DESIGN AND VALIDATION OF AN ALIGNMENT FREE CANCELABLE FINGERPRINT TEMPLATE PROTECTION SCHEME

By

BADIUL ALAM

A dissertation submitted to the Department of Electrical and Electronics Engineering,

Lee Kong Chian Faculty of Engineering and Science,

Universiti Tunku Abdul Rahman,

in partial fulfilment of the requirements for the degree of

Master of Engineering Science

July 2018

ABSTRACT

DESIGN AND VALIDATION OF AN ALIGNMENT FREE CANCELABLE FINGERPRINT TEMPLATE PROTECTION SCHEME

BADIUL ALAM

Biometric based authentication systems have been widely deployed on mobile devices and security applications for Internet of Things. Security and privacy issues arise especially when the biometric templates stored in centralised database or personal portable devices are obtained by adversaries for malicious use. To make matters worse, unlike password, biometric traits are irreplaceable once compromised. Despite the fact that a number of methods have been reported to protect biometric template, there are rare solutions that satisfy the criteria of template protection simultaneously (i.e., non-linkability, cancelability, non-invertibility and performance). In this dissertation, we propose an alignment free (i.e., pre-registration of fingerprint image is not required before authentication) cancelable template scheme to protect fingerprint minutiae. The proposed template scheme is the extended version of the polar grid based 3-tuple quantisation with condensed feature length for lower computation cost. To enhance the non-invertible property, bit-toggling strategy is proposed to inject noise into the proposed fingerprint template. Furthermore, cancelability is also achieved by incorporating discrete Fourier transform and random projection on the proposed template. Due to the use of discrete Fourier transform, the resultant template will be converted into complex form which increases the difficulty of attacker in breaking its security. The proposed template scheme is evaluated on FVC2002 and FVC2004 databases (DB1, DB2 and DB3) and the experimental results demonstrate a comparable accuracy over the existing methods. The observation from the security and privacy analysis suggests that the proposed template is robust against the major attacks, e.g., template inversion attack, attack via record multiplicity, etc. Lastly, we demonstrate the application that the proposed template can be applied in the bio-cryptosystems.

ACKNOWLEDGEMENT

By the name of Allah, the merciful, I am acknowledging that, his guidance and blessing gave me the strength to finish my work successfully. Here I am also acknowledging that, this dissertation could not be possible finish successfully without the help of many people. First and foremost, it is my pleasure to give heartiest thanks to my supervisor, Dr. Wun-She Yap and my co-supervisor Ir. Prof. Dr. Goi Bok Min for their continuous support and guidance about project. Besides they have been very helpful throughout my research project and dissertation. I would not forget to give thanks to Dr. Jin Zhe for his valuable guidance and help as an un-official co-supervisor.

I would love to convey my appreciation to all of my fellow friends, who continuously assisted me by giving moral support and strength throughout the research of my master's study.

Finally, I would like to confess that I am forever indebted to my beloved parents. They are very supportive and helpful especially when I fall down at lowest point of life. They provide all kind of support from my childhood to present. Finally, I wish to applaud all the people for motivating me and encouraging me with their best wishes.

LEE KONG CHIAN FACULTY OF ENGINEERING AND SCIENCE

UNIVERSITI TUNKU ABDUL RAHMAN

Date: ___________________

SUBMISSION OF DISSERTATION

It is hereby certified that BADIUL ALAM (ID No: **15UEM08212**) has completed this dissertation entitled "**DESIGN AND VALIDATION OF AN ALIGNMENT FREE CANCELABLE FINGERPRINT TEMPLATE PROTECTION SCHEME**" under the supervision of Dr. Yap Wun She (Supervisor) and Ir. Prof. Dr. Goi Bok Min (Co-supervisor) from the Department of Electrical and Electronic Engineering, Lee Kong Chian Faculty of Engineering and Science.

I understand that University will upload softcopy of dissertation in pdf format into UTAR Institutional Repository, which may be made accessible to UTAR community and public.

Yours truly,

____

(Badiul Alam)

APPROVAL SHEET

This dissertation entitled **“DESIGN AND VALIDATION OF AN ALIGNMENT FREE CANCELABLE FINGERPRINT TEMPLATE PROTECTION SCHEME”** was prepared by BADIUL ALAM and submitted as partial fulfilment of the requirements for the degree of Master of Engineering Science at Universiti Tunku Abdul Rahman.

Approved by:

____
(Dr. Yap Wun She)
Date:……………..
Supervisor
Department of Electrical and Electronic Engineering
Lee Kong Chian Faculty of Engineering and Science
Universiti Tunku Abdul Rahman

____
(Ir. Prof. Dr. Goi Bok Min)
Date:…………………..
Co-supervisor
Department of Mechatronics and Biomedical Engineering
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 Badiul Alam

Date ______________________________

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

1.1 Background

Biometric authentication refers to an automated process to verify and/or identify individual using either physiological characteristics ((e.g., fingerprint (Lee and Kim, 2010; Li et al., 2010), palmprint (Leng and Zhang, 2011), iris (Bolle et al., 2002; Mehrotra et al., 2010) and face (Gunes and Piccardi, 2007)) or behaviour characteristics (e.g., voice (North et al., 2017), DNA (Kaur and Attri, 2017), handwritten signature (Shahzad et al., 2017) and keystroke (Liu et al., 2015)). Biometric verification has been widely applied on telecare medicine information systems (Masdari and Ahmadzadeh, 2017), key management in wireless body area network (Masdari et al., 2017), wireless sensor networks in internet of things environments (Li et al., 2018) and mobile devices (Liu et al., 2015).

Biometric authentication inherits a number of advantages over conventional authentication system. Firstly, biometrics can never be lost or forgotten as compared to the traditional used smart card and password. Secondly, biometrics is attached to the user. Thirdly, biometrics is not as easy to be shared or forged as compared to password.

Among all biometric authentication systems, fingerprint based authentication system has been widely deployed in numerous access control applications due to its well public acceptability and admissibly uniqueness (Campisi, 2013). The popularity of fingerprint based authentication can be observed from the integration of fingerprint scanner into mobile devices, such as mobile computer, tablet and smart phone.

1.2 Fingerprint Recognition System

Generally, fingerprint based authentication is performed by matching the features extracted from the fingerprint of a user in real-time with the pre-enroled fingerprint template stored in a database. The features extracted from fingerprints can be classified into two categories: global level and local level (Maltoni et al., 2009). Global level features shape a special pattern of ridges and valleys, called singular point. The singular point includes core and delta point while the ridge line shape of the singular points are useful to do fingerprint classification and indexing. However, global level features are not sufficient for accurate fingerprint matching due to the lower distinctiveness (Maltoni et al., 2009). Local level features consider a group of ridge endings and bifurcations called minutia for matching purposes. Minutiae points are more reliable and robust than global level features in fingerprint matching system (Maltoni et al., 2009). Figure 1.1 depicts that the two most prominent ridge characteristics extracted from a fingerprint (Maltoni et al., 2009) where black and blue arrows indicate the ridge termination minutiae and ridge bifurcation minutiae respectively.

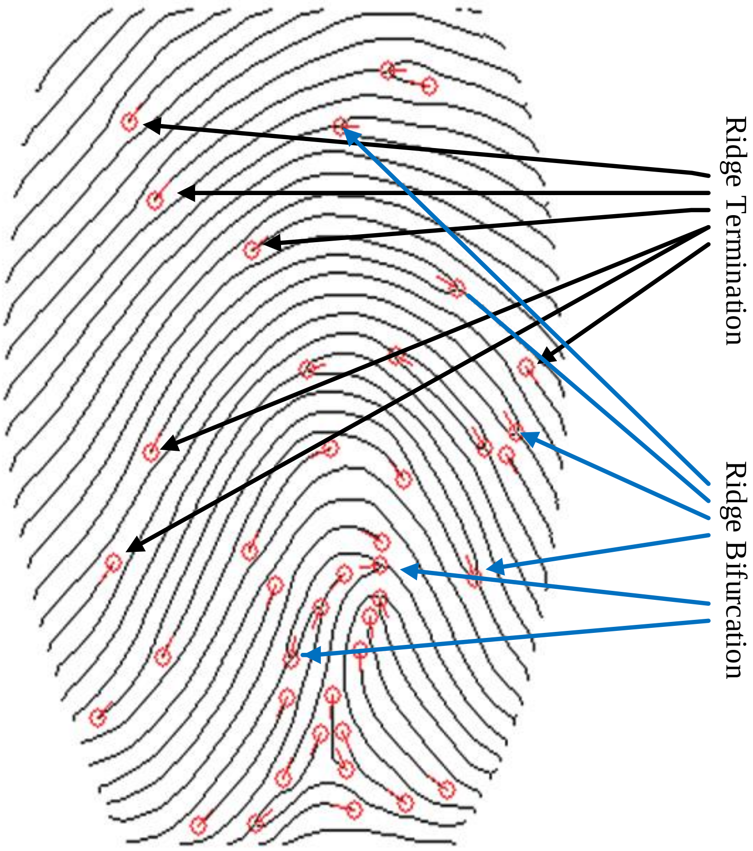

Figure 1.1: Two most prominent ridge characteristics extracted from a fingerprint (Tao et al., 2012)

Fingerprint recognition system can be divided into two types, i.e., fingerprint verification and fingerprint identification. A fingerprint verification system verifies a user by comparing a captured fingerprint template with his/her previously enroled template in the database. Fingerprint verification introduces one-to-one comparison to verify the user identity (Ahmed et al., 2018). On the other hand, fingerprint identification system identifies a user by comparing his /her fingerprint template with the fingerprint templates of all users stored in a database. Hence, fingerprint identification introduces one-to-many comparison to identify a user from many users that have the access to the database.

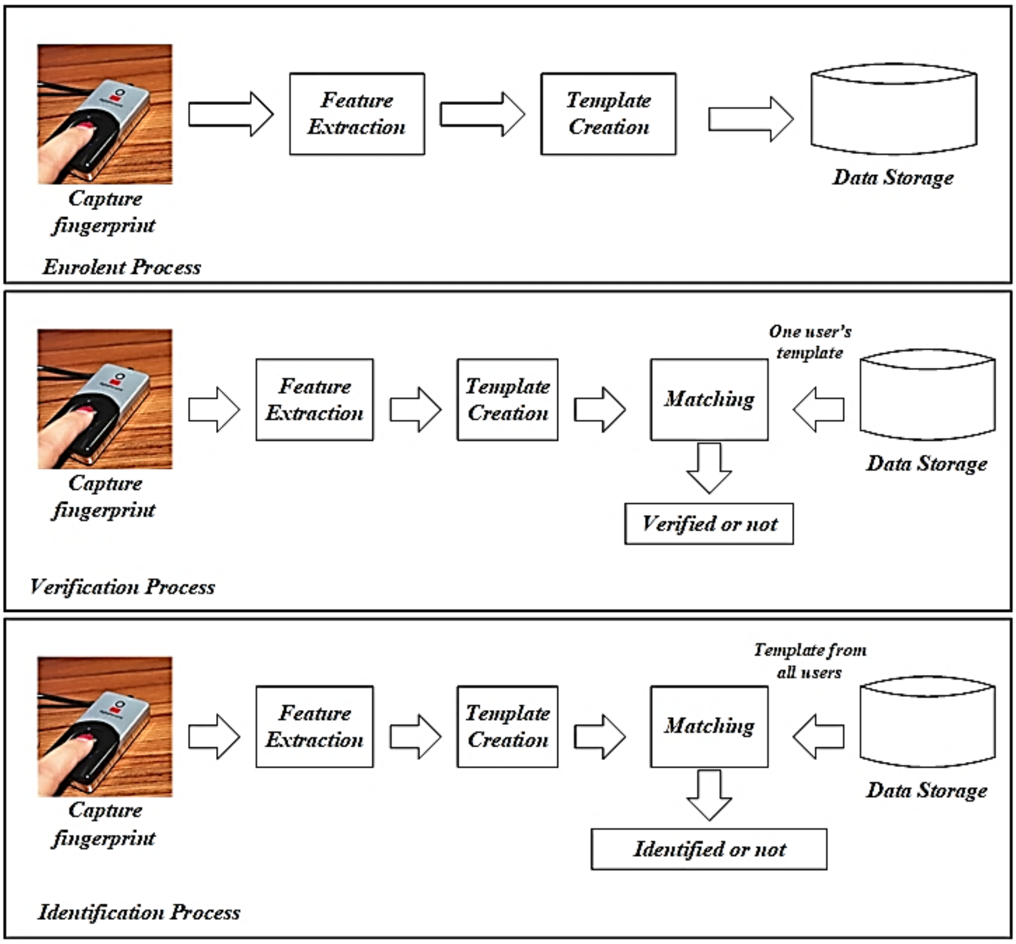

Figure 1.2: Overview of fingerprint enrolment, verification and identification

Figure 1.2 shows a fingerprint recognition system. The fingerprint recognition system consists of the following modules:

- Fingerprint Scanner: To obtain digital representation of fingerprint feature, a fingerprint scanner is used to capture the user fingerprint as an image.
- Feature Extraction: Feature extraction is performed to extract the fingerprint features from the fingerprint image.

- Template Generation: The extracted features are then processed to generate a fingerprint template for matching process.
- Data Storage: The generated fingerprint template will be stored in a database for matching purposes. This database shall be protected to prevent outsider attacks.

A fingerprint verification system consists of enrolment and verification processes while a fingerprint identification system consists of enrolment and identification processes. These three possesses are further explained as follows:

- Enrolment: Enrolment process is to register one or multiple user fingerprint templates in the system storage. During the enrolment process, a fingerprint scanner is used to capture the user fingerprint image. Subsequently, useful features are extracted from the fingerprint image to generate a fingerprint template. In the fingerprint verification system, only one user fingerprint template will be stored in the database while multiple user fingerprint template will be stored in the database for the fingerprint identification system.
- Verification: Verification process is to authenticate a user. The user is requested to scan his/her fingerprint on the spot. A template will then be generated by feeding the scanned fingerprint image to the feature extraction and template generation. This template will then be compared with the template stored in the database. If both templates are matched, the user is considered legitimate user.

- Identification: In identification system, same process like verification has to be done. However, instead to have one template to single user template comparison, comparisons of one template to multiple user templates need to be conducted.

1.3 Problem Statement

Ensuring strong security of a system or application is very crucial and is a difficult problem in the modern digitalised world (Mathew et al., 2010). Any application or system such as biometric authentication system can be hacked by any adversary. Biometric authentication system can be hacked in many ways such as attacks at user interface device, attacks may happen at the interface between modules, software modules attacks, attacks on the template storage system etc. (Jain et al., 2008). Among all of the attacks, attacks on the template database is the weakest link of a biometric authentication system. Attacks on the database that stores biometric templates (e.g., fingerprint template) may direct to the following insecurities: (a) Genuine templates are substituted by imposter templates to obtain illegal access to the system (Ross et al., 2007). (b) Fake template can be generated from the stolen original template where the attacker can access multiple applications with this fake template if the user uses same fingerprint in multiple applications (Adler, 2004; Cappelli et al., 2007). (c) Stolen fingerprint template can be reused to get unauthorised entrance to the secure system (Jain et al., 1999). Therefore, it is important to propose a fingerprint template technique that is secure from common attacks. Generally, common attacks can be categorized into hill climbing (Jin et al., 2004) and template inversion (Jain et al., 2008). Hill climbing is an attack technique where the adversary guesses the minutiae points and subsequently tweaks their guessed minutiae points on the basis of the matching score procured by comparing the guessed minutiae points with the pre-enroled fingerprint template. Besides, template inversion is the technique practiced by the adversary to get back the original biometric image from the corresponding features reversed from the robbed template. To address the problem discussed above, a fingerprint template protection scheme maintaining the trade-off between security and performance and fulfilling the following criteria needs to be developed:

(a) Non-linkability: It should be computationally hard to distinguish whether different biometric templates are generated from the same biometrics. This property does not allow cross-matching across different applications.

(b) Revocability: If the template is compromised, the compromised template can be revoked and new template can be re-generated based on the same biometric feature.

(c) Non-invertibility: It is computationally difficult to retrieve the original biometric from the compromised templates. This criterion prevents the attacker to reconstruct the original template from the stolen template.

(d) Performance: The transformed biometric template should not deteriorate the recognition performance. The template protection technique should preserve the performance after intentionally distorting the template.

A possible way to achieve the aforementioned aims is to enhance the fingerprint template protection scheme proposed by Jin et al. (2012). Jin et al. (2012) proposed polar grid based 3-tuple quantisation (PGTQ) method to generate fingerprint template. Jin et al. (2012) suggested to use whole fingerprint to generate a bit string leading to a lengthy bit-string generation which is ineffective to database storage system. Even though their proposed method achieved acceptable performance but security evaluation of their proposed scheme is not emphasised in their work.

