Fingerprint-Based Biometric Authentication with Template Protection

Submitted by

Muhammad Shahzad

B.Sc., Bahauddin Zakariya University, 2009

M.Sc., Blekinge Institute of Technology, 2015

A thesis submitted in total fulfillment
of the requirements for the degree of
Doctor of Philosophy

Department of Engineering
College of Science, Health and Engineering

La Trobe University
Melbourne, Victoria 3086
Australia

September 2020

Declaration of Authorship

Except where reference is made in the text of the thesis, this thesis contains no material published elsewhere or extracted in whole or in part from a thesis submitted for the award of any other degree or diploma.

No other person's work has been used without due acknowledgement in the main text of the thesis.

The thesis has not been submitted for the award of any degree or diploma in any other tertiary institution.

Signed:
MUHAMMAD SHAHZAD

Date:
29 September 2020

Abstract

Fingerprint-based biometric authentication has been widely used in a range of applications, such as national ID card, border control and e-passport. However, despite its great deployability, fingerprint biometrics have security and privacy concerns. Hence, there has been ongoing research on fingerprint template protection and several state-of-the-art schemes have been introduced. This thesis presents two novel cancelable fingerprint template algorithms as well as an efficient fingerprint authentication system, specifically designed for resource-constrained Internet of Things (IoT) devices.

In the first research contribution, an alignment-free cancelable fingerprint template design is proposed with dual protection. Unlike most of the existing schemes, the proposed method combats security threats such as attacks via record multiplicity (ARM), masquerade attacks and pre-image attacks. The proposed dual protection is achieved via a window-shift-XOR model and partial discrete wavelet transform. The former defuses the ARM threat and is combined with the latter to produce cancelable templates as well as enhance matching performance. Furthermore, the proposed scheme meets the tough unlinkability criteria at both local and global levels.

The second proposed scheme for cancelable fingerprint templates is based on feature-adaptive random projection. Traditional random projection-based cancelable templates are prone to the ARM, where an adversary obtains multiple transformed templates from different applications and the associated user keys to assemble them into a full-rank linear system of equations, thereby retrieving the original feature vector. Different to the existing random projection-based techniques, the proposed method is implemented by generating the projection matrixes from one basic matrix in conjunction with local feature slots. The generated projection matrixes, which are key to the ARM, are discarded after use, thus making it difficult for the adversary to launch this attack.

In the third research contribution, a lightweight and secure fingerprint authentication system is designed to address the energy efficiency issue of IoT devices. The proposed system intelligently reduces the size of a fingerprint template, thus requiring less storage and computational power. Moreover, the proposed system is secure against the attack vectors and attack resources that may reveal the raw features of a fingerprint template stored in an IoT device.

Publications

The following papers have been published or are under review for publication in various international journals based on the discussion and material in this thesis:

- **M. Shahzad**, S. Wang, G. Deng, W. Yang, "Alignment-free Cancelable Fingerprint Templates with Dual Protection." *Pattern Recognition*, Vol. 111, 2020. (IMPACT FACTOR: 7.196).
- W. Yang, S. Wang, **M. Shahzad**, W. Zhou, "A Cancelable Biometric Authentication System Based on Feature-Adaptive Random Projection", *Accepted for publication in Journal of Information Security and Applications* (IMPACT FACTOR: 2.327)

Acknowledgements

First and foremost, I would like to express my indebtedness to my principal supervisor, Dr Song Wang for all her kind support throughout my candidature. Without her guidance and valuable advice, this submission wouldn't have been possible. She has been a true motivation for me throughout this period which will most certainly be a guide to me throughout my future research endeavours. Moreover, I would like to acknowledge the support provided by my mentor and co-supervisor A/Prof. Dennis Deng who is indeed an inspirational teacher.

I would like to express my appreciation to my lab mates in the Department of Electronic Engineering for their support and useful discussions especially Mr Waseem Waheed, Miss Marzieh Rahmani, Mr Hussein Al-bandawi, Dr Mukhalad Al-Nasrawi and Mrs Aseel Esho. For their continuous technical support, special credit goes to the IT staff in the Department of Engineering, Mr Steven Wang, Mr Peter Stewart and Mr Mark Gentile.

I would also like to acknowledge the financial support provided by the Government of Punjab and the University of Agriculture, Faisalabad, Pakistan.

I would like to thank my lovely wife Shafia Arshad, and sons Abdul Hadi and Abdul Rafay. Living alone and away from such a lovely family was the biggest challenge. Thanks for all of your patience and trust.

Finally, I would like to thank my Mum and Dad for their unlimited support and love. I cannot adequately express my gratitude for your sacrifices, tears and prayers. I believe this achievement of mine will make you proud.

Muhammad Shahzad

Melbourne, September 2020

Contents

List of Figures

List of Tables

List of Abbreviations

AFIS	Automatic Fingerprint Identification System
FAR	False Acceptance Rate
FRR	False Rejection rate
ERR	Equal Error Rate
FMR	False Match Rate
ARM	Attack via Record Multiplicity
DWT	Discrete Wavelet Transform
IoT	Internet of Things
MCC	Minutia Cylinder-Code
FTP	Fingerprint Template Protection
FC	Fingerprint Cryptosystem
FV	Fuzzy Vault
CIRF	Correlation-Invariant Random Filtering
RMQ	Random Multispace Quantization
MVD	Minutia Vicinity Decomposition
RMVD	Random Minutia Vicinity Decomposition
DITOM	Densely Infinite-To-One mapping

DFT	Discrete Fourier transform
RGHE	Randomized Graph-Based Hamming Embedding
CNN	Convolutional Neural Network
VGG	Visual Geometry Group
IoM	Index-of-Max
SC-IoM	Sparse Combined Index-of-Max
MLC	Multiline Code
PLS	Partial Local Structure
DPSM	Discrete Partial Structure Map
PR-NNLS	Permuted Randomized Non-Negative Least Square
FFT	Fast Fourier Transform
PMCC	Protected Minutia Cylinder Code
k-NNS	k-Nearest Neighbour Local Structures
FVC	Fingerprint Verification Competition
DCT	Discrete Cosine Transform
ROC	Receiver Operating Characteristics
FCMR	False Cross Match rate
FNCMR	False Non-Cross Match Rate
MP	Minutia Pair
RNG	Random Number Generator
LGS	Local Greedy Similarity
MAP	Maximum Aposteriori Probability
FWT	Fast Wavelet Transform

CWT	Complex Wavelet Transform

Chapter 1

Introduction

"Everything has its wonders, even darkness and silence, and I learn, whatever state I may be in, therein to be content."

– Helen Keller

1.1 Overview of a biometric recognition system

Biometric recognition is an emerging technology for authentication purposes, due to its stability and the individuality of biometric identifiers (or simply, biometrics) [1]. Moreover, biometrics are considered reliable because they can't be easily shared, misplaced or forged compared to traditional token- or knowledge-based methods, e.g., keys, ID cards, passwords or PINs. Over the years, a large number of biometric technologies have been developed and deployed successfully. The most commonly used biometric traits are fingerprints, iris, face and hand geometry. Each trait has its own strengths and weaknesses and the choice of a particular trait usually depends on the application itself.

Of all the biometric traits, fingerprints are well-known to be distinct and exhibit other persistent properties such as collectability, universality, permanence,

acceptability, performance and circumvention. For this reason, forensic and law enforcement agencies worldwide were the early adopters of fingerprints, and developed automatic fingerprint identification systems (AFIS) [1]. At present, biometric systems have been adopted in various applications e.g., legal (justice and law enforcement), government (border control, aviation and health care), commercial (security, finance, smart phones, automotive industry) etc.

A typical fingerprint image possesses a pattern which contains several point features called minutiae. A minutia refers to a small detail which in the context of a fingerprint is various ways ridges tend to be discontinuous at local levels, as shown in Figure 1.1. A point at which a ridge comes to an end or divides into two ridges

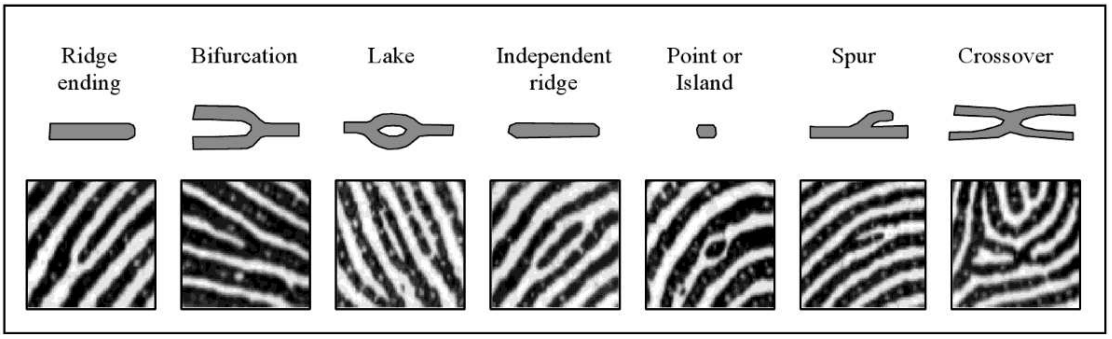

FIGURE 1.1: Most common minutiae types [1].

is called ridge ending or bifurcation, respectively. Ridge ending and bifurcation are most widely used features to represent a fingerprint pattern in biometric systems. A set of minutiae points $\mathbf{M}$ extracted from a fingerprint image can be denoted as follows:

$$\mathbf{M} = \{M_k(x_k, y_k, \theta_k, t_k)\}_{k=1}^{m} \tag{1.1}$$

where m is the total number of minutiae and x_k, y_k, θ_k and t_k represent x, y coordinates, orientation and type of kth minutia in a fingerprint, respectively.

Figure 1.2 presents a typical fingerprint recognition system with two basic processes i.e., enrollment and identification. The system uses modules like *scanner*, *feature extraction*, *template creation*, *pre-selection and matching* and *system database*. The fingerprint scanner captures the raw digital fingerprint image which

may either act as an enrollment or identification sample. The feature extraction module processes the fingerprint image and extracts a set of minutiae features. The template creation module organizes the feature set in the form of an enrolled template and stores it in the system database. The pre-selection stage is the part of a fingerprint identification system which involves the process of reducing the size of the database by selecting the potential data for matching. Consequently, the query template needs to be matched only to a small group of enrolled templates. A matcher in biometric identification takes the feature set from the query fingerprint and a set of N enrolled templates from the system database to perform matching. Unlike a biometric identification process, the biometric verification process involves matching the query feature set to only one specified enrolled template. The similarity between the query feature set and the enrolled template is computed in the form of a similarity score, also known as a matching score. A final decision which might be "identified" or "not identified" is made by comparing the similarity score with a pre-defined threshold. The system database is dedicated to storing templates and other related information about the user. The system storage for templates may be internal or external devices, or a smart card issued to the user.

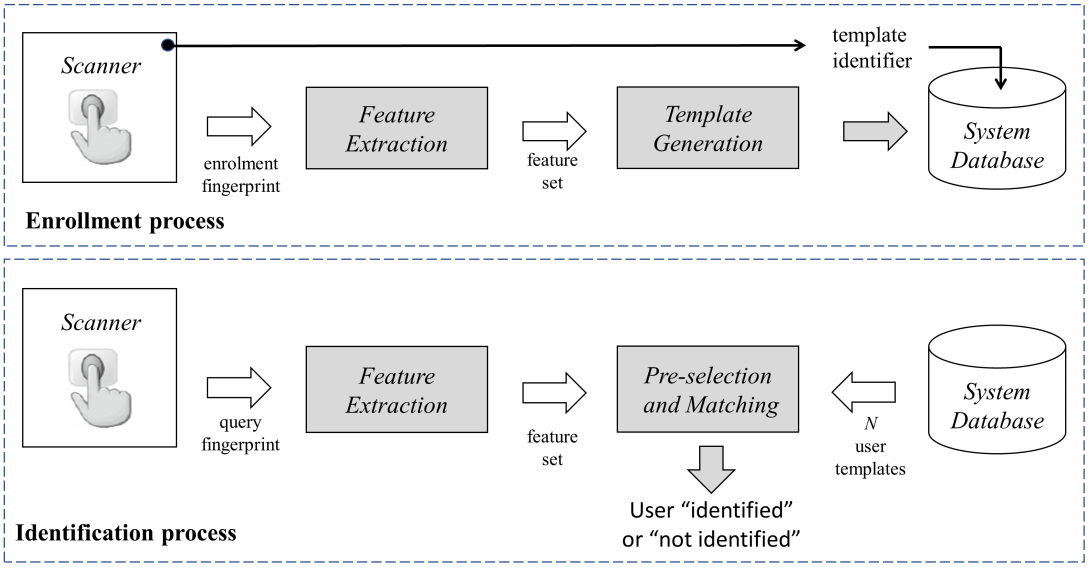

FIGURE 1.2: Enrollment and identification processes of an unsecure fingerprint recognition system (adapted from [1]).

1.2 Motivation and Objectives

Despite the significant deployability of fingerprints for biometric-based authentication systems, there are concerns related to their security and privacy [2]. For instance, if an enrolled template is stolen from the database/storage, it is lost forever and can't be reissued or replaced, unlike a stolen password or a token. Moreover, a compromised template may leak raw features which can be used to restore the fingerprint image. For instance, Cappeli et al. [3] proposed a scheme to reconstruct a fingerprint image based on a standard template. Feng and Jain [4] developed a method which uses phase image to reconstruct the whole grayscale fingerprint image. Moreover, Wang and Hu [5] developed a scheme to reconstruct a full fingerprint from a partial fingerprint. Therefore, an enrolled template in a biometric system's database is vulnerable if security measures are not taken [2].

Over the last decade, researchers have been working towards developing biometric template protection schemes to secure biometric systems. These schemes can be classified as biometric cryptosystems, cancelable templates, hybrid techniques and homomorphic encryption. The major focus of this PhD thesis is cancelable templates which are discussed in detail in Chapter 2 (along with a brief description of other schemes).

A cancelable template scheme converts the biometric features into a secured template which is stored in the database as an enrolled template. However, it is still prone to the following attacks.

- An attack via record multiplicity (ARM) allows an adversary to retrieve the original template by exploiting multiple cancelable templates obtained from same biometric features.
- A pre-image attack allows an adversary to use an inverted version of the cancelable template.

- Masquerade attacks compromise a biometric system by allowing an adversary to access with a biometric template which is very close to the original template.

The main objective of this thesis is to address the aforementioned security threats to cancelable templates.

- A novel scheme named window-shift-XOR is introduced in this thesis which helps combat the ARM attack on cancelable templates. Experiment results show that it avoids pre-image and masquerade attack threats. Furthermore, it offers superior recognition accuracy as compared to the existing methods, which is another contribution of this thesis.
- A novel random projection-based method is presented to mitigate the ARM threat with the help of the projection matrix derived from biometric features and auxiliary data.
- A lightweight fingerprint-based authentication system is developed for access control in the IoT environment which is presented in Chapter 5.

1.3 Cancelable template and its properties

First introduced in [6], [7], cancelable templates or cancelable biometrics provide protection to biometrics. Typically, a cancelable template is obtained by transforming the original template using a one-way transformation function, as shown in Figure 1.3. This transformation is usually applied in the feature domain. After transformation, instead of the original template, a cancelable template is stored in the system database as an enrolled template. Therefore, in the context of cancelable biometrics, a fundamental difference between an unsecure and a secure biometric system is that a secure system has an extra block of one-way transformation which ensures the security of the system, (Figure 1.2 and 1.3). In a case where a biometric system is protected, if a database is compromised and an

enrolled template is stolen, an adversary can't reverse engineer the cancelable template to retrieve the original template. Since a cancelable template ensures system protection, for convenience, a term protected template is used for a cancelable template and an unprotected template for the original template.

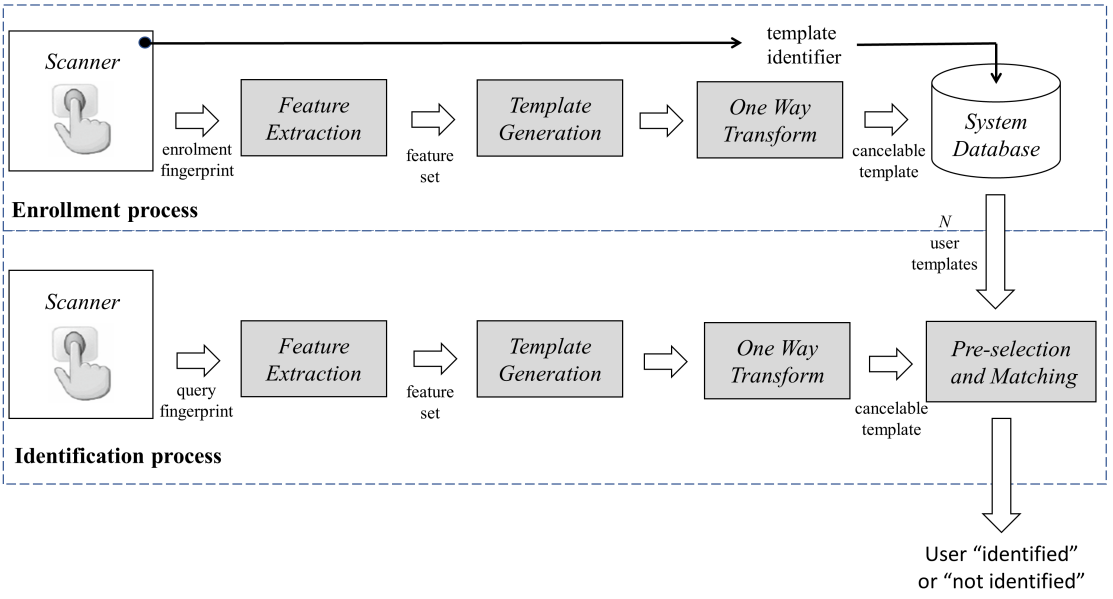

FIGURE 1.3: Enrollment and identification processes of a secure fingerprint recognition system (adapted from [1]).

An algorithm for developing cancelable templates provides the following properties:

Non-reversibility: it must be computationally infeasible to retrieve the unprotected template from the protected template using an inverse or a pseudo-inverse function. Since transformation needs to be non-reversible, fingerprint matching must be carried out in the transformed space. However, it is extremely difficult to attain high matching accuracy in the transformed domain.

Accuracy: fingerprint recognition accuracy must be preserved or smoothly degraded in transformed space. Recognition accuracy and security are two competing demands. A trade-off between the two is sometimes necessary. A well-designed transformation function needs to preserve the discriminatory features of a fingerprint as well as recognition accuracy.

Revocability: if a protected template is compromised, it must be possible to revoke it and issue a new and template as a replacement. The revocability property is a direct consequence of diversity in which numerous unrelated templates can be generated from the same fingerprint to be used in different applications. As a result of this revocability property, protected templates are known as cancelable or renewable (or private) templates.

Unlinkability: it is necessary that the protected templates produced from the same fingerprint for different applications are not able to be cross-matched [8]. Unlinkability prevents privacy invasion and its essence dictates that there should not exist a method to determine if two templates produced for two different applications have are extracted from a same fingerprint.

1.4 Performance metrics

One of the fundamental challenges associated with cancelable templates is that it comes at the expense of recognition accuracy. Therefore, we need to simultaneously determine the performance of the template protection algorithm in terms of accuracy and security. The accuracy of a fingerprint recognition system is determined in terms of its matching errors. In a secure fingerprint recognition system, the matching module provides a matching score between the enrolled template and the query template in the interval [0,1]. A score which is closer to 1 indicates that the query fingerprint came from the same finger as the enrolled template. The final decision in the form of "identified" or "not identified" is regulated by a score threshold. The term "identified" or "not identified" by the system can be interchangeably used with "accepted" or "rejected' by the system.

The matching module can commit to two types of errors: (TYPE 1) mistaking the query fingerprint and the enrolled template from two different fingers to be from the same finger, namely false acceptance, and (TYPE 2) mistaking the query fingerprint and the enrolled template from the same finger to be from different fingers , namely false rejection. Based on the false acceptance and false rejection

errors made by a system, we can measure its performance by computing the false acceptance rate (FAR) or false match rate (FMR), false rejection rate (FRR) or false non-match rate (FNMR) and equal error rate (EER).

False acceptance rate (FAR): FAR is calculated from an imposter score distribution in which a large number of scores are produced by comparing query and enrolled templates from different fingers. FAR is then the probability of TYPE 1 error and is simply calculated as the ratio of the number of false accepts to the total number of imposter attempts.

False rejection rate (FRR): FRR is calculated from a genuine score distribution in which a large number of scores are produced by comparing query and enrolled templates from the same finger. FRR is then, the probability of TYPE 2 error and is calculated as the ratio of the number of false rejects to the total number of genuine attempts.

Equal-error rate (EER): EER represents an error rate at a certain threshold t where FAR = FRR. Although EER is a good performance indicator, a biometric system rarely uses the threshold point corresponding to the EER. Often there is a stricter threshold set to achieve a desired FAR.

ZeroFMR: This is defined as the minimum FRR at which the system achieves the FAR equal to zero.

FMR1000: This is defined as the minimum FRR at which the system achieves the FAR equal to 0.1%.

1.5 Databases

To evaluate any cancelable template scheme in terms of security and accuracy, it needs to be tested on a large enough amount and variety of data. The cancelable templates proposed in this thesis have been extensively tested over maximum of five public databases, namely FVC2002 DB1, DB2 and DB3 [9] and FVC2004 DB1 and DB2 [10]. These databases contain fingerprints of varying quality with

some example images shown in Figure 1.4. Information on the five databases is

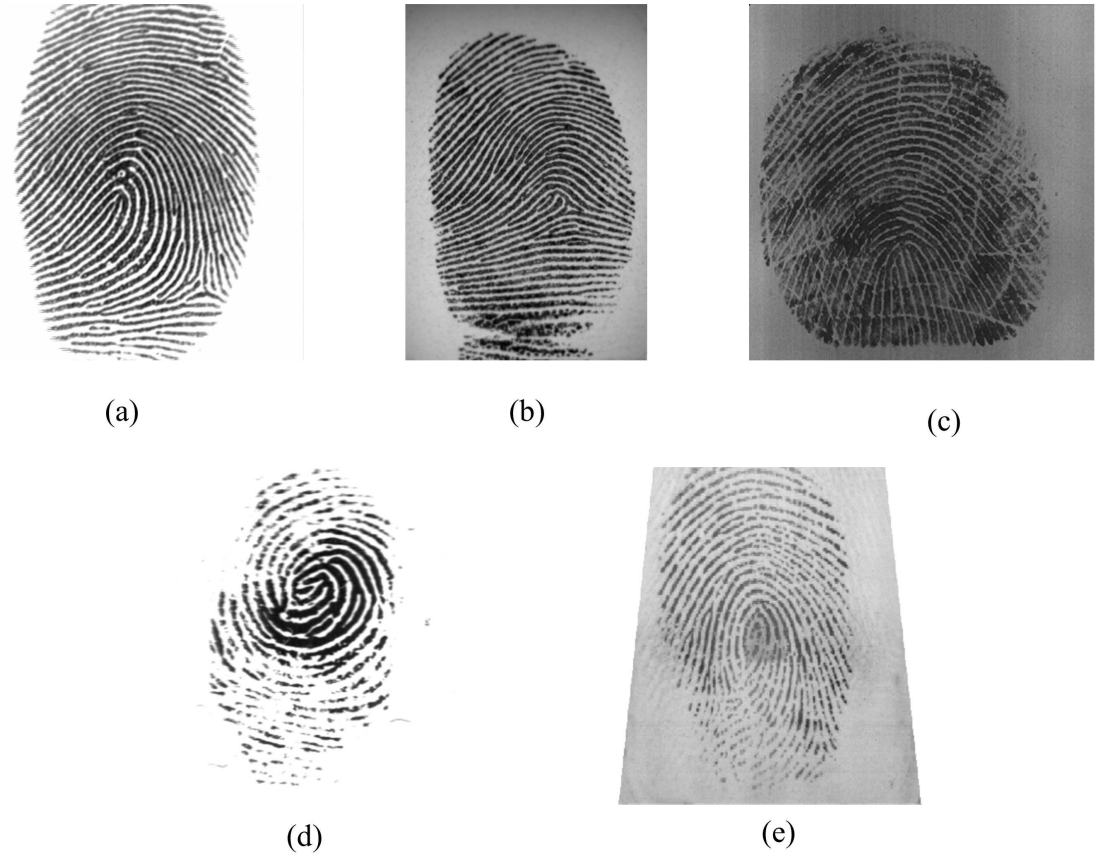

FIGURE 1.4: Example fingerprint images: (a) FVC2002DB1-Impression 2 of finger 26, (b) FVC2002DB2-Impression 2 of finger 22, (c) FVC2002DB3-Impression 1 of finger 89, (d) FVC2004DB1-Impression 2 of finger 59, (e) FVC2004DB2-Impression 2 of finger 98

summarised in Table 1.1. We employed the commercial fingerprint recognition software VeriFinger SDK [11] to extract minutia points from fingerprint images in these databases.

