect minutiae-based fingerprint templates. *Proceedings of SPIE*, 6539, pp. 65390E–1–8.

Sutcu, Y., Rane, S., Yedidia, J., Draper, S. and Vetro, A., 2008. Feature extraction for a slepian-wolf biometric system using ldpc codes. *Proceedings of International Symposium on Information Theory*, 6-11 July 2008 Toronto, pp. 2297-2301.

Jea, T. Y. and Govindaraju, V., 2005. A minutia-based partial fingerprint recognition system. *Pattern Recognition*, 38(10), pp. 1672–1684.

Tan, S. Y. Jin, Z. Teoh, A. B. J. Goi, B. M., and Heng, S. H., 2012. On the realization of fuzzy identity-based identification scheme using fingerprint biometrics. *Security and Communication Networks*, 5(12), pp. 1312-1324.

Teoh, A. B. J., Ngo, D. C. L. and Goh, A., 2004. Biohashing: Two factor authentication featuring fingerprint data and tokenised random number. *Pattern Recognition*, 37, pp. 2245−2255.

Teoh, A. B. J., Goh, A. and Ngo, D. C. L., 2006. Random Multispace Quantisation as an Analytic Mechanism for BioHashing of Biometric and Random Identity Inputs. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 28(12), pp. 1892-1901.

Teoh, A. B. J. and Ngo, D. C. L., 2006. Biophasor: Token supplemented cancellable biometrics. *Proceedings of the 9th International Conference on Control, Automation, Robotics and Vision*, 5 - 8 December 2006 Singapore, pp. 1-5.

Teoh, A. B. J. and Chong, T. Y., 2007. Cancellable Biometrics Realization with Multispace Random Projections. *IEEE Transaction SMC Part B - Special Issue on Recent Advances in Biometrics Systems*, 37(5), pp. 1096-1106.

The Wall Street Journal, 2014. *The Global Government Biometric Systems Market 2014-2024* [Online]. Available at: http://www.marketwatch.com/story/the-global-government-biometric-systems-market-2014-2024-2014-04-29. [Accessed: 2 August 2015]

Tico M. and Kuosmanen, P., 2003. Fingerprint Matching Using an Orientation-based Minutia Descriptor, *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 25(8), pp. 1009-1014.

Tulyakov, S., Farooq, F. and Govindaraju, V., 2005. Symmetric Hash Functions for Fingerprint Minutiae. *Proceedings of International Workshop on Pattern Recognition for Crime Prevention, Security and Surveillance*, 22 August 2005 Bath UK, 3687, pp. 30-38.

Uludag, U., Pankanti, S. and Jain A., 2005. Fuzzy Vault for Fingerprints. *Proceedings of the 5th International Conference on Audio- and Video-based Biometric Person Authentication*, 20-22 July 2005 New York, pp. 310−319.

Uludag, U. and Jain, A., 2006. Securing fingerprint template: Fuzzy vault with helper data. *Proceedings of the 2006 Conference on Computer Vision and Pattern Recognition Workshop*, 17-22 June 2006, New York, pp. 163.

VeriFinger SDK, *Neurotechnology* [Online]. Available at: http://www.neurotechnology.com/ [Accessed: 1 June 2014].

Vielhauer, C., Steinmetz, R. and Mayerhöfer, A., 2002. Biometric hash based on statistical features of online signatures. *Proceedings of 16th International Conference on Pattern Recognition*, 11-15 August 2002 Quebec, 1, pp. 123-126.

Wahab, A. Chin, S.H. and Tan, E.C., 1998. Novel approach to automated fingerprint recognition, *IEE Proceedings Visual Image Signal Processing*, 145(3), pp. 160–166.

Wang, S., and Hu, J., 2012. Alignment-free cancelable fingerprint template design: A densely infinite-to-one mapping (DITOM) approach. *Pattern Recognition*, 45(12), pp. 4129-4137.