1.4 Objectives

This dissertation contributes on the design of a secure fingerprint template protection scheme that protects the user privacy even though the attacker manages to obtain the fingerprint templates stored in the database. Meanwhile, the recognition performance should be well preserved after adding security protection on the resultant fingerprint templates. Thus, the objectives of this dissertation as follows:

- To design a secure and efficient alignment free cancellable fingerprint template protection scheme based on minutiae

1.5 Contributions

A minutia is generally represented by using *x*-coordinate, *y*-coordinate and orientation θ, where *x*- and *y*-coordinates pertaining to the location of minutia in the fingerprint and the orientation θ, pertaining to the ridge line angle to which the minutia is attached. Jin et al. (2012) proposed polar grid based 3-tuple quantisation (PGTQ) technique to generate a revocable minutiae-based template. PGTQ is an alignment free minutiae descriptor that utilises variable-sized decorated quantisation in polar coordinate. More precisely, regions near the reference minutia have shorter space and vice versa. This directs to a shorter (larger respectively) quantisation step around (farther apart from respectively) the reference minutia to endure fingerprint resilient deformity. In the original PGTQ descriptor, polar coordinate approach uses the entire fingerprint image and thus generates a lengthy bit string template, which is unattractive for practical applications as large storage of templates is needed. In this dissertation, we propose an alignment free cancelable fingerprint template protection scheme by enhancing the scheme proposed by Jin et al. (2012) as follows:

- Instead of covering the entire fingerprint image, we modify the PGTQ descriptor in a way that polar coordinates cover partial fingerprint image only to generate a condensed but computational- and storage- effective descriptor of bit string, namely dubbed condensed polar grid based 3-tuple quantisation (C-PGTQ).

- We also apply random bit flipping approach (Farooq et al., 2007) on C-PGTQ to strengthen the non-invertibility and produce a protected descriptor, called P-PGTQ.
- To provide revocability, discrete Fourier transform (DFT) and random projection (RP) are further employed to generate cancelable templates, named 2C-PGTQ.

Finally, an application using the proposed fingerprint template (i.e., 2C-PGTQ) for key binding bio-cryptosystem is demonstrated. The feasibility of the proposed template protection method is justified through the experiments conducted over six public domain fingerprint datasets, i.e., FVC2002DB1, FVC2002DB2, FVC2002DB3, FVC2004DB1, FVC2004DB2 and FVC2004DB3.

1.6 Organisation of the Dissertation

The organisation of the remaining part of this dissertation is as follows. Literature review about existing fingerprint template protection techniques is presented in Chapter 2. Chapter 3 presents our proposed alignment free cancelable fingerprint template protection scheme based on minutiae. Extensive experiments and its analysis on different recognised fingerprint datasets are presented in Chapter 4. Finally, some concluding remarks and future work are given in Chapter 5.

CHAPTER 2

LITERATURE REVIEW

Fingerprints are the most unique part of the human being to claim his/her identity in an authentication system (Jain et al., 1999). Humans have different types of fingerprint characteristics and these fingerprint characteristics stay permanently for whole life. Fingerprint consists of many types of ridges and furrows. Different types of ridge characteristics are shown in Figure 2.1 (Lee et al., 2001).

.

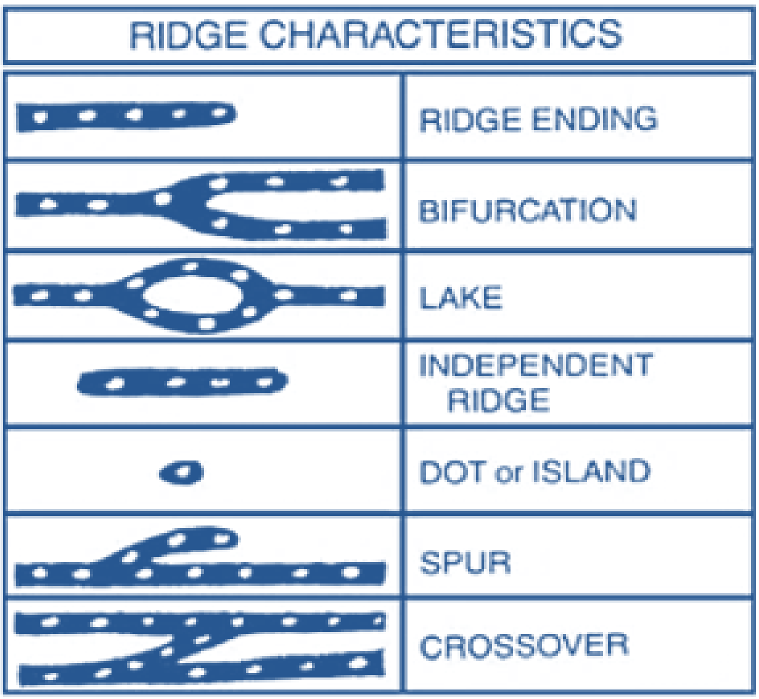

Figure 2.1: Different types of fingerprint ridge characteristics

Fingerprints cannot be distinguished by ridges and furrows. However, it can be distinguished by points on the local ridge characteristic. The local ridge characteristic also known as minutiae. Minutiae can be divided into two types, i.e., ridges ending minutia and ridge bifurcation minutiae.

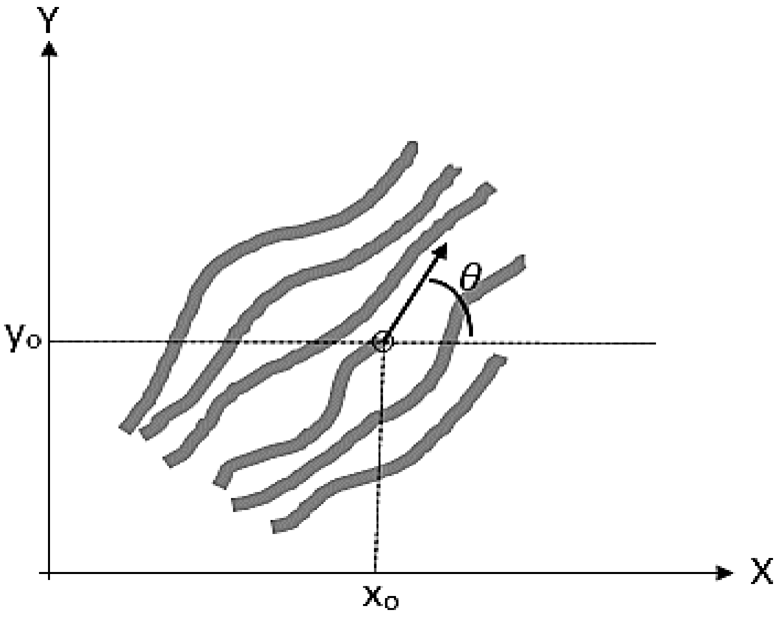

Figure 2.2: Ridge ending minutiae

Figure 2.2 and Figure 2.3 depict the ridge ending minutiae and ridge bifurcation minutiae respectively. These two types of minutiae play important role in distinguishing and identifying the user identity of fingerprint based authentication system.

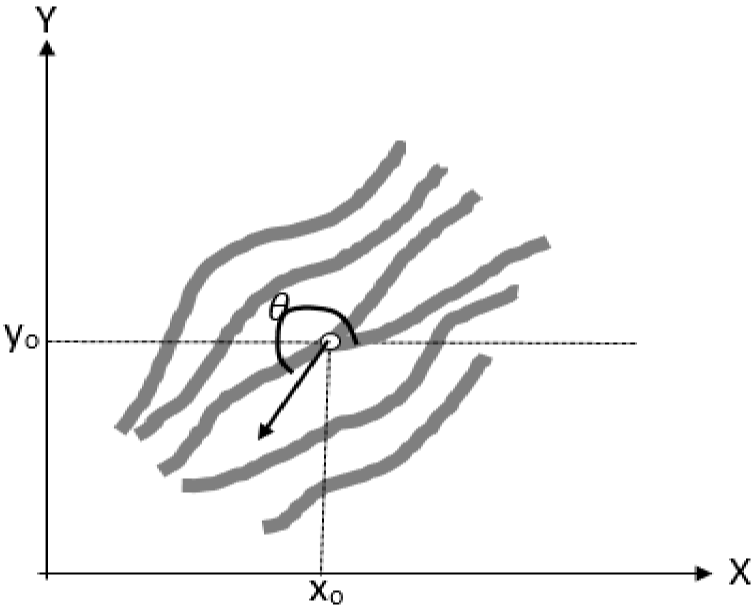

Figure 2.3: Ridge bifurcation minutiae

The ridge ending minutiae end abruptly and the ridge bifurcation minutiae divide into two branches (Espinosa-Duro, 2002). For both Figures 2.2 and 2.3' *Xo* and *Yo* show the location of a minutia point and θ denotes the orientation angle of a minutia point. A fingerprint image with good quality should have 40 to100 minutiae (Jain et al., 1997).

There is another characteristic of fingerprint image called global ridge characteristic. Some classes of global ridge characteristics are arch, tented arch, left-loop, right-loop and whorl. Global ridge characteristic is also known as singular point. Singular point has two types of characteristic: core and delta points (Maltoni et al., 2009). Orientation of fingerprint image tends to converge in the core point while it tends to diverge in the delta point. The fingerprint classification will greatly depend on the number of core and delta points exist in the fingerprint image. For example, an arch does not have any singular point in the image. On the other hand, tented arch, left-loop and right-loop have one core and one delta points in the fingerprint image while whorl has two core points and two delta points. Figure 2.4 presents all types of singular points of the fingerprint image. Symbol ‘O’ and symbol ‘∆’ represent the core and delta points of a fingerprint image respectively (Chua et al., 2014).

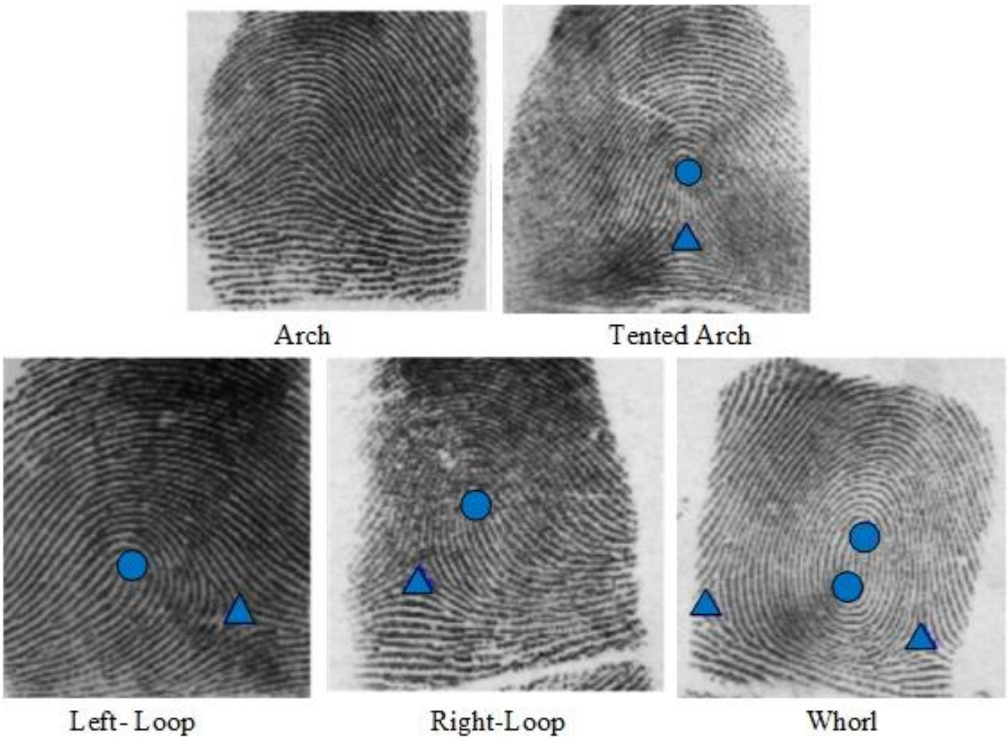

Figure 2.4: Global ridge characteristic of a fingerprint image

2.1 Description of Fingerprint Datasets

Fingerprint evidence plays a crucial role in crime scene forensics. As the fingerprint of a user will not change for whole life, fingerprint can be used to confirm or disproves the person quickly and effectively. To achieve high fingerprint recognition performance, reliable and recognised public domain fingerprint datasets are needed for testing purposes. National Institute of Standard and technology (NIST) took the first step to provide the first large public domain fingerprint database for both academia and industry.

NIST fingerprint database provides a suitable benchmark for automated fingerprint identification system development (Shen, 1994) and fingerprint classification. NIST DB4 (Watson and Wilson, 1992a), NIST DB9 (Watson and Wilson, 1992b), NIST DB10 (Watson, 1993a) and NIST DB14 (Watson, 1993b) consist of thousands of fingerprint images collected from rolled inked fingerprint impressions by scanning but the scanned quality is not good as of live-scan images. Meanwhile, NIST DB24 contains 100 live sequences for 10 users in video form. However, static frame extracted from the video is not suitable for testing purpose (Watson, 1998). NIST DB27 is a special fingerprint database which provides more developed fingerprint database compared to previously published NIST fingerprint databases. NIST DB27 was developed by collecting grayscale fingerprint impressions and respective minutiae data in conjunction with the Federal Bureau of Investigation (Garris and McCabe, 2000).

Later on, Fingerprint Verification Competition (FVC) was organised in 2000, 2002, 2004 and 2006 respectively to focus on fingerprint verification software technology. Different fingerprint datasets were provided to benchmark the state-of-the-art in fingerprint technology. Table 2.1 describes the brief summary of the FVC datasets.

Table 2.1: Brief summary of the FVC datasets

Competition	**Number of datasets**	**Size of each dataset**	**Remarks**
FVC 2000 (Maio et al., 2002a)	4	A: 100×8 B: 10×8	i) Half of the volunteers are male ii) The images were taken in two different sessions iii) Quality was not checked properly iv) Acceptable performance for DB1, DB2 and DB4 compared to DB3
FVC 2002 (Maio et al., 2002b)	4	A: 100×8 B: 10×8	i) Volunteers are 20 years old averagely and unhabituated students. ii) The images were taken in three different sessions iii) Quality was not checked properly iv) Four impressions were taken for each finger in each session v) Acceptable performance for DB1, DB2, DB3 and DB4
FVC 2004 (Cappelli et al., 2006; Maio et al., 2004)	4	A: 100×8 B: 10×8	i) Volunteers are 24 years old averagely and unhabituated students ii) The images were taken in three different sessions iii) Quality was not checked properly iv) Four impressions were taken for each finger in each session v) Slightly low performance for DB1, DB2, DB3 and DB4
FVC 2006 (Cappelli et al., 2007)	4	A:140×12 B: 10×12	i) Four datasets were generated adopting three different scanners ii) The final dataset was selected according to NIST quality index iii) Much acceptable performance for DB2 and DB4 compared to DB1 and DB3

(P.S: A denotes evaluation set and B denotes training sets of each dataset.)

The generation of cancelable template can be broadly divided into two categories: registration based and registration-free based (Wang and Hu, 2012). For registration based method, singular points are needed to pre-align the fingerprint image before generating fingerprint template (Jin et al., 2011). Impropriate registration of fingerprint image may cause the generation of fraud minutiae (Zhang et al., 2011) especially that precise registration is a non-trivial task. Besides, dirt, moisture, creases and other false noises may lead to miss-detection of singular point (Wang et al., 2007). In contrast to registration based method, no singular points are needed for registration-free method. Instead of using singular points, the relative-, rotation- and shift-invariant relationship between minutiae points are utilised to generate a fingerprint template (Wang and Hu, 2016).

2.2 Biometrics Template Protection Techniques

Biometric templates are stored inside a database for verification purpose. As the user privacy will be lost forever once the attacker manages to attack the database, obtain the biometric template and recover the user biometrics, the biometric templates should be protected such that the attacker cannot recover the user biometric even though he can obtain the biometric template stored in the database. More precisely, biometric template protection technique must satisfy non-invertibility, non-linkability, revocability and performance as mentioned in Section 1.3. Biometric template protection techniques can be divided into two approaches: Feature Transformation and

Biometric Cryptosystems. Figure 2.5 picturises the whole biometric template techniques:

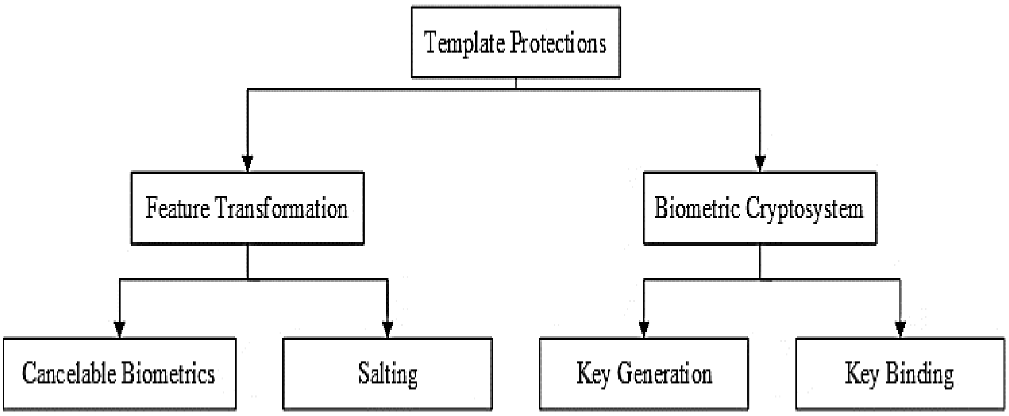

Figure 2.5: Biometric template protection techniques

2.2.1 Feature Transformation

In the feature transformation template protection technique, a one-way transformation function needs to be applied to the biometric templates. This one-way function takes secret key or password and biometric template as inputs. More precisely, the one-way function transforms the biometric template to the enrolment template stored in the database based on the secret key or password. During the verification process, the template is transformed using the same one-way function and same secret key. Therefore, matching algorithm can be performed between these two templates because they appear in the same transformed space. Depending on the characteristic of one-way function, the transformation approaches can be divided into two types: cancelable biometrics and salting approach (Jain et al., 2008).