TABLE 1.1: Information about the databases used in our experiments.

Database	FVC2002 DB1	FVC2002 DB2	FVC2002 DB3	FVC2004 DB1	FVC2004 DB2
No. of fingers	100	100	100	100	100
Images/finger	8	8	8	8	8
Resolution	500 dpi	569 dpi	500 dpi	500 dpi	500 dpi
Sensor type	Optical	Optical	Capacitive	Optical	Optical
Image size	388×374	296×560	300×300	640×480	328×364
Image quality	Good – Medium	Medium	Medium – Low	Extremely low	Very low

1.6 Types of performance evaluation protocols

There are two protocols available to evaluate the performance of cancelable templates. These protocols are based on the method of producing the genuine score distribution. Each database (Table 1.1) has 800 fingerprint impressions from 100 different fingers and 8 impressions for each finger. We compute the imposter scores by comparing the first impression of each finger to the first impression of the other fingers in a non-redundant fashion. Hence, for each database, we essentially compute 4950 ($=\frac{100(100-1)}{2}$) imposter scores. Genuine scores, on the other hand, can be computed as follows:

1vs1 protocol: The first impression of each finger is compared to the second impression of the same finger. Since we have impressions from 100 different fingers, there are 100 genuine scores in the 1vs1 protocol.

FVC protocol: For each finger, there are 8 impressions and each impression is compared to every other impression from the same finger. Since there are 100 fingers and 8 impressions per finger, the total number of genuine scores is 2800 ($=\frac{8(8-1)}{2} \times 100$).

Fingerprint quality continues to reduce from impression 1 to impression 8 for each finger. Since we only use the first two impressions of each finger to produce genuine scores in the 1vs1 protocol, it offers better performance compared to the FVC protocol where all 8 impressions are used for genuine testing. However, the robustness of any cancelable template algorithm should reflect both protocols because only then will it verify whether the algorithm works successfully on good as well as bad quality fingerprint images.

1.7 Overview of research outcomes

This PhD thesis focuses on fingerprint template protection by introducing two new schemes for cancelable templates. Moreover, a lightweight and secure biometric system has been developed for the Internet of Things (IoT) applications.

Alignment-free cancelable fingerprint templates with dual protection

The first research contribution includes the design of alignment-free cancelable fingerprint templates with dual protection. Cancelable biometrics is an important biometric template protection technique. However, many existing cancelable fingerprint templates suffer post-transformation performance deterioration, attacks via record multiplicity (ARM), pre-image attacks and masquerade attacks. The proposed method offers two layers of protection which is achieved by the window-shift-XOR model and partial discrete wavelet transform (DWT). The former combats the ARM threat and the latter provides dual protection with enhanced recognition accuracy. Moreover, the method is extensively tested and the experiments prove the excellent security against masquerade and pre-image attacks. The designed cancelable templates meet the requirements of non-invertibility, diversity and revocability and demonstrate superior recognition accuracy, when evaluated over the public databases presented in Table 1.1.

A cancelable biometric authentication system based on feature-adaptive random projection

Random projection-based cancelable biometrics is an efficient and effective technique to achieve biometric template protection. However, existing random projection-based cancelable template design suffers from the ARM. The aim of this work is to design an intelligent random projection-based scheme for cancelable templates which can avoid this threat. The idea is based on feature-adaptive random projection, in which the projection matrixes, the key to the ARM, are generated from one basic matrix in conjunction with local feature slots. The generated projection matrixes are deleted after use to mitigate the ARM threat. Furthermore, the random projection in the proposed scheme is based on local features. This feature-adaptive random projection ensures recognition accuracy is maintained, as the error is localised to a part of the transformed feature vector and not the entire vector. The proposed method is evaluated on four public databases FVC2002 DB1-DB3 and FVC2004 DB2 and demonstrates satisfactory performance.

A lightweight and secure fingerprint authentication system for IoT devices

Energy efficiency, or the green issue of IoT devices, is a significant challenge which needs to be addressed since many of these devices have limited storage, power and computing capability. As a third research contribution, this thesis proposes a lightweight and secure fingerprint authentication system for IoT devices. The system addresses the energy efficiency issue of IoT devices by intelligently reducing the size of a fingerprint template in a robust manner, hence requiring less storage and computational power. Moreover, the proposed system offers security against the attack vectors and attack resources which may expose the raw features of a fingerprint template stored in an IoT device. The proposed system uses the state-of-the-art minutia cylinder-code (MCC) representation of fingerprints since it demonstrates a superb recognition performance. The experiment results demonstrate that the proposed system suffers almost no loss of recognition accuracy even after a significant reduction in size of an MCC template.

1.8 Thesis organisation

The thesis comprises seven Chapters, including this one. The rest of the thesis is organized as follows.

Chapter 2 presents a literature survey related to the fingerprint template protection categories and schemes. It focusses on the work related to cancelable templates and only briefly discusses the other categories.

Chapter 3 presents an idea for cancelable templates which ensures fingerprint template security at two levels. The first level of protection is designed to combat the ARM attack, which most of the existing cancelable template schemes are not able to resist. The second level is dedicated to produce cancelable templates using partial DWT. We tested the proposed method using five public databases and found that it outperforms all existing cancelable template schemes.

Chapter 4 presents a feature adaptive, random projection based approach to develop cancelable templates. Unlike traditional random projection-based approaches, the proposed method does not suffer from the ARM threat because projection matrixes are discarded after use. The security analysis and the experimental results validate the proposed method.

Chapter 5 presents a secure and light-weight fingerprint authentication system for IoT devices. The proposed system addresses the energy-efficiency issue of IoT devices i.e., limited data storage and computational capacity, by reducing the size of the binary minutia cylinder-code (MCC) templates. Moreover, the proposed method allows secure authentication with a minimal loss in the accuracy of the fingerprint system.

Chapter 6 presents a summary of the thesis.

Chapter 7 presents the possible future research directions.

1.9 A note on the contribution of the collaborators

Since the research work presented in this thesis is interdisciplinary and collaborative in nature, several researchers contributed to the completion of the work. The following section outlines the contribution of the collaborators involved.

Valuable support and guidance (both theoretically and experimentally) was always available from my supervisors, Dr Song Wang and Dr Dennis Deng and a colleague from another university, Dr Wencheng Yang (Edith Cowan University). The work in Chapters 1 and 2 represents the author's own knowledge and thoughts. Chapter 3 presents alignment-free cancelable fingerprint templates using a window-shift-XOR model and partial DWT. The window-shift-XOR model was developed and matured by the author and Dr Song Wang. DWT was proposed by Dr Dennis Deng. The experiments were carried out by the author, guided by Dr Song Wang and Dr Wencheng Yang.

Chapter 4 is related to the development of cancelable templates via feature-adaptive random projection. The idea was developed and matured by Dr Wencheng Yang and Dr Song Wang. Experiments were designed and carried out by Dr Wencheng Yang and the author.

Chapter 5 deals with the novel design of a secure and lightweight fingerprint authentication system for IoT devices. The system was designed by Dr Song Wang and Dr Wencheng Yang. The system's experimental testing for security and efficiency was carried out by the author. Dr Dennis Deng provided support for analysing the security of the system.

Chapter 2

Related work on fingerprint template protection

"The meaning of the things lies not in the things themselves, but in our attitudes to them."

– Antoine De Saint-Exupery

This chapter presents a survey of the previous works related to the fingerprint template protection (FTP). A typical FTP scheme comprises two stages i.e., feature extraction and feature protection, as shown in Figure 1.3. Since feature extraction plays a crucial a role in FTP in terms of achieving good recognition accuracy, this survey also highlights the schemes which are well-known for this purpose. With reference to feature protection, an FTP design may be categorised into four classes i.e., fingerprint cryptosystem, feature transformation (or cancelable templates), hybrid technique and homomorphic encryption, as shown in Figure 2.1. Since the main contribution of this thesis is more on FTP based on cancelable templates, we particularly focus on this category. In the first section, an overview of all FTP categories is presented and the second section includes a comprehensive survey on cancelable templates by non-invertible feature transformation.

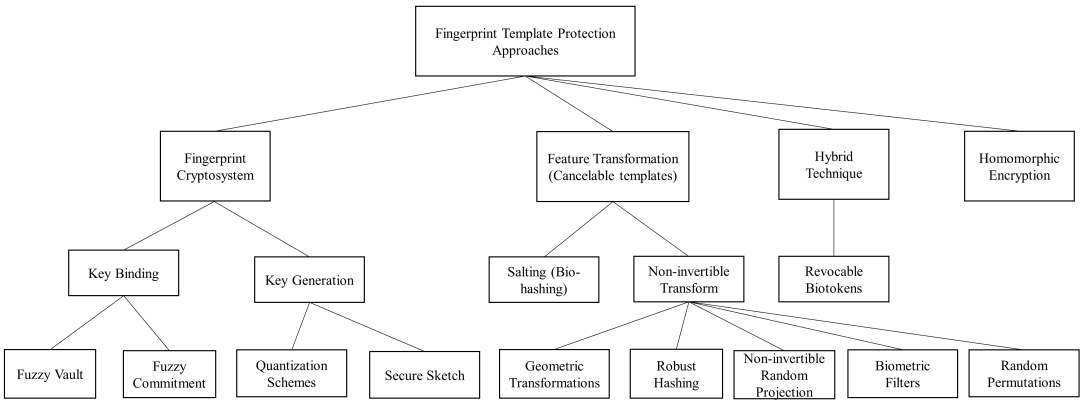

FIGURE 2.1: Classification of FTP schemes (adapted from [12]).

2.1 An overview of FTP schemes

2.1.1 Fingerprint cryptosystem (FC)

The idea of a fingerprint cryptosystem (FC) was originally developed to secure or generate a cryptographic key using fingerprint features [13]. Later, researchers found it to be useful as a protection mechanism for fingerprint and other biometric traits [14]. In this mechanism, some public information about the fingerprint template, known as helper data, is stored [15]. The helper data doesn't reveal a significant amount of information about the original fingerprint template and a cryptographic key is required to extract it and validate the query fingerprint at the matching stage. In real-life applications of a fingerprint cryptosystem, intra-user variations among different scans are inevitable and are handled by error correction coding schemes. Based on the way helper data is extracted, fingerprint cryptosystems are further divided into two categories i.e., key binding and key generation systems.

The key binding system involves the generation of the helper data free from the features of the fingerprint template [16]. It is computationally infeasible to estimate the template from the key with no knowledge of the original fingerprint data. Practically, a key binding system doesn't provide revocability and diversity in the protected templates [1]. However, some efforts have been made to induce

these two properties in the key binding systems such as fuzzy vault and fuzzy commitment.

The fuzzy vault (FV) framework was first proposed in [17] for a cryptographic construction. Since then, many researchers have used it for encrypting biometric traits including fingerprints [18–22], iris [23–30], face [31–36], retina [37] and palmprint [38–42]. The success of this technique for biometric template protection lies in its ability to handle fuzziness or uncertainty which heavily prevails in biometric data. The FV scheme manages uncertainty using Reed-Solomon (RS) error correction coding schemes [17, 18]. Fuzzy commitment is an easy and efficient scheme to protect biometric features [43]. However, constraints such as keys with low entropy and implementational difficulty in error correction coding techniques, make it less useful compared to FV. Even so, it has been used for iris [44–48], fingerprint [49, 50] and face [51, 52].

In a key generation cryptosystem, a cryptographic key is generated directly from fingerprint data [1][53]. The main drawback of this scheme is that it is extremely hard to generate keys that can preserve entropy and stability in the presence of intra-user variations in the templates [54]. Moreover, it is difficult to generate very different keys for different individuals. Nevertheless, it has been used for encrypting biometrics [55] such as fingerprint [56, 57], face [58, 59], iris [60–62], voice [63] and palm vein [64].

2.1.2 Feature transformation

In this category of FTP, a transformation function, characterized by a user-specific key, is used to transform the fingerprint features. At the matching stage, a query fingerprint follows the same transformation process and matching occurs in transformed space. Feature transformation can be divided into two types i.e., salting and non-invertible transformation. In salting, an unprotected template is transformed by a function defined by an external/user-specific key. Salting has several advantages like low false accept rates and its tendency to generate multiple secured

templates using multiple user-defined keys. However, it isn't robust and its recognition performance is deteriorated due to the presence of intra-user variations. Furthermore, if the key is revealed, one can apply the inverse transformation and retrieve the original features, which is the major limitation of this method [1].

The security issue in salting is addressed by the non-invertible or one way transformation. The transformation function is characterized by a key which should be presented when authentication has to be undertaken [14]. If the key is compromised, it is still computationally infeasible to invert the transformed template which is its main advantage over salting. Moreover, non-invertible transformation provides revocability and diversity to the transformed templates. However, robustness still depends on the trade-off between non-invertibility and the discriminability of the transformation.

2.1.3 Hybrid technique and homomorphic encryption

The hybrid technique for FTP uses a combined approach of feature transformation and the fingerprint cryptosystem. Ong et al. [65] developed secure fingerprints using salting with a key binding approach combined with the use of traditional cryptographic hashing functions. Nandakumar et al. [66] used a key binding salting approach combined with a fuzzy vault with a user-specific password. The last category called the homomorphic encryption allows calculation on the encrypted data. It combines homomorphic encryption with a fingerprint recognition system [67]. Rane et al. [68] presented a hamming distance calculation for their FTP scheme. Moreover, Barni et al. [69] developed a cryptosystem-based distributed biometric system to protect the privacy of the fingerprint template.

More recently, a fixed-length fingerprint representation of only 200 bytes, named DeepPrint [70], demonstrated superior authentication accuracy in the encrypted domain using fully homomorphic encryption. Given the importance of fingerprint feature extraction and representation in the scheme of things, this novel, compact fingerprint representation lays a great foundation for the future development of

fingerprint template protection methods. In addition, homomorphic encryption is worthy of further study to determine how to apply it to fingerprint matching with protected (transformed) templates.

2.2 Cancelable templates by non-invertible feature transformation

In recent years, significant effort has been made towards developing cancelable templates using non-invertible transformation. We shall not only discuss the available feature transformation methods but also the feature extraction approaches which contribute significantly to improving the efficiency of an FTP project. Cancelable templates can be divided into two categories namely registration-based and registration-free templates. In registration-based approaches, the accurate detection of the singular points (core and delta) is needed prior to the transformation [71]. For this purpose, there are several approaches available [71–74]. However, the accurate detection of singular points still remains a challenge which leads to poor recognition accuracy in registration-based cancelable templates.

To mitigate the effects of pre-registration and to better cope with local distortions, registration-free or alignment-free cancelable templates have gained a new research potential in recent years. As pre-registration of the fingerprint image isn't needed in this category, it makes the process computationally light and robust to non-linear distortion. In the following section, we discuss types of cancelable templates based on the different types of non-invertible transformation available.

2.2.1 Geometric transformation

In their pioneering work on cancelabale templates, Ratha et al. [75] proposed registration-based templates using geometric, non-invertible transformation functions namely cartesian, polar and functional. The key idea is to transform the

minutiae features in such a way that a minutia matcher can still be used in transformed domain. In cartesian transformation, a fingerprint image in minutiae space is tessellated into a rectangular grid and minutiae positions are measured with reference to the position of the singular point. All cells in the grid are then translated according to the new positions set by the user key as shown in Figure 2.2. All the minutiae within the cells retain their relative locations even after key-based repositioning and yet it is impossible to retrieve the original position of the minutiae.

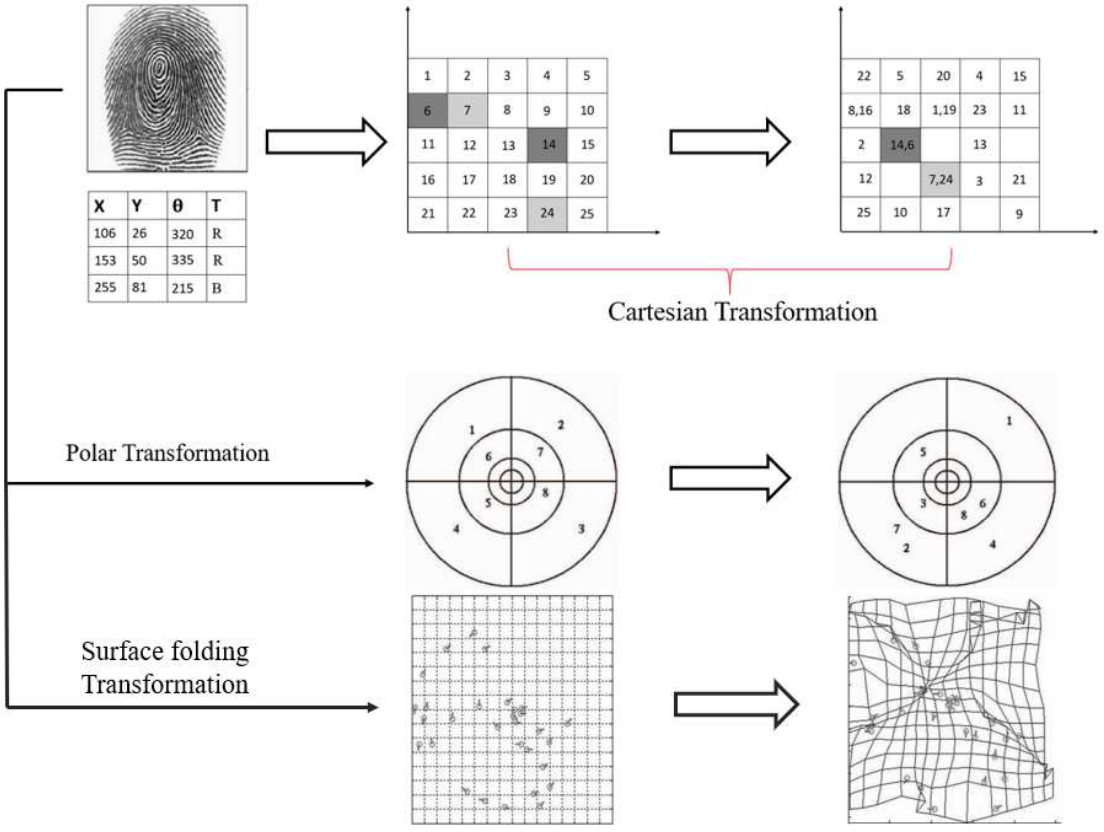

FIGURE 2.2: Ratha et al.'s [75] geometrical transformation approach using cartesian, polar and functional transformation (reproduced from [75]).

The polar transformation is similar to the cartesian transformation except that the minutiae space is now translated into a polar space with reference to the core position. In this process, polar space is divided into polar sectors and numbered as depicted in Figure 2.2. Since the size of the sectors near the centre are smaller than the sectors far from the centre, transformation is performed using a controlled

key in order to retain consistency in the radial distance between the transformed sector and the original position of the sector.

In cartesian and polar transformation, a small change in the minutia position in the original fingerprint may amplify this change after transformation. This leads to the greater intra-user variation at the matching stage and hence reduces matching accuracy. To address this issue and to achieve high performance, a smooth yet non-invertible transformation function is used. The parametric form of this transformation function is governed by a random key and involves several constraints in order to achieve cancelability. For instance, the function should offer a locally smooth transformation such that small changes in the minutia position before transformation do not introduce a large change in the minutia position after transformation. Moreover, minutiae positions before and after transformation should not be highly correlated which otherwise may lead to easy invertibility. In other words, transformation should only provide local smoothing and not global smoothing so that the discriminability of the minutiae is largely preserved to avoid invertibility.

Inspired by [75], Yang et al. [76] proposed a scheme for registration-based revocable fingerprint templates using non-invertible geometrical transformation. In this algorithm, an original minutiae-based template is mapped to a protected coordinate-based template by a combination of parameter-controlled, linear and non-linear transformation. Compared to the geometric transformation in [75] in which large error rates are caused if the coordinates themselves are deeply distorted, the proposed method takes advantage of both linear and non-linear geometrical transformation to achieve desirable matching performance and high non-invertibility.

In [77], Lee et al. proposed alignment-free cancelable templates using local minutiae information. In this scheme, a feature vector which is invariant to rotation and translation is extracted from each minutia using the orientation information within its neighbouring region and a user-specific random vector. The invariant feature vector is based on a similar idea as that in [78] and [79]. The neighbouring

region corresponding to each minutia is in the form of concentric circles around it with a fixed number of sampling points on each circle, ordered counter clockwise. The local orientation for the region is estimated at each sampling point using a gradient-based approach [80] which yields the feature vector. An invariant value to a corresponding feature vector is computed as the inner product of the normalized invariant feature vector and the normalized user-specific random vector. In order to generate a cancelable template, a movement or transformation to each minutia is provided by using two changing functions namely the distance changing function and the orientation changing function which uses the invariant value as an input. The changing functions are user defined and can be replaced with new ones in order to revoke a compromised template. The proposed method offers reasonable security because it is extremely difficult to retrieve the original data from the transformed template even if an attacker knows the transformed template as well as the transformation method. However, the proposed algorithm doesn't perform well for poor quality fingerprint images which is a major drawback.

Yang et al. [81] proposed parametrized geometric alignment in order to generate cancelable templates. This algorithm involves the transformation of the original minutia vicinity into a geometrically-aligned and secured minutia vicinity controlled by randomly generated parameters. Minutia vicinity refers to the minutia itself together with some nearest minutiae in the neighbourhood. Unlike conventional geometric alignment, this algorithm doesn't need the core or delta as a geometric reference. The algorithm demonstrates a reasonable resistance against brute-force attack, template inversion attack and linking attack. This work is extended in [82] in which Yang et al. proposed a binary representation of the protected diversified minutia vicinities. The binary version of the minutia vicinity-based protected template requires less storage compared to its unsecured counterparts. Template revocability and diversity is achieved by choosing different parameters for all minutiae vicinities.

Exploiting the excellent stability of the Delaunay triangle-based local structure, Yang et al. [83] proposed an alignment-free cancelable template. The Delaunay

triangle-based local structure is generated predicated on the Delaunay triangulation net. In order to implement the design, a Voronoi diagram is generated which divides the entire fingerprint region into several small cells so that each cell has a minutia located in the centre of the cell. The Delaunay triangulation net is then constructed by joining the centres of every cell and its neighbouring cells. Delaunay triangles that share a common vertex constitute the local structure. The central minutia in the Delaunay-triangle based local structure acts as an origin of a polar space with a 0-degree axis along its orientation.

For all the triangles in the local structure, several features can be computed, such as the distance between the vertices, the angle between the 0-degree axis and the vertices, and the differences between the orientations of the vertices. These features are translation- and rotation-invariant and need protection against various attacks. The feature vector is concealed by applying a non-invertible transformation as proposed by Ratha et al. [75] in polar coordinates. The polar transformation is applied to every triangle in the local structure by changing their positions through transformation matrices. The union of the transformation matrices acts as a secrete key so if the transformed template is compromised, it can be re-issued to generate a new template.

2.2.2 Biometric filters

Hirata et al. [84] introduced a novel method for cancelable biometrics for correlation-based matching. In this method, a biometric image is first transformed using number theoretic transform i.e., a Fourier like transform computed over a finite space. Transformation is followed by a random filter process to mask the transformed data. Correlation is now computed between the registered image and the input matching image in the masked domain. The masking process efficiently hides the transformed features to ensure secrecy and non-invertibility. By varying the random filter, the revocation of the template is achieved.

Following from [84], Takahashi et al. [85], developed registration-based cancelable fingerprint templates based on the chip matching algorithm and correlation-invariant random filtering (CIRF). It offers two versions of cancelable templates i.e., a basic version and a minutiae hiding version. In the basic version, a parameter contains the original minutiae coordinates, which, if compromised, may risk the privacy. To address this privacy issue, the minutiae hiding version conceals the original minutiae by adding chaff points. Both versions, however, provide foolproof security in terms of the irreversibility of the cancelable templates.

2.2.3 Non-invertible random projection

In this category of cancelable templates, fingerprint features are secured using user-defined random projection. In the realm of random projection-based cancelable biometrics, Biohashing is one of the well-known methods, initiated by Teoh et al. [86]. It exploits a function defined by user-specific key to transform the biomteric features. In this method, the authors devised a user-specific random projection algorithm and a discretization process to generate a binary vector, leading to a cancelable template. Specifically, given a feature vector Γ which is extracted from a biometric image, e.g., fingerprint, a user-specific transformation matrix r is randomly generated, associated with a USB token or smartcard. The matrix r is further processed to be an orthonormal matrix r' by applying the Gram-Schmidt process. Then the inner product of the feature vector Γ and matrix r' is computed, i.e., $x = r'\Gamma$. The resultant vector x is quantized into binary values of $b_i = 1$, if $x \geq t$, and $b_i = 0$, if $x < t$, where t is a predefined threshold, usually set to 0. Teoh et al. [87] made more improvements to the original BioHashing scheme using random multispace quantization (RMQ) which extends the single random subspace formulation to multiple subspaces. The information content and robustness of the generated template are increased by RMQ. Biohashing-based transformation becomes invertible if user-specific the key is compromised. However, most of the recent random projection-based cancelable tamplates are non-invertible even if the user-specific key is compromised.