Wang, S. and Hu, J., 2013. A Hadamard Transform-Based Method for the Design of Cancellable Fingerprint Templates. *Proceedings of 6th International Congress on Image and Signal Processing*. 16-18 December 2013 Hangzhou, 3, pp. 1682-1687.

Wang, S. and Hu, J., 2014. Design of alignment-free cancelable fingerprint templates via curtailed circular convolution. *Pattern Recognition*, 47(3), pp. 1321-1329.

Wang, Y., Rane, S., Draper, S. C. and Ishwar, P., 2012. A theoretical analysis of authentication, privacy, and reusability across secure biometric systems. *IEEE Transactions on Information Forensics and Security*, 7(6), pp. 1825-1840.

Weinreb, H. J., 1985. Fingerprint patterns in Alzheimer's disease. *Archives of neurology*, 42(1), pp. 50-54.

Weiss, Y., Torralba, A. and Fergus, R., 2009. Spectral hashing, *Advances in neural information processing systems*, pp. 1753-1760.

Williams, T. J., Pepitone, M. E., Christensen, S. E., Cooke, B. M., Huberman, A. D., Breedlove, N. J., ... & Breedlove, S. M., 2000. Finger-length ratios and sexual orientation. *Nature*, 404(6777), pp. 455-456.

Wong, W. J., Teoh, A. B. J., Wong, D. M. L. and Kho, Y. H., 2013. Enhanced multi-line code for minutiae-based fingerprint template protection, *Pattern Recognition Letters*, 34(11), pp. 1221-1229.

Wu, G. Chang, E. Y. and Zhang, Z., 2005. An analysis of transformation on non-positive semidefinite similarity matrix for kernel machines. *Proceedings of the 22nd International Conference on Machine Learning*. 11-17 August 2005 Bonn, vol 8.

Xu, H., Veldhuis, R. N., Kevenaar, T. A., Akkermans, A. H. and Bazen, A. M., 2008. Spectral minutiae: A fixed-length representation of a minutiae set. *IEEE Conference on Computer Vision and Pattern Recognition Workshops*, 23-28 June 2008 Anchorage, Alaska, pp. 1-6.

Xu, H., Veldhuis, R. N., Bazen, A. M., Kevenaar, T. A., Akkermans, T. A. and Gokberk, B., 2009. Fingerprint verification using spectral minutiae

representations. *IEEE Transactions on Information Forensics and Security*, 4(3), pp. 397-409.

Xu, H., 2012. *Spectral minutiae representation for fingerprint recognition*. PhD thesis, Universiteit Twente, Netherlands.

Yang, B., and Busch, C., 2009. Parameterized geometric alignment for minutiae-based fingerprint template protection. *Proceedings of IEEE 3rd International Conference on Biometrics: Theory, Applications, and Systems*, 28-30 September 2009 Washington DC, pp. 1-6.

Yang, B., Busch, C., Gafurov, D. and Bours, P., 2010a. Renewable minutiae templates with tunable size and security. *Proceedings of 20th International Conference on Pattern Recognition*, 23-26 August 2010, Istanbul, pp. 878-881.

Yang, B., Hartung, D., Simoens, K., & Busch, C., 2010b. Dynamic random projection for biometric template protection. *Proceedings of 2010 Fourth IEEE International Conference on Biometrics: Theory Applications and Systems*, 27-29 September 2010 Washington DC, pp. 1-7.

Yang, B. and Busch, C., 2012. Generalized fingerprint minutiae vicinities. *Proceedings of 5th IAPR International Conference on Biometrics*. 29 March – 1 April 2012 New Delhi, India, pp. 202-207.

Yang, S. and Verbauwhede, I., 2005. Automatic secure fingerprint verification system based on fuzzy vault scheme. *Proceedings of IEEE International Conference on Acoustics, Speech, and Signal Processing, (ICASSP'05).* 18-23 March 2005 Pennsylvania, 5, pp. v-609.