2.2.1.1 Cancelable Biometrics

Cancelable biometrics is also known as non-invertible biometrics (Bolle et al., 2002). In normal authentication system, password can be renewed countless time, while in biometric authentication system, if the biometric data once compromised, it will be lost for entire life of a user (Kaur and Khanna, 2016). Soutar et al. (1998) took the initiatives to mitigate this serious problem by introducing revocable and renewable biometric templates. This notation was then explored and introduced by Ratha et al. (2001) as cancelable biometrics. If the biometric templates are compromised from database storage, cancelable biometrics helps to revoke and renew the compromised templates like password. Renewed and revoked templates should be unique to every application even though all the renewed templates are generated based on same biometric feature. Cancelable biometric can be described as “a way of systematically, intentional and repeated distortion on the original biometric data in order to protect the user specific important, valuable and sensitive information by storing distorted template and not matching them in the original format” (Kaur and Khanna, 2016). Formally, renewability means the process of generating distinct and multiple templates from same biometric feature which can be used to authenticate the user and it will not disclose any information of the original biometric template.

2.2.1.2 Salting Approach

Salting is also known as biohashing which is one of the biometric template protection techniques (Jin et al., 2004; Teoh et al., 2006). Salting is a two-factor approach. In this approach, biometric templates are transformed by using a user specific external key or password. Salting biometric template protection technique is invertible. Since the salting biometric template transformation is invertible, the user defined key or password used during the process of transformation need to be stored securely and the specific key or password need to be presented during the verification/identification. If somehow the user defined key or password is compromised, the information of biometric templates associated with that key or password is no longer secure. Thus, the attacker can invert the transformed template to the original one (Maltoni et al., 2009). To increase the strength of the biometric template security using salting approach, the user specific key should not be stored in the database with the transformed template, it should be recalled by the individual and need to be appeared during the validation.

2.2.2 Biometric Cryptosystems

Biometric cryptosystem is another biometric template protection technique. A cryptographic key is either secured or generated using biometric feature. Some public data about the biometric template is stored in the database as helper data. This helper data does not reveal any information about the original biometric template, but it helps to extract the cryptographic key from the query biometric during verification process. Key binding and key generation are two types of biometric cryptosystem which are divided by depending on how the helper data or public data is obtained.

2.2.2.1 Key Binding

If the helper data is derived from biometric template by binding a key with respective template, it is called as key binding biometric cryptosystem template protection technique. In the key binding biometric cryptosystem, a key namely cryptographic key and biometric feature template are merged together in between a cryptographic framework. Helper data are publicly available, but this helper data or public data does not provide any significant information about original biometric template or key (Jain et al., 2008). Without knowing the key or biometric template, helper data could not help the adversary to get beck the original biometric template from the stolen transformed template. More details about key binding cryptosystem are presented by Davida et al. (1999), Johnson et al. (1998) and Soutar and Tomko (1996).

2.2.2.2 Key Generation

If the helper data or public data is extracted from biometric feature template and the cryptographic key is directly generated from the helper data or public data and query biometric templates, it is called key generation biometric cryptosystem. Indirectly, this approach generates a cryptographic key directly from the biometric template. However, this approach suffers from intra-user variability.

Key generation approaches undergo from low discriminability that can be expressed in terms of two entropy: key stability and key entropy. Key stability depends on the repeatability of the number of cryptographic keys generated form the biometric helper data while key entropy refers to the number of distinct cryptographic keys generated from the biometric helper data. In a scheme, if the generated cryptographic key from the biometric helper data is repeatable, the scheme is said to achieve high key stability stage but zero key entropy. This situation leads to high false acceptance rate. On the contrary, if a method produces different cryptographic keys of different biometric templates for the same individual, the scheme is said to achieve zero key stability stage and high key entropy. This situation leads that scheme to high false rejection rate. Thus, it is a critical challenge to design a template protection scheme that can achieve high key stability and key entropy simultaneously (Jain et al., 2008).

2.3 Existing Registration-Free Fingerprint Template Protection Schemes

In 2007, Lee et al. (2007) proposed a scheme to generate alignment free fingerprint cancelable templates based on the rotation and translation invariant value computed from the minutiae. This invariant value is then used as the input of two changing functions. Besides the invariant value, the changing functions also take a user personal identification number (PIN) as the input. If the generated template is compromised, a new template can be generated to revoke the old template by changing the user PIN. Lee et al. (2007) conducted the experiments on the recognition performance of their proposed scheme by using FVC2002 DB1. The success rate for a brute-force attack to invert a transformed template depends greatly on the range of invariant values.

Meanwhile, Farooq et al. (2007) proposed a method to present an alignment free cancelable template based on a set of triangles derived from sets of three minutiae. Farooq et el. (2007) used seven invariants, i.e., three parts of a triangle, three angles of the triangle and the altitude of the longest triangle side to generate a binary string. A key based non-invertible transformation was then performed on this binary string. By reissuing a new different key, the old fingerprint template can then be revoked. As a drawback, the scheme requires high computational cost.

By exploiting a new fingerprint representation, Chikkerur et al. (2008) proposed a new method to generate registration-free cancelable fingerprint template. Instead of using minutiae points directly, Chikkerur et al. (2008) exploited the rare patterns formed by pixel patches around minutiae extracted from a fingerprint image. Random projection was then applied on this fingerprint representation to generate cancelable fingerprint templates. Chikkerur et al. (2008) showed that the recognition performance of their scheme is with acceptable equal error rate (EER).

Thereafter, Ahn et al. (2008) proposed a scheme to generate an alignment free cancelable biometric fingerprint template using triplets of minutiae points. In this scheme, Ahn et al. (2008) derived geometrical properties from minutiae triplets to veil their coordinates, scale and direction of minutia. The goal of the scheme was to obtain non-invertibility property of the transformed templates without degrading the discriminating capability. The only acceptable performance for the scheme was found in database FVC2002DB2 while FVC2002DB1 and FVC2002DB3 recorded lower performance comparatively. In addition, Ahn et al. (2008) did not evaluate the proposed scheme against attack via record multiplicity (ARM) and brute force attack.

Subsequently, Lee and Kim (2010) proposed a scheme to produce registration-free cancelable fingerprint template from fingerprint minutiae. First, Lee and Kim (2010) preselected a three-dimensional array consisting of cell. After that, Lee and Kim (2010) selected a minutia as a reference point and other minutiae were translated and rotated accordingly to map the minutiae into the cells. Finally, the cells were binarised based on the minutia point mapped into the cell. The binarised template was then permuted based on the reference point and a user specific key. If the attacker compromised the fingerprint template, new template can be generated by using a different permutation and a new user key. However, the performance of this scheme degrades when the user specific key is compromised due to quantisation error and image distortion.

Inspired by polar transformation introduced by Ratha et al. (2007), Ahmed et al. (2011) also proposed a scheme to generate alignment free cancellable fingerprint templates. The proposed scheme relies on the local features where a pair of minutiae points represented in polar coordinate system is utilised. However, the recognition performance of their proposed method over FVC2002 DB1, DB2, and DB3 are of high equal error rate (i.e., 9%, 6% and 27% respectively).

As the precise extraction of singular points is hard to achieve, Yang et al. (2014) modified Voronoi neighbor structures to generate a fixed-length of bit string. Their proposed scheme is able to compensate the change of Voronoi neighbor structures caused by massive non-linear distortion. In this scheme, encrypted matching was performed and secure sketch is used for protection. The security analysis of their proposed scheme was provided while the recognition performance of their proposed scheme was measure using publicly available databases.

Differ with previous proposed schemes, Jin et al. (2012) utilised variable-sized tessellated quantisation in polar coordinate to propose an alignment free minutiae descriptor, namely polar grid-based 3-tuple quantisation (PGTQ). The core concept of PGTQ is to have smaller areas for those sectors allocated near the reference minutiae. This directs to a smaller (respectively larger) quantisation step nearer to (respectively farther apart from) the reference minutiae to endure fingerprint resilient deformity. However, polar coordinate covers the entire fingerprint image and thus generates a lengthy bit string template, which is unattractive for practical applications due to larger storage of transformed templates. The experimental results showed that the recognition performance of PGTQ over FVC2002 DB1, FVC2002 DB2, FVC2004 DB1 and FVC2004 DB2 is with EER of 5.19%, 5.65%, 15.76% and 11.64% respectively. The security analysis of their proposed scheme against brute attack was presented by Jin et al. (2012).

Based on the minimum distance graph (MDG) Das et al. (2012) introduced a scheme known as registration-free fingerprint hashing algorithm. The MDG is generated by connecting some sets of nodes and those nodes are assembled by calculating the distance between core point and next nearest minutia. However, the performance of this scheme is not that much acceptable because this method confides on the detection of core points of the fingerprint image. Remark that, the detection of the accurate core points from the fingerprint image is challenging as their distinctiveness is not efficient for precise matching performance. (Maltoni et al., 2009).

Wang and Hu (2102, 2014) proposed two schemes to generate alignment free cancelable templates by exploiting pair-minutiae vectors. Both schemes generate a binary string by quantising the invariant feature of each pair of minutiae to tackle the difficulty of singular point detection. However, both schemes use different approaches in treating the binary string. As compared to the use of large matrices as user-specific keys by Wang and Hu (2012), Wang and Hu (2014) used a smaller size of key consisting a sequence of points. By reissuing different user-specific keys, a new template can be generated and thus fulfilling the property of revocability. In comparison with performance according to EER, the improved method yields better accuracy performance over FVC2002 DB1 and DB3.

By using K-nearest neighbor structure (K-NNS) formed from fingerprint minutiae, a new alignment free cancelable template protection scheme was proposed by Sandhya and Prasad (2015). Such structure was quantised to result a binary string. Subsequently, the binary string was applied with discrete Fourier transform (DFT) to generate a complex vector. Finally, the property of revocability was achieved by multiplying the complex vector with a user-specific key (i.e., a matrix). The recognition performance of their proposed scheme over FVC2002 DB1, DB2, and DB3 is still within acceptable range (i.e., 4.71%, 3.44% and 8.79% respectively in terms of EER). Different scenarios in attacking K-NNS had been analysed by Sandhya and Prasad (2015). Besides using K-nearest neighbor structure to generate fingerprint templates, Sandhya and Prasad (2017) studied the possibility in generating a cancelable template based on two transformed features from minutiae points, i.e., local structure and distant structure. The experimental results proved the tenability of the proposed scheme.

As compared to Sandhya and Prasad (2015) and Sandhya and Prasad (2017), Sandhya et al. (2016) exploited the Delaunay triangle feature set constructed from the fingerprint minutiae. The feature set was quantised and mapped into a three-dimensional array to produce a fixed length of one-dimensional bit string. Afterward, discrete Fourier transform was applied to the bit string template to generate a complex vector. Finally, a user key was applied to multiply with the complex vector to generate a cancelable template

A cancelable framework for fingerprints was proposed by Sadhya and Singh (2017) by using cryptographic hash functions to get benefit of the sufficient levels of security. Before going through the hashing level, pre-alignment technique was employed on the fingerprint. The feature extraction was done based on hexagonal grid-based quantisation. Finally, Sadhya and Singh (2017) showed that their proposed framework can achieve reasonable recognition performance in terms of EER

Recently, Wang and Hu (2016) proposed a scheme to generate alignment free cancelable template based on blind system identification. Instead of protecting the binary string generated from the quantisation of each pair of minutiae, Wang and Hu (2016) protected frequency samples of generated binary strings. Besides, a sequence with finite length was used as the user-specific key to achieve the property of revocability. The recognition performance of their proposed scheme over FVC2002 DB1, DB2, and DB3 is still within acceptable range (i.e., 4%, 3% and 8.5% respectively in terms of EER).

It is common to design a cancelable template protection scheme using binary representation due to the matching and storage effectiveness and simplicity in feature representation. Independently from our work, Wang et al. (2017) also proposed the use of discrete Fourier transform to convert the template from a binary string to a complex vector given that many binaries based cancellable biometric templates suffer from security shortfalls. Different from our work, they used the partial Hadamard transformation approach to absolutely protect the binary template.

2.4 Existing Registration Based Fingerprint Template Protection Schemes

Ratha et al (2007) introduced a scheme to generate registration based cancelable fingerprint template using three transformations namely Cartesian, polar and surface folding transformations of the minutiae position. Rectangular coordinates and polar coordinates were used in Cartesian transformation and polar transformation respectively. Lastly, surface folding transformation which consists of locally smooth but globally not smooth functions was used to improve the recognition performance since a small change in minutiae position in the original fingerprint can lead to a large change of minutiae position after both Cartesian and polar transformations. However, Quan et al. (2008) showed that the scheme proposed by Ratha et al. (2007) was vulnerable to ARM, brute-force attack and solving-equation attack due to poor many-to-one property of the underlying scheme

On the other hand, Takahashi and Hirata (2009) proposed methods to generate registration based cancelable fingerprint template with provable security based on correlation-invariant random filtering and the chip matching algorithm. The recognition performance of their scheme relies on the number of chaff points added to transform the template. By adding 20 chaff points, the

EER achieved experimentally was 2.85%. If the parameters are compromised, the time complexity of brute-force attack is only around 2^{35}.

At the same time, Yang et al. (2009) proposed a novel method to perpendicularly project the distance between a pair of minutiae to a circle. To improve the recognition performance, both local and global features were utilised, such as relative angles between the pair of minutiae, orientation, ridge frequency and so on. Besides, bin-based quantisation was used to generate the cancelable templates. The property of revocability was achieved by involving different keys to generate different feature vectors. The recognition performance of their proposed scheme is of high EER, i.e., 13% for a bin size of 30.

2.5 Summary of Literature Review

Table 2.2 summarises the techniques used in existing fingerprint template protection schemes. As a nutshell, most of the existing template protection schemes suffer from the following drawback:

1. Performance degradation issues after template protection (Ahmad et al., 2011; Das et al., 2012; Lee et al., 2007; Lee and Kim, 2010; Takahashi and Hirata, 2009; Yang et al., 2009).

Table 2.2: Summary of the techniques used in existing fingerprint template protection schemes

Source	Registration	Technique Used
(Wang and Hu, 2012)	×	Dense infinite to one
(Jin et al., 2012)	×	Polar grid based 3-tuple
(Farooq et al., 2007)	×	Triangle based technique
(Chikkerur et al., 2008)	×	Pixel Patch
(Wang and Hu, 2016)	×	Blind system identification
(Das et al., 2012)	×	Minutiae distance graph
(Lee et al., 2007)	×	Distance-and orientation-changing function
(Yang et al., 2014)	×	Vornoi neighbour structure
(Lee and Kim, 2010)	×	Three-dimensional array
(Ahn et al., 2008)	×	Minutiae triplets
(Ahmad et al., 2011)	×	Minutiae pair
(Sandhya and Prasad, 2015)	×	K-nearest neighbor structure
(Sandhya and Prasad, 2017)	×	Local structure and distance structure
(Sandhya et al., 2016)	×	Delaunay triangle structure
(Sadhya and Singh, 2017)	×	Hexagonal grid-based quantization
(Wang and Hu, 2014)	×	Circulated circular convolution
(Wang et al., 2017)	×	Partial Hadamard transform
(Ratha et al., 2007)	√	Cartesian, polar and surface folding transformation
(Takahashi and Hirata, 2009)	√	Distance between minutiae pair
(Yang et al., 2009)	√	Local triangle features

2. Lacking of security analysis against ARM (Ahmad et al., 2011; Ahn et al., 2008; Farooq et al., 2007; Jin et al., 2012; Ratha et al., 2007; Sandya and Prasad, 2015; Wang and Hu, 2012; Wang and Hu, 2016).

In this dissertation, a fingerprint template protection technique (namely 2C-PGTQ descriptor) is proposed to overcome these issues. The proposed method is motivated from PGTQ descriptor presented by Jin et al. (2012). The proposed method satisfies the requirements of a protected biometric template, i.e., performance preservation after transformation, cancelability and non-invertibility.

CHAPTER 3

METHODOLOGY

In this dissertation, the scheme proposed by Jin et al. (2012) is improved by reducing the storage size of the transformed templates and enhancing the security of the PGTQ. More precisely, the PGTQ descriptor is modified such that polar coordinates cover partial fingerprint image only to generate a condensed but computational- and storage- effective descriptor of bit string, namely dubbed condensed polar grid based 3-tuple quantisation (C-PGTQ). Besides, additional transformations are proposed, i.e., random bit flipping strategy, discrete Fourier transform (DFT) and random projection (RP) , to provide stronger non-invertibility, revocability and non-linkability. Finally, an application of bio-cryptosystem is demonstrated using the proposed alignment free cancelable fingerprint template protection scheme.