Pillai et al. [88] proposed sector-based random projection to overcome the issue of varying quality in different parts of an iris. The low-quality region tends to corrupt the data of the good-quality region if random projection is applied to the whole iris image. By dividing the iris into many sectors and applying random projection to each sector separately, the negative effect of the low-quality region is restricted locally. Pillai et al. [89] introduced an iris recognition framework based on random projection and sparse representation. Random projection together with random permutation is employed to enable revocability, while sparse representation is used for iris image selection. Since the dimension reduction by means of projection makes an underdetermined system, even if the projection matrix, i.e., the key, and the transformed template are stolen, it is computationally infeasible for the hacker to retrieve the original fingerprint features.

Jin et al. [90] developed a cancelable fingerprint template based on two-dimensional random projection using a minutia local structure called minutia vicinity decomposition (MVD). The MVD features is represented by a matrix of size $N \times 36$, where N is the number of minutia vicinity extracted from a fingerprint sample. A projection matrix with pseudo-random numbers is generated and converted into an orthonormal projection matrix by using Gram–Schmidt orthogonalization. A dimension-reduced transformation matrix obtained from this orthonormal matrix via a user-defined key is exploited to transform the MVD feature matrix. This transformation is non-invertible even if the user key is compromised. Moreover, the transformed template is made cancelable by using a transformation matrix produced with a different user key.

Chikkerur et al. [91] presented alignment-free cancelable templates based on localized, self-aligned texture features in contrast to the global texture descriptor in the registration based method [86]. This paper also demonstrates that purely local measurements are sufficient for alignment-free templates and pre-registration isn't always a strict requirement. The development of cancelable templates is achieved in two stages. In the first stage, a localized texture-based scheme is used to represent a fingerprint and to perform enrolment. It implies that instead of using a

minutiae-based template, a fixed size pixel patch is extracted around each minutia and the orientation of the patch is aligned with that of the minutia.

In practice, each patch carries unique information about the unique identity of the individual and common patches exhibit identical information. Only a few patches that show a strong association are used during the matching for verification purposes. The texture of each patch is encoded using a robust compact signature vector, which is immune against the effects of intra-user variation and noise. Cancelable templates are developed on top of the minutia signature using a user-specific projection matrix. In order to make the transformation non-invertible, non-linearities are introduced as proposed in [75].

In [92] Yang et al. proposed a non-invertible transform for generating secure cancelable fingerprint templates using local and global features. The implementation scheme starts with feature extraction in which local features such as the distances between any two neighbouring minutiae and their relative angles are computed and projected perpendicularly to the circle centred around the core. The projection radius can be controlled by a secret key which, as long as hidden, makes the process irreversible. These local features are robust to the non-linear and geometric distortion that may occur during fingerprint acquisition. Since multiple minutiae pairs can be mapped at the same points in the circle, it makes the scheme irreversible.

The computation of local features is not restricted to the use of pair minutiae and may be extended to minutiae triangular features. In order to consolidate the scheme by preserving the high correlation among intra-users, global features such as orientation, ridge frequency and the total number of minutiae of the blocks sampled along a line are used. Finally, a cancelable template is generated by bin-based quantization using a predefined number of bins. The quantization of all local and global features follows the same procedure and fused at the end of the process. The security of the proposed algorithm is assured by parametric feature extraction and bin-based quantization.

Template protection by means of random projection achieves good diversification but is prone to lost-key attacks, as noted in [93], in which a two-factor cancelable formulation is made using multispace random projections. Moreover, random projections are linear operations that preserve the distance very well and cause a security threat. In order to address these security concerns, Yang et al. [94] proposed a dynamic random projection based method which adds an extra computational cost to the search for unprotected features. In this method, a random matrix is dynamically constructed for projections instead of using a fixed random matrix. To achieve dynamic random matrices, several random vector slots are made public with each slot containing multidimensional random real-valued vectors. From each slot, one of the random vectors is chosen for projecting the biometric features so that an attacker has no clue which random vector out of many in a slot is chosen for projection.

In [95], Ahmad et al. proposed a design for registration-free cancelable templates in a pair-polar coordinate space. This scheme uses the localised features, such as position of a minutia relative to the positions of the other minutiae in the polar coordinate space. Only those minutiae points whose distance is greater than a specified threshold are chosen for the feature generation. For each pair of the selected minutiae, three localized features are computed which are, the radial distance between the reference and the neighbouring minutia, the angle between the orientation of the reference minutia and the line segment connecting the pair, and the angle between the orientation of the neighbouring minutia and the line segment. The pre-transformed template is produced putting all local features corresponding to all reference minutiae in a vector form. In order to perform the transformation, the polar space is divided into several sectors similar to [75] and mapped to random positions based on a user-defined random vector. This scheme offers many-to-one mapping hence making the transformation non-invertible. Based on the pair-polar coordinate space [95] and the Delaunay triangulation-based net [83], Yang et al. [96] proposed mobile template protection which offers relatively high recognition accuracy.

Wang et al. [97] proposed a mathematical model for developing alignment-free cancelable templates based on densely infinite-to-one mapping (DITOM). The scheme starts with the binary template generation from a minutiae-based fingerprint using the method in [98]. A binary template is first converted into frequency domain samples using discrete Fourier transform (DFT) and then cancelable templates are generated using infinite-to-one mapping from a line, a plane or a hyperplane. A simple but a representative example for a line, a plane and a hyperplane is provided in Figure 2.3. In the paper, the implementation is made as a linear parametric

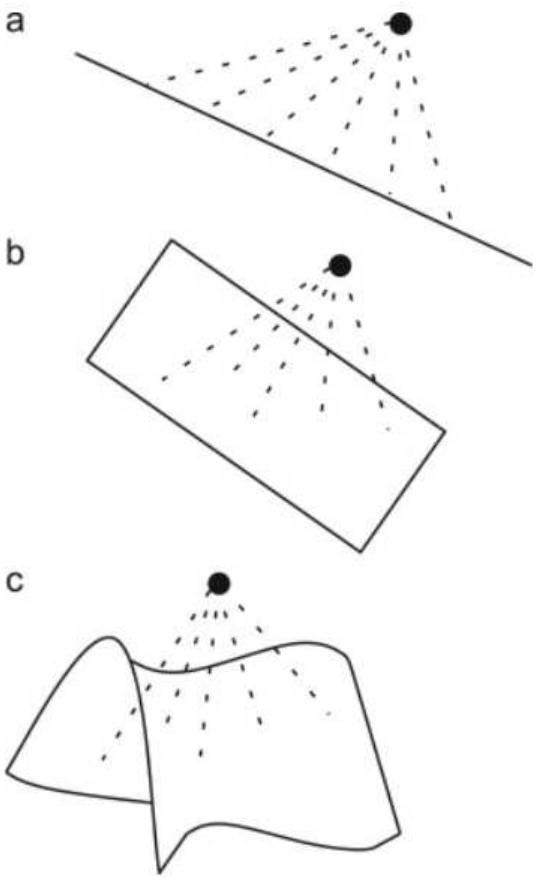

FIGURE 2.3: Infinite-to-one mapping from a line, a plane and a hyperplane[97].

transformation in algebraic domain. The transformation is achieved by the multiplication of the matrix with the complex-valued raw feature vector resulting in the complex-valued cancelable template. The matrix in this transformation plays the role of the randomly generated parametric key. So, a compromised template can be revoked and a new one can be generated using a different key.

In [99], Jin et al. proposed a randomized graph-based hamming embedding (RGHE) to produce cancelable templates. The algorithm follows the construction of a set of the minutiae vicinity that reports the nearest neighbourhood in Euclidean space. Inspired by [100], the minutiae vicinity for a reference minutia is constituted by the three nearest neighbours (minutiae). However, a local structure corresponding to this form of minutia vicinity becomes unstable as a result of the distortion added by missing or spurious minutia. The issue is addressed by decomposing the minutia vicinity into four triplets, in which case, if one triplet is distorted by a missing or spurious minutia, the other three are still stable. Multiple robust and invariant features are computed from each triplet in the minutia vicinity structure.

Most prominent features related to a triplet are the length of the sides, the angle between the sides and the minutia orientation, the internal angles of the triplet etc. A feature representation is formed by accumulating all features of all local minutia vicinity structures into a matrix. Cancelability is achieved by randomizing minutia vicinity decomposition (RMVD), in which a feature matrix is transformed by a random projection as initiated in [86]. A user-specific minutia vicinities collection (UMVC) produces a stable set of features corresponding to user-specific local structures by making multiple use of training samples for each individual. A binary implementation corresponding to RMVD features is achieved by a graph based hamming embedding (GHE).

Wang et al. [101][102] proposed alignment-free cancelable templates using partial Hadamard transform. It uses the Hadamard matrix which is created in a recursive manner. The Hadamard matrix has some interesting properties such as: all entries in it are either +1 or -1 and it is symmetric and orthogonal. The property of the Hadamard matrix being made up of only ± 1 makes the transformation computationally efficient as it involves only additions and subtractions. The proposed transformation is partial Hadamard-based because a column rank-deficient submatrix derived from a full order Hadamard matrix is used for transformation. The submatrix doesn't have an inverse or pseudo-inverse because it is derived from an orthogonal matrix, which makes the transformation non-invertible. In order to

obtain a rank deficient Hadamard matrix, a user specified random key is used that selects only the specific rows from the full order Hadamard matrix. The proposed model uses the binary strings' frequency domain samples, represented as a complex valued vector, as detailed in [97]. The complex vector, when transformed using the rank deficient Hadamard matrix, yields a transformed template in a complex domain. The partial Hadamard transform has a property of stochastic distance preservation which ensures the satisfactory performance in the lost token scenario. Another benefit of the proposed method is that the transformation matrix does not need to be stored in the database or the smart card and it can be readily constructed from the full order Hadamard matrix using the parameter key.

Jindal et al. [103] protected face templates using the deep convolutional neural network (CNN) with random projection. A feature vector is first extracted from each face image with a pre-trained Visual Geometry Group (VGG)-Face CNN. Then the extracted feature vector is transformed using random projection, which reduces its dimension from 4096 to 1599. In this way, redundancy in the feature vector can be removed. Meanwhile, the proposed random projection acts as a cancelable transformation.

2.2.4 Robust hashing

These methods offer fingerprint template protection by applying non-invertible transformation using hash functions. A hash function takes a minutia point as input and returns a hash value which is stored in the database. Non-invertibility is achieved by keeping the number of hash functions less than the number of minutiae in the fingerprint.

With no requirement of pre-registration, Tulyakov et al. [104] developed symmetric hash functions for secure fingerprint biometric systems. Missing or spurious information or a change in the order of the input pattern may lead to a significant change in the hash value. This special class of hash functions, known as symmetric hash functions, are invariant to the order of the input pattern. In

the proposed method, matching is performed only on the localized minutia sets. Global matching is achieved as a collection of the local matchings with identical transformation parameters. During matching, all localized sets corresponding to the query pattern are compared with all the localized sets in the stored pattern, and the matches with the highest confidence are retained to produce a composite match score. A compromised template can simply be revoked by using randomly generated hash functions based on the user key. This method can also be generalized for other biometric modalities in which locations of certain image artefacts are used as primary features.

In an extension to the cancelable templates based on symmetric hash functions in [104], Kumar et al. [105] proposed the use of a combination of symmetric hash functions to enhance security against brute force attacks and also retain a reasonable performance.

Jin et al. [106] proposed two factor cancelable biometrics and named it the Index-of-Max (IoM) hashing. IoM hashing uses external random parameters and transforms the biometric features (real valued) into hash codes with a discrete index. In this paper, the authors demonstrated two realizations from the notion of IoM hashing based on Gaussian random projection and uniform random permutation. IoM hashing has merits such as strong non-invertibility and robustness to translational and rotational variations. Furthermore, the scale-invariance of hash codes aids in feature alignment and matching. If the transformed template is compromised, a new token-based seed is generated for random permutation to produce new transformed template which automatically revokes the compromised template.

Based on IoM hashing, Kim and Toeh [107] proposed a sparse combined Index-of-Max hashing (SC-IoM). This scheme produces two-set hash vectors (integer-valued) which are further transformed via a probabilistic many-to-one function. In the end, two binary vectors are combined to produce a single and compact sparse binary vector. Both schemes [106][107] demonstrate good recognition performance and meet the revocability and unlinkability criteria.

Abdullahi et al. [108] exploited the Fourier-Mellin transform and the fractal coding to generate a robust and secure hash from a fingerprint. The proposed scheme makes use of the Fourier-Mellin transform for feature alignment and produces a fixed-length minutiae representation. Then, fractal coding is used to exploit texture compression and dimensionality reduction to generate a compact and robust hash for improved recognition and security. The proposed scheme fulfils the revocability and difficult unlinkability criteria with a satisfactory recognition performance.

2.2.5 Random permutations

Random permutation, which is mostly applied to binary templates, exploits user-defined random keys to achieve cancelable templates. Farooq et al. [109] proposed several techniques to create cancelable templates using binary string representations. In the proposed scheme, a minutiae based fingerprint is first represented as a binary template and is then transformed into an anonymous representation using a unique personal key. In order to determine the bit-based representation, the invariant features of minutiae triplets are used inspired by the early work of Germain et al. [110].

An example of a minutiae triplet and the features drawn from it are shown in Figure 2.4. Even under the grid transformation, the geometry of the triangle doesn't change which makes the transformation robust. From the minutiae triplets, multiple translation and rotation invariant features are computed in the form of a vector. It comprises the length of the sides, the angles between the minutiae orientation and the sides, triangle height, triangle handedness, ridge count between the sides etc. These features are more stable and easier to compute. Each invariant feature in the feature vector is quantized using the appropriate step sizes in a way that is neither too coarse so that it loses its discriminative power nor too fine as it is sensitive to slight distortions. Finally, quantized features are converted to binary numbers using an appropriate number of bits.

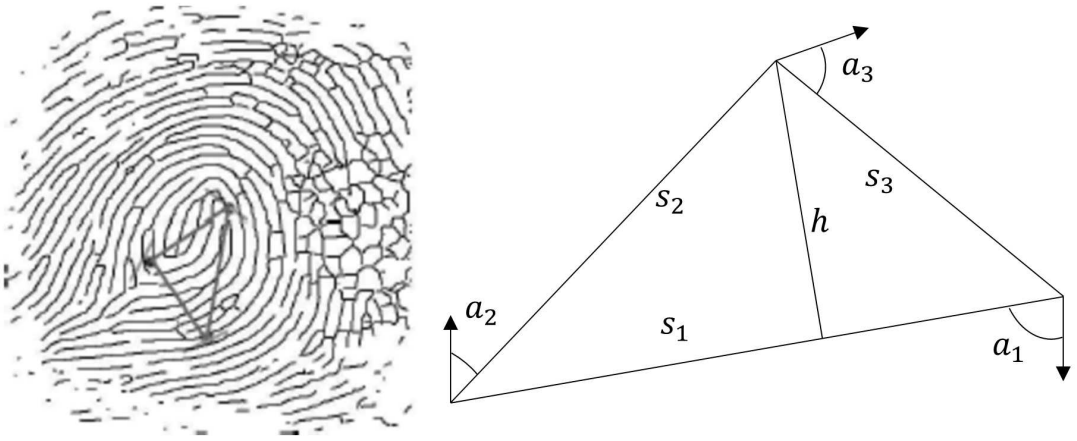

FIGURE 2.4: An example of minutiae triplet (left). Invariant features from the minutiae triplet (right) (reproduced from [109])

Once binary vectors are acquired from the minutiae-based fingerprints, a number of operations similar to the standard genetic algorithm can be performed to generate cancelable templates. One of the available operations is known as mutation in which a binary vector is mutated randomly. Using an empirically established threshold and random probability, each 0 bit is set 1 and vice versa. Another operation, known as randomization, uses a randomly generated user key to permute the binary feature vector. Key selection introduces diversity and revocability in the method. It is worth noting that a bit-based implementation of this method makes it computationally feasible at the matching stage.

In [111], Jin et al. proposed random triangle hashing-based alignment-free cancelable templates in binary format. In this method, all minutiae points in a fingerprint are first translated with reference to a selected minutia. Based on the principle of random triangle hashing, a hash string is constructed by counting the number of minutiae in the random triangular regions. Randomness of the triangular regions is achieved by a secret key which identifies the location of the three vertices. In each triangular region, based on the orientation of each minutia, the number of minutiae falling in the pre-defined orientation range are counted. If no minutia is observed with an orientation that can fit in a certain range, the minutiae count for that range is zero. The process is repeated for all triangular regions and a hash (integer) vector is constructed in which each number represents a minutia

count in a particular orientation range. The hash integer vector is binarized using a bit block coding operation. A compromised template can be revoked by using a different key with new index locations.

Jin et al. [98], [112] proposed cancelable templates using localized binary features based on minutiae pairs. The scheme is initiated with the computation of translation and rotation invariant features in the binary format from the minutiae pairs. After this, a key specific transformation is applied to the binary features to produce non-invertible and cancelable templates. The invariant features attached to a pair are the distance between two minutiae, the angle between the orientation of two minutiae, the angles between the orientation of each minutia and the line segment connecting them. After computation, these invariant features are quantized using the appropriate step sizes. Another purpose of performing quantization is to decrease the effect of distortion induced during fingerprint acquisition. The next crucial step is to convert all the quantized features into a binary number by choosing an appropriate number of bits for each feature. Altogether, if N bits are required to binarize all features, there are 2^N bins with first bin made up of N zeros and last bin made up of N ones. A binary feature vector is initialized with a zero vector of length 2^N. We inspect each binary number i.e., computed from a quantized one, and index a bin by one in the binary feature vector. It is likely that some bins are indexed multiple times which are made zero in order to remove the redundant features and to make sure that the feature vector strictly stays binary. However, this binary feature vector is vulnerable as an adversary can use it to access the associated biometric system [113]. In [113], a cancelable template is constructed in binary format using 3-tuple quantization based on a polar grid. In [98], [112] and [113] the resultant binary vector is permuted with a user-specific key. However, if the key is exposed, the quantized minutiae positions are vulnerable.

In [114], Lee et al. proposed bit-string based alignment-free cancelable templates. The bit-based implementation is mainly performed by mapping all the minutiae points into a predefined 3-dimensional cell array. The array is inspected to locate the cells which contain the minutiae. In order to perform this operation, all the

minutiae in the fingerprint are translated and rotated to get mapped into the cells based on the position and the orientation of one reference minutia. Cells with more than one minutia in it are set to one and 0 otherwise. A bit string is generated by sequentially arranging all the cells in the 3D array. Once the bit string is achieved, cancelable templates are achieved by permutation based on the type of reference minutia and the user's PIN.

A multiline code (MLC)-based template protection scheme is proposed by Wong et al. [115] which is deployed on minutiae-based fingerprints, like other conventional methods. To ensure robustness, the scheme requires a descent minutiae extraction process before applying the transformation. The minutiae extraction process consists of six stages which are segmentation, orientation field estimation, contextual filtering, binarization, thinning and minutiae detection. In the proposed scheme, a straight line is drawn passing through and centred at a reference minutia in the direction of the orientation of the minutia. On the line, equi-distant sample points are marked. For each sample point, a circular bit-wise mask is applied to obtain the number of minutiae within the area in different angular partitions. The relative angle between the orientation of the reference minutia and that of the neighbouring minutia provides an angular partition in which a minutia falls.

A real valued line code for the reference minutia is formed by sequentially arranging all minutiae that fall in the overlapping cylinder. At the end of the process, an MLC is obtained by stacking up all the individual line codes that represent an unprotected fingerprint template. This multiline code is secured by applying a simple permutation based on a user-specific random key. Although MLC provides non-invertible implementation, it requires large storage compared to binary code. This limitation is addressed in [116] in which Wong et al. generated a binary MLC. A loss of accuracy caused as a result of the generation of binary MLC is compensated by an enhanced similarity measure called dynamically weighted integrated dice similarity.

Performance preservation is a big challenge in the process of developing cancelable templates. This challenge is somehow addressed in [117] in which Kho et

al. proposed a cancelable template design for fingerprints with randomized non-negative least squares. The structure of the proposed model consists of three stages, namely training, enrollment and verification. From each minutia and its neighbourhood, a partial local structure (PLS) is derived during enrollment which is essentially a collection of direction-based partial structure map (DPSM) vectors. A non-invertible transformation to PLS descriptors is formulated by solving the permuted randomised non-negative least square (PR-NNLS) optimization problem. DPSM vectors act as training data for PR-NNLS which is essentially a least-squares regression problem. Permutation is achieved by a user key which is used to introduce revocability and diversity. The proposed method exhibits good security and excellent recognition accuracy for good as well as poor quality fingerprint images. However, matching the two cancelable templates is a complex and computationally expensive process.

2.2.6 Non-invertible transformation functions

Wang et al. [118] proposed a design for alignment-free cancelable templates via curtailed circular convolution. Two sequences of finite duration with lengths M and N, such that $N < M$, when convolved via linear convolution or augmented circular convolution, produces a resultant sequence with length $M + N - 1$. With the knowledge of one sequence and the resultant sequence, the other sequence can be reverse engineered. However, if implemented in a suppressed fashion, M point circular convolution, with a resultant length M, makes the process non-invertible because the first $N - 1$ points in the resultant are corrupted by aliasing.

Circular convolution when applied in a suppressed fashion is called curtailed circular convolution and is used to generate cancelable templates. A binary feature string of length p is extracted from the fingerprint using the scheme in [98] and convolved with another randomly generated finite-duration sequence on length q such that $q < p$. The length of the resultant vector is p and acts as a transformed template. The first $q-1$ entries in the transformed template are corrupted by aliasing, ensuring the security of the transformation even if an adversary has knowledge of

the transformed template and the randomly generated sequence. A compromised template can be replaced by a new template generated using another user defined random sequence. The design is implemented using p-point fast Fourier transform (FFT) which makes the implementation computationally efficient.

Ferrara et al. [119] developed alignment-free revocable templates based on the Minutia Cylinder Code (MCC) [120]. MCC is a state-of-the-art local minutia representation based on 3D structures called cylinders. Cylinders are created by using only the position and the orientation of the minutiae. A cylinder with radius R and height 2π is created with the base centred at the reference minutia location in the direction of minutia orientation. The cylinder is enclosed inside a cuboid which is discretized into $N_C = N_S \times N_S \times N_D$ cells. Figure 2.5 shows a graphical representation of the cylinder associated with a reference minutia in which the cuboid is rotated so that axis i is aligned to the direction of the corresponding minutia. Each cell represents a small cuboid with a base of size $\Delta_S \times \Delta_S$ and height Δ_D where $\Delta_S = \frac{2.R}{N_S}$ and $\Delta_D = \frac{2\pi}{N_D}$. For each cell, a numerical value

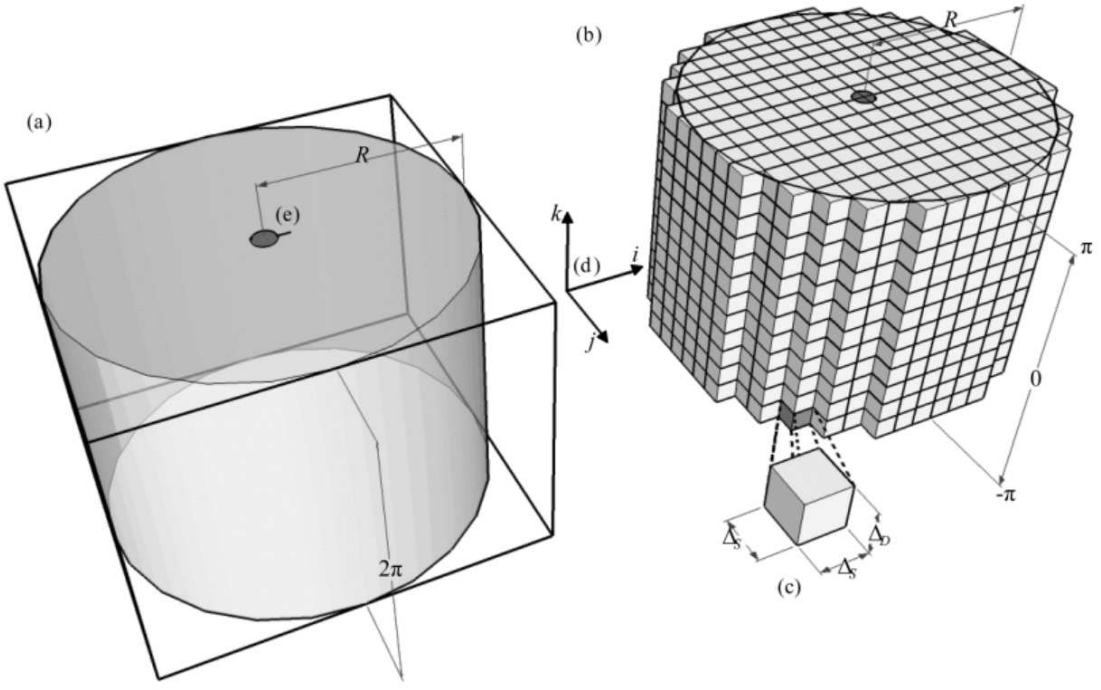

FIGURE 2.5: (a) The cylinder with the enclosing cuboid (b) Discretization of the cuboid into cells [120].

is calculated by acquiring an accumulative contribution from each minutia in its

neighbourhood. The accumulative contribution includes a spatial and directional contribution from the neighbouring minutia. In order to limit the contribution of the dense minutiae clusters, each cell value is constrained in the range [0,1] using a sigmoid function. The validity of each cell is determined with reference to a certain threshold and invalid cells are assigned a value of zero. Finally, a cylinder set is created by stacking up all cells in a vector starting from the cells in the base of the cylinder. A bit-based implementation is made possible by a unit step function which converts a real-valued cylinder set in a binary cylinder set. If there are no invalid cylinders, for M minutiae in fingerprint, there are M corresponding binary strings that represent an MCC feature template. However, MCC templates are not secure nor cancelable as demonstrated in [121], hence an attack strategy can be devised with a high precision of minutiae retrieval. A non-invertible MCC representation, also known as protected MCC (PMCC), is achieved by binary KL-transform. Although PMCC representation is non-invertible, it is not cancelable. Cancelability is achieved by a user-specific key that acts as a seed for the partial permutation of the PMCC features as reported in [119].