Yang, W., Hu, J., Wang, S. and Yang, J., 2013. Cancelable fingerprint templates with delaunay triangle-based local structures. *Proceedings of*

Cyberspace Safety and Security. 13-15 November 2013 Zhangjiajie, China, pp. 81-91.

Yang, W., Hu, J. and Wang, S., 2014a. A delaunay quadrangle-based fingerprint authentication system with template protection using topology code for local registration and security enhancement. *IEEE Transactions on Information Forensics and Security*, 9(7), pp. 1179-1192.

Yang, W., Hu, J., Wang, S. and Stojmenovic, M., 2014b. An alignment-free fingerprint bio-cryptosystem based on modified Voronoi neighbor structures. *Pattern Recognition*, 47(3), pp. 1309-1320.

Zhang, N., Yang, X., Zang, Y., Jia, X. and Tian, J., 2013. Generating registration-free cancelable fingerprint templates based on Minutia Cylinder-Code representation. *Proceedings of IEEE Sixth International Conference on Biometrics: Theory, Applications and Systems*, 29 September – 2 October 2013 Washington DC, pp. 1-6.

Zhou, X. Kuijper, A. Veldhuis, R. N. J. and Busch, C., 2011. Quantifying privacy and security of biometric fuzzy commitment. *Proceedings of IEEE International Joint Conference on Biometrics*, 11-13 October 2011 Washington DC, pp. 1-6.

Zhou, X., 2012. *Privacy and security assessment of biometric template protection*. Ph.D. thesis, Technical University Darmstadt, German.

ACHIEVEMENTS

Publications:

A. Conference Papers

[1] Jin, Z., Teoh, A. B. J., Goi, B.M. and Tay, Y.H., 2013. A Non-invertible Graph-based Hamming Embedding Transform for Fingerprint Minutiae Protection. *The 6th International Congress on Image and Signal Processing (CISP 2013)*, pp. 1688 – 1693.

[2] Jin Z., Goi, B.M., Teoh, A. B. J. and Tay, Y.H., 2014. Non-invertible Analysis on Graph-based Hamming Embedding Transform for Protecting Fingerprint Minutiae. *The 13th International Conference on Electronics, Information, and Communication (ICEIC 2014)*, pp. 1-2.

[3] Jin Z., Goi, B.M., Teoh, A. B. J. and Tay, Y.H., 2015. Analysis of Small Angle Approximation Attack on Biometric Templates. *IEEE International Conference on Consumer Electronics-Taiwan (IEEE 2015 ICCE-TW)*.

B. Journal Articles

[1] Jin, Z., Goi, B.M., Teoh, A. B. J. and Tay, Y.H., 2013. A Two-dimensional Random Projected Minutiae Vicinity Decomposition-based Cancellable Fingerprint Template. *Security and Communication Networks*, 5(12), pp. 1312-1324.

[2] Jin, Z., Lim, M.H., Teoh, A. B. J. and Goi, B.M., 2014. A non-invertible Randomized Graph-based Hamming Embedding for generating cancelable fingerprint template. *Pattern Recognition Letters*, 42, pp. 137-147.

[3] Jin, Z., Lim, M.H., Teoh, A. B. J., Goi, B.M., and Tay, Y.H., 2015. Generating Fixed-length Representation from Minutiae Using Kernel Methods for Fingerprint Authentication. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, submitted.

[4] Jin, Z., Teoh, A. B. J., Goi, B.M. and Tay, Y.H., 2015. Biometric Cryptosystems: A New Biometric Key Binding and Its Implementation for Fingerprint Minutiae-based Representation. *Pattern Recognition*, submitted.

Research Project:

[1] Biometric Encryption: Generating Fixed-length Cancellable Fingerprint Representations for Preserving Human Privacy and Securing Biometric based Systems, e-Science Fund, 2015 – 2017.

[2] Biometric Encryption Scheme for Preserving Human Privacy and Securing Biometric-based Systems, UTAR research Fund, 2014 – 2014.