3.1 The Specification of the Proposed Method

Figure 3.1 shows the higher view of the proposed alignment free cancelable fingerprint template protection scheme. The proposed scheme consists of the following three processes, namely condensed polar grid based 3-tuple quantisation (C-PGTQ), protected PGTQ (P-PGTQ) and cancelable PGTQ (2C-PGTQ):

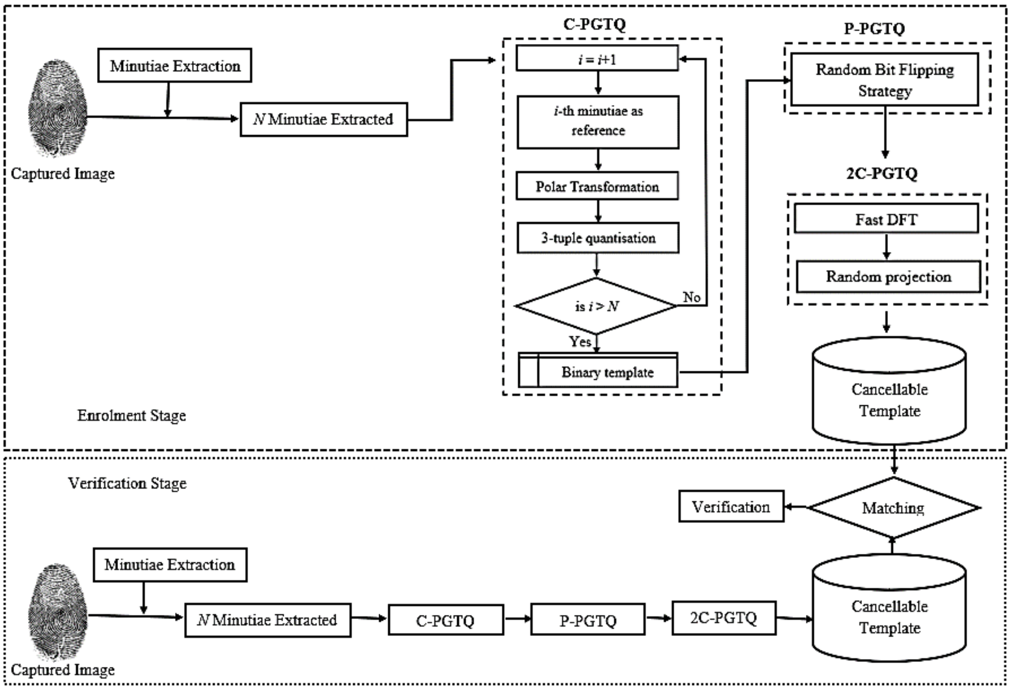

Figure 3.1: The higher view of the proposed alignment free fingerprint template protection scheme

3.1.1 Steps to Generate C-PGTQ Template:

C-PGTQ consists of the following steps: set pre-defined radius, reference minutia based polar transform, polar transformation, 3-tuple based quantisation and bit-String Generation

3.1.1.1 Set Pre-Defined Radius

To reduce the storage size of the transformed templates, a portion of the fingerprint image with a pre-defined radius R is selected from a selected reference minutia, $m_r = \{x_r, y_r, \theta_r\}$, where x_r is measured in pixel while y_r

and θ_r are measured in degree {0, 360}. The symbol r, refer to reference minutia. Figure 3.2 shows an example of setting radius as 70in pixels.

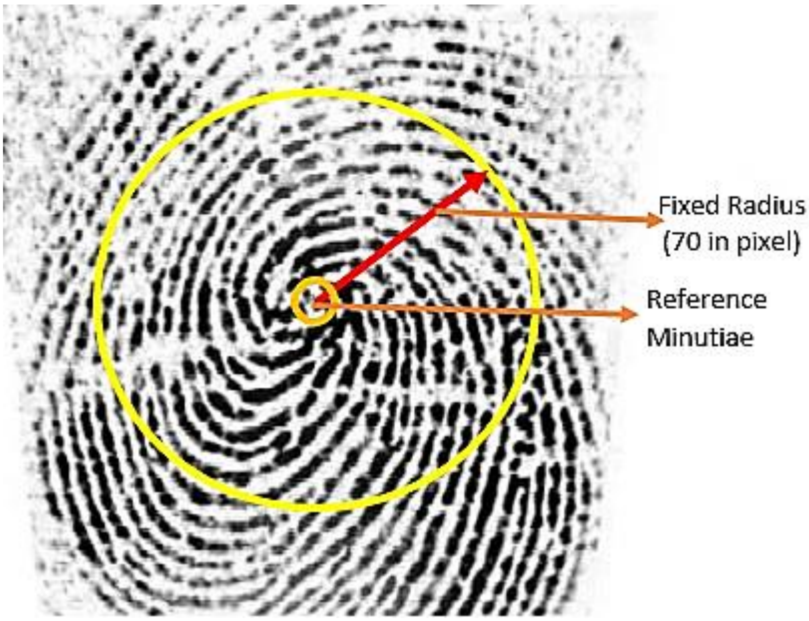

Figure 3.2: Setting R = 70 in pixels

3.1.1.2 Reference Minutia Based Polar Transform

The neighbouring minutiae located within the pre-defined radius R from the reference minutia are first aligned by applying the translation and rotation based on the reference minutia. Let $m_i = \{x_i,\ y_i, \theta_i | i = 1, \ldots.., N\}$ be a set of minutiae located within the pre-defined radius R from the reference minutia where x_i and y_i illustrate the location of minutiae point in cartesian polar coordinate system while $\theta_i \in [0, 2\pi]$ denotes the orientation of minutiae point. The aligned minutiae, represented as $m^t = \{x_i^t, y_i^t, \theta_i^t \,|\, i = 1, \ldots, N-1\}$, can then be obtained via Equation (1) and Equation (2), where total number of minutiae is denoted by N within a pre-defined radius R.

$$\begin{bmatrix} x_i^t \\ y_i^t \end{bmatrix} = \begin{bmatrix} \cos\theta_r & -\sin\theta_r \\ \sin\theta_r & \cos\theta_r \end{bmatrix} \begin{bmatrix} x_i - x_r \\ -(y_i - y_r) \end{bmatrix}. \tag{1}$$

$$\theta_i^t = \begin{cases} \theta_i - \theta_r & if\ \theta_i > \theta_r \\ 360 + \theta_i - \theta_r & if\ \theta_i < \theta_r \ . \end{cases} \tag{2}$$

3.1.1.3 Polar Transformation

The translated and rotated minutiae and the reference minutiae are then converted into polar coordinates using Equation (3) and Equation (4). Notice that ρ_i and $\alpha_i \in [0,360]$ are the radial distance (in pixels) and radial angle (in radian) of the i-th minutiae in polar coordinate system, respectively.

$$\rho_i = \sqrt{(x_i^t)^2 + (y_i^t)^2}\,. \tag{3}$$

$$\alpha_i = \arctan\left(\frac{y_i^t}{x_i^t}\right) + \frac{\pi}{2} \quad . \tag{4}$$

3.1.1.4 3-Tuple Based Quantisation

The 3-tuple based quantisation is a sector based quantisation that involves all neighbouring minutiae. Each quantised minutia can then be represented as a vector $v = (\rho_i, \alpha_i, \theta_i)$ transformed using Equation (5), Equation (6) and Equation (7) as follows:

$$\rho_i^b = \left\lfloor \frac{\rho_i}{C_x} \right\rfloor. \quad (5)$$

$$\alpha_i^b = \left\lfloor \frac{\alpha_i}{C_y} \right\rfloor. \quad (6)$$

$$\theta_i^b = \left\lfloor \frac{\theta_i}{C_z} \right\rfloor. \quad (7)$$

Notice that C_x, C_y and C_z denote the radius for each polar grid (measured in pixels), radial angle for tolerance (i.e., [0, 360]) and orientation for tolerance (i.e., [0, 360]) respectively. The quantisation level is determined by C_x, C_y and C_z to eliminate the loss of discriminative information of the feature. Figure 3.3 depicts the details of polar grid on polar coordinate system.

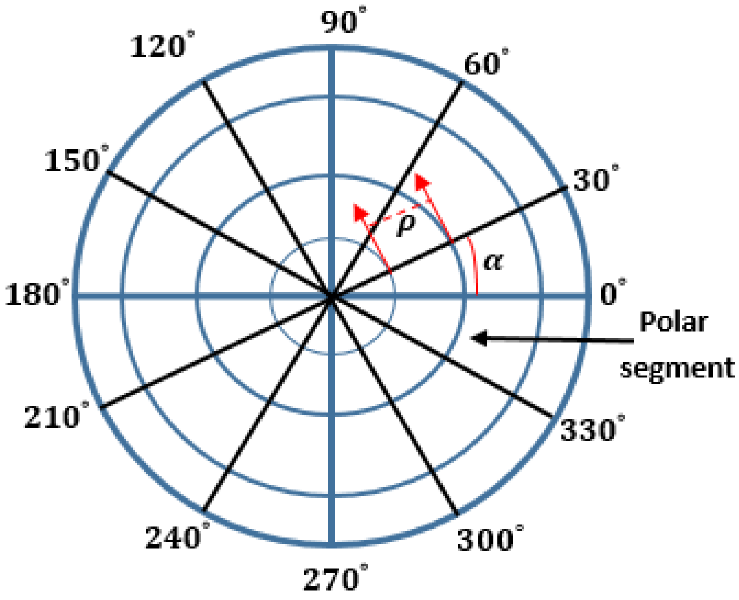

Figure 3.3: Polar grid on polar coordinate system

3.1.1.5 Bit-String Generation

As shown in Figure 3.3, there exist a number of polar grid segments in a polar grid. For each polar grid segment, containing more than one minutia in the polar grid segment, a bit ‘1’ is generated, else bit ‘0’ is generated otherwise. By joining the output bits together generated from the polar grid segments, a bit string with length equals to the number of polar grid segments $l = \left\lceil \frac{R}{C_x} \right\rceil \times \left\lceil \frac{360}{C_y} \right\rceil \times \left\lceil \frac{360}{C_z} \right\rceil$ where $\lceil \bullet \rceil$ is the ceiling function.

Section 3.1.1 is repeated by selecting the remaining minutiae as the reference minutia to generate the full binary C-PGTQ descriptor. Since the total number of minutiae *N* derived from each fingerprint image can be distinctive, the generated bit string is called as C-PGTQ template *t*.

3.1.2 Protected PGTQ (P-PGTQ)

If the C-PGTQ templates are compromised by the adversary, the adversary can launch template replay attack and spoof construction attack to access the recognition system illegitimately. To alleviate these issues, a random bit flipping strategy is adopted to randomly flip a fraction of bit string. This process add noise to the template that increases the difficulty in inverting the C-PGTQ templates. In this process, a total of 10 bits will be selected randomly and flipped such that bit ‘1’ is toggled to ‘0’ and vice-versa. The transformed template is then denoted as template *T*. Notice that the selection of 10 bits is justified in chapter 4.

3.1.3 Cancelable PGTQ (2C-PGTQ)

If the template *T* is compromised, the template will be considered as permanently lost. To re-issue a new template based on the same fingerprint image, discrete Fourier transform (DFT) and random projection (RP) are applied on the template *T* to generate the 2C-PGTQ cancelable template. These processes are included to achieve revocability and non-linkability.

3.1.3.1 Discrete Fourier Transforms

Fast DFT is applied on template *T* to convert the binary form to complex form as it is more difficult to invert the template from complex form (Wang and Hu, 2012). Let $T_{r,c}$ denotes the element of row *r* and column *c* of template *T* and the length of each row (i.e., number of columns) denoted as c_t. The resulting template, denoted as Ω, can be generated using Equation (8) as follows:

$$\Omega_{r,c} = \sum_{k=0}^{c_t-1} T_{r,c} e^{-j2\pi c \frac{k}{c_t}} , \quad c = 0,1, \ . \ . \ . \ , \ c_t - 1, \qquad (8)$$

where $\Omega_{r,c}$ denotes the element of row *r* and column *c* of template **Ω** while *k* is the beginning element of row, *r*. Fast DFT is then applied on remaining rows of the template *T* where *r* = 1, . . . , *N*, using Equation (8).

3.1.3.2 Random Projection

Biometric feature maps by random projection (RP) onto a set of orthonormal random vectors (Teoh & Yuang, 2007; Yang et al., 2010) to achieve the property of cancelability. In random projection, high dimensional spaces are replaced by random low dimensional linear combination of the components in original form. The Johnson-Lindenstrauss Lemma (Fedoruk et al., 2017), the root of random projection techniques, justifies that with high probability, the high-dimensional matrixes are embedded in a lower dimensional Euclidean space in the sense that pairwise distances and inner products among the projected-down lower dimensional matrixes are preserved. Dimensional reduction refers to the reduction of the dimension of matrix from high to lower. This dimensional reduction in this dissertation was performed by using random projection. For example, the product of high dimensional matrix with randomly generated low dimensional matrix creates a low dimensional matrix. Besides, the generated low dimensional matrix preserves the distance as justified by the Johnson-Lindenstrauss Lemma theory. Hence, Cancelable transformation is defined by multiplying projection matrix with the generated template, Ω to generate the template ω as follows:

$$\omega = \Omega \times \mathbb{R} \tag{9}$$

where Ω is a $N \times l$ matrix while $\mathbb{R}$ represents the $l \times l/2$ projection matrix. Meanwhile, ω denotes the transformed template for 2C-PGTQ (i.e., a $N \times l/2$ matrix).

3.2 Matching of Templates at Different Phases

To check whether the recognition performance of the proposed alignment free fingerprint template protection scheme is preserved, different matching experiments for C-PGTQ templates t, P-PGTQ templates T and 2C-PGTQ templates ω are conducted respectively.

3.2.1 Matching of C-PGTQ Templates *t*

Figure 3.4 shows the matching between two C-PGTQ templates denoted as t^q and t^e query and enroled, respectively. Suppose t^q and t^e consists of *n* and *m* number of rows, respectively where each row has a length, *l*. Row *i* of t^q and row j of t^e are denoted as t_i^q and t_j^q, respectively. Since the fingerprint images captured by the fingerprint scanner vary even though the fingerprint images are from the same finger, thus row number *m* and *n* may not be equal to each other. Notice that we have *i* = 1, . . ., *n* and *j* = 1, . . ., *m*.

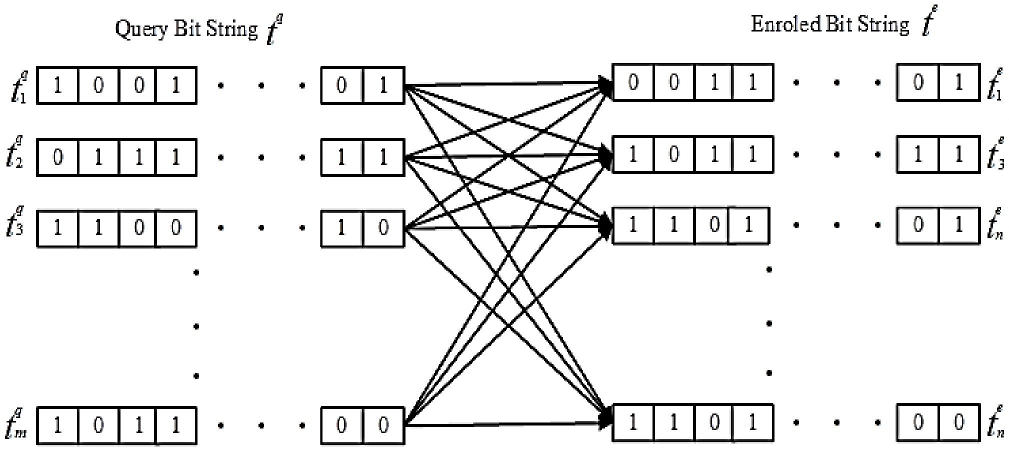
Query Bit String t^q
Enroled Bit String t^e
t_1^q 1 0 0 1 · · · 0 1
t_2^q 0 1 1 1 · · · 1 1
t_3^q 1 1 0 0 · · · 1 0
t_m^q 1 0 1 1 · · · 0 0
0 0 1 1 · · · 0 1 t_1^e
1 0 1 1 · · · 1 1 t_3^e
1 1 0 1 · · · 0 1 t_n^e
1 1 0 1 · · · 0 0 t_n^e

Figure 3.4: Matching between two C-PGTQ templates

To measure the matching or similarity score between two C-PGTQ templates, a two-stage of matching procedure consisting of local matching and global matching is performed. Local matching compares two binary bit strings (i.e., two C-PGTQ templates) and finds the intersection of two-bit strings. Due to the large difference of magnitude determine by the intersection of two-bit strings, the matching score is normalised as follows:

$$Score_{i,j} \;=\; \frac{(n_j^q+n_i^e)\sum_{k=1}^{l}(t_{j,k}^q \bullet t_{i,k}^e)}{(n_j^q)^2+(n_i^e)^2} \tag{10}$$

$$n_j^q \;=\; \sum_{k=1}^{l} t_{j,k}^q \tag{11}$$

$$n_j^e \;=\; \sum_{k=1}^{l} t_{i,k}^e \tag{12}$$

where • denotes a bitwise AND operator while *i* and *j* denotes the row of t^q and t^e respectively. Implicitly, $\sum_{k=1}^{l}(t_{j,k}^q \bullet t_{i,k}^e)$ counts the number of positions where the bit k of both t^q and t^e equals '1'. In addition, n_j^q and n_j^e denote the total number of 1's of the query and enroled templates. The matching score ranges from 0 to 1 where a score of 1 indicates a perfect match and otherwise. A matrix $S^t = \{Score_{i,j}\}$ is used to store all the matching scores. Thus, S^tconsists of m × n elements where each element represents a matching score.

Global matching is then performed on S^t to find out the final matching score of C-PGTQ templates as s_{C-PGTQ} . The final matching score of C-PGTQ templates, s_{C-PGTQ} is computed as follows:

1. Find the maximum distance a_j, for each column of S^t, such that $a_j \;=\; max_i\{Score_{i,j}\}$.
2. Find the mean of the maximum distance $\overline{c}$, for each column of S^t, such that $\overline{c} \;=\; \frac{1}{n}\sum_{j=1}^{n} a_j$.

3. Find the maximum distance b_i, for each row of S^t, such that $b_i = max_i\{Score_{i,j}\}$.

4. Find the mean of the maximum distance $\overline{r}$, for each column of S^t, such that $\overline{r} = \frac{1}{m}\sum_{i=1}^{m} b_i$.