Sandhya et al. [122] proposed alignment-free cancelable templates by constructing k-nearest neighbourhood local structures (k-NNS) in a minutiae-based fingerprint. The local structure is constructed with reference to each minutia in the fingerprint by considering k minutiae in its nearest neighbourhood. Some of the rotation invariant features related to the structure can be computed by accounting the distance between the reference and each of the neighbouring minutia, and an average of the orientation of reference and each of the neighbouring minutia. The process involves the computation of all features for all local structures and is organised in the form of a feature vector. In order to achieve a fixed size feature vector, the structure is quantized into cells and mapped onto a 2-dimensional array. Cells with one or more minutia in it are assigned a value of 1 (and 0 otherwise), which enables a bit-based implementation of the method. Prior to generating a cancelable template, a binary vector is converted into a complex valued feature vector using discrete Fourier transform (DFT). Finally, a cancelable template is obtained by applying a user-specific random key of size less than the size of the

binary vector which makes the transformation non-invertible. Cancelability is simply achieved by changing the user key.

Wang et al. [123] developed a blind system identification approach to generate cancelable templates based on a quantized pair-minutiae vector [112]. In blind system identification, if the identifiability condition is not met, the source signal cannot be identified and it provides a base for the proposed model. The implementation involves a user-specific parameter key and a Toeplitz feature matrix which contains the frequency samples (obtained by taking DFT) of the corresponding binary features from the quantized pair-minutiae vector. The Toeplitz feature matrix is constructed in such a way that its length is equal to the length of the parameter key. From an implementation point of view, cancelable templates are obtained simply by multiplying the key with the feature matrix. In relation to this, the important identifiability condition for inversion depends on the length of the parameter key. If the length of the parameter key is less than the half of the length of the feature vector, the transformation process is not invertible. However, a smaller key leads to more distortion which affects performance.

In [124], Wang et al. proposed a feature extraction method based on zoned minutia pairs and developed cancelable templates using partial DFT. The process involves the extraction of features such as the relative distance and angle between two minutiae as locally as possible which are invariant to global translation and rotation [125]. For this purpose, the minutiae set is zoned into several local circular regions each centred at every minutia with a fixed radius. Minutia pairs are formed between the central minutia and all other minutiae within each zone. The invariant features related to each zoned minutia pair include, the distance between the central and other minutia and two relative angles between the orientation of both the minutiae and the line segment (see Figure 2.6).

Quantizing each feature by appropriate step size allows the effects of elastic distortion to be mitigated. In order to locate each minutia in a zone, a cuboid is defined with three axes representing three features i.e., length and two relative angles. The cuboid is divided into cubicles based on the step size used to quantize

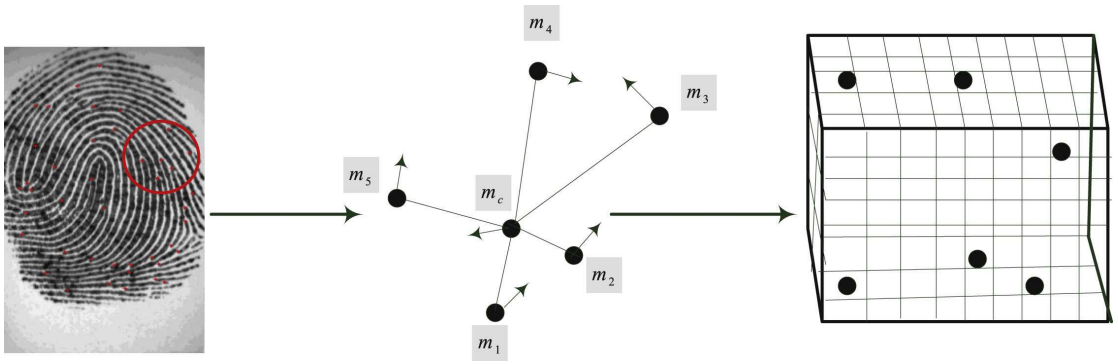

FIGURE 2.6: Local minutia structure. Left: selection of a circular local zone in red. Middle: minutia pairs constructed from the selected zone. Right: quantized minutia pairs matched to the corresponding bins in the cuboid [123].

each feature. Each cubicle is assigned a value of 1 if its location is matched with the quantized feature vector, and all other cubicles are assigned a value of 0. A binary string is formed by concatenating all 0s and 1s in a cuboid and it represents the local zone. For a fingerprint with N minutiae, there are N local zones and N corresponding binary strings. A modulo operation on each binary string enables many-to-one mapping and addresses the attacks via record multiplicity [126]. Finally, cancelable templates are formed using partial DFT in which the FFT matrix is made column rank deficient by a user-defined random key which makes the transformation non-invertible.

TABLE 2.1: Characteristics and EER (%) performance comparison of some well-known cancelable template designs in the lost-key scenario (the 1vs1 protocol).

Cancelable fingerprint template design	Signal Representation	Key Employing	Alignment free	FVC2002 DB1	FVC2002 DB2	FVC2002 DB3	FVC2004 DB1	FVC2004 DB2
Ahmad et al. [95]	Pair-polar feature	Random Projection	Yes	9	6	27	–	–
Das et al. [127]	Minimum Distance Graph	Random Projection	Yes	2.27	3.79	–	–	–
Jin et al. [113]	Binary Polar Feature	Random Permutation	Yes	5.19	5.65	–	–	–
Wong et al. [116]	Enhanced MLC Feature	Random Permutation	Yes	1.97	2.54	–	–	–
Jin et al. [99]	RGHE Feature	Random Projection	Yes	4.36	1.77	–	–	–
Wang and Hu [97]	Geometric Trans. Feature	Random Projection	Yes	3.50	4	7.50	–	–
Wang and Hu [118]	Curtailed Circular Conv.	Keyed Conv. Mtx.	Yes	2	2.30	6.12	–	–
Wang and Hu [123]	Toeplitz Transform Feature	Keyed Toeplitz Mtx.	Yes	3	2	7	–	–
Wang et al. [102]	Partial Hadamard Transform	Random Projection	Yes	1	2	5.2	–	–
Wang et al. [124]	Partial DFT Feature	Keyed DFT Mtx.	Yes	0.19	1	4.29	–	9.01
Yang et al. [96]	Multiple Schemes	Random Projection	Yes	0.32	0.64	4.57	–	9.9
Kho et al. [117]	R-NNLS	Random Permutation	Yes	0	0	2	–	4

2.3 Summary

This chapter presents a comprehensive survey of research work on fingerprint template protection (FTP). FTP is divided into four categories i.e., fingerprint cryptosystem, feature transformation (or cancelable templates), hybrid technique and homomorphic encryption. Three categories were summarised in the first section and an exposition on the fourth category i.e., cancelable template is presented in the second section. Cancelable templates have been categorised based on the transformation methods. Most commonly used transformation methods are geometric, robust hashing, random projection, biometric filters, random permutations, non-invertible transformation functions, etc. At the end, a performance comparison is presented for some existing models for cancelable templates.

Chapter 3

Alignment-free Cancelable Fingerprint Templates with Dual Protection

He who has a why to live can bear almost any how.

– Friedrich Nietzsch

3.1 Introduction

With good reliability and recognition accuracy, fingerprint-based biometric authentication technology [1] is widely used in civil, commercial and financial sectors. The raw fingerprint features of enrolled users, known as templates, are often stored in central databases or on smart cards and mobile devices (see Figure 1.2). Due to the intrinsic bond between template data and one's identity, the consequence of having one's fingerprint template compromised is serious and therefore, template protection [125] is critical for fingerprint biometric systems.

In this chapter, an alignment-free cancelable fingerprint template scheme is proposed which allows fingerprint security at two levels. The first security level in the

proposed method is achieved by a simple yet an intelligent process that induces uncertainties in the fingerprint's binary features by a window-shift-XOR model. This step ensures fingerprint protection against threats like ARM attacks. Following this, one-way transformation is achieved via partial DWT which constitutes the second level of protection as well as allowing the development of cancelable templates. These cancelable templates come with the inherent properties of accuracy, non-invertibility, revocability, diversity and unlinkability. DWT also offers a good denoising property which preserves or even enhances the recognition accuracy of the proposed method [128].

Feature extraction and representation play a pivotal role in the design of cancelable fingerprint templates since these directly affect the matching performance. In the proposed scheme, MCC [120] which is a state-of-the-art local minutia descriptor, is used for this purpose. The alignment-free, binary MCC template has excellent matching performance over a number of public databases, e.g., FVC2002 DB1-DB4 [9]. However, the MCC template can be reverted to recover the original minutiae and thus has security shortfalls. Ferrara et al. [121] designed a protected MCC (P-MCC) template to strengthen the security of the MCC. Although the P-MCC is non-invertible, it is not cancelable. Compared to this, the proposed method allows the production of cancelable fingerprint templates built upon MCC.

One of the key strengths of DWT [128] is to capture abrupt changes in signals and images. The MCC binary feature vectors are characterized with such abrupt changes, as these changes carry meaning. With the added benefit of denoising, the DWT prevents the post-transformation performance from deteriorating. Consequently, partial DWT not only realises non-invertibility but also enhances the matching accuracy. When evaluated over public databases FVC2002 [9] and FVC2004 [10], the proposed alignment-free cancelable templates outperform almost all the existing methods. The main contributions of the proposed scheme are summarised as follows:

1. The window-shift-XOR model effectively defends the ARM with simple operations. Window segmentation and shifting as well as XOR logic are easy

to implement and have little computational complexity.

2. The proposed alignment-free cancelable templates show superior performance. In particular, it is equal to the performance of the MCC template and does not suffer from post-transformation performance degradation. In addition, the proposed method significantly increases the security of the MCC and converts it into a cancelable template.

3. With dual protection, the designed cancelable template has increased security. It is able to thwart the ARM and satisfies the requirements of non-invertibility, diversity and revocability for cancelable biometrics.

The rest of the chapter is organized as follows. Section 3.2 introduces wavelets and the DWT and reviews the MCC. Section 3.3.1 details the window-shift-XOR model and partial DWT of the proposed scheme. Section 3.4 presents the experiment results and discusses the security of the proposed alignment-free cancelable templates. The summary of the proposed work is given in Section 3.5.

3.2 Preliminaries on wavelets and the MCC

3.2.1 Wavelets and the DWT

In this section, we present the fundamentals of wavelets and introduce the DWT. A wavelet is a finite-duration, rapidly decaying wave with zero mean. The most prominent characteristic of wavelets is good time-frequency localization and therefore, wavelets are best suited for dealing with signals that have abrupt changes, such as the binary MCC template. Moreover, wavelets come in different sizes and shapes. The availability of a wide variety of wavelets makes wavelet analysis attractive because different wavelets can be chosen for different applications. The essential components of a wavelet include the lowpass filter $\mathbf{C}$, the highpass filter $\mathbf{D}$ and the decimation (i.e., downsampling) step, denoted by the symbol $\downarrow 2$ (see Figure 3.1 adapted from [128]). The lowpass filter $\mathbf{C}$ computes the averages of the

inputs at each stage (or decomposition level), while the highpass filter **D** takes the differences of the inputs at each decomposition level. The downsampling step follows both the lowpass filter **C** and the highpass filter **D** to keep only the even-numbered components of the filtered outputs, so that the wavelet transform yields the same number of coefficients as the length of the input signal. Obviously, this saves memory.

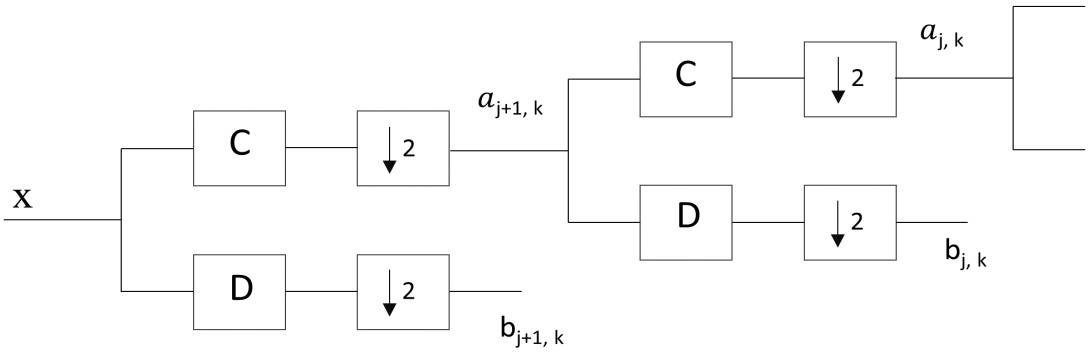

FIGURE 3.1: The operation of wavelets (adapted from [128]).

The wavelet transform [128] operates in continuous time on functions and in discrete time on vectors. To suit our need, we focus on the DWT (discrete wavelet transform). Since each element in the DWT has a position in time, denoted by k, as well as a position in frequency (also called scale or decomposition level), denoted by j, it is better to use a double index j, k, where $j = 0, 1, \cdots, J-1$ and $k = 0, 1, \cdots, 2^j - 1$, with J being the total number of decomposition levels. In Figure 3.1, assume that the input vector $\mathbf{x}$ is of length $N = 2^J$. In the wavelet operation shown by Figure 3.1, levels j and $j+1$ are related such that the averages and differences of the inputs at each level can be computed recursively, expressed by

$$\begin{aligned} a_{j,k} &= \frac{1}{\sqrt{2}}(a_{j+1,2k} + a_{j+1,2k+1}) \\ b_{j,k} &= \frac{1}{\sqrt{2}}(a_{j+1,2k} - a_{j+1,2k+1}) \end{aligned} \tag{3.1}$$

where the averages $a_{j,k}$ are the inputs to the next level $j-1$ and the differences $\mathbf{b}_{j,k}$ at each level j are kept as the final wavelet coefficients.

At each level j, we find 2^j differences and averages until we reach level 0 with an overall average and an overall difference (i.e., first half average - second half average). This is best illustrated by a finite pyramid [128] with an input vector of length $N = 2^3$, as shown in Figure 3.2. In this example (see Figure 3.2), the input

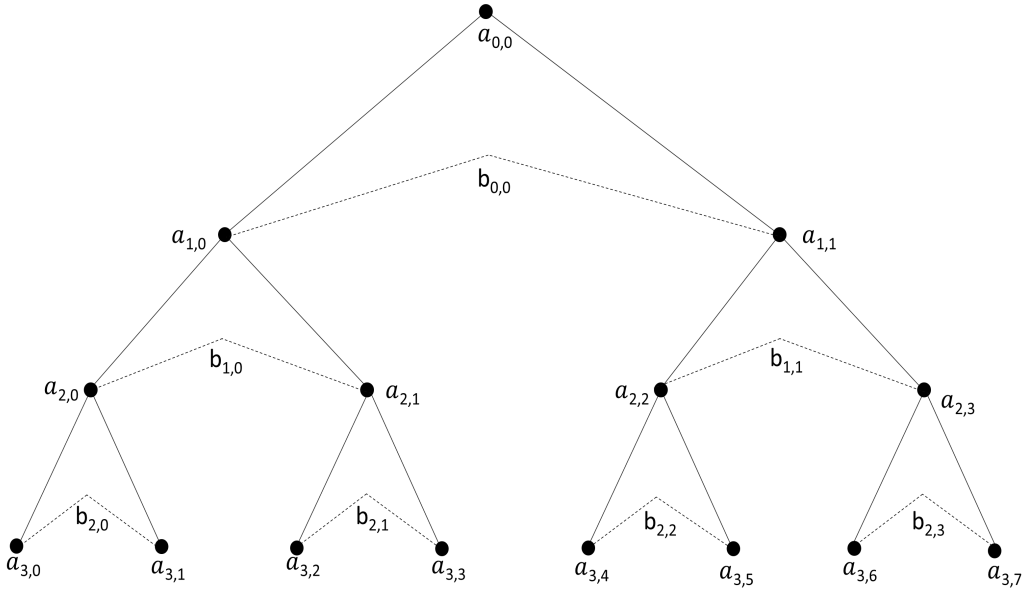

FIGURE 3.2: Averages $a_{j,k}$ go up the pyramid and differences $b_{j,k}$ stop (adapted from [128]).

has $N = 2^3 = 8$ elements. The DWT has a total of $J = 3$ decomposition levels and produces 8 wavelet coefficients, since

$$4 \text{ differences} + 2 \text{ differences} + 1 \text{ difference} + 1 \text{ overall average} = 8$$

The wavelet coefficients are obtained by concatenating all differences with an overall average, thus completing the process of the DWT.

In (3.1), the combination of lowpass/highpass filtering and downsampling can be represented by the rectangular matrices $\boldsymbol{C}_j$ and $\boldsymbol{D}_j$, respectively, each of which

consists of 1×2 blocks:

$$\boldsymbol{C}_j = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & & & & \\ & & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & & \\ & & & & \cdot & \cdot \end{bmatrix} \tag{3.2}$$

$$\boldsymbol{D}_j = \begin{bmatrix} \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} & & & & \\ & & \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} & & \\ & & & & \cdot & \cdot \end{bmatrix} \tag{3.3}$$

The matrices $\boldsymbol{C}_j$ and $\boldsymbol{D}_j$ are each of size $2^j \times 2^{j+1}$, where $j = 0, 1, \cdots, J-1$, denoting the decomposition level.

The recursive nature of the wavelet operation allows us to construct the matrix $\mathbf{A}$ of size $2^J \times 2^J$, expressed in the form of matrix multiplication:

$$\mathbf{A} = \begin{bmatrix} \boldsymbol{A}_0 & & & & \\ & \boldsymbol{I}_0 & & & \\ & & \boldsymbol{I}_1 & & \\ & & & \ddots & \\ & & & & \boldsymbol{I}_{J-2} \end{bmatrix} \cdots \begin{bmatrix} \boldsymbol{A}_j & & & & \\ & \boldsymbol{I}_j & & & \\ & & \boldsymbol{I}_{j+1} & & \\ & & & \ddots & \\ & & & & \boldsymbol{I}_{J-2} \end{bmatrix} \cdots \begin{bmatrix} \boldsymbol{A}_{J-2} & \\ & \boldsymbol{I}_{J-2} \end{bmatrix} \boldsymbol{A}_{J-1} \tag{3.4}$$

where $\boldsymbol{I}_j$ is the identity matrix of size $2^{j+1} \times 2^{j+1}$ and matrix $\boldsymbol{A}_j$ is formed by matrix $\boldsymbol{C}_j$ in (3.2) and matrix $\boldsymbol{D}_j$ in (3.3), given by

$$\boldsymbol{A}_j = \begin{bmatrix} \boldsymbol{C}_j \\ \boldsymbol{D}_j \end{bmatrix}$$

The size of $\mathbf{A}_j$ is $2^{j+1} \times 2^{j+1}$, where $j = 0, 1, \cdots, J-1$. Based on matrix $\mathbf{A}$ in (3.4), the DWT is performed on an input vector $\mathbf{x}$, written as

$$\mathbf{b} = \mathbf{A}\mathbf{x} \tag{3.5}$$

where the output vector $\mathbf{b}$ contains the wavelet coefficients, and both the input

vector $\mathbf{x}$ and output vector $\mathbf{b}$ are of length $N = 2^J$. Thus, the DWT outputs the same number of wavelet coefficients as the length of the input.

It is not hard to see that the structure of matrix $\mathbf{A}$ in (3.4) allows fast computation of the DWT. This is known as the fast wavelet transform (FWT). The FWT is asymptotically faster than the fast Fourier transform (FFT), requiring only $O(N)$ computations [128].

Remark: For clarity and brevity, in the above, we have used the simplest lowpass filter with only two coefficients $\frac{1}{\sqrt{2}}\{1, 1\}$[1], which means that the corresponding highpass filter also has only two coefficients $\frac{1}{\sqrt{2}}\{1, -1\}$. Despite this simplicity, the concept and operation of wavelets remain the same with other filters of more taps.

3.2.2 A local minutia descriptor – MCC

Since the input to the proposed scheme is the binary feature vectors of the MCC [120], let us briefly review the MCC. In the MCC representation, a 3D local structure, called cylinder, is constructed for each (reference) minutia by encoding the relative spatial and directional relationships of the reference minutia with its neighboring minutiae within a prescribed range. Each cylinder is discretized into a number of cells. Based on the likelihood of finding minutiae that are close to the center of the cell in terms of location and direction, a numerical value is calculated for each cell. As a result, a binary bit-string is created for each cylinder. The MCC is a well-known minutia-based template for fingerprint recognition, but it is not a cancelable template and can be reverted to rebuild the original minutiae [121]. We make use of the MCC's binary representation and strong performance to design cancelable templates, as detailed in Chapter 2.

[1]In the filter $\frac{1}{\sqrt{2}}$ is a scale factor, which can be ignored in practical implementation.

3.3 Proposed scheme

The proposed scheme comprises the following three key components:

- The window-shift-XOR model: The model offers single protection.
- The partial DWT: This, in conjunction with the window-shift-XOR model, renders dual protection.
- Fingerprint matching in the transformed domain

3.3.1 The window-shift-XOR model

The proposed scheme's single protection is featured by the window-shift-XOR model, aiming to defuse the ARM threat [126]. The ARM weakens the security of many existing cancelable fingerprint templates, e.g., [77], [114], [97]. The root cause of the ARM is that cancelable templates for different applications are actually generated from the same feature data. When an adversary acquires sufficient amounts of templates from multiple applications, the original feature data can be restored. To prevent the ARM threat, we have to ensure the stored templates in different applications come from different feature data which are unrelated to one another.

Taking advantage of MCC's feature representation, we utilize the MCC binary bit-strings as the input to the window-shift-XOR model. Specifically, the window-shift-XOR model creates new vectors by adding random uncertainties to MCC's binary feature vectors. The new vectors are parameter-controlled so that they can be made different and unrelated from one application to another. Suppose that MCC's binary vector of the cth valid cylinder is written as

$$\mathbf{x}_c = [x_c(1), x_c(2), \cdots, x_c(M)] \tag{3.6}$$

where M is the length of $\mathbf{x}_c$ and $c = 1, 2, \cdots, C$ with C being the total number of valid cylinders from the MCC. The window-shift-XOR model is depicted in Figure 3.3.

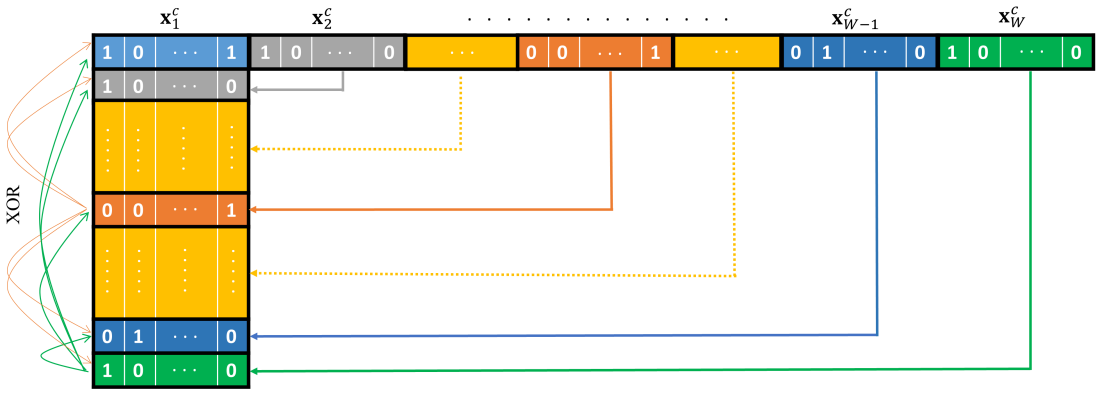

FIGURE 3.3: The window-shift-XOR model.