5. Compute the final matching score of C-PGTQ templates, s_{C-PGTQ} as the maximum of $\overline{r}$ and $\overline{c}$, i.e., $s_{C-PGTQ} = \max\{\overline{c}, \overline{r}\}$.

3.2.2 Matching of P-PGTQ Templates *T*

Since the matching of P-PGTQ templates is similar with the matching of C-PGTQ templates excepts that certain number of bits in a P-GTQ template is flipped, thus the matching details of P-PGTQ templates are ignored. The same matching procedure can be applied as both C-PGTQ and P-PGTQ templates consist of same structure, i.e., same number of rows, same number of columns and each intersection is a binary element.

3.2.3 Matching of 2C-PGTQ Templates *ω*

Differ from C-PGTQ and P-PGTQ templates, 2C-PGTQ templates are in complex form. Thus, different matching procedure is needed in comparing 2C-PGTQ templates. Euclidean distance is used to find the matching score $s_{2C-PGTQ}$ (Wang and Hu, 2012) as follows:

$$s_{2C-PGTQ} \;=\; 1 - \frac{\left\|\omega_e - \omega_q\right\|_2}{\|\omega_e\|_2 + \left\|\omega_q\right\|_2} \;. \tag{13}$$

where ω_e and ω_q are the enroled 2C-PGTQ template and the query 2C-PGTQ template, respectively. We took 2-norm of $\|\omega_e\|$ and $\left\|\omega_q\right\|$ which are the Euclidean length of ω_e and ω_q, respectively. Because of complex form of the templates, we took 2-norm to normalize the final score, $s_{2C-PGTQ}$. Meanwhile, $\left\|\omega_e - \omega_q\right\|$ is the Euclidean distance between $\|\omega_e\|$ and $\left\|\omega_q\right\|$. Lastly, $\|\bullet\|_2$ denotes the 2-norm. Similar to $Score_{i,j}$, $s_{2C-PGTQ}$ ranges from 0 to 1 where the score of 1 indicates perfect matching.

3.3 Application to Key Binding Scheme

Key binding application based on the technique of chaffing and winnowing (Rivest, 1998) is applied to demonstrate that the recognition performance (i.e., in terms of EER) is preserved even though the key length is increased. In this key binding application, *k* different random matrices are used to bind *k*-bit key. A total of *k* protected templates will be produced and those templates will be stored in the database for matching purpose. Same matching process is performed *k* times based on *k* enroled template stored in the database. Each successful matching will release 1-bit of the key. Thus, the key will be successfully released if *k* matchings are successfully done. Due to different used random matrices, there are no correlation between these *k* enroled templates. Each matching is independent with each other and the recognition performance is preserved with different key lengths against FVC2002 DB1 and DB2. In the experiment, we set *k* as 16, 32, 64 and 128 respectively. The details of methodology for key binding application using cancelable template can be found in Jin et al. (2016).

For key binding application, a *k*-bit length binary key is used to bind 1's from *k*-key with original templates (P-PGTQ) while 0's bonded with synthetic templates. Synthetic templates are generated randomly with same size of original templates. Different random protection matrices are applied to either original or synthetic templates to complete the binding process along with the generation of the cancelable protected templates. It is noted that for *k*-bits key, *k* cancelable transformations are needed to bind the whole key. Thus, *k* original and synthetic cancelable templates are generated and stored in the database.

On the other hand, key release stage consists of two-steps procedure: a) *k* cancelable transformations are applied to the query templates to generate *k* cancelable query templates; b) matching cancelable query templates with stored cancelable templates to compare the matching score, *S* with pre-selected threshold value, τ. If the matching score $S \geq \tau$, it will release 1; otherwise 0. The key binding application process is illustrated in Figure 3.5.

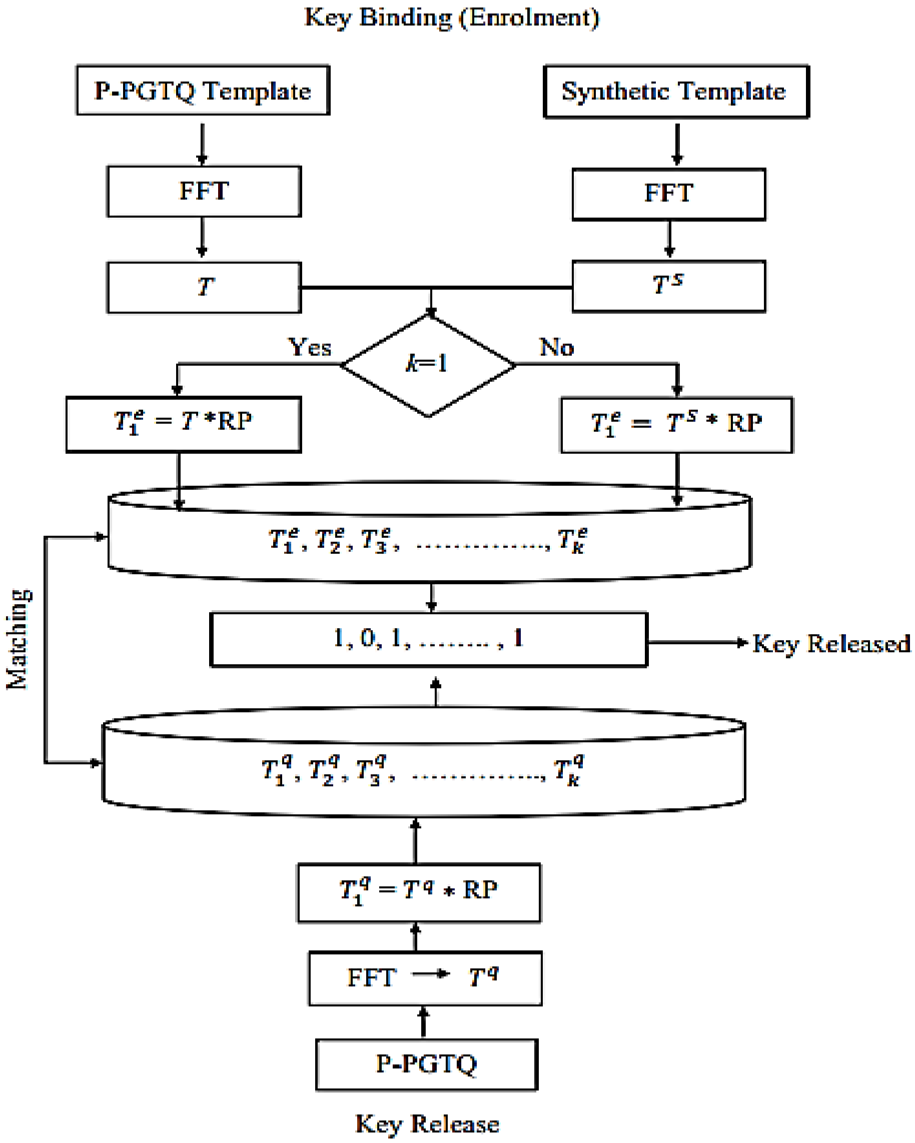

Figure 3.5: Overview of key binding application

CHAPTER 4

RESULTS AND DISCUSSION

To evaluate the feasibility of the proposed alignment free cancelable fingerprint template protection scheme, several experiments on the recognition performance of the proposed scheme are conducted using public domain fingerprint datasets FVC2002DB1, FVC2002DB2, FVC2002DB3, FVC2004DB1, FVC2004DB2 and FVC2004DB3. Each dataset contains 100 users with eight impressions (also known as fingerprint images) per user. Thus, there is a total of 800 fingerprint images in each dataset. Throughout the experiments, VeriFinger 6 SDK (Verifinger SDK) is used for minutiae extraction from the fingerprint image. Besides, two protocols, namely FVC protocol and 1vs1 protocol, are used. For both protocols, both impostor score and genuine score are computed to find out the false acceptance rate percentage (FAR) and the false rejection rate percentage (FRR). FAR is the rate of falsely accept an unauthorised user to a recognition system while FRR is the rate of falsely reject an authorised user to a recognition system. For 1vs1 matching protocol, the first impression of a user is matched against the second impression of the same user to generate the genuine score for FRR calculation. This process is repeated for 100 users and thus yields 100 genuine scores. For FVC matching protocol, the samples from a user are matched with each other to generate the genuine score for FRR calculation. This process is repeated for 100 users and thus yields (7+6+5+4+3+2+1) × 100 = 2800 genuine scores. Meanwhile, for both protocols, impostor scores are computed for FAR calculation by matching the first impression of each user with the first impression of the remaining users. Thus, this process yields 99 + 98 +. . .+ 2 + 1 = 49 × 100 + 50 = 4950 impostor scores. The recognition performance of the proposed scheme is evaluated using equal error rate (EER) where EER is the sum of false acceptance rate (FAR) and false rejection rate (FRR) divided by two (i.e., EER = $\frac{\text{FAR+FRR}}{2}$). The false acceptance rate, or FAR, is the measurement of the possibility that biometric security system incorrectly accepts an access attempt by an unauthorized identity. The false rejection rate, or FRR, is the measurement of the possibility that biometric security system incorrectly rejects an access attempt by an authorized identity. To check whether each process (i.e., C-PGTQ, P-PGTQ and 2CPGTQ) are preserving the performance or not, the recognition performance EERs are computed through all the experiments.

4.1 The Recognition Performance of C-PGTQ Templates

Different quantisation parameters of C-PGTQ are applied to find out the parameters that can achieve better EER of the proposed scheme. Table 4.1 shows the EER of the C-PGTQ templates for different tuned parameters of C-PGTQ.

Table 4.1: The tuned parameters that yield best EER performances over C-PGTQ templates

Fingerprint Dataset	Radial distance in pixel (x)	Radial angle in degree (y)	Orientation angle in degree (z)	EER FVC (%)	EER 1vs1 (%)
FVC2002DB1	10	20	20	5.71	1.00
FVC2002DB2	10	20	20	6.34	2.07
FVC2002DB3	10 20	20 20	20 20	11.06 10.45	6.11 10.14
FVC2004DB1	10	20	20	17.04	15.44
FVC2004DB2	10	20	20	14.85	9.15
FVC2004DB3	20	20	20	16.75	9.28

4.2 The Recognition Performance of P-PGTQ Templates

Experiments in measuring the recognition performance of P-PGTQ templates are conducted by flipping 5-, 10- and 15-bit randomly of C-PGTQ templates. Flipping bits from templates intentionally distort the template and thus degrade the recognition performance of the template. However, it also increases the computational complexity in recovering the original template. To achieve the balance between the recognition performance and security of the proposed scheme, our experimental results and analysis recommend the flipping of 10 bits. Table 4.2 shows the average EER of P-PGTQ templates after randomly flipping 10 bits of C-PGTQ templates 100 times.

Table 4.2: The tuned parameters that yield best EER performances over P-PGTQ templates

Fingerprint Dataset	Radial distance in pixel (x)	Radial angle in degree (y)	Orientation angle in degree (z)	EER FVC (%)	EER 1vs1 (%)
FVC2002DB1	10	20	20	5.56	1.18
FVC2002DB2	10	20	20	6.4	2.13
FVC2002DB3	10 20	20 20	20 20	10.21 10.56	8.18 9.96
FVC2004DB1	10	20	20	17.73	14.02
FVC2004DB2	10	20	20	15.94	12.30
FVC2004DB3	20	20	20	17.84	11.14

As only 10 bits are flipped from each template with large number of bits (e.g., each PPGTQ template generated from FVC2002DB1, FVC2002DB2 and FCV2002DB3 consists of 76792, 95505 and 51093 bits respectively), the recognition performance of P-PGTQ templates can be preserved while introducing noise to each resultant template.

4.3 The Recognition Performance of 2C-PGTQ Templates

Table 4.3 shows the EER of 2C-PGTQ templates after randomly flipping 10 bits of C-PGTQ templates 100 times. As compared to Table 4.1 and Table 4.2, the recognition performance of 2C-PGTQ templates is preserved even after applying random bit flipping strategy, discrete Fourier transform and random projection. This observation tallies with the claim given by Johnson and Lindenstrauss (Johnson & Lindenstrauss, 1984) where the Euclidean distance between two points is almost preserved if the dimension of the points is reduced.

Table 4.3: The tuned parameters that yield best EER performances over 2C-PGTQ templates

Fingerprint Dataset	Radial distance in pixel (x)	Radial angle in degree (y)	Orientation angle in degree (z)	EER FVC (%)	EER 1vs1 (%)
FVC2002DB1	10	20	20	5.95	1.97
FVC2002DB2	10	20	20	6.99	1.99
FVC2002DB3	10 20	20 20	20 20	11.40 11.03	7.89 11.29
FVC2004DB1	10	20	20	18.17	15.57
FVC2004DB2	10	20	20	16.52	13.52
FVC2004DB3	20	20	20	18.50	12.16

4.4 Recognition Performance Comparison with Other Existing Schemes

Table 4.4 serves the performance comparison between the proposed 2C-PGTQ with representative cancelable fingerprint protection methods (Ahmed et al., 2011; Jin et al., 2012; Sandhya and Prasad, 2015; Wang and Hu, 2012; Wang and Hu, 2014; Wang and Hu, 2016) available in literature on the public fingerprint datasets (i.e., FVC2002 DB1, DB2, DB3 and FVC2004 DB1, DB2, DB3). In order to have fair justification, same datasets and experiment protocols (e.g., 1vs1 and FVC) are adopted to conduct the experiments. The proposed 2C-PGTQ outperforms the majority of existing methods (Ahmed et al., 2011; Jin et al., 2012; Wang and Hu, 2012; Wang and Hu, 2014; Wang and Hu, 2016;). For example, 2C-PGTQ provides better performance for 1vs1 protocol under same key scenario (same random matrix) over methods (Sandhya and Prasad, 2015) that may be due to the lacking of optimal parameters (e.g; k, C_x, C_y) tuned for ideal performance. Although Jin et al. (2012) offers slightly better accuracy, 2C-PGTQ provides favourable security and privacy improvement by proposing random bit flipping, discrete Fourier transform and random projection techniques. More specifically, a portion of bits among C-PGTQ descriptor are randomly flipped, this offers one-way property against template inversion attack while the accuracy performance retains well with the parameters carefully selected (i.e., number of bits for flipping).

Table 4.4: The recognition performance of different cancelable fingerprint template protection schemes

Method	FVC2002			FVC2004		
	DB1	DB2	DB3	DB1	DB2	DB3
1 vs 1 Protocol						
(Wang and Hu, 2012)	3.5	5	7.5	-	-	-
(Jin et al., 2012)	1.19	6.94	-	16.35	8.66	-
(Wang and Hu, 2016)	3	2	7	-	-	-
Lee et al., 2007	3.4	-	-	-	-	-
(Ahmed et al., 2011)	9	6	27	-	-	-
(Yang et al., 2014)	3.38	0.59	9.80	16.52	14.88	-
(Sandhya and Prasad, 2015)	4.71	3.44	8.79	-	-	-
(Sandhya and Prasad, 2017)	2.19	1.6	6.14	11.89	12.71	17.60
(Sandhya et al., 2016)	3.96	2.98	6.89	12.17	13.29	17.73
(Wang et al., 2017)	1	2	5.2	-	13.3	-
(Wang and Hu, 2014)	2	3	6.12	-	-	-
Proposed Scheme (2C-PGTQ)	**1.97**	**1.99**	**7.89**	**15.57**	**13.52**	**12.16**
FVC Protocol						
(Ahn et al., 2008)	7.18	3.61	11.8	-	-	-
(Yang et l., 2014)	11.84	10.38	16.52	-	-	-
(Sadhya and Singh, 2017)	5.8	5.3	-	15.8	14.5	-
Proposed Scheme (2C-PGTQ)	**5.95**	**6.99**	**11.03**	**18.17**	**16.52**	**18.50**

4.5 Security Analysis of the Proposed Scheme

In this dissertation, an alignment free cancelable fingerprint template protection scheme is proposed. The security of the proposed scheme (e.g., non-invertibilty, non-linkability and revocability) is discussed.

4.5.1 Non-Invertibility

We refer non-invertibility as the computational complexity in recovering the fingerprint minutiae from the 2C-PGTQ templates ω. We assume that the attacker obtains multiple 2C-PGTQ templates (i.e., attack via record multiplicity) and has the knowledge of random projection. This scenario is considered as a stronger attack model which is more favourable to the attacker.

Table 4.5: The number of guesses needed to recover the C-PGTQ templates

Fingerprint Datasets	l	N		Number of Guesses	
		Min	Max	Lower Bound	Upper Bound
FVC2002DB1	2268	6	68	$\binom{6}{1}\binom{2268}{10} \approx 2^{92.238}$	$\binom{68}{1}\binom{2268}{10} \approx 2^{95.741}$
FVC2002DB2	2268	7	87	$\binom{7}{1}\binom{2268}{10} \approx 2^{92.461}$	$\binom{87}{1}\binom{2268}{10} \approx 2^{96.096}$
FVC2002DB3	2268	6	51	$\binom{6}{1}\binom{2268}{10} \approx 2^{92.238}$	$\binom{51}{1}\binom{2268}{10} \approx 2^{95.326}$
FVC2004DB1	2268	8	88	$\binom{8}{1}\binom{2268}{10} \approx 2^{92.652}$	$\binom{88}{1}\binom{2268}{10} \approx 2^{96.113}$
FVC2004DB2	2268	9	75	$\binom{9}{1}\binom{2268}{10} \approx 2^{92.823}$	$\binom{75}{1}\binom{2268}{10} \approx 2^{95.882}$
FVC2004DB3	1296	14	128	$\binom{14}{1}\binom{1296}{10} \approx 2^{85.364}$	$\binom{128}{1}\binom{1296}{10} \approx 2^{88.556}$

Given the knowledge of random projection and 2C-PGTQ templates ω, an attacker can invert the 2C-PGTQ templates ω to recover P-PGTQ templates T as one can compute the inverse of random projection and the inverse of discrete Fourier transform easily. The random projection are assumed to be invertible. Subsequently, the attacker can use multiple recovered P-PGTQ templates T to recover C-PGTQ templates t. Solving of this problem is easier if similar C-PGTQ templates are generated given the same fingerprint image is always being captured. Assume that similar C-PGTQ templates (where same minutiae are captured) are generated, the attacker can perform comparison check between multiple P-PGTQ templates. However, different C-PGTQ templates are generated as the minutiae captured vary. More importantly, we ensure that the selected random projection is non-square which implies that this random projection is not invertible. This violates the earlier assumption that the random projection is invertible. More details of how random projection can provide the various constraints for the cancelability provided by Pillai et al. (2011).

In addition, by using FVC2002DB1 as the example, each C-PGTQ template is a matrix with size of N × 2268 where N is the number of rows. A total of 10 bits (i.e., element of a matrix) is flipped randomly when converting a C-PGTQ template to a PPGTQ template. More precisely, 10 out of 2268 columns are first selected randomly. Then, for each out of 10 selected columns, one element is flipped. If the attacker has the knowledge of one P-PGTQ template only, the attacker needs to guess $\binom{N}{1}\binom{2268}{10}$ attempts to find out the 10 flipped bits. Throughout the experiments, N varies from 6 to 68 for FVC2002 DB1, depending on the number of minutiae captured. Thus, the number of guesses varies from $\binom{6}{1}\binom{2268}{10} \approx 2^{92.238}$ to $\binom{68}{1}\binom{2268}{10} \approx 2^{95.741}$. This justifies that the random bit toggling strategy adds noise on C-PGTQ templates.

Table 4.5 shows the number of guesses needed to recover the C-PGTQ templates from P-PGTQ templates where *N* is the number of rows and *l* is the number of columns.

Besides, it is not straightforward for an attacker to recover the fingerprint minutiae information from the C-PGTQ templates due to lossy binarization. For each polar grid segment, if the polar grid segment contains more than one minutia, a bit `1' is generated. Thus, there exists more than one way in generating a bit `1' (i.e., many-to-one mapping (Jin et al., 2012)). Finally, it is well known that the Fourier transform decorrelates highly correlated signal samples to a relatively flat spectrum (Wang et al., 2017). This implies that many signal samples are possible and make the search of correct signal sample more difficult.

As a nutshell, the proposed scheme can achieve the property of non-invertibility and is able to strengthen the scheme proposed by Jin et al. (2012) against ARM and template inversion attacks due to the newly added random bit flipping strategy, random projection and discrete Fourier transform.

4.5.2 Revocability

The revocability is evaluated by matching a particular template with other fingerprint templates generated from distinct random projection. A total of 100 different random projection matrix are selected randomly to generate a total of 100 fingerprint templates based on a fingerprint image. This process is repeated using the same random projection matrices for the remaining users to produce a total of 100 × 8 × 100 = 80000 pseudo-impostor scores. The entire process is applied on six different public domain fingerprint datasets, i.e., FVC2002DB1, FVC2002DB2, FVC2002DB3, FVC2004DB1, FVC2004DB2 and FVC2004DB3. Figure 4.1 to Figure 4.6 shows the distribution of pseudo-impostor and impostor scores for six different fingerprint datasets.

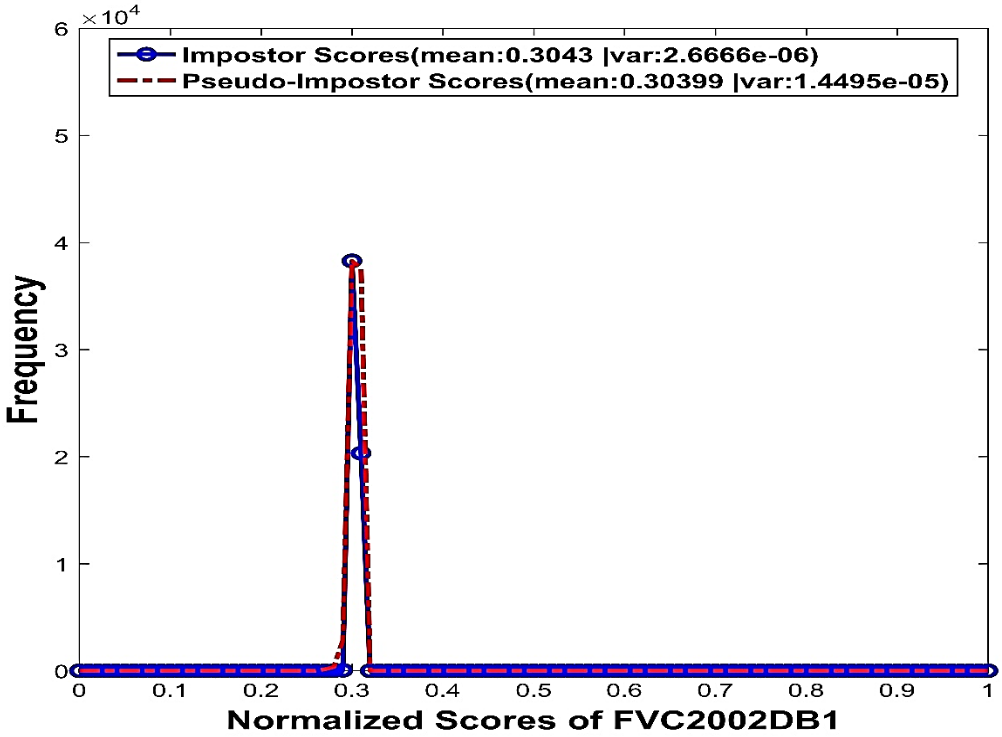

Figure 4.1: The distribution of pseudo-impostor and impostor scores for FVC2002DB1 fingerprint dataset

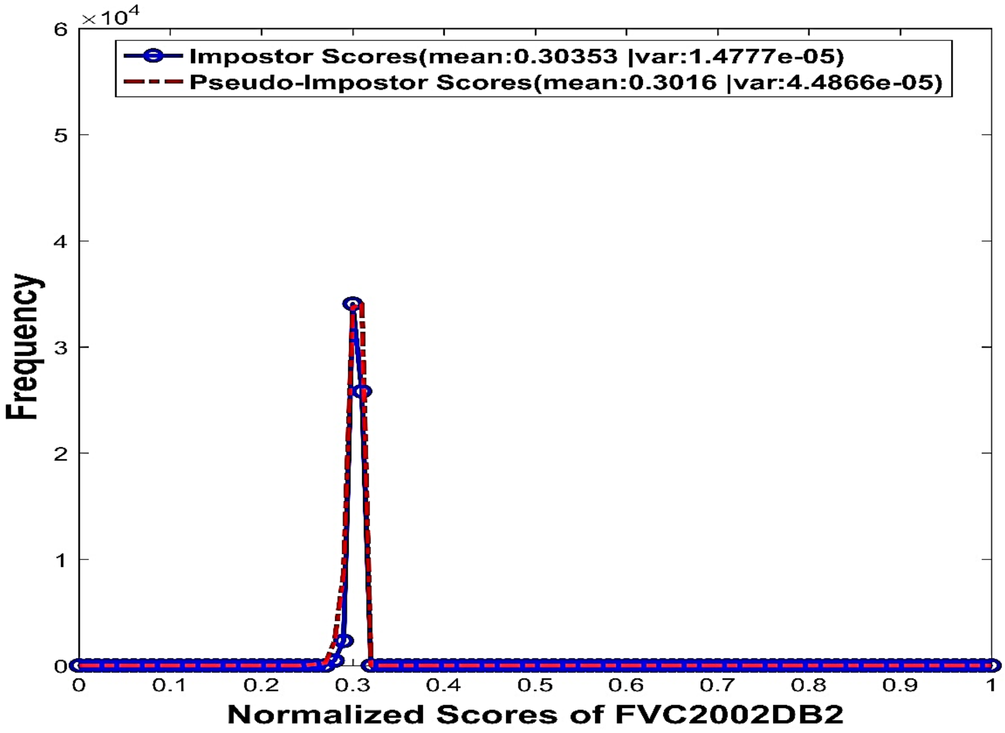

Figure 4.2: The distribution of pseudo-impostor and impostor scores for FVC2002DB2 fingerprint dataset

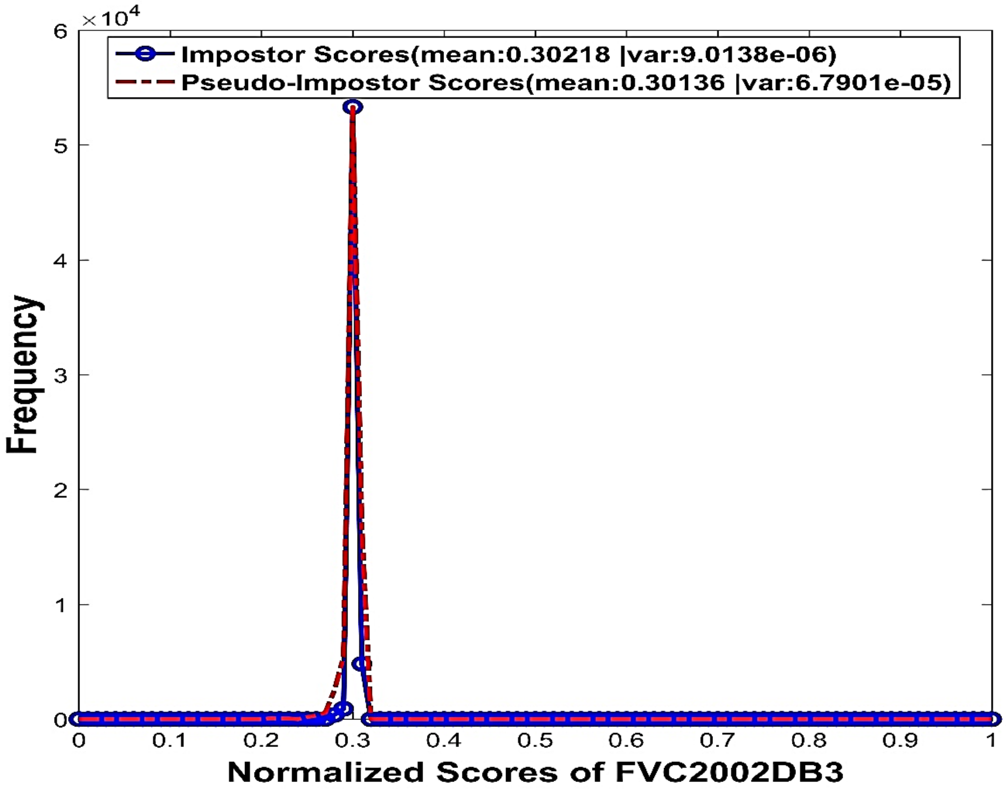

Figure 4.3: The distribution of pseudo-impostor and impostor scores for FVC2002DB3 fingerprint dataset

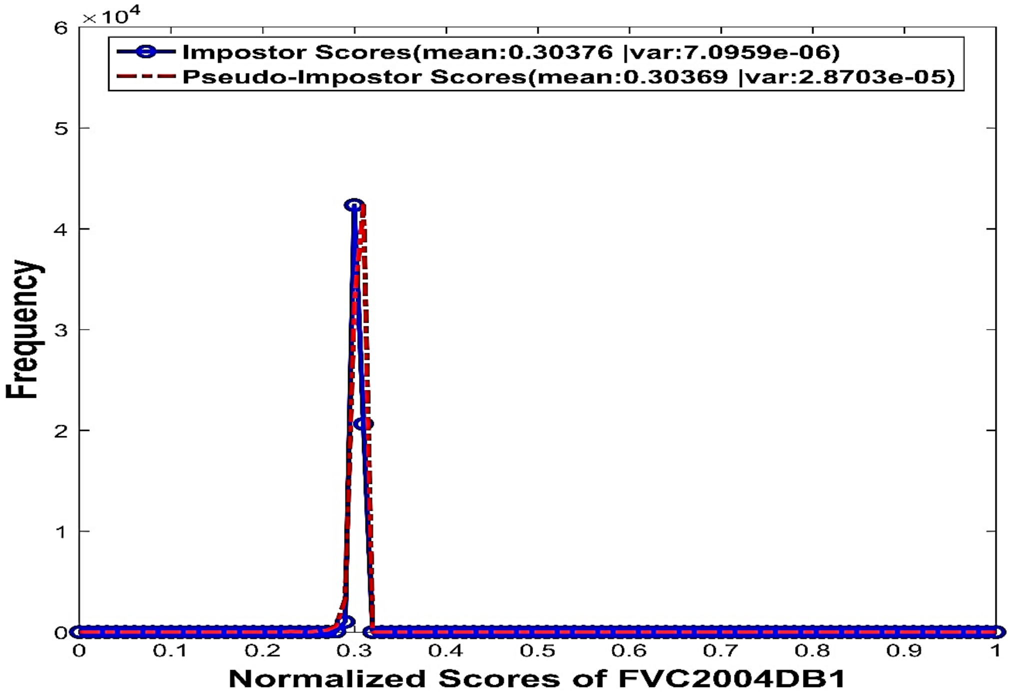

Figure 4.4: The distribution of pseudo-impostor and impostor scores for FVC2004DB1 fingerprint dataset

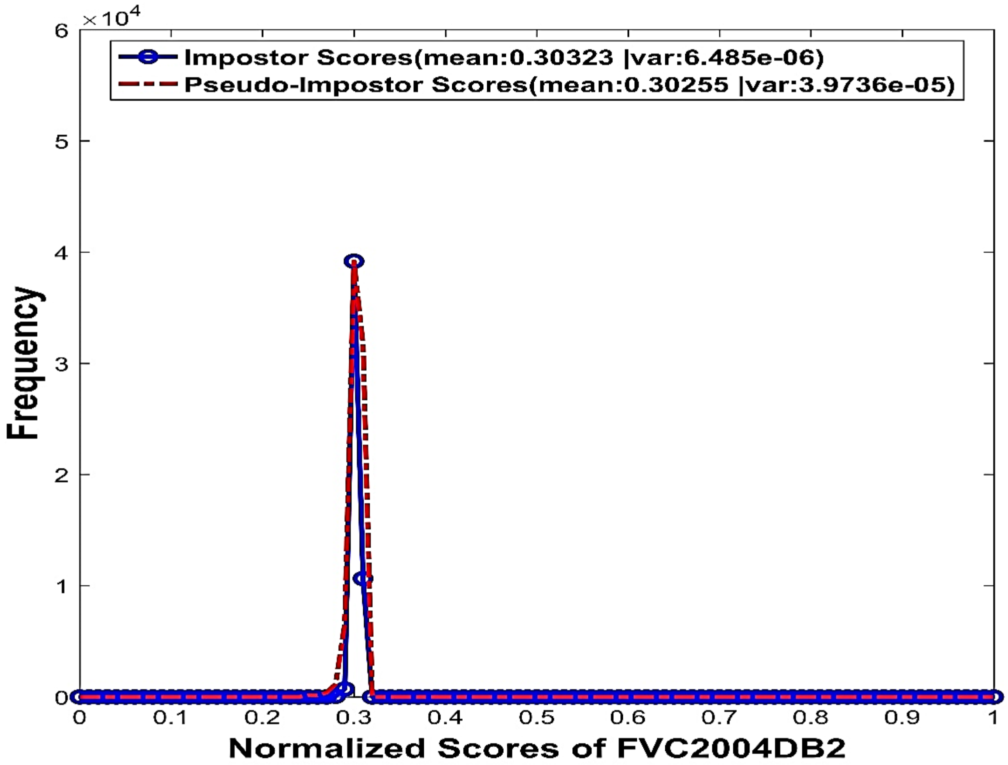

Figure 4.5: The distribution of pseudo-impostor and impostor scores for FVC2004DB2 fingerprint dataset

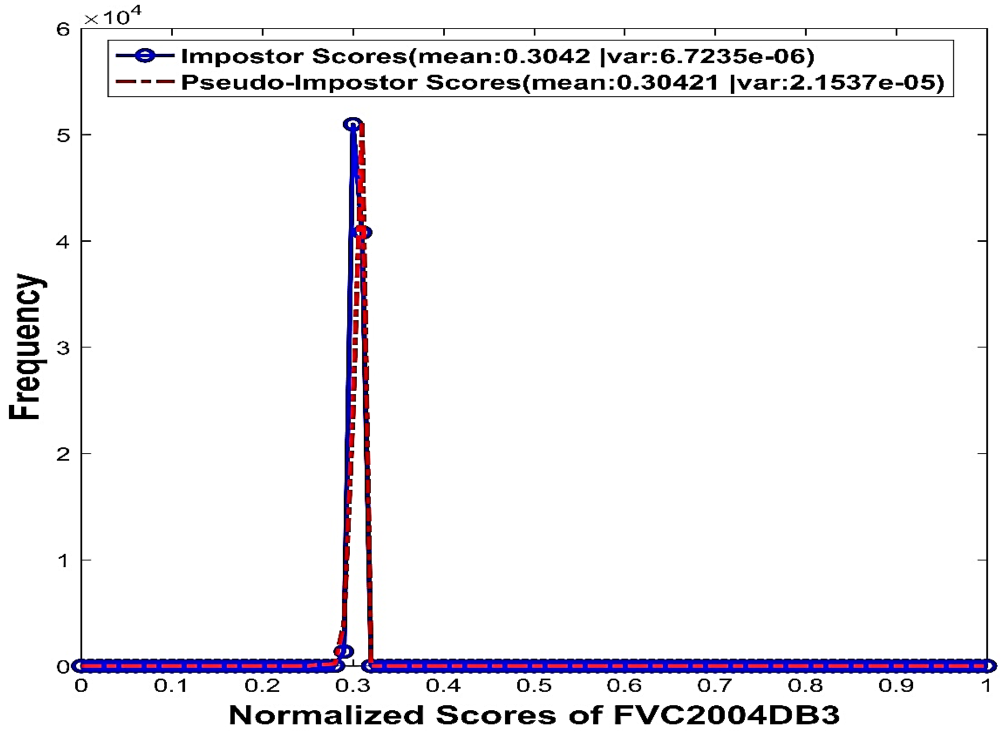

Figure 4.6: The distribution of pseudo-impostor and impostor scores for FVC2004DB3 fingerprint dataset

Refer to Figure 4.1 to Figure 4.6, as the distribution of pseudo-impostor scores resembles the distribution of impostor scores, this shows that the newly generated cancelable fingerprint templates are indistinguishable to each other. Thus, this justifies the proposed alignment free cancelable fingerprint template protection scheme can achieve the property of revocability. Besides, Pillai et al. (2011) showed that random projection meets the various constraints required for cancellability.