First, we divide $\mathbf{x}_c$ into W segments[1] using a window of fixed size S, i.e., $W = \lceil M/S \rceil$. The vector $\mathbf{x}_c$ can be rewritten as

$$\mathbf{x}_c = [\mathbf{x}_1^c, \mathbf{x}_2^c, \cdots, \mathbf{x}_W^c] \tag{3.7}$$

where $\mathbf{x}_r^c = [x_r^c(1), x_r^c(2), \cdots, x_r^c(S)]$, $r = 1, 2, \cdots, W$. It is readily seen that the elements of $\mathbf{x}_c$ in (3.6) and (3.7) are related by

$$x_c(S(r-1)+k) = x_r^c(k), \quad r = 1, 2, \cdots, W \text{ and } k = 1, 2, \cdots, S \tag{3.8}$$

Next, we shift the second segment $\mathbf{x}_2^c$ of $\mathbf{x}_c$ in (3.7) till the last segment $\mathbf{x}_W^c$ one by one beneath the first segment $\mathbf{x}_1^c$ and align them vertically element by element. This shifting process can be expressed by the following matrix:

$$\mathbf{M} = \begin{bmatrix} \mathbf{x}_1^c \\ \mathbf{x}_2^c \\ \vdots \\ \mathbf{x}_W^c \end{bmatrix} = \begin{bmatrix} x_1^c(1) & x_1^c(2) & \dots & x_1^c(S) \\ x_2^c(1) & x_2^c(2) & \dots & x_2^c(S) \\ \vdots & \vdots & \cdots & \vdots \\ x_W^c(1) & x_W^c(2) & \dots & x_W^c(S) \end{bmatrix} \tag{3.9}$$

[1]The last segment is appended with 0 so that its length is S if M/S is not an integer.

The size of matrix $\mathbf{M}$ is $W \times S$.

Finally, we randomly select a candidate segment $\mathbf{x}_r^c$, or equivalently, row r of $\mathbf{M}$, $1 \leq r \leq W$, and perform the element-wise XOR between the rth row and any other rows of $\mathbf{M}$. That is,

$$y_j^c(k) = x_r^c(k) \oplus x_j^c(k), \quad j \neq r, \ 1 \leq j, r \leq W \tag{3.10}$$

where $\oplus$ denotes the XOR operation and $k = 1, 2, \cdots, S$. Upon the completion of the element-wise XOR, the rth row of $\mathbf{M}$, $\mathbf{x}_r^c$, is discarded for the purpose of security (see Security Analysis in Section 3.4.5). A new binary vector $\mathbf{y}_c$ is formed by concatenating the post-XOR rows $\mathbf{y}_j^c = [y_j^c(1), y_j^c(2), \cdots, y_j^c(S)]$, $j = 1, 2, \cdots, W-1$. The new size-reduced binary vector $\mathbf{y}_c$ is given by

$$\mathbf{y}_c = [\mathbf{y}_1^c, \mathbf{y}_2^c, \cdots, \mathbf{y}_{W-1}^c]^T \tag{3.11}$$

The length of $\mathbf{y}_c$ is $N = M - S$, shortened by S elements compared with the length M of the original MCC binary vector $\mathbf{x}_c$, because of the removal of the rth row of $\mathbf{M}$ after the XOR operation.

Despite originating from the same $\mathbf{x}_c$, thanks to the window-shift-XOR model, vector $\mathbf{y}_c$ can be built differently and made unrelated in different applications by changing window size S and selecting the candidate segment $\mathbf{x}_r^c$ for the XOR operation. Therefore, the ARM is defensible.

3.3.2 The partial DWT

The binary vector $\mathbf{y}_c$ in (3.11) is created with uncertainty by the window-shift-XOR model. To heighten its security, we further protect $\mathbf{y}_c$ with the partial DWT. It is well known that the DWT is good at denoising [128], so it helps to preserve recognition accuracy after the transformation, which is an added benefit.

We first take the N-point discrete cosine transform (DCT) [129] on $\mathbf{y}_c$ to obtain $\mathbf{z}_c$ and $\mathbf{z}_c$ is a real vector. This step is necessary because elements of $\mathbf{y}_c$ are binary,

which might narrow the search space for finding $\mathbf{y}_c$. The (full-order) DWT (3.5) cannot be used to protect $\mathbf{z}_c$, since the DWT matrix $\mathbf{A}$ in (3.4) is non-singular given that $\mathbf{A}$ is orthogonal or orthonormal, namely, $\mathbf{A}^T\mathbf{A} = \boldsymbol{I}$ and $\mathbf{A}^{-1} = \mathbf{A}^T$, allowing $\mathbf{z}_c$ to be restored easily. However, the DWT matrix $\mathbf{A}$ possesses some nice properties. For example, the rows of $\mathbf{A}$ are orthogonal. If we only select a portion of the rows of $\mathbf{A}$ to form a rectangular submatrix $\bar{\mathbf{A}}$, then $\bar{\mathbf{A}}$ is column rank deficient and singular.

We take the partial DWT on $\mathbf{z}_c$ using the submatrix $\bar{\mathbf{A}}$:

$$\mathbf{w}_c = \bar{\mathbf{A}}\mathbf{z}_c \tag{3.12}$$

where $\bar{\mathbf{A}}$ is formed by randomly selecting R rows of $\mathbf{A}$ using an index vector $\mathbf{k}$, given by

$$\mathbf{k} = [k_1, k_2, \cdots, k_R] \tag{3.13}$$

where $R < N$ and N is the length of $\mathbf{z}_c$. All elements of $\mathbf{k}$ are strictly positive integers with $k_i \neq k_j$ for all $i \neq j$. The ith row of $\bar{\mathbf{A}}$ is the k_ith row of $\mathbf{A}$ for $i = 1, 2, \cdots, R$. The size of $\bar{\mathbf{A}}$ is $R \times N$, so it is a column rank deficient matrix. The partial DWT (3.12) corresponds to an underdetermined system, which does not have unique solutions. The true $\mathbf{z}_c$ is just one of the many solutions of this underdetermined system. Thus, the partial DWT (3.12) is a non-invertible transformation.

Remarks:

1. The vector $\mathbf{k}$ in (3.13) serves the role of a parameter key. Altering $\mathbf{k}$ gives different $\bar{\mathbf{A}}$, which produces different $\mathbf{w}_c$. Therefore, $\mathbf{w}_c$ is a cancelable template. The MCC has a total of C valid cylinders, each of which yields $\mathbf{w}_c$, for $c = 1, 2, \cdots, C$.

2. The availability of a broad range of wavelets is a main advantage of wavelet analysis. We choose Daubechies wavelets to evaluate the performance of

the designed cancelable template, because they are orthogonal wavelets and have high vanishing moments, offering good approximation (see experiment results in Section 3.4). Daubechies wavelets also have compact support, providing good time-frequency localization.

3. We can exploit the computational advantage of FWT algorithms [128] to expedite the calculation of $\mathbf{w}_c$ in (3.12). The FWT is faster than the FFT, as discussed in Section 3.2.1.

3.3.3 Fingerprint matching in the transformed domain

For security reasons, fingerprint matching is conducted in the transformed domain. Query fingerprints undergo the same process as template fingerprints. To distinguish between the template and the query, we use the letters 't' and 'q'. Suppose that there are C_t valid cylinders in the template, each generating $\mathbf{y}_{c_t}$ in (3.11) and subsequently $\mathbf{w}_{c_t}$ in (3.12), for $c_t = 1, 2, \cdots, C_t$. The same applies to the query. Note that $C_t \neq C_q$ as the template and the query usually have a different number of cylinders.

The similarity score between $\mathbf{y}_{c_t}$ and $\mathbf{y}_{c_q}$ with single protection and the similarity score between $\mathbf{w}_{c_t}$ and $\mathbf{w}_{c_q}$ with dual protection are given by

$$S_1(\mathbf{y}_{c_t}, \mathbf{y}_{c_q}) = 1 - \frac{||\mathbf{y}_{c_t} \oplus \mathbf{y}_{c_q}||_2}{||\mathbf{y}_{c_t}||_2 + ||\mathbf{y}_{c_q}||_2} \tag{3.14}$$

$$S_2(\mathbf{w}_{c_t}, \mathbf{w}_{c_q}) = 1 - \frac{||\mathbf{w}_{c_t} - \mathbf{w}_{c_q}||_2}{||\mathbf{w}_{c_t}||_2 + ||\mathbf{w}_{c_q}||_2} \tag{3.15}$$

where $c_t = 1, 2, \cdots, C_t$ and $c_q = 1, 2, \cdots, C_q$. Symbol $\oplus$ denotes the element-wise XOR and $||\cdot||_2$ represents the 2-norm [130]. The values of $S_1(\mathbf{y}_{c_t}, \mathbf{y}_{c_q})$ and $S_2(\mathbf{w}_{c_t}, \mathbf{w}_{c_q})$ range from 0 to 1. The two scores indicate the extent of similarity between a cylinder in the template and a cylinder in the query. The larger the scores, the more similar the cylinder pair.

Since there are C_t cylinders in the template and C_q cylinders in the query, to make a match or non-match verdict, we must compute the similarity scores for all

cylinder pairs between the template and the query. This leads to a score matrix of size $C_t \times C_q$, from which a single global score is determined using the local greedy similarity algorithm in the MCC SDK [120].

3.4 Experiment results and analysis

To evaluate the proposed cancelable template design, we conducted extensive tests over five public databases FVC2002 DB1, DB2 and DB3 [9] as well as FVC2004 DB1 and DB2 [10]. These databases contain fingerprints of varying quality. Information about these databases is summarised in Table 1.1 in Chapter 1. We employed the commercial fingerprint recognition software *VeriFinger SDK* [11] to extract minutia points from fingerprint images in these databases. The performance measures applied in our tests are the FAR, FRR and EER. The two testing protocols we adopted are the 1vs1 protocol and the original FVC protocol from [121] (also refer to Chapter 1 for further details).

3.4.1 Matching performance with single protection

By changing window size S, we tested the matching performance of the proposed scheme with single protection – the window-shift-XOR model. The original length for each binary string of the MCC template is 1536 bits, so with single protection only, the length 1536 is reduced to 1152 if the window size $S = 384$. Under the 1vs1 and original FVC protocols, the EER results are reported and compared with those of the reproduced MCC templates in Tables 3.1 and 3.2, respectively. From Tables 3.1 and 3.2, we observe that different window sizes have a marginal effect on the matching performance, and the proposed scheme with single protection suffers no or negligible performance loss when compared to the reproduced MCC template.

In the window-shift-XOR model, different candidate segments, e.g., a head segment, a middle segment, a tail segment or any other segment, can be chosen to

TABLE 3.1: EER (%) under different window sizes (with single protection only) in comparison with the reproduced MCC under the 1vs1 protocol (the last segment is the candidate segment).

Window size S	FVC2002 DB1	FVC2002 DB2	FVC2002 DB3	FVC2004 DB1	FVC2004 DB2
Reproduced MCC	0.01	0	1.41	7	5
150	0.04	0	2	8	5
275	0.04	0	2	7.93	5
384	0	0	2	7.42	5

TABLE 3.2: EER (%) under different window sizes (with single protection only) in comparison with the reproduced MCC under the original FVC protocol (the last segment is the candidate segment).

Window size S	FVC2002 DB1	FVC2002 DB2	FVC2002 DB3	FVC2004 DB1	FVC2004 DB2
Reproduced MCC	1.54	1.29	4	8.60	7.64
150	1.68	1.43	4.95	9.25	8.57
275	1.96	1.85	5.6	9.92	8.46
384	1.82	1.64	4.81	9.85	8.34

perform the element-wise XOR with other segments. We tested the impact of different candidate segment selections on the matching performance with window size $S = 384$. The results are given in Tables 3.3 and 3.4. It is shown that candidate segment selection has little or no impact and the EER of the proposed single protection is similar to that of the reproduced MCC.

TABLE 3.3: EER (%) under different candidate segment selections (with single protection only) in comparison with the reproduced MCC under the 1vs1 protocol ($S = 384$).

Window location	FVC2002 DB1	FVC2002 DB2	FVC2002 DB3	FVC2004 DB1	FVC2004 DB2
Head segment	0.02	0	1	8	5
Middle segment	0.06	0	2	7	5
Tail segment	0	0	2	7.42	5

3.4.2 Matching performance with dual protection

With dual protection, we evaluated the performance of the proposed scheme in the worst-case scenario, where a user-specific key is lost. We simulated this scenario by assigning all users the same key $\mathbf{k}$ in (3.13). Key $\mathbf{k}$ was generated randomly.

TABLE 3.4: EER (%) under different candidate segment selections (with single protection only) in comparison with the reproduced MCC under the original FVC protocol ($S = 384$).

Window location	FVC2002 DB1	FVC2002 DB2	FVC2002 DB3	FVC2004 DB1	FVC2004 DB2
Head segment	1.83	1.61	4.60	9.78	8.20
Middle segment	1.87	1.57	4.82	9.75	8.50
Tail segment	1.82	1.64	4.81	9.85	8.34

Daubechies wavelets were used to perform the partial DWT (3.12). As vanishing moments affect the wavelet's ability to capture different characteristics of a signal, after testing the EER performance of Daubechies wavelets with different vanishing moments, we found that Daubechies wavelet "db15" (i.e. 15 vanishing moments) exhibits fairly good performance. Thus, the ensuing results for all databases are based on Daubechies wavelets "db15" with window size $S = 384$.

TABLE 3.5: EER (%) with different key lengths in the lost-key scenario (with dual protection) in comparison with the reproduced MCC under the 1vs1 protocol.

Key length R	FVC2002 DB1	FVC2002 DB2	FVC2002 DB3	FVC2004 DB1	FVC2004 DB2
Reproduced MCC	0.01	0	1.41	7	5
300	0.02	0	2	8	5
500	0	0	1.63	7.35	4.69

TABLE 3.6: EER (%) with different key lengths in the lost-key scenario (with dual protection) in comparison with the reproduced MCC under the FVC protocol.

Key length R	FVC2002 DB1	FVC2002 DB2	FVC2002 DB3	FVC2004 DB1	FVC2004 DB2
Reproduced MCC	1.54	1.29	4	8.60	7.64
300	1.88	1.75	6.11	12.28	8.93
500	1.57	1.50	4.93	10.49	8.62

We assessed how the key length R in (3.13) impacted the performance of the proposed method. Under the 1vs1 and original FVC protocols, the test results are shown in Tables 3.5 and 3.6, respectively, as compared with the reproduced MCC template. We can see from Tables 3.5 and 3.6 that a longer key (i.e., a larger value of R) generally yields better performance, although this comes at the expense of template security, because more information before the partial DWT

is kept in the resultant cancelable template. This manifests the tradeoff between security and recognition accuracy [131]. Furthermore, the performance of the proposed method with dual protection is close enough to that of the reproduced MCC template, showing that the designed transformations do not degrade the recognition accuracy.

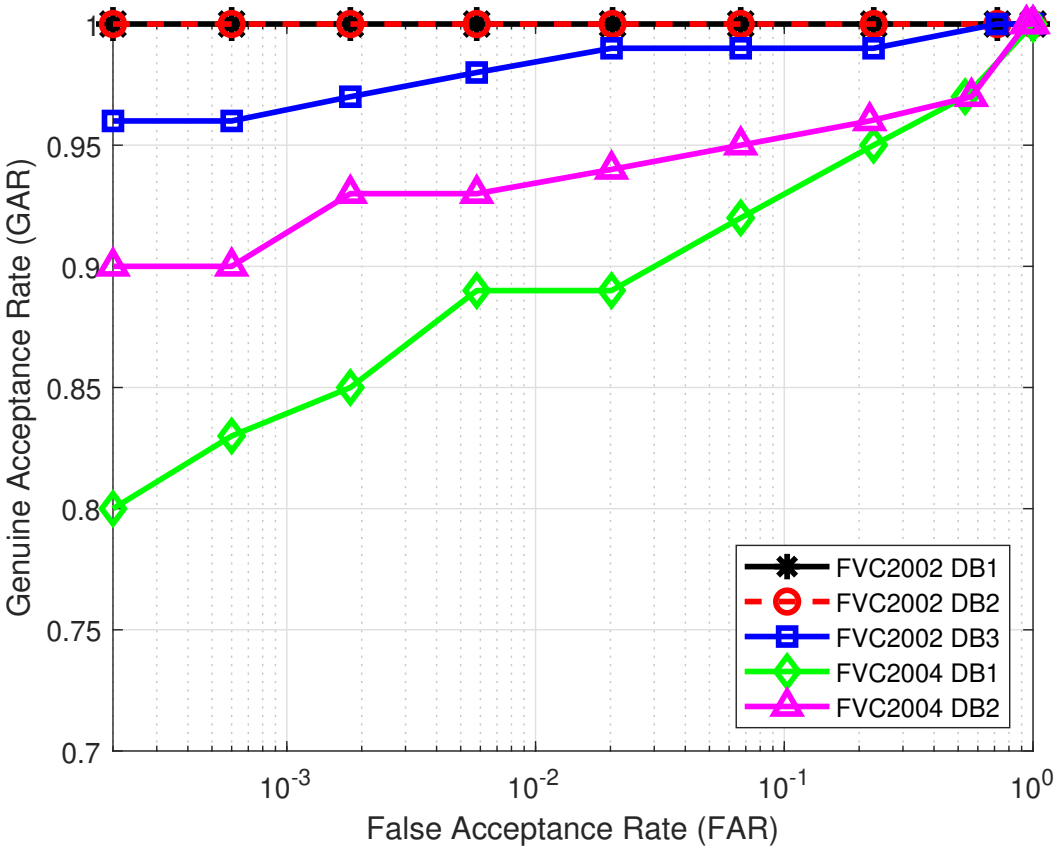

FIGURE 3.4: ROC curves for FVC2002 DB1, DB2, DB3, FVC2004 DB1 and DB2 in the lost-key scenario under the 1vs1 protocol.

In addition to the EER, we considered the lowest FRR at FAR$\leq$ 0.1% and at FAR= 0% for the proposed method in comparison with the reproduced MCC in the lost-key scenario under both protocols. These evaluation metrics are more indicative of verification accuracy in a real-world setting. With dual protection, we set the window size $S = 384$ with the last segment selected as the candidate segment and the key length $R = 500$. The experiment results are reported in Tables 3.7 and 3.8, where we can see that the recognition accuracy of the proposed method measures up to that of the reproduced MCC.

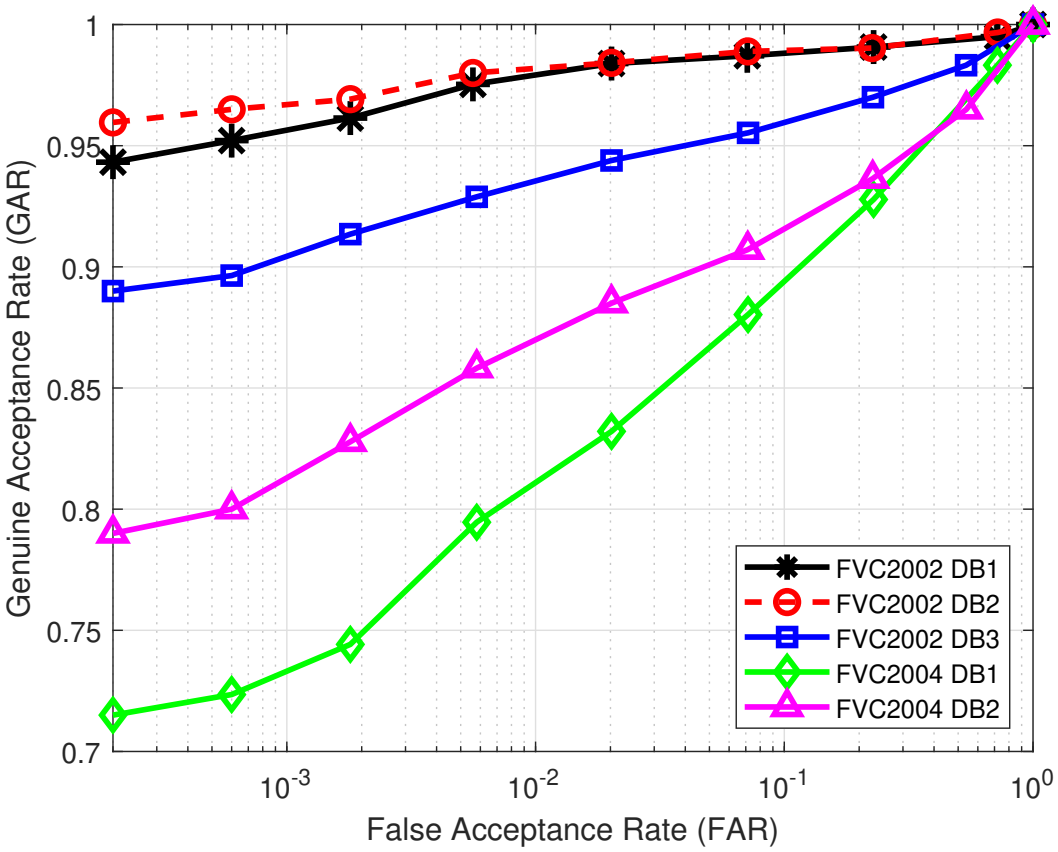

FIGURE 3.5: ROC curves for FVC2002 DB1, DB2, DB3, FVC2004 DB1 and DB2 in the lost-key scenario under the original FVC protocol.

TABLE 3.7: Recognition accuracy in the lost-key scenario (with dual protection) in comparison with the reproduced MCC under the 1vs1 protocol (all values expressed as percentages).

Database	FVC2002 DB1	FVC2002 DB2	FVC2002 DB3	FVC2004 DB1	FVC2004 DB2
EER (Reproduced MCC)	0.01	0	1.41	7	5
EER (Proposed method)	0	0	1.63	7.35	4.69
FRR at FAR$\leq$ 0.1% (Reproduced MCC)	0	0	2	16	9
FRR at FAR$\leq$ 0.1% (Proposed method)	0	0	3	16	8
FRR at FAR= 0% (Reproduced MCC)	1	0	7	16	10
FRR at FAR= 0% (Proposed method)	0	0	6	17	10

With window size $S = 384$, we set the key length $R = 500$ and plotted the receiver operating characteristic (ROC) in the lost-key scenario for all databases under the

TABLE 3.8: Recognition accuracy in the lost-key scenario (with dual protection) in comparison with the reproduced MCC under the original FVC protocol (all values expressed as percentages).

Database	FVC2002 DB1	FVC2002 DB2	FVC2002 DB3	FVC2004 DB1	FVC2004 DB2
EER (Reproduced MCC)	1.54	1.29	4	8.60	7.64
EER (Proposed method)	1.57	1.50	4.93	10.49	8.62
FRR at FAR$\leq$ 0.1% (Reproduced MCC)	3.21	2.21	10.75	21.21	17.64
FRR at FAR$\leq$ 0.1% (Proposed method)	4.10	2.89	9.71	25.21	17.53
FRR at FAR= 0% (Reproduced MCC)	9.39	4.60	12.50	24.17	20.96
FRR at FAR= 0% (Proposed method)	8.56	5.61	12.64	27.32	21.85

1vs1 and original FVC protocols in Figure 3.4 and Figure 3.5, respectively. Tables 3.9 and 3.10 show the performance comparison between the proposed method (with window size $S = 384$ and key length $R = 500$) and the existing cancelable template design in the lost-key scenario under both protocols. It can be seen from Tables 3.9 and 3.10 that for all five databases, the proposed scheme outperforms all the existing methods except the method proposed by Kho et al. [117] over one database – FVC2004 DB2.

TABLE 3.9: EER (%) comparison between the proposed method and the existing cancelable template design in the lost-key scenario (the 1vs1 protocol).

Cancelable fingerprint template design	FVC2002 DB1	FVC2002 DB2	FVC2002 DB3	FVC2004 DB1	FVC2004 DB2
Ahmad et al. [95]	9	6	27	–	–
Das et al. [127]	2.27	3.79	–	–	–
Jin et al. [113]	5.19	5.65	–	–	–
Wong et al. [116]	1.97	2.54	–	–	–
Jin et al. [99]	4.36	1.77	–	–	–
Wang and Hu [97]	3.50	4	7.50	–	–
Wang and Hu [118]	2	2.30	6.12	–	–
Wang and Hu [123]	3	2	7	–	–
Wang et al. [102]	1	2	5.2	–	–
Wang et al. [124]	0.19	1	4.29	–	9.01
Yang et al. [96]	0.32	0.64	4.57	–	9.9
Kho et al. [117]	0	0	2	–	4
Proposed method (single protection)	0	0	2	7.42	5
Proposed method (dual protection)	0	0	1.63	7.35	4.69

TABLE 3.10: EER (%) comparison between the proposed method and the existing cancelable template design in the lost-key scenario (the original FVC protocol).

Cancelable fingerprint template design	FVC2002 DB1	FVC2002 DB2	FVC2002 DB3	FVC2004 DB1	FVC2004 DB2
Wang and Hu [123]	4	3	8.5	–	–
Yang et al. [96]	5.75	4.71	10.22	–	12
Kho et al. [117]	2.28	1.25	6.4	–	7
Proposed method (single protection)	1.82	1.64	4.81	9.85	8.34
Proposed method (dual protection)	1.57	1.5	4.93	10.49	8.62

3.4.3 Revocability and diversity

Revocability and diversity are essential properties for cancelable fingerprint templates. If a stored template is compromised, we must be able to revoke it and issue a new one to replace it. Despite being generated from the same biometric data, the new template should be different to the old one. To test revocability and diversity, we generated 100 transformed templates from the first impression of each finger in FVC2002 DB2 using different keys, that is, randomly generating 100 different $\mathbf{k}$ in (3.13). These pseudo-imposter templates were matched against the original ones.

In Figure 3.6, we plotted the genuine, imposter and pseudo-imposter distributions. We can see from Figure 3.6 that the pseudo-imposter and imposter distributions overlap. The mean and standard derivation of the pseudo-imposter distribution are 0.3562 and 0.0083, respectively, compared with 0.3545 (mean) and 0.0069 (standard derivation) of the imposter distribution. These results show that the pseudo-imposter templates are unrelated and different as if they were generated from different fingerprints.

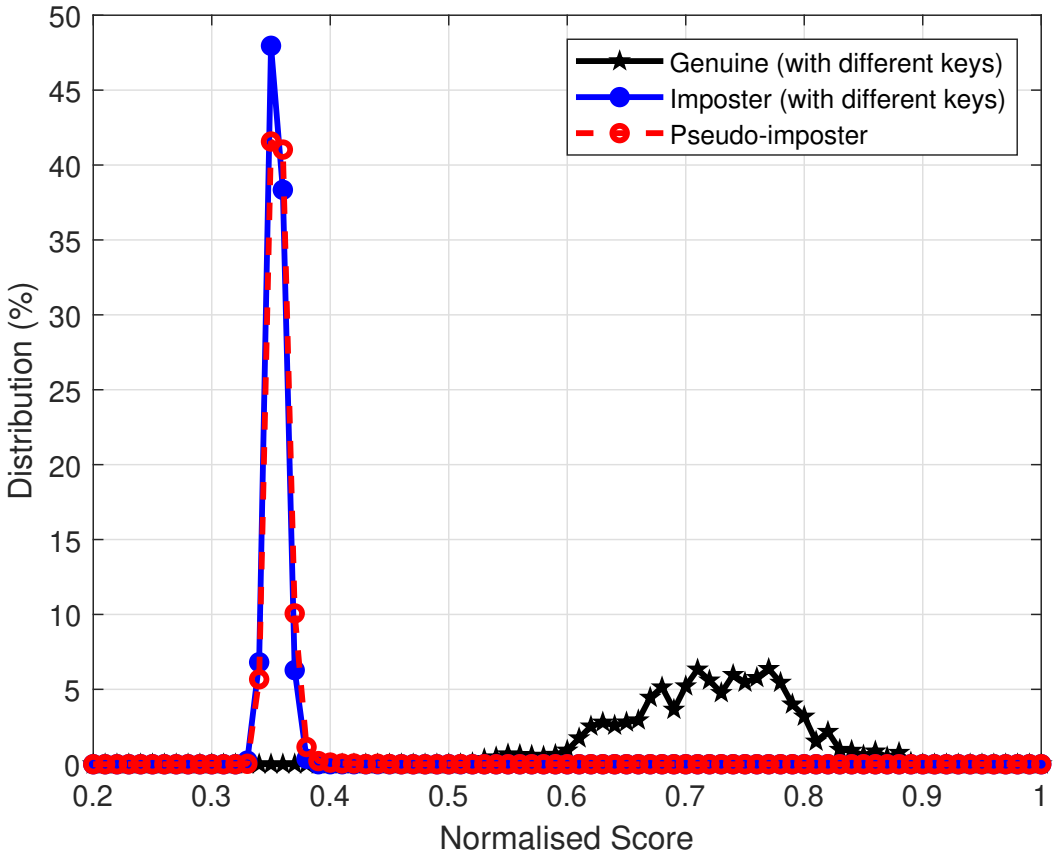

FIGURE 3.6: Genuine, pseudo-imposter and imposter distributions for FVC2002 DB2.

3.4.4 Unlinkability

Unlinkability requires that the transformed templates of the same fingerprint for different applications should not be able to be cross-matched. Unlinkability can be evaluated according to two indicators [8] – the false cross-match rate (FCMR) and the false non-cross-match rate (FNCMR). FCMR is defined as the ratio of successful matching attempts between non-mated pairs to the total matching attempts of non-mated pairs, and FNCMR is defined as the ratio of unsuccessful matching attempts between mated pairs to the total matching attempts of mated pairs.

The unlinkability test was conducted over FVC2002 DB2. To calculate the FNCMR, we matched the transformed templates of the first and second impressions of each finger in FVC2002 DB2. To calculate the FCMR, the transformed template of the first impression of each finger was matched against the transformed template

of the first impression of all other fingers in the database. The FCMR versus FNCMR curve is plotted in Figure 3.7, which shows that FCMR + FNCMR ≈ 1, so the proposed method exhibits the expected behavior for unlinkability.

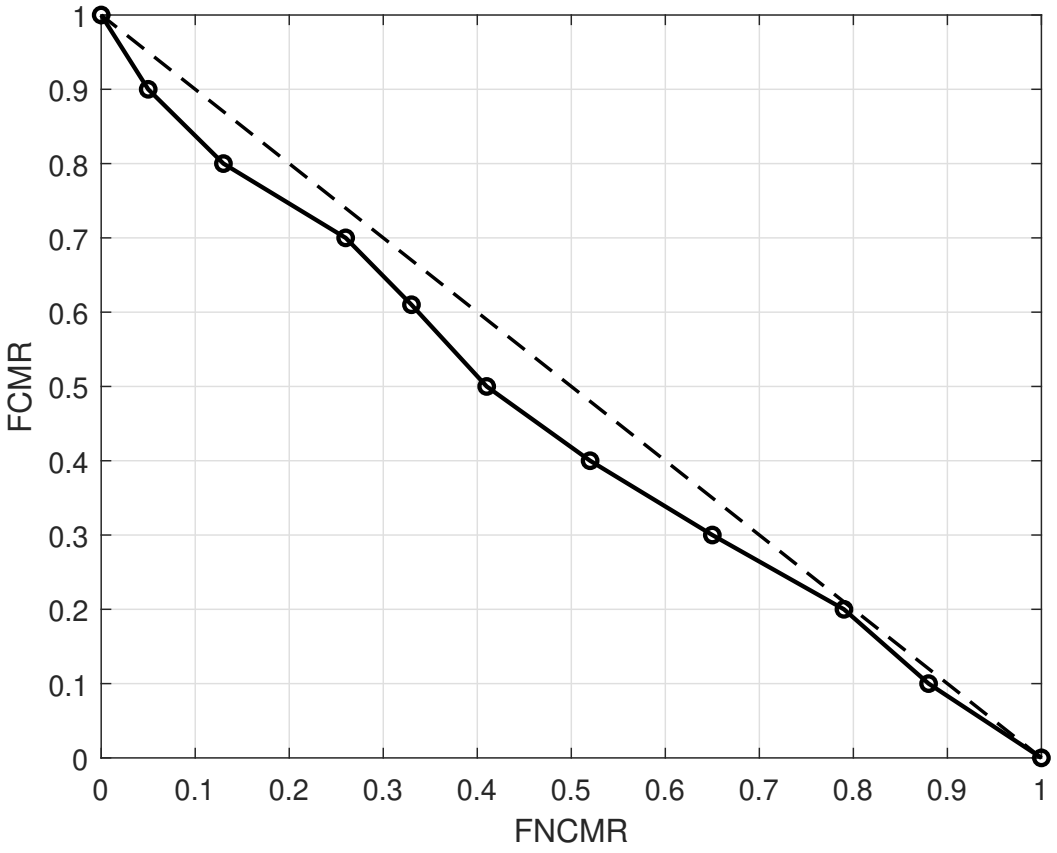

FIGURE 3.7: Unlinkability analysis with mated and non-mated score distribution (single protection).

Recently, Gomez-Barrero et al. [132], [133] proposed a general framework to evaluate the unlinkability of protected biometric templates. Based on this framework, unlinkability should be measured by two types of score distributions, known as mated and non-mated sample score distributions. Mated sample scores are computed by comparing templates extracted from the same impression of a finger using different keys, while non-mated sample scores are obtained by comparing templates extracted from different fingers using different keys. According to [132], unlinkability is measured at both local and global levels, denoted by score-wise linkability $D_{\leftrightarrow}(s)$ and system overall linkability $D_{\leftrightarrow}^{\mathbf{sys}}$, respectively. Score-wise linkability $D_{\leftrightarrow}(s)$ measures the linkability of a biometric template protection system for each specific matching score s from mated and non-mated score distributions.

For a particular score s, if $\mathrm{D}_{\leftrightarrow}(s) = 0$, two templates are deemed fully unlinkable, whereas if $\mathrm{D}_{\leftrightarrow}(s) = 1$, two templates are deemed fully linkable. Any value of $\mathrm{D}_{\leftrightarrow}(s)$ between 0 and 1 indicate a certain degree of linkability. In contrast, the global measure $\mathrm{D}_{\leftrightarrow}^{\mathbf{sys}} \in [0, 1]$ estimates the linkability of the whole system independent of scores, with $\mathrm{D}_{\leftrightarrow}^{\mathbf{sys}} = 0$ (or $\mathrm{D}_{\leftrightarrow}^{\mathbf{sys}} = 1$) meaning that the template protection system is fully unlinkable (or fully linkable).

We conducted the unlinkability analysis of the proposed scheme under both single and dual protections using FVC2002 DB2. With single protection, we created six datasets using two window sizes 384 and 275 in combination with three different candidate segment selections i.e., head, middle and tail segments. For instance, the first dataset is created by choosing the window size 384 and a head segment. The second dataset is formed by choosing the window size 384 and a middle segment and so on. The window size and candidate segment location serve as the key of a dataset, which means six different keys for six different datasets. The reason why we set up six datasets is because the recommendation from [132] is that the number of datasets for testing unlinkability should be greater than five. To generate the mated sample score distribution, we used all eight impressions of each finger in FVC2002 DB2, leading to 4800 ($= 800 \times 3 \times 2$) mated scores. To generate the non-mated sample score distribution, we used the first impression of each finger in FVC2002 DB2, yielding 29700 ($= 4950 \times 3 \times 2$) non-mated scores. The mated and non-mated score distributions are shown in Figure 3.8. It can be seen from Figure 3.8 that the mated and non-mated score distributions partially overlap for score values in $[0.17, 0.34]$, making the system under single protection semi-linkable with $\mathrm{D}_{\leftrightarrow}^{\mathbf{sys}} = 0.35$. This shows that single protection is not strong enough to conceal the same identity of MCC's binary feature vectors, which is why we have dual protection to strengthen the security and unlinkability of the proposed scheme.

To test unlinkability under dual protection, we produced 100 transformed templates of the first impression of each finger in FVC2002 DB2 with randomly generated different keys $\mathbf{k}$ in (3.13), each key of length 500. The mated sample score distribution was obtained by matching each transformed template with 100 newly

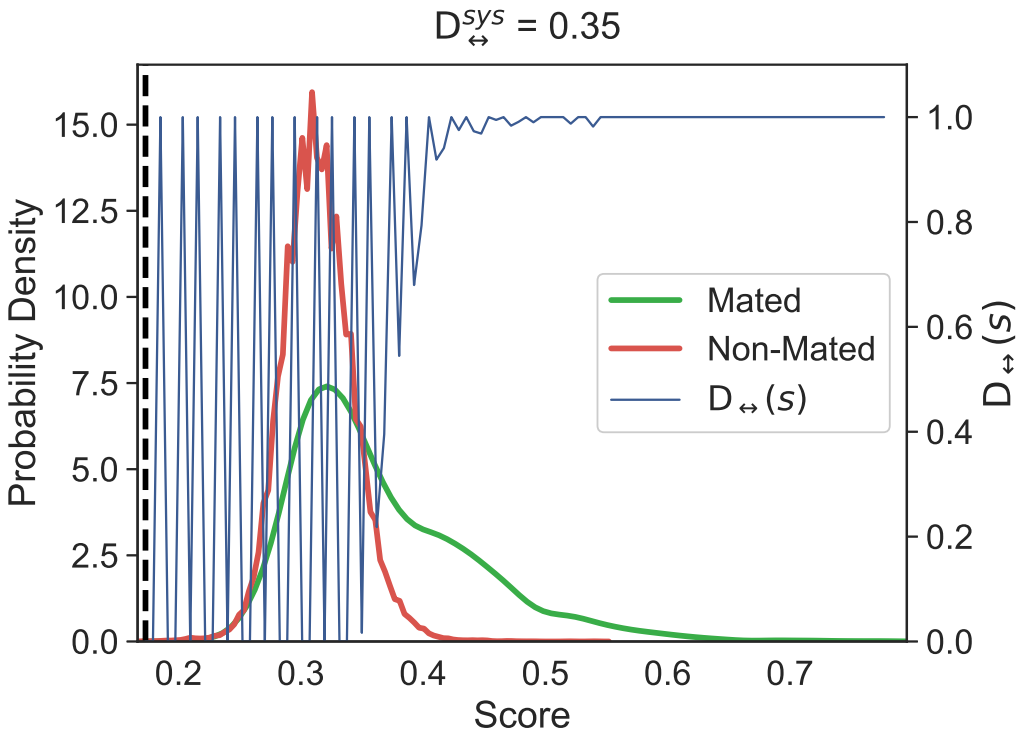

FIGURE 3.8: Unlinkability analysis with mated and non-mated score distribution (single protection).

generated (mated) templates using different keys, which gives 10000 ($= 100 \times 100$) mated scores. Similarly, 4950 non-mated scores were computed by comparing the transformed template of each finger with that of a different finger. The mated and non-mated score distributions are plotted in Figure 3.9, which shows that they highly overlap with each other with $\mathbf{D^{sys}_{\leftrightarrow}} = 0.06$. Hence, the proposed scheme under dual protection is almost fully unlinkable.

3.4.5 Security analysis

We now analyse the security of the designed cancelable templates. In the proposed method, single protection is offered by the window-shift-XOR model. This model in combination with the partial DWT provides dual protection. Our security analysis covers both.

The window-shift-XOR model aims to uncertainty to the MCC binary vectors through the window-based XOR operation. Upon completion of this operation,

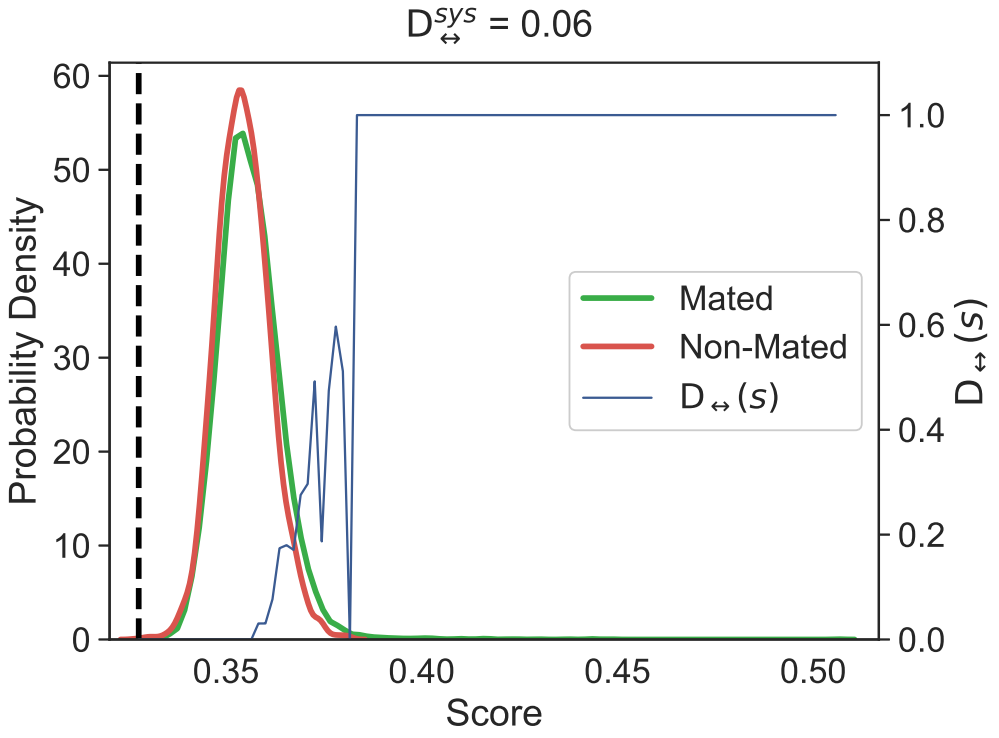

FIGURE 3.9: Unlinkability analysis with mated and non-mated score distribution (dual protection).

the candidate segment chosen for performing XOR is discarded. To restore the MCC binary vector $\mathbf{x}_c$ from the output $\mathbf{y}_c$ (see (3.11)) of the window-shift-XOR model, the adversary must recover the discarded candidate segment and other (pre-XOR) bits in $\mathbf{x}_c$. Given a Boolean variable a, performing XOR yields $a \oplus 0 = a$ and $a \oplus 1 = \bar{a}$, where $\bar{a}$ denotes the complement of a. Thus, to retrieve the pre-XOR bits, it depends on the bits in the (discarded) candidate segment. For instance, if the bit in the candidate segment is 1 and the post-XOR result is g, then the pre-XOR bit must be $\bar{g}$. In the MCC representation 0s and 1s are not uniformly distributed and there are many more 0s than 1s. Take the window size $S = 384$ for example. If we use the last segment as the candidate, it performs element-wise XOR with other segments and is then discarded. There are about 5% 1s in this segment, i.e., 22 bits. To find these binary 1 bits requires $\begin{pmatrix} 384 \\ 22 \end{pmatrix} = 3.45 \times 10^{35} \approx 2^{118}$ attempts. Given that there are 30-60 minutiae in a fingerprint image and each minutia is associated with one $\mathbf{x}_c$, it leads to a total of $2^{3540} (= 2^{118 \times 30})$ attempts

in order to reconstruct all $\mathbf{x}_c$. This is computationally infeasible. However, if a smaller window is set, say $S = 150$, it would take less effort to pinpoint the binary 1 bits (calculation omitted for brevity). Therefore, the proposed method has dual protection to further strengthen template security.

With the aid of the window-shift-XOR model, the ARM can be resisted by setting different window sizes and selecting different candidate segments for the XOR operation. Doing so renders $\mathbf{y}_c$ distinct in different applications, although they are derived from the same fingerprint. For two applications, even if only one bit is different in $\mathbf{y}_c$, vector $\mathbf{z}_c$ would be totally different after the DCT. This addresses the root problem in the ARM. Moreover, the partial DWT is applied to $\mathbf{z}_c$ such that the original MCC binary vector $\mathbf{x}_c$ is given dual protection. Matrix $\bar{\mathbf{A}}$ in (3.12) is always column rank deficient, thus making the mapping from $\mathbf{z}_c$ to $\mathbf{w}_c$ many to one. Even when both $\bar{\mathbf{A}}$ and $\mathbf{w}_c$ are compromised, it is hard to determine the true $\mathbf{z}_c$ due to this many-to-one mapping.

3.4.5.1 Pre-image attacks

It is a security hazard if an adversary can build a dictionary that contains possible pre-images of the original biometric feature. This is known as the pre-image attack, which was recently formulated as the similarity-based attack (SA) by Chen et al. [134]. The most computationally feasible way to create a pre-image of the proposed cancelable template is to apply the pseudo-inverse to (3.12), which is expressed by

$$\hat{\mathbf{z}}_c = \bar{\mathbf{A}}^{\dagger}\mathbf{w}_c \tag{3.16}$$

where $\bar{\mathbf{A}}^{\dagger}$ is the pseudo-inverse of $\bar{\mathbf{A}}$ and $\hat{\mathbf{z}}_c$ the least-squares estimate of $\mathbf{z}_c$. Suppose that the adversary acquires two stored (transformed) templates $\mathbf{w}_c^{(X)}$ and $\mathbf{w}_c^{(Y)}$ of the same user from Applications X and Y and their associated transformation matrices $\bar{\mathbf{A}}^{(X)}$ and $\bar{\mathbf{A}}^{(Y)}$. It follows from (3.16) that $\hat{\mathbf{z}}_c^{(X)}$ and $\hat{\mathbf{z}}_c^{(Y)}$ can be found. Using the normalized inner product, we can measure how close $\hat{\mathbf{z}}_c^{(X)}$ and

$\hat{\mathbf{z}}_c^{(Y)}$ are as well as how close either of them is to the true $\mathbf{z}_c$. That is,

$$d_1(\mathbf{z}_c, \hat{\mathbf{z}}_c^{(X)}) = 1 - \frac{\mathbf{z}_c^T \hat{\mathbf{z}}_c^{(X)}}{||\mathbf{z}_c||_2 \, ||\hat{\mathbf{z}}_c^{(X)}||_2} \tag{3.17}$$

$$d_2(\mathbf{z}_c, \hat{\mathbf{z}}_c^{(Y)}) = 1 - \frac{\mathbf{z}_c^T \hat{\mathbf{z}}_c^{(Y)}}{||\mathbf{z}_c||_2 \, ||\hat{\mathbf{z}}_c^{(Y)}||_2} \tag{3.18}$$

$$d_3(\hat{\mathbf{z}}_c^{(X)}, \hat{\mathbf{z}}_c^{(Y)}) = 1 - \frac{(\hat{\mathbf{z}}_c^{(X)})^T \hat{\mathbf{z}}_c^{(Y)}}{||\hat{\mathbf{z}}_c^{(X)}||_2 \, ||\hat{\mathbf{z}}_c^{(Y)}||_2} \tag{3.19}$$

Using a subset of FVC2002 DB2, Fingers 30-50, for each of these fingers, we apply (3.16) to determine their most computable pre-images of $\mathbf{z}_c$, i.e., two least-squares estimates with two randomly generated keys $\mathbf{k}$ in (3.13), thus simulating Applications X and Y. Then based on (3.17)-(3.19), we calculate the distance between the true $\mathbf{z}_c$ and either of the two least-squares estimates and the distance between the two estimates. All the above are computed using MATLAB with the results given in Table 3.11. We can see that neither of the estimates is close to the true $\mathbf{z}_c$, nor are the two estimates close.

TABLE 3.11: The average Euclidean distance (in pixels) between the actual and modelled minutiae of each finger in the database FVC2002 DB2 (100 fingers).

Finger No.	30	31	32	33	34	35	36
$d_1(\mathbf{z}_c, \hat{\mathbf{z}}_c^{(X)})$	0.6523	0.6746	0.6251	0.6163	0.6188	0.6443	0.6491
$d_2(\mathbf{z}_c, \hat{\mathbf{z}}_c^{(Y)})$	0.6721	0.6398	0.6240	0.5910	0.6456	0.6399	0.6387
$d_3(\hat{\mathbf{z}}_c^{(X)}, \hat{\mathbf{z}}_c^{(Y)})$	0.8463	0.8199	0.8122	0.7831	0.7757	0.7886	0.7929
Finger No.	37	38	39	40	41	42	43
$d_1(\mathbf{z}_c, \hat{\mathbf{z}}_c^{(X)})$	0.6487	0.6523	0.6583	0.6917	0.6420	0.6337	0.6239
$d_2(\mathbf{z}_c, \hat{\mathbf{z}}_c^{(Y)})$	0.6691	0.6664	0.6788	0.6406	0.6495	0.6488	0.6516
$d_3(\hat{\mathbf{z}}_c^{(X)}, \hat{\mathbf{z}}_c^{(Y)})$	0.8141	0.8626	0.8462	0.7833	0.8058	0.8254	0.8383
Finger No.	44	45	46	47	48	49	50
$d_1(\mathbf{z}_c, \hat{\mathbf{z}}_c^{(X)})$	0.6354	0.6461	0.6724	0.6208	0.6184	0.6325	0.6155
$d_2(\mathbf{z}_c, \hat{\mathbf{z}}_c^{(Y)})$	0.6332	0.6378	0.6761	0.6355	0.6476	0.6068	0.6442
$d_3(\hat{\mathbf{z}}_c^{(X)}, \hat{\mathbf{z}}_c^{(Y)})$	0.8217	0.8027	0.7891	0.7880	0.8395	0.7779	0.8391

To validate through experiments whether the proposed scheme can ward off pre-image attacks, we carried out two attack scenarios [121]:

- *Type-I Attack*: A reconstructed template is used to attack a system containing the original template, i.e., a template created from the same impression.