4.5.3 Non-Linkability

Pseudo-genuine score is introduced to evaluate the property of non-linkability. Pseudo-genuine scores are computed by matching the fingerprint template generated from different fingerprint samples of the same user using 100 different random projection matrixes. This process yields (7+6+5+4+3+2+1) ×100 = 2800 pseudo-genuine scores by each user because of having eight samples per user. This experiment is applied on six different public domain fingerprint datasets. Figure 4.7 to Figure 4.12, shows the distribution of pseudo genuine and pseudo-impostor scores for six different fingerprint datasets.

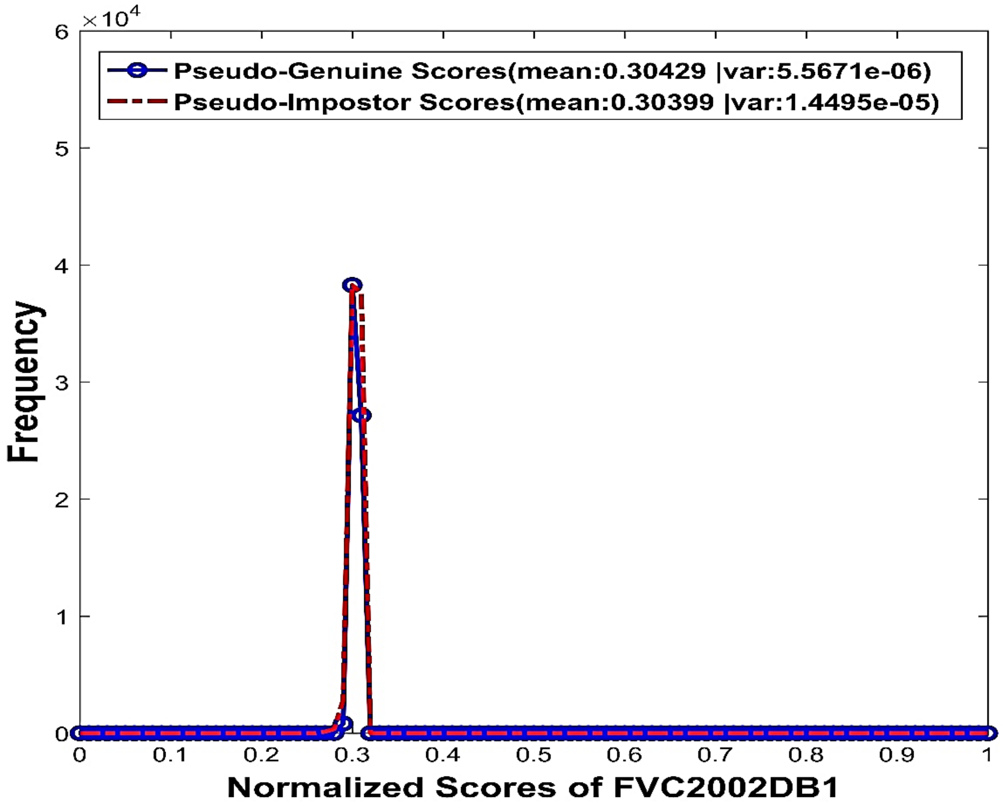

Figure 4.7: The distribution of pseudo-genuine and pseudo-impostor scores for FVC2002DB1 fingerprint dataset

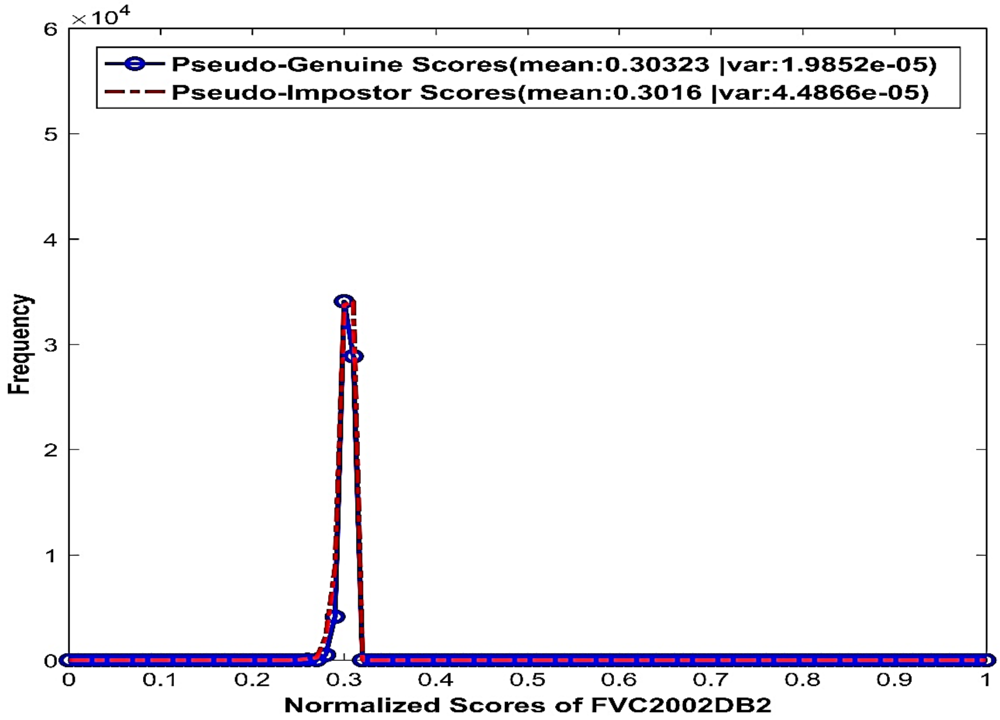

Figure 4.8: The distribution of pseudo-genuine and pseudo-impostor scores for FVC2002DB2 fingerprint dataset

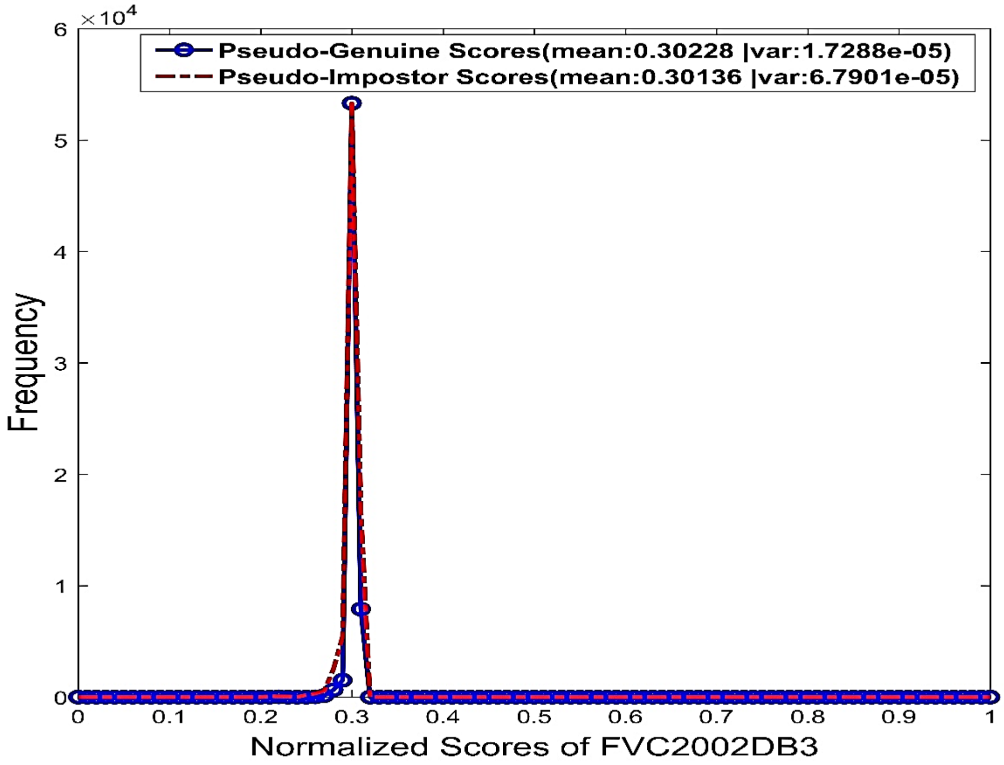

Figure 4.9: The distribution of pseudo-genuine and pseudo-impostor scores for FVC2002DB3 fingerprint dataset

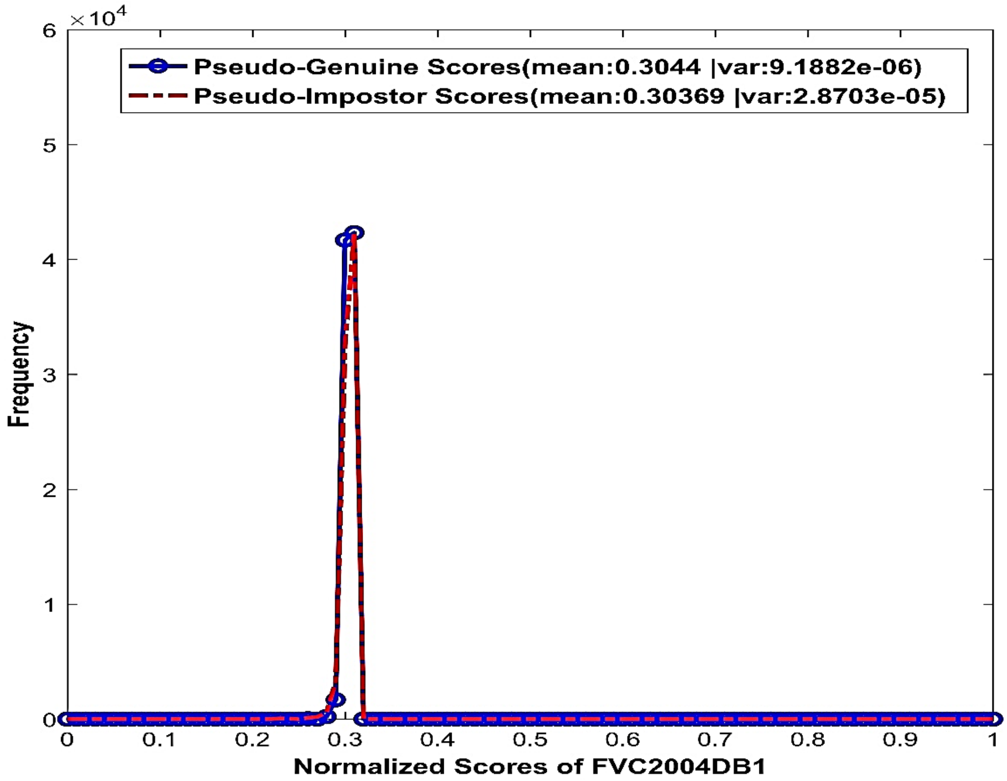

Figure 4.10: The distribution of pseudo-genuine and pseudo-impostor scores for FVC2004DB1 fingerprint dataset

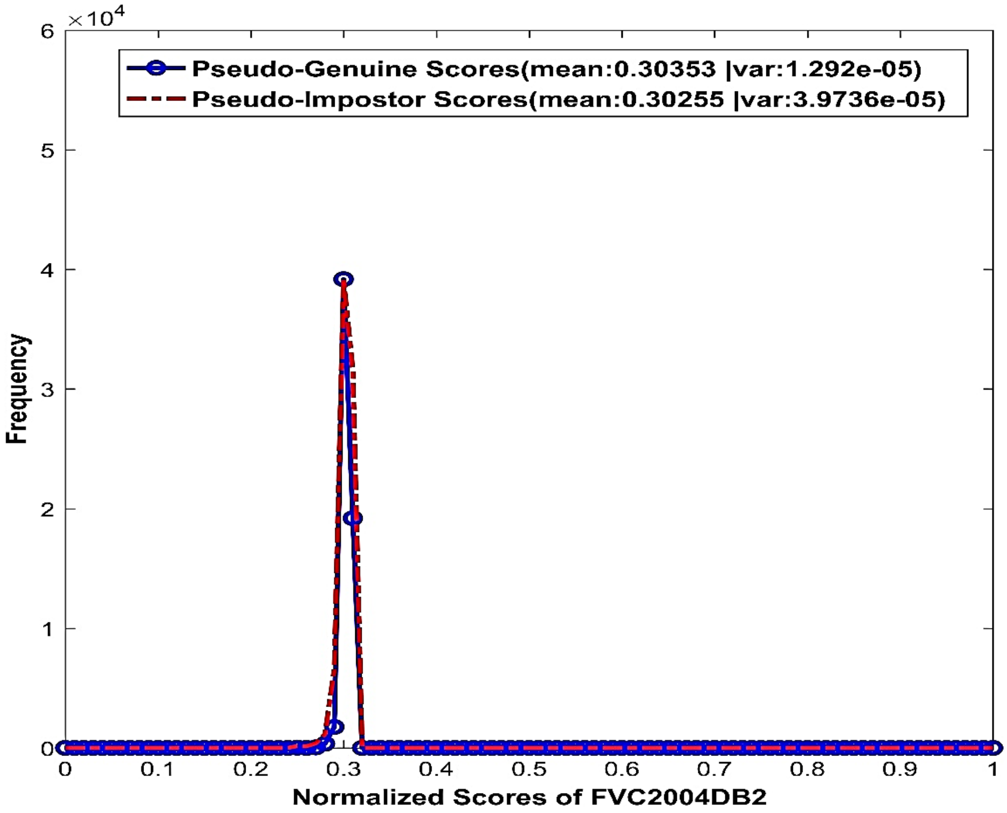

Figure 4.11: The distribution of pseudo-genuine and pseudo-impostor scores for FVC2004DB2 fingerprint dataset

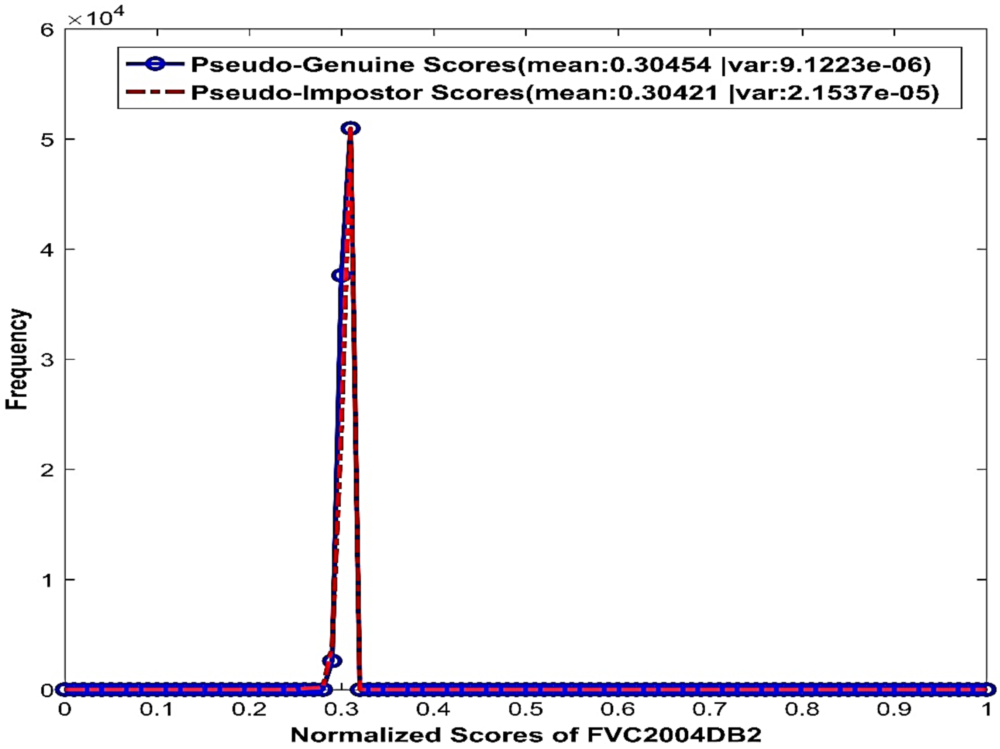

Figure 4.12: The distribution of pseudo-genuine and pseudo-impostor scores for FVC2004DB3 fingerprint dataset

Refer to Figure 4.7 to Figure 4.12, as the distribution of pseudo-genuine scores almost resembles the distribution of pseudo-impostor scores, this shows that the attacker cannot distinguish whether the fingerprint templates are generated from the same user fingerprint. Thus, this justifies that the proposed alignment free cancelable fingerprint template protection scheme can achieve the property of non-linkability.