- *Type-II Attack*: A reconstructed template is used to attack a system containing a template created from another impression of the same finger.

With the pre-image $\hat{\mathbf{z}}_c$ obtained from (3.16), we tested Type-I Attack and Type-II attack scenarios using FVC2002 DB2. For Type-I Attack, a total of $800(= 8 \times 100)$ attacks were launched. For Type-II Attack, there were $2800(= ((8 \times 7)/2) \times 100)$ attacks in total. Moreover, Type-I and Type-II attack scenarios were each evaluated at two different security levels [121]:

1. Medium security – the verification threshold is set to 0.1% FAR.
2. High security – the verification threshold is set to 0% FAR.

Table 3.12 reports the percentage of successful pre-image attacks at both security levels. Figure 3.10 shows the score distributions of the proposed scheme against pre-image attacks in comparison with genuine and imposter score distributions. It is evident from Table 3.12 and Figure 3.10 that the proposed method is immune to pre-image attacks.

TABLE 3.12: Percentage of successful pre-image attacks at medium and high security levels

Security level	Type-I Attack	Type-II Attack
Medium security	0 %	0 %
High security	0 %	0 %

3.4.5.2 Masquerade attacks

Masquerade attacks are similarity-based attacks [134], where the synthetic input bears a large degree of resemblance to the actual template. We simulated the masquerade attack by producing binary vectors that are very similar to the MCC's binary template $\mathbf{x}_c$; see (3.6). Specifically, in our experiments, we varied a small number of bits, say n bits, in the synthetic binary input such that the fabricated binary vectors resemble the actual $\mathbf{x}_c$ to a large extent. For example, with each

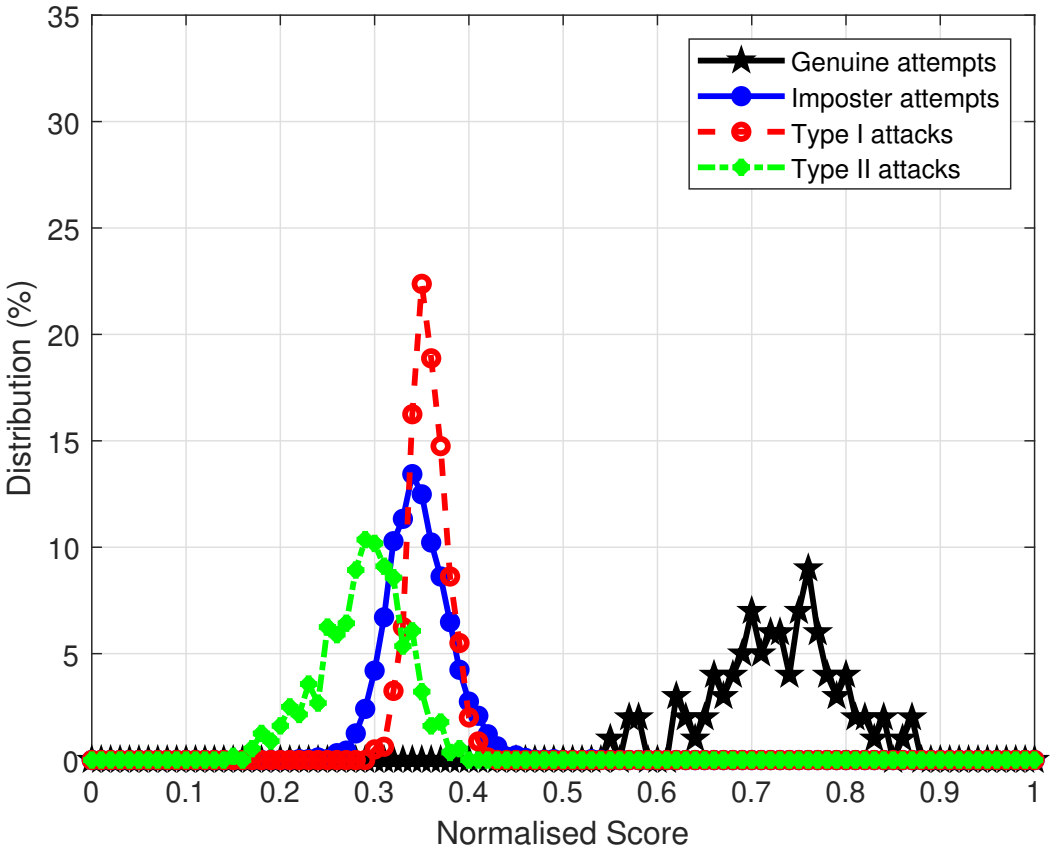

FIGURE 3.10: Score distributions of the proposed scheme against pre-image attacks in comparison with genuine and imposter score distributions.

TABLE 3.13: Percentage of successful masquerade attacks at medium and high security levels

No. of bits*	Medium security		High security	
	Type-I Attack	Type-II Attack	Type-I Attack	Type-II Attack
20	0.87%	0.14%	0%	0%
30	0.37%	0%	0%	0%
45	0%	0%	0%	0%

* No. of bits in the synthetic input that are different to MCC's template.

binary string of the MCC template being 1536 bits long, if $n = 30$, it means that only 30 bits in the synthetic binary input are different to $\mathbf{x}_c$; or equivalently, 1506 (out of 1536) bits are identical to $\mathbf{x}_c$. It is worth mentioning that the selection of these n bits to fabricate the synthetic binary input is totally random. In other words, the location of these n bits is random and can be anywhere in the synthetic input that is different to the MCC's binary template.

As discussed earlier, we evaluated the ability of the proposed cancelable template

design to tackle masquerade attacks under Type-I and Type-II attack scenarios at both medium and high security levels using FVC2002 DB2. Note that in either the Type-I or Type-II attack scenario, we used in our tests different user-specific parameter keys $\mathbf{k}$ in (3.13). This is agreeable with the real-life case where each user has his/her own secret key. With a varying number of bits different to the MCC's binary template, e.g., $n = 20, 30, 45$, we show in Table 3.13 the percentage of successful masquerade attacks at medium and high security levels, respectively. We can see from Table 3.13 that when $n = 45$, although each synthetic binary input has a ma-jority of bits (1491 out of 1536 bits) that are the same as the MCC's actual template, the proposed scheme can 100% defend masquerade attacks at both security levels. For $n = 30$, in Figure 3.11 we plot the score distributions of the proposed scheme against masquerade attacks in comparison with genuine and imposter score distributions. It can be clearly observed from Table 3.13 and Figure 3.11 that the proposed method is able to avert masquerade attacks.

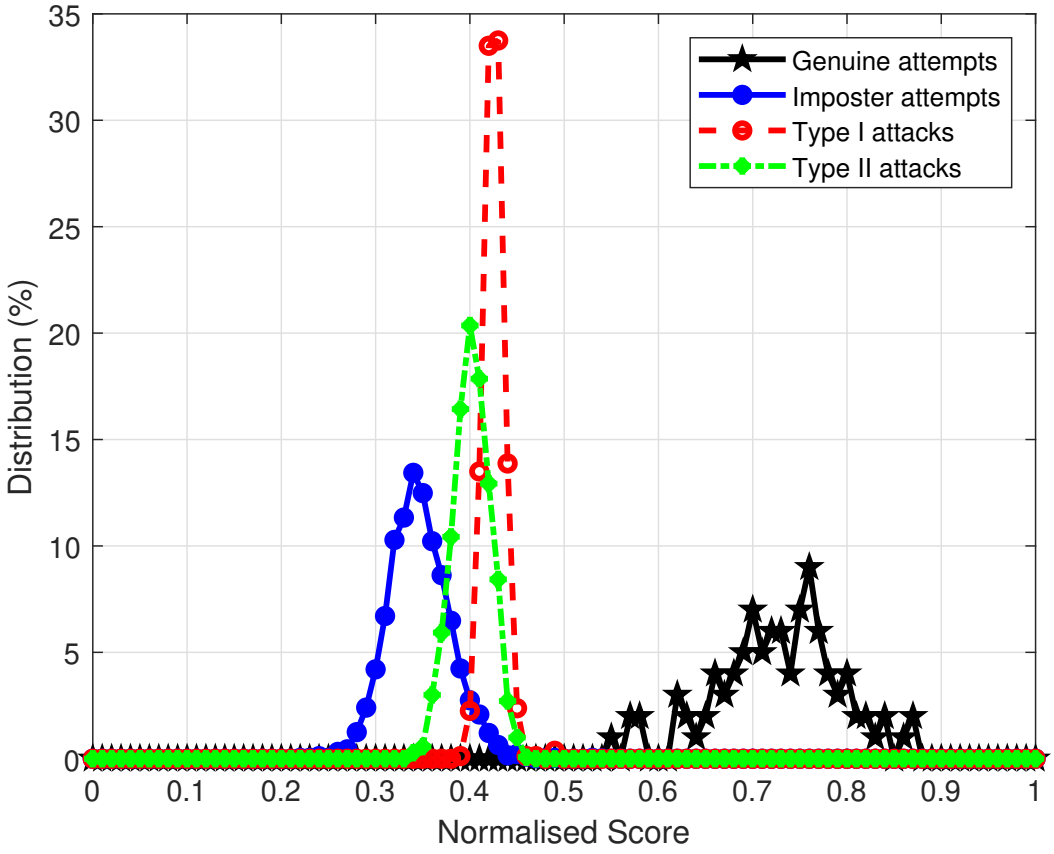

FIGURE 3.11: Score distributions of the proposed scheme against masquerade attacks in comparison with genuine and imposter score distributions.

The low or zero successful masquerade attack rate reported in Table 3.13 is attributable to the window-shift-XOR model and the partial DWT. The window-shift-XOR operation enables the flipped n bits in the synthetic binary input to affect other parts of the input. Then the DCT and partial DWT transform the output from the window-shift-XOR model according to the user-specific key, thus further impacting the overall result.

3.5 Summary

Cancelable fingerprint template design faces challenges such as performance degradation after transformation and the ARM threat. With the aim of addressing these issues, we propose alignment-free cancelable fingerprint templates. The proposed method is equipped with dual protection, provided by the window-shift-XOR model and the partial DWT. The former tackles the ARM and is combined with the latter to further strengthen security and enhance performance. Built upon the state-of-the-art MCC minutia descriptor, the designed cancelable templates demonstrate excellent recognition accuracy, which is equal to the performance of the MCC template and is better than nearly all existing alignment-free cancelable templates. For instance, the EER of the proposed method in the lost-key scenario under the 1vs1 protocol is 0% for both FVC2002 DB1 and DB2, 1.63% for FVC2002 DB3, 7.35% for FVC2004 DB1 and 4.69% for FVC2004 DB2.

Chapter 4

A Cancelable Biometric Authentication System Based on Feature-Adaptive Random Projection

I would rather have questions that can't be answered than answers that can't be questioned.

– Richard Feynman

4.1 Introduction

As discussed in Chapter 2, there are several methods available that allow one way transformation to produce cancelable biometrics (Figure 2.1). Random projection is one of those transformation methods which efficiently and effectively achieve biometric template protection. In a random projection-based method, template protection is provided by projecting the original template feature vector into another feature vector of lower dimensions, which is also known as many-to-one

mapping. The projection is guided by a projection matrix, which is created with the help of a user-specific key.

Unlike standard encryption methods, e.g., AES, which assume that these parameters, e.g. user-specific keys are secret [94], in biometrics, the user-specific key and all other transformation parameters are assumed to be public. For the reason that usually transformation parameters are kept in a token, it is called a token-stolen scenario if the token is compromised. Since storing these parameters raises the same security concerns as storing the original template data, it is desirable that the disclosure of these parameters does not threaten system security, especially the security of template data.

ARM suggests that an original biometric feature vector is retrievable from multiple transformed templates and relevant user-keys by reconstructing the projection matrix. Hence, traditional random projection-based biometrics are prone to ARM [126] in the stolen-token scenerio. In this chapter, we propose a random projection-based cancelable fingerprint template which mitigates the ARM threat by constructing the projection matrix from within the local feature slots of a fingerprint and is discarded after use. In such a case, the original fingerprint feature vector is irretrievable even if the user-specific key is lost. When template data are secure, user identity is safe, which ensures that personal data or sensitive information stored in the database or other devices can only be accessed by legitimate users. The extensive experiments demonstrate that the proposed scheme not only preserves recognition accuracy but also prevents ARM.

The rest of the chapter is organized as follows. The motivation and contributions of this work are presented in Section 4.2. The proposed system is detailed in Section 4.3. In Section 4.4, the experiment results and analysis are discussed. Finally, the summary is provided in Section 4.5.

4.2 Motivation and Contribution

4.2.1 Motivation

In traditional random-projection based methods (refer to Chapter 2), the irreversibility of the many-to-one mapping is guaranteed based on the theory that in a linear system, there are infinite solutions if the linear equation system is non-full-rank [135]. However, if the adversary obtains multiple protected templates generated from the same original feature vector, the projection matrix can be made to be full-rank by concatenating multiple non-full-rank ones, ARM scheme [126, 136] (readers can refer to [126, 136] for details of the ARM). We illustrate the ARM attack strategy targeting cancelable templates through a simple example. From the analysis of the ARM attack, we show that one key element in random projection-based cancelable template systems could be used by the attacker to launch the ARM. To protect this key element, we propose our solution against the ARM.

Here, an example is given to demonstrate how the ARM can threaten cancelable systems that use many-to-one random project or mapping [137]. Assume that, in application A, the original template feature $\mathbf{X} = [x_1, x_2, x_3, x_4, x_5] = [1, 2, 3, 4, 5]$, and its corresponding transformation matrix is

$$\mathbf{M} = \begin{bmatrix} 2 & 3 & 3 \\ 4 & 2 & 5 \\ 1 & 4 & 3 \\ 3 & 2 & 4 \\ 3 & 1 & 2 \end{bmatrix}$$

By the many-to-one projection equation, $\tilde{\mathbf{X}} = \mathbf{XM}$, a transformed template feature is obtained as $\tilde{\mathbf{X}} = [40, 32, 48]$. In this case, even if $\tilde{\mathbf{X}}$ and $\mathbf{M}$ are known to

the adversary, it is difficult to find the original template feature $\mathbf{X}$ through (4.1),

$$\begin{aligned} 2x_1 + 4x_2 + x_3 + 3x_4 + 3x_5 &= 40 \\ 3x_1 + 2x_2 + 4x_3 + 2x_4 + x_5 &= 32 \\ 3x_1 + 5x_2 + 3x_3 + 4x_4 + 2x_5 &= 40 \end{aligned} \tag{4.1}$$

The solutions to $\mathbf{X}$ are infinite because the number of variables in (4.1) is larger than the number of equations, so $\mathbf{X}$ is safe in this case. But, if there is another projection matrix $\mathbf{M}'$ and its corresponding transformed feature $\tilde{\mathbf{X}}'$ is also acquired by the attacker in application B, where

$\mathbf{M}' = \begin{bmatrix} 3 & 3 & 1 \\ 6 & 5 & 1 \\ 4 & 2 & 3 \\ 2 & 5 & 4 \\ 2 & 1 & 4 \end{bmatrix}$ and $\tilde{\mathbf{X}}' = [45, 44, 48]$, then the attacker is able to obtain (4.2) below:

$$\begin{aligned} 3x_1 + 6x_2 + 4x_3 + 2x_4 + 2x_5 &= 45 \\ 3x_1 + 5x_2 + 2x_3 + 5x_4 + x_5 &= 44 \\ x_1 + x_2 + 3x_3 + 4x_4 + 4x_5 &= 48 \end{aligned} \tag{4.2}$$

By combining the linear equations from both (4.1) and (4.2), the attacker will have enough information to uniquely determine the value of $\mathbf{X}$ that is $[1, 2, 3, 4, 5]$.

In the above example, the key is that multiple random projection matrixes are obtained and utilized by the adversary to generate a full-rank linear equation system and launch the ARM. Our proposed solution is based on the observation that if neither $\mathbf{M}$ nor $\mathbf{M}'$ is available to the adversary, then the adversary cannot calculate the original feature vector $\mathbf{X} = [x_1, x_2, x_3, x_4, x_5]$. Therefore, preventing the transformation matrix from being known by the adversary is a feasible solution to combat the ARM.

4.2.2 Contribution

In this chapter, we propose a new cancelable biometric authentication system using a feature-adaptive random projection method to provide user authentication while protecting biometric template data against the ARM. The main contributions of this chapter are as follows:

1. In the proposed method, the generation of the projection matrix for performing random projection is feature-adaptive. In other words, the projection matrix is generated from one basic matrix together with a number of vectors extracted from local feature slots. With a different feature slot, the generated projection matrix is different. Moreover, the projection matrixes after usage will be discarded. In this way, the adversary is unable to obtain enough information to launch the ARM, which is a clear advantage over traditional random projection-based schemes.

2. In most existing random projection schemes, random projection is carried out on the whole feature vector. Instead, in the proposed method, the random projection is performed locally on feature slots, each of which is part of the feature vector. In this way, any inaccuracy or errors are localised rather than affecting the entire transformed feature vector. Obviously, this is different to the traditional random projection based cancelable template design and is an improvement over the existing methods.

3. The proposed method has good compatibility. No matter how feature data are extracted from whatever biometric traits, e.g., face, finger-vein, iris, as long as they are in the binary format, the proposed method is applicable. This allows the proposed method to be exploited by biometric authentication systems in general, e.g., face or fingerprint recognition systems, thus benefiting applications in different scenarios.

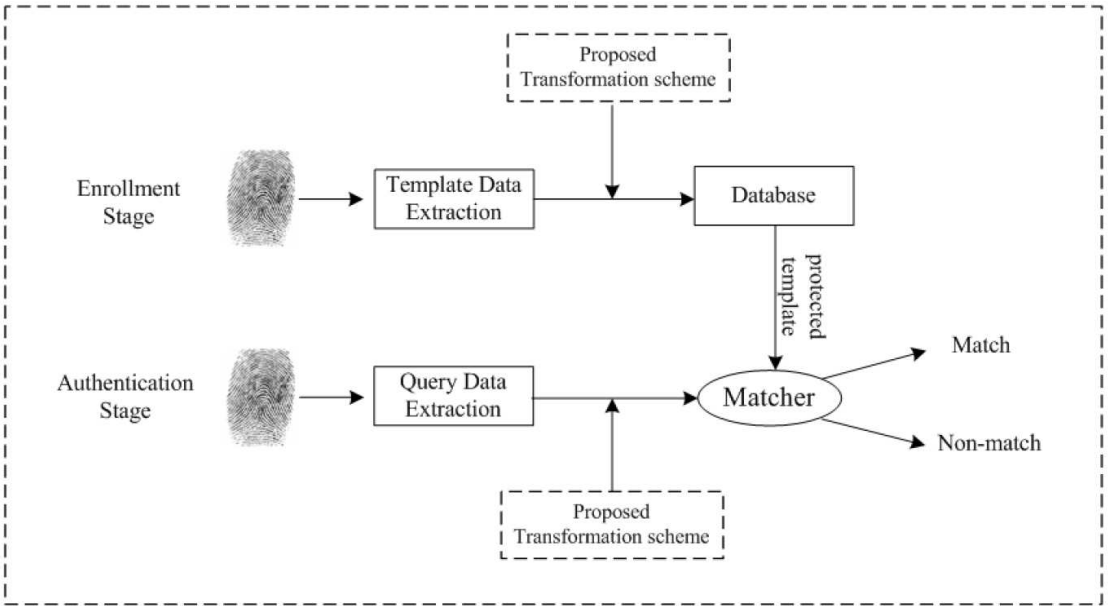

FIGURE 4.1: An overview of the proposed cancelable biometric authentication system (adapted from [131]).

4.3 Proposed System

An overview of the proposed cancelable biometric authentication system is illustrated in Figure 4.1. The proposed system comprises three major steps, namely, stable biometric feature extraction, feature data protection with feature-adaptive random projection and matching in the encrypted domain, detailed as follows.

4.3.1 Stable Biometric Feature Extraction

The first step is to extract stable biometric features. A fix-length feature descriptor of fingerprint minutiae, named minutia pair (MP), is used to perform this task. The initial version and the variant of the MP descriptor can be found in our previous work [97] and [138], respectively. In this section, we explain the foundation for the minutia descriptor [97][112].

4.3.1.1 Invariant Features from Minutiae Pairs

Given any two minutiae $m_i = x_i, y_i, \theta_i, t_i$ and $m_j = x_j, y_j, \theta_j, t_j$ from a minutia set, a local structure can be constructed as shown in Figure 4.2. The process of

creating local structures is immune to noise to a certain degree since the minutiae points in a pair are redundantly combined. The local structure can be expressed as an invariant feature vector as:

$$V_{ij} = (L_{ij}, \alpha_i, \alpha_j, t_i, t_j) \tag{4.3}$$

where

1. L_{ij} represents the length of the line connecting minutiae m_i and m_j in pixels.
2. α_i and α_j are the angles between the orientation of minutiae m_i , m_j and the line segment in the counter-clockwise direction, respectively. The range of α_i and α_j is (0, π).
3. t_i and t_j are the minutia types of minutiae m_i and m_j, respectively.

4.3.1.2 Quantization

To accommodate biometric uncertainty such as elastic distortion, feature vector V_{ij} is further quantized with suitable quantization step sizes set for L_{ij}, α_i and α_j, respectively. For instance, L_{ij} is quantized into q segments using a step size of $\frac{L_{ij}}{q}$ pixels. The number q is converted into a binary form using $log2(\frac{L_{ij}}{q})$ bits. Similarly, α_i and α_j are quantized by choosing an appropriate step size and the resultant is represented in a binary notation using the required number of bits Figure 4.3. The values of t_i and t_j are binary, where '0' represents ridge ending and '1' ridge bifurcation, so no quantization is needed for t_i and t_j. Let $n_{L_{ij}}, n_{\alpha_i}, n_{\alpha_j}$ be the number of bits required to represent the quantized L_{ij}, α_i and α_j, respectively, therefore, $n = n_{L_{ij}} + n_{\alpha_i} + n_{\alpha_j} + 2$ total bits are required to represent V_{ij} in (4.3). The binary equivalent of each V_{ij} is represented as $V_{ij}^{(b)}$ of n bits and a set $\mathbf{V}^{(b)}$ can be formed as

$$\mathbf{V}^{(b)} = \{\, V_{ij}^{(b)} : \quad 1 \leq i, j \leq m \;\; and \;\; i \neq j\} \tag{4.4}$$

where m represents the total number of minutiae.

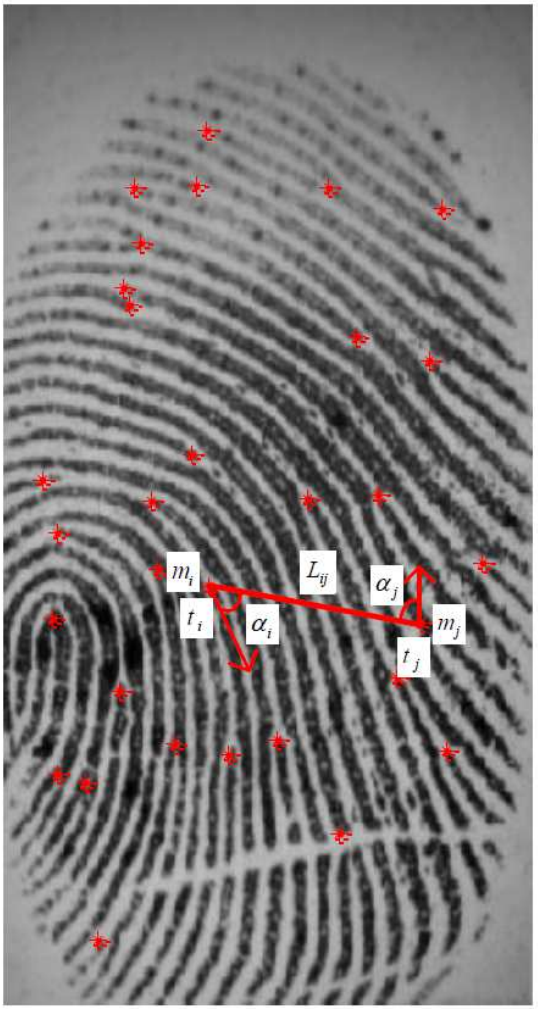

FIGURE 4.2: An example of a local minutia structure - minutia pair (MP). (adapted from [138]).