4.6 EER Result of Key Binding Application

EER results of key binding application for different key lengths (i.e., 16-, 32-, 64- and 128-bit) are shown in Table 4.6.

Table 4.6: The EER of key binding application for different key lengths

Database	Key Length	Threshold Value	FRR(%)	FAR(%)	EER(%)
FVC2002DB1	16	0.39	6.43	2.06	4.25
	32		7.14	1.56	4.35
	64		7.29	1.68	4.49
	128		7.43	1.07	4.25
FVC2002DB2	16	0.40	7.71	3.15	5.43
	32		7.42	2.61	5.02
	64		8.29	3.08	5.68
	128		7.71	3.09	5.40

CHAPTER 5

CONCLUSION

5.1 Conclusion

In this dissertation, extensive existing literature review related to fingerprint template protection techniques has been studied. A secure and efficient alignment free cancelable fingerprint template scheme, namely 2C-PGTQ has been proposed. The proposed secure and efficient cancelable fingerprint template protection scheme is accomplished by a series of transformation: (1) formation of adoptive minutiae descriptor (C-PGTQ), (2) generation of protected minutiae descriptor (P-PGTQ), and (3) production of cancelable template (2C-PGTQ). Transformation (1) takes care of the computational efficiency by modifying the PGTQ descriptor while transformation (2) provides strong non-invertible property by adopting random bit toggling strategy and transformation (3) enables cancelable property using discrete Fourier transform and random projection. Due to the randomness in transformation (2) and dimensionality reduction using random projection in transformation (3) specified in Section 3.1.3 respectively, the generated template possesses the strong capability to protect against security and privacy attacks by fulfilling the criteria such as non-invertibilty, revocability and non-linkability.

Lastly, extensive experiments have been done with public datasets and those experiments provided a reasonable performance accuracy result that can be justified by theoretical analysis. Other than the conversional authentication, we have demonstrated that the proposed cancelable template is also applicable to the biometric key binding scheme. This enhances the usefulness of the proposed template, and also is rare explained in the existing literature.

5.2 Future Work

Some possible directions for future research on improving the work conducted in this research project are presented as follows:

1. Investigating the effect of number of bit flipping with the accuracy of recognition performance.
2. Investigating the effect of dimension reduction size of the projection matrix with the accuracy of recognition performance and computational complexity.
3. Replacing the random projection and discrete Fourier transform to other lightweight operations while preserving the security of the proposed alignment free cancelable fingerprint template protection scheme.

REFERENCES

Adler, A., 2004. Images can be regenerated from quantized biometric match score data. In *Electrical and Computer Engineering,* 2-5 May 2004 Ontario, Canada. *Canadian Conference on*, 1, pp. 469-472).

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

Ahmed, M.A.O., Reyad, O., AbdelSatar, Y. and Omran, N.F., 2018. Multi-filter Score-Level Fusion for Fingerprint Verification. In *Advanced Machine Learning Technologies and Applications*, 26th January 2018 Egypt. *International Conference on* (Vol. 273, pp. 624-633). Springer.

Ahn, D., Kong, S.G., Chung, Y.S. and Moon, K.Y., 2008. Matching with secure fingerprint templates using non-invertible transform. In *Congress on Image and Signal Processing, CISP'08,* 27-30 May 2008 Sanya, Hainan, China. 2, pp. 29-33.

Bolle, R.M., Connell, J.H. and Ratha, N.K., 2002. Biometric perils and patches. *Pattern Recognition*, 35(12), pp.2727-2738.

Chikkerur, S., Ratha, N.K., Connell, J.H. and Bolle, R.M., 2008. Generating registration-free cancelable fingerprint templates. In *IEEE International Conference on Biometrics: Theory, Applications and Systems, BTAS,* 29 Sept. – 1 Oct. 2008 Arlington, VA, USA. pp. 1-6.

Cappelli, R., Ferrara, M., Franco, A. and Maltoni, D., 2007. Fingerprint verification competition 2006. *Biometric Technology Today*, 15(7), pp.7-9.

Cappelli, R., Maio, D., Maltoni, D., Wayman, J.L. and Jain, A.K., 2006. Performance evaluation of fingerprint verification systems. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 28(1), pp.3-18.

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

Chua, S.C., Wong, E.K. and Tan, A.W.C., 2014, April. Singular point detection in fingerprint images: An investigation on quantization approach. In *Region 10 Symposium,* 14-16 April 2014 Kuala Lumpur, Malaysia. pp. 606-611.

Davida, G.I., Frankel, Y., Matt, B. and Peralta, R., 1999. On the relation of error correction and cryptography to an online biometric based identification scheme. In *Proceedings of WCC99, Workshop on Coding and Cryptography, 1999.*

Das, P., Karthik, K. and Garai, B.C., 2012. A robust alignment-free fingerprint hashing algorithm based on minimum distance graphs. *Pattern Recognition*, 45(9), pp.3373-3388.

Espinosa-Duro, V., 2002. Minutiae detection algorithm for fingerprint recognition. *IEEE Aerospace and Electronic Systems Magazine*, 17(3), pp.7-10.

Farooq, F., Bolle, R.M., Jea, T.Y. and Ratha, N., 2007, June. Anonymous and revocable fingerprint recognition. In *Computer Vision and Pattern Recognition, CVPR'07. IEEE Conference on*, 16 July 2007 Minneapolis, MN, USA. pp. 1-7.

Fedoruk, J., Schmuland, B., Johnson, J. and Heo, G., 2018. Dimensionality reduction via the Johnson–Lindenstrauss Lemma: theoretical and empirical bounds on embedding dimension. *The Journal of Supercomputing*, pp.1-17.

Garris, M.D. and McCabe, R.M., 2000. NIST special database 27: Fingerprint minutiae from latent and matching tenprint images. *NIST Technical Report NISTIR*, *6534*.

Gunes, H. and Piccardi, M., 2007. Bi-modal emotion recognition from expressive face and body gestures. *Journal of Network and Computer Applications*, 30(4), pp.1334-1345.

Jain, A.K., Bolle, R.M. and Pankanti, S., 1999. *BIOMETRIC: Personal identification in networked society*, Kluwer Academic Publishers.

Jain, A.K., Nandakumar, K. and Nagar, A., 2008. Biometric template security. *EURASIP Journal on Advances in Signal Processing*, 8, pp.1-17.

Jin, A.T.B., Ling, D.N.C. and Goh, A., 2004. Biohashing: two factor authentication featuring fingerprint data and tokenised random number. *Pattern Recognition*, 37(11), pp.2245-2255.

Jin, Z., Ong, T.S., Tee, C. and Teoh, A.B.J., 2011, August. Generating revocable fingerprint template using polar grid based 3-tuple quantization technique. In *IEEE 54th International Midwest Symposium on Circuits and Systems,* 7-10 Aug. 2011 Seoul, South Korea. pp. 1-4.

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., Teoh, A.B.J., Goi, B.M. and Tay, Y.H., 2016. Biometric cryptosystems: A new biometric key binding and its implementation for fingerprint minutiae-based representation. *Pattern Recognition*, 56, pp.50-62.

Johnson, E.G. et al., 1998. Optical recognition of phase-encrypted biometrics. *Optical Engineering*, 37(1), pp.18-26.

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

Kaur, E.S. and Attri, E.V.K., 2017. Review on DNA Computing based Authentication Techniques. *International Journal of Advanced Research in Computer Science*, 8(5), pp.2691-2694.

Kaur, H. and Khanna, P., 2016. Biometric template protection using cancelable biometrics and visual cryptography techniques. *Multimedia Tools and Applications*, 75(23), pp.16333-16361.

Lee, C., Choi, J.Y., Toh, K.A. and Lee, S., 2007. Alignment-free cancelable fingerprint templates based on local minutiae information. *IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics)*, 37(4), pp.980-992.

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

Lee, H.C., Ramotowski, R. and Gaensslen, R.E. eds., 2001. *Advances in fingerprint technology* 2nd ed. London: CRC press.

Leng, L. and Zhang, J., 2011. Dual-key-binding cancelable palmprint cryptosystem for palmprint protection and information security. *Journal of Network and Computer Applications*, 34(6), pp.1979-1989.

Li, P. et al., 2010. An alignment-free fingerprint cryptosystem based on fuzzy vault scheme. *Journal of Network and Computer Applications,* 33(3), pp.207-220.

Li et al., 2018. A three-factor anonymous authentication scheme for wireless sensor networks in internet of things environments. *Journal of Network and Computer Applications*, 103, pp.194-204.

Liu, C.L., Tsai, C.J., Chang, T.Y., Tsai, W.J. and Zhong, P.K., 2015. Implementing multiple biometric features for a recall-based graphical keystroke dynamics authentication system on a smart phone. *Journal of Network and Computer Applications*, 53, pp.128-139.

Maio, D., Maltoni, D., Cappelli, R., Wayman, J.L. and Jain, A.K., 2002a. FVC2000: Fingerprint verification competition. *IEEE Transactions on Pattern Analysis and Machine Intelligence,* 24(3), pp.402-412.

Maio, D., Maltoni, D., Cappelli, R., Wayman, J.L. and Jain, A.K., 2002b. FVC2002: Second fingerprint verification competition. In *Proceedings of International Conference on Pattern recognition,* 11-15 Aug. 2002 Quebec, Canada. 3, pp. 811-814.

Maio, D., Maltoni, D., Cappelli, R., Wayman, J.L. and Jain, A.K., 2004. FVC2004: Third fingerprint verification competition. In *Biometric Authentication*, pp. 1-7. Springer, Berlin, Heidelberg.

Maltoni, D., Maio, D., Jain, A.K. and Prabhakar, S., 2009. *Handbook of fingerprint recognition* 2nd ed. Springer Science & Business Media.

Masdari, M. and Ahmadzadeh, S., 2017. A survey and taxonomy of the authentication schemes in Telecare Medicine Information Systems. *Journal of Network and Computer Applications*, 87, pp.1-19.

Masdari, M., Ahmadzadeh, S. and Bidaki, M., 2017. Key Management in Wireless Body Area Network: Challenges and Issues. *Journal of Network and Computer Applications*, 91, pp. 36-51.

Mathew, S., Petropoulos, M., Ngo, H.Q. and Upadhyaya, S.J., 2010. A Data-Centric Approach to Insider Attack Detection in Database Systems. In *Recent Advances in Intrusion Detection*. *Springer*, pp. 382–401.

Mehrotra, H., Majhi, B. and Gupta, P., 2010. Robust iris indexing scheme using geometric hashing of SIFT key points. *Journal of Network and Computer Applications*, 33(3), pp.300-313.

North, R., Norris, J. and Chu, F., Adt Us Holdings, Inc., 2017. *Voice activated application for mobile devices*. U.S. Patent 9,639,682.

Pillai, J.K., Patel, V.M., Chellappa, R. and Ratha, N.K., 2011. Secure and robust iris recognition using random projections and sparse representations. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 33(9), pp.1877-1893.

Quan, F., Fei, S., Anni, C. and Feifei, Z., 2008, December. Cracking cancelable fingerprint template of Ratha. In *Proceeding of the International Symposium on Computer Science and Computational Technology,* 20-22 Dec. 2008 Shanghai, China. 2, pp. 572-575.

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.

Rivest, R.L., 1998. Chaffing and winnowing: Confidentiality without encryption. *CryptoBytes (RSA laboratories)*, 4(1), pp.12-17.

Ross, A., 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.

Sandhya, M. and Prasad, M.V., 2015, May. k-Nearest Neighborhood Structure (k-NNS) based alignment-free method for fingerprint template protection.

In *International Conference on Biometrics*, 19-22 May 2015 Phuket, Thailand. pp. 386-393.

Sandhya, M. and Prasad, M.V., 2017. Securing fingerprint templates using fused structures. *IET Biometrics*, 6(3), pp.173-182.

Sandhya, M., Prasad, M.V. and Chillarige, R.R., 2016. Generating cancellable fingerprint templates based on Delaunay triangle feature set construction. *IET Biometrics*, 5(2), pp.131-139.

Sadhya, D. and Singh, S.K., 2017. Design of a cancelable biometric template protection scheme for fingerprints based on cryptographic hash functions. *Multimedia Tools and Applications*, 76, pp.1-25.

Shahzad, M., Liu, A.X. and Samuel, A., 2016. Behavior Based Human Authentication on Touch Screen Devices Using Gestures and Signatures. *IEEE Transactions on Mobile Computing*, 16(10), pp. 2726-2741.

Shen, W., 1994. October. Automated fingerprint identification system (AFIS) benchmarking using the National Institute of Standards and Technology (NIST) Special Database 4. In *International Carnahan Conference on Security Technology,* 12-14 Oct. 1994 Albuquerque, NM, USA. pp. 188-194.

Soutar, C., Roberge, D., Stoianov, A., Gilroy, R. and Kumar, B.V., 1998. Biometric encryption using image processing. In *Optical Security and Counterfeit Deterrence Techniques,* 3314, pp. 178-189.

Soutar, C. and Tomko, G.J., 1996. Secure private key generation using a fingerprint. In *Cardtech/Securetech Conference Proceedings*, 13-16 May 1996 Atlanta, Georgia. 1, pp. 245-252.

Takahashi, K. and Hitachi, S.H., 2009, September. Generating provably secure cancelable fingerprint templates based on correlation-invariant random filtering. In *IEEE International Conference on Biometrics: Theory, Applications, and Systems, BTAS'09*, 28-30 Sept. 2009 Washington, DC, USA. pp. 1-6.

Tao, X., Chen, X., Yang, X. and Tian, J., 2012. Fingerprint recognition with identical twin fingerprints. *PloS one*, 7(4), pp. e35704.

Teoh, A.B., Goh, A. and Ngo, D.C., 2006. Random multispace quantization 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 Yuang, C.T., 2007. Cancelable biometrics realization with multispace random projections. *IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics)*, 37(5), pp.1096-1106.

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., 2014. Design of alignment-free cancelable fingerprint templates via curtailed circular convolution. *Pattern Recognition*, 47(3), pp.1321-1329.

Wang, S. and Hu, J., 2016. A blind system identification approach to cancelable fingerprint templates. *Pattern Recognition*, 54, pp.14-22.

Wang, Y., Hu, J. and Phillips, D., 2007. A fingerprint orientation model based on 2D Fourier expansion (FOMFE) and its application to singular-point detection and fingerprint indexing. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 29(4), pp.573-585.

Wang, S., Deng, G. and Hu, J., 2017. A partial Hadamard transform approach to the design of cancelable fingerprint templates containing binary biometric representations. *Pattern Recognition*, 61, pp.447-458.

Watson, C.I., 1998. NIST Special Standard Reference Database 24, NIST Digital Video of Live-Scan Fingerprint Database, U.S. *National Institute. Standards and Technology,* NIST Technical Report.

Watson C.I., 1993a. NIST Special Database 14, Fingerprint Database, U.S. *National Institute of Standards and Technology,* NIST Technical Report.

Watson C.I., 1993b. NIST Special Database 10, Supplemental Fingerprint Card Data (SFCD) for NIST Special Database 9, Fingerprint Database., U.S. *National Institute of Standards and Technology,* NIST Technical Report.

Watson, C. I., & Wilson, C. L., 1992a. NIST special database 4. Fingerprint Database, U.S. *National Institute of Standards and Technology*, NIST Technical Report. 17, pp.77.

Watson, C.I. and Wilson, C.L., 1992b. NIST special database 9. Fingerprint Database, U.S. *National Institute of Standards and Technology*, NIST Technical Report.

Yang, B., Busch, C., Bours, P. and Gafurov, D., 2010. Robust minutiae hash for fingerprint template protection. In *Media Forensics and Security*, 28 Jan. 2010 San Jose, California, United States. 7541, pp.75410.

Yang, H., Jiang, X. and Kot, A.C., 2009, August. Generating secure cancelable fingerprint templates using local and global features. In *IEEE International Conference on Computer Science and Information Technology,* 8-11 Aug. 2009 Beijing, China. pp. 645-649.

Yang, W., Hu, J., Wang, S. and Stojmenovic, M., 2014. An alignment-free fingerprint bio-cryptosystem based on modified Voronoi neighbor structures. *Pattern Recognition*, 47(3), pp.1309-1320.

Zhang, P., Hu, J., Li, C., Bennamoun, M. and Bhagavatula, V., 2011. A pitfall in fingerprint bio-cryptographic key generation. *Computers & Security*, 30(5), pp.311-319.

List of Publication

- Alam, B., Jin, Z., Yap, W.S. and Goi, B.M., 2018. An alignment free cancelable fingerprint template for bio-crytosystems. *Journal of Network and Computer Application*, 115, pp.20-32.

- Alam, B., Jin, Z., Yap, W.S. and Goi, B.M., 2017. Cancellable Fingerprint Minutiae Template Protection Using Bit Toggling Technique for Privacy Preserving. *International Journal of Cryptology Research*, 7(1), pp.27-41.