4.3.1.3 Histogram binning

Histogram binning is a crucial step towards producing binary features. The process is initialized by creating a null vector of length of 2^n bins. After this, a bin corresponding to the decimal equivalent to each $V_{ij}^{(b)}$ in set $\mathbf{V}^{(b)}$ is indexed by one. During this process, some bins might be indexed more than once hence the resultant vector at the end of the binning process isn't strictly binary.

4.3.1.4 Binarization

After histogram binning, a final feature vector is obtained in a such a way that the bins which are indexed only once are assigned a value of 1 and all other bins are

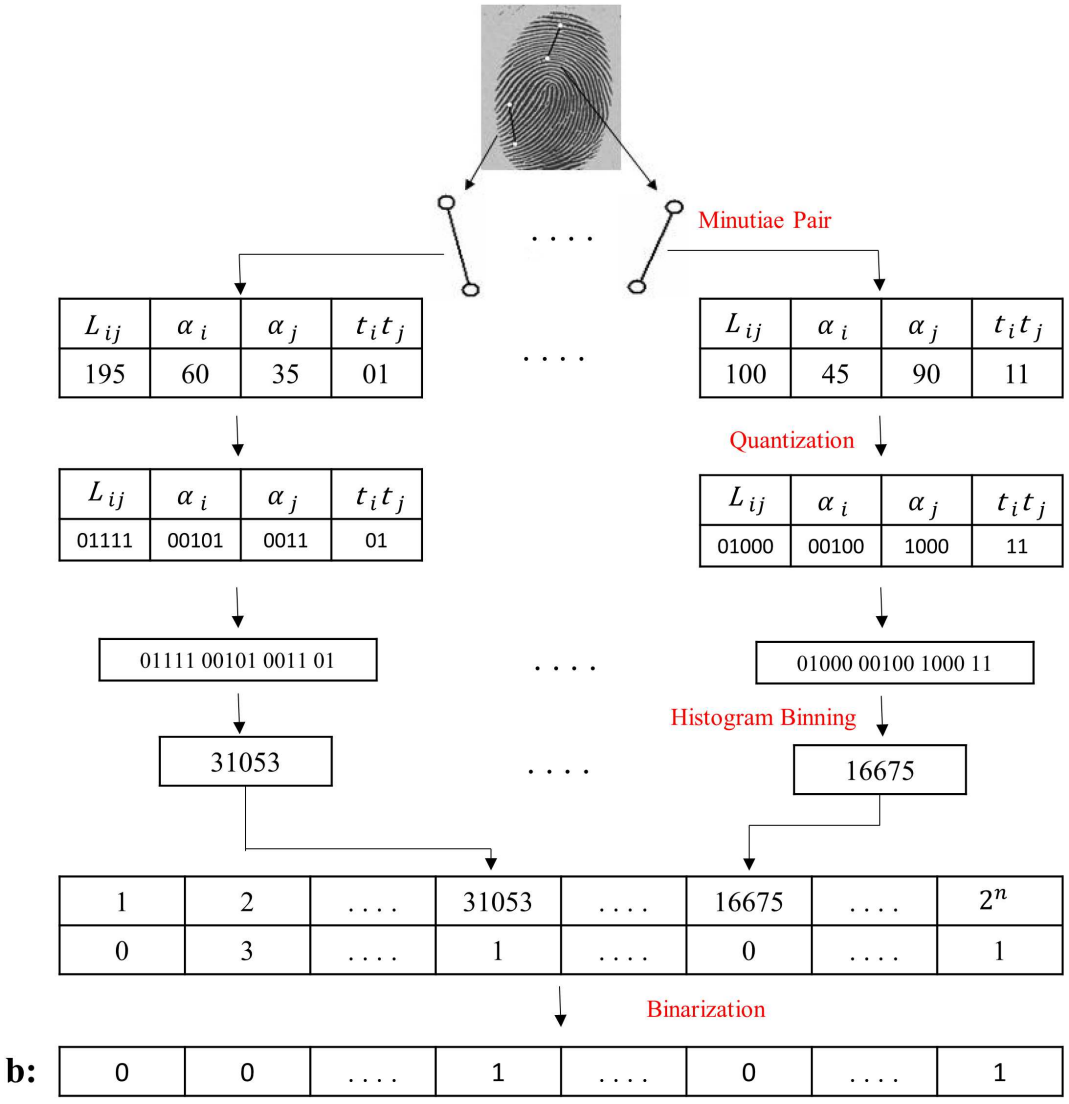

FIGURE 4.3: Binary feature extraction from minutia pair. (adapted from [112]).

assigned a value of 0. Hence, the resultant vector is strictly binary and is denoted by **b** as shown in Figure 4.3. Then, we protect **b** using the proposed feature-adaptive random projection method (see details in Section 4.3.2) and perform matching in the encrypted domain (see details in Section 4.3.3).

4.3.2 Feature Data Protection Using Feature-Adaptive Random Projection

To secure the extracted biometric feature data, as discussed in Section 4.3.1, in this section, a feature-adaptive random projection-based transformation method

is proposed. The entire transformation process of the proposed method is demonstrated in Figure 4.4. We enhance the random projection in such a way that the projection matrices must adapt to biometric local feature slots and be discarded after use. This makes it difficult for the adversary to determine the actual projection matrices and to launch the ARM. The steps of the proposed method are detailed as follows.

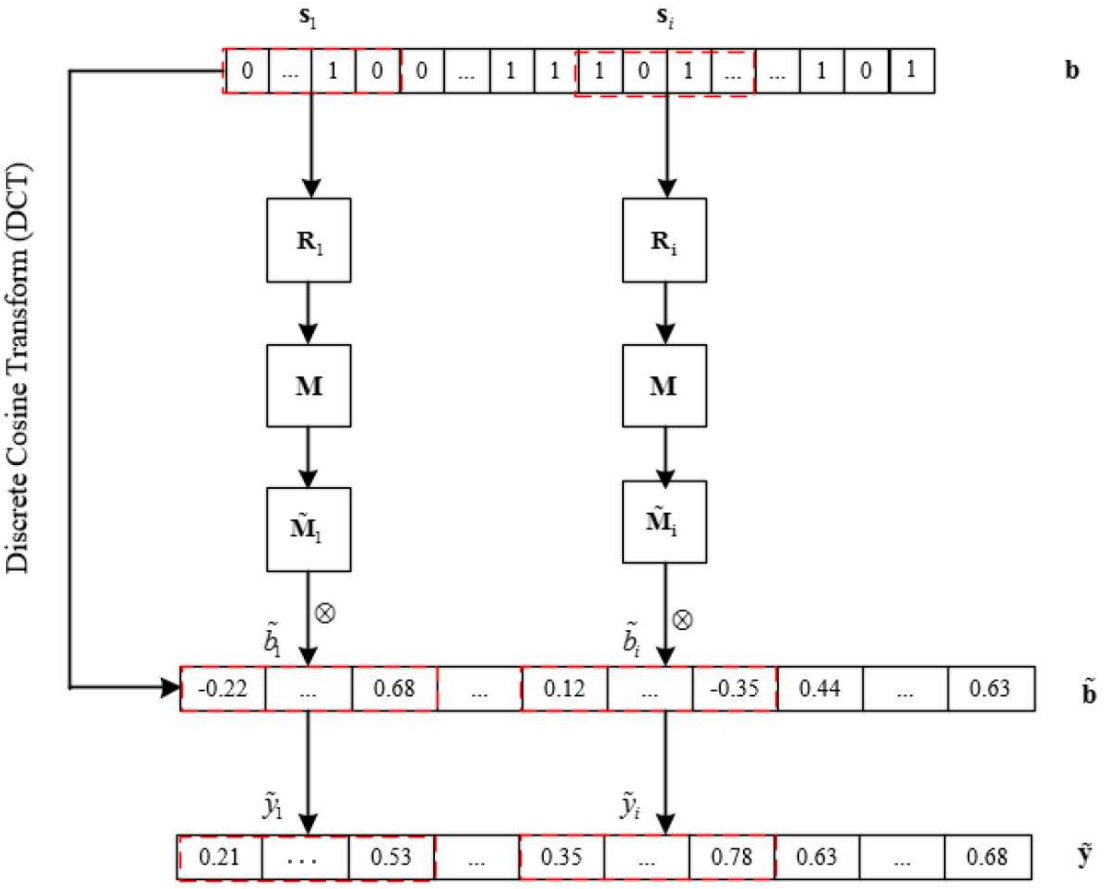

FIGURE 4.4: The proposed feature-adaptive random projection-based transformation.

Suppose the extracted binary feature vector $\mathbf{b} = [0, 1, ..., 0, 0]$ of length l is derived from the feature extraction process conducted on an input biometric image. With a user-specific random projection matrix $\mathbf{M}$, which should have more rows than columns, the conventional random projection in the context of biometric template protection can be expressed by

$$\mathbf{y} = \mathbf{bM} \tag{4.5}$$

Our objective is to increase the security of the above transformation by altering both binary feature vector $\mathbf{b}$ and projection matrix $\mathbf{M}$.

Since biometric feature vector b contains only values of 0 and 1, and is usually sparsely distributed, it might make the search space for the solution of b narrow, when $\mathbf{y}$ and $\mathbf{M}$ in (4.5) are both acquired by the attacker. To address this problem, we first apply the DCT to the binary-valued feature vector $\mathbf{b}$, i.e., $\tilde{\mathbf{b}} = \mathrm{DCT}(\mathrm{b})$ before performing random projection. The DCT transfers $\mathbf{b}$ from a binary-valued feature vector into the real-valued feature vector $\mathbf{b}$, and hence randomness and the search space are increased, making it harder for the attacker to tackle the random projection and restore $\mathbf{b}$. Note that the purpose of taking the DCT prior to the random projection is not to attain the property of non-invertibility in that the DCT is invertible [138]. Non-invertibility is realized by the subsequent feature-adaptive random projection. The DCT simply transforms the binary vector $\mathbf{b}$ to the real vector $\tilde{\mathbf{b}}$.

To alter projection matrix $\mathbf{M}$, we adapt it to $\tilde{\mathbf{M}}_i$ with the help of a set of feature-specific matrices $\mathbf{R}_i$, generated from local feature slots $\mathbf{s}_i$, where i is the slot number. When random projection is performed, we use the feature-adapted projection matrix $\tilde{\mathbf{M}}_i$ in a slot-by-slot manner instead of fixed matrix $\mathbf{M}$. We call this local feature projection. After local feature projection is done, projection matrix $\tilde{\mathbf{M}}_i$ is discarded. Although $\mathbf{M}$ is a user-specific parameter key stored in the database, it is hard for the adversary to work out $\tilde{\mathbf{M}}_i$ from $\mathbf{M}$, so ARM can be defended (see security analysis in Section 4.4.3).

We now describe local feature projection in detail. Let matrix $\mathbf{M}$ of size $j \times q$ be user-specific with $j > q$. We divide the binary feature vector $\mathbf{b}$ into p slots and each slot contains j elements (here $p \times j = l$), denoted by $\mathbf{b} = \mathbf{s}_1||...||\mathbf{s}_i||...||\mathbf{s}_p$. The i^{th} slot of $\mathbf{b}$ can be written as $\mathbf{s}_i = [s_{i-1}, ..., s_{i-j}]$, where $i \in [1, p]$. Vector s_i and its slot number i are used as the seed and input into a random number generator (RNG), *rand*(.) , which outputs a real-valued, slot-feature related matrix $\mathbf{R}_i$ of

size $j \times q$, i.e.,

$$\mathbf{R}_i = rand(\mathbf{s}_i, i) \tag{4.6}$$

The RNG function *rand*(.) can be any generic random number generator; for example, the well-known linear congruential generator, which is defined by the recurrence relation $X_{n+1} = aX_n \bmod m$, where m is the modulus, a is the multiplier and X_0 is the seed [139]. The size of matrix $\mathbf{R}_i$ is the same as that of $\mathbf{M}$, namely $j \times q$. Since $\mathbf{s}_i$ is used as part of the seed for *rand*(.) , if any of the j elements in $\mathbf{s}_i$ are changed, then the generated $\mathbf{R}_i$ are totally different. Therefore, the slot length j of vector $\mathbf{s}_i$ is an important parameter which impacts the system's recognition performance and thus needs careful tuning (see detailed discussion in Section 4.4).

Once $\mathbf{R}_i$ is generated, it is treated as a kernel and used to alter the user-specific key, matrix $\mathbf{M}$ as follows:

$$\tilde{\mathbf{M}}_{\mathrm{i}} = f(\mathbf{R}_i, \mathbf{M}) \tag{4.7}$$

where function f(.) calculates the average of two corresponding elements from $\mathbf{R}_i$ and $\mathbf{M}$. In this way, matrix $\mathbf{M}$ is adapted to become $\tilde{\mathbf{M}}_{\mathrm{i}}$, which is the same size as $\mathbf{M}$ but with different elements. We use $\tilde{\mathbf{M}}_{\mathrm{i}}$ as the projection matrix to transform $\tilde{b}_i$, which is the i^{th} slot of the post-DCT feature vector $\tilde{\mathbf{b}} = \tilde{b}_1||...||\tilde{b}_i...||\tilde{b}_p$. Through this feature-adaptive random projection process, the feature slot $\tilde{b}_i$ is transformed to $\tilde{y}_i$, i.e.,

$$\tilde{y}_i = \tilde{b}_i \tilde{\mathbf{M}}_{\mathrm{i}} \tag{4.8}$$

In regard to $\tilde{b}_i$ of length j, the above feature slot-based random projection produces a size-reduced vector $\tilde{y}_i$ of length q. Moreover, for security reasons, the feature-adapted projection matrix $\tilde{\mathbf{M}}_{\mathrm{i}}$ is discarded after use. After applying (4.8) to each of the p slots in $\tilde{\mathbf{b}} = \tilde{b}_1||...||\tilde{b}_i...||\tilde{b}_p$, we concatenate the p outputs to form vector $\tilde{\mathbf{y}} = \tilde{y}_1||...||\tilde{y}_i...||\tilde{y}_p$, which is the transformed and protected feature vector.

4.3.3 Matching in the Encrypted Domain

In accordance with the proposed feature data protection in Section 4.3.2, once the transformed feature vectors $\tilde{\mathbf{y}}^T$ and $\tilde{\mathbf{y}}^Q$ are obtained from the template and query images, respectively, matching is conducted in the encrypted domain. Here, superscript T represents 'template', while Q represents 'query'. The similarity score between $\tilde{\mathbf{y}}^T$ and $\tilde{\mathbf{y}}^Q$ is given by the following equation according to [120],

$$S(\tilde{\mathbf{y}}^T, \tilde{\mathbf{y}}^Q) = 1 - \frac{||\tilde{\mathbf{y}}^T - \tilde{\mathbf{y}}^Q||_2^2}{||\tilde{\mathbf{y}}^T||_2^2 + ||\tilde{\mathbf{y}}^Q||_2^2} \tag{4.9}$$

where $||.||_2$ denotes the 2-norm. The similarity score $S(\tilde{\mathbf{y}}^T, \tilde{\mathbf{y}}^Q)$ is in the range of [0, 1], where 0 means two feature vectors are completely different, while 1 means they are the same.

Remarks: (i) A binarization procedure is applied to the MP descriptor. Binarization is a quantization technique, which can lessen feature differences caused by biometric uncertainty. The binary feature slot $\mathbf{s}_i$ is part of the seed to generate $\mathbf{R}_i$ (see (4.6)). As analyzed in Section 4.3.2, any change in the elements of $\mathbf{s}_i$ would cause $\mathbf{R}_i$ to be different. Therefore, the binarization procedure is important and indispensable. This is why we choose the MP descriptor, which is a binary feature representation. (ii) To generate $\mathbf{R}_i$, we need the feature slots $\mathbf{s}_i$, but they come from the original binary feature vector $\mathbf{b}$, so it is likely to result in the same $\mathbf{R}_i$ in different applications. This presents a risk of the cross-matching attack [140]. To address this, a key-guided permutation function *perm*(.) can be applied to the original binary feature vector $\mathbf{b}$, e.g., $perm(\mathbf{b}, k_{indx})$, where k_{indx} is a permutation index key and is application-dependent, set differently in different applications.

4.4 Experimental results and analysis

4.4.1 Experimental Results

In this section, the proposed system is evaluated over four public fingerprint databases FVC2002 DB1-DB3 [9] and FVC2004 DB2 [10] and compared with the state-of-the-art methods,. The details of these four databases are given in Table 1.1. Fingerprint minutiae are extracted using the commercial software package, VeriFinger [11]. We applied the proposed feature-adaptive random projection method to secure the MP-based feature representation, which we call S_MP to ease notation. The binary feature representation is produced by the MP descriptor, as explained in Section 4.3.1. For the RNG, we adopted the built-in function *rand*(.) in MATLAB. To evaluate the recognition performance of the proposed

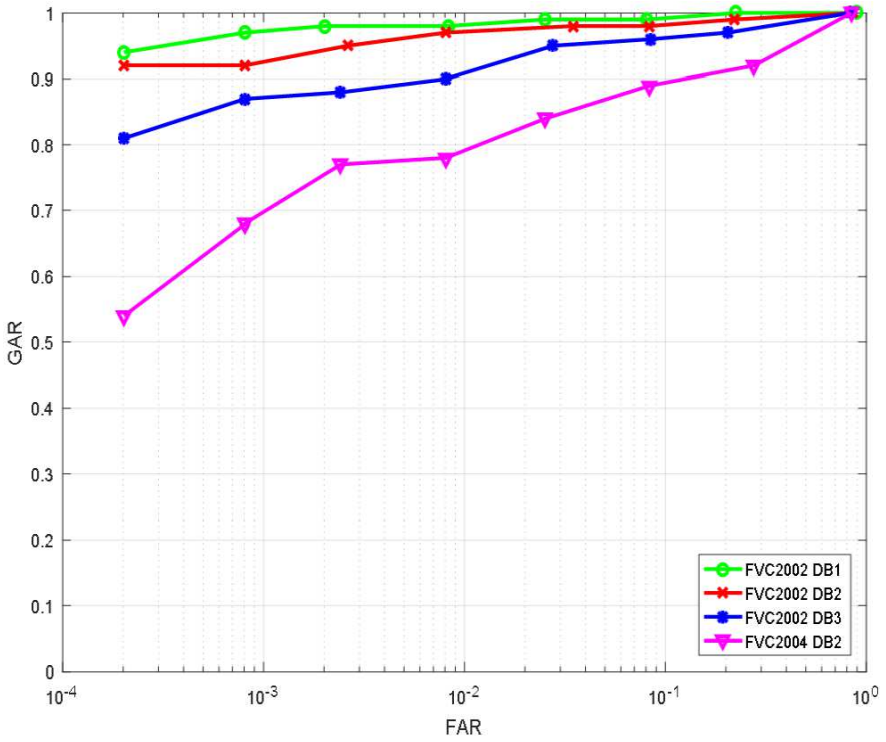

FIGURE 4.5: The ROC curves of the protected system S_MP.

system, we employ several commonly used performance indices i.e., FAR, FRR, EER, as mentioned in Chapter 1. In our experiments, two test cases are carried out on each database. Specifically, in the first test case, the first fingerprint image

is compared with the second fingerprint image of the same finger to calculate the FRR or GAR. This test case produces the FRR or the GAR. In the second test case, the first fingerprint image of each finger is compared with the first fingerprint image of all other fingers. This test case measures the FAR [141].

(1) *System performance using different parameter settings*: In the proposed method, the binary feature vector $\mathbf{b}$ is divided into a number of slots $\mathbf{s}_i$ of equal length. The length j of each slot affects the system's recognition performance. The proposed system is tested using different slot lengths and the corresponding recognition performance in terms of the EER is given in Table 4.1. From Table 4.1, it can be seen that when the slot length j increases, the EER of S_MP deteriorates on databases FVC2002 DB1 and FVC2004 DB2, while no obvious trend is found on the other two databases (FVC2002 DB2 and DB3). Moreover, we observe that under the optimal parameter setting, S_MP performs best on database FVC2002 DB1 with EER=1.00% and performs worst on database FVC2004 DB2 with EER=11.00%. This is because the fingerprint image quality of FVC2004 DB2 is much worse than that of FVC2002 DB1. The receiver operating characteristic (ROC) of S_MP under the best parameter setting is also plotted in the lost-key scenario, as demonstrated in Figure 4.5, where it shows that the FAR increases with the GAR.

TABLE 4.1: The system's recognition performance in terms of the EER(%) with different slot lengths

Slot length, j	**2002DB1**	**2002DB2**	**2002DB3**	**2004DB2**
10	1.00	2.46	4.00	11.00
15	1.00	2.00	7.00	11.00
20	1.05	4.20	6.00	12.11
25	4.00	2.82	7.08	15.00
30	4.00	3.00	7.00	15.43

The parameter q is fixed to be 5 in the experiment.

(2) *Performance comparison with similar existing methods*: Similar to most existing cancelable biometric methods, the proposed method is evaluated in the lost-key scenario, which is the worst case in practice. The recognition performance comparison of the proposed system with the existing random projection-based methods in terms of the EER is reported in Table 4.2. It can be seen from Table 4.2

that our system S_MP and the method in [21] achieve the equal best performance on FVC2002 DB1 and DB2, whereas S_MP performs best on FVC2002 DB3 and FVC2004 DB2. It is worth pointing out that apart from the satisfactory performance of S_MP, the proposed method is invulnerable to the ARM, against which many existing random projection-based cancelable biometric systems cannot compete.

TABLE 4.2: Comparison of recognition performance in terms of the EER (%) under the lost-key scenario

Slot length, j	**FVC2002 DB1**	**FVC2002 DB2**	**FVC2002 DB3**	**FVC2004 DB2**
Jin et al. [90]	3.07	1.02	–	–
Jin et al. [99]	4.36	1.77	–	21.82
Das et al. [127]	2.27	3.79	–	–
Wang and Hu [97]	3.50	4.00	7.50	–
Wang and Hu [123]	3.00	2.00	7.00	–
Wang et al. [102]	1.00	2.00	5.20	13.30
S_MP (proposed method)	1.00	2.00	4.00	11.00

4.4.2 Revocability

Revocability ensures that a compromised template can be canceled and replaced with a new one generated from the same biometric data [106]. It is one of the basic requirements for cancelable biometrics. In the revocability test, 50 transformed templates were created from the first image of each finger in FVC2002 DB2 by assigning different keys, e.g., different $\mathbf{M}$ and different permutation index key k_{indx}. This leads to 5000 ($= 50 \times 100$) new templates in total. The first template was matched against the remaining 49 templates generated from the same finger, so there was a total of 4900 comparisons in this pseudo-imposter test. The score distribution of the test is plotted in Figure 4.6, from which it can be seen that the score distribution almost overlaps with that of the imposter test with different keys for each different finger. This demonstrates that the transformed templates of the same fingerprint are uncorrelated.

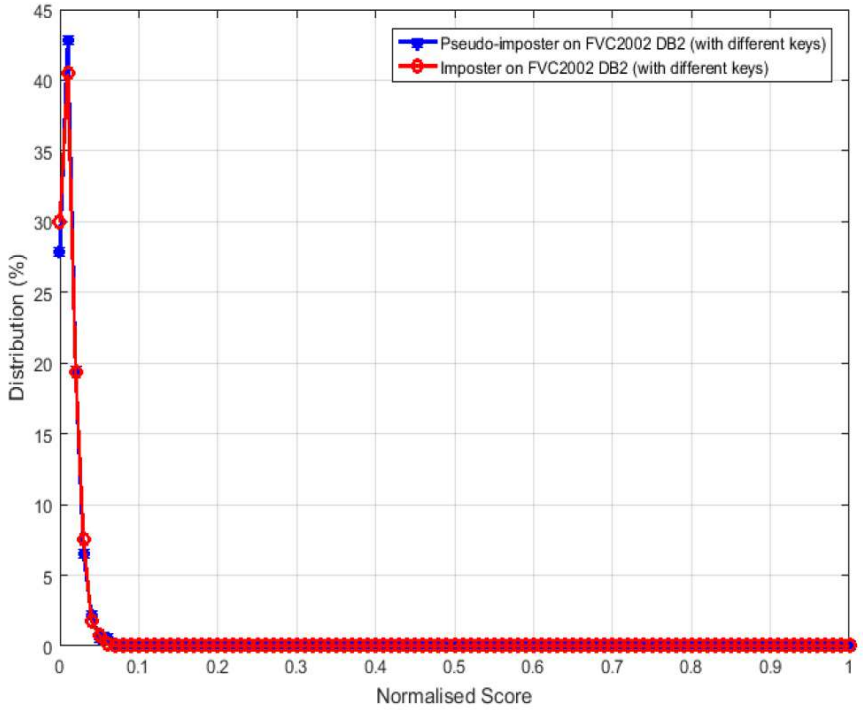

FIGURE 4.6: The imposter and pseudo-imposter distributions for the revocability test using S_MP.

4.4.3 Security Analysis

In this section, we analyze why the proposed method can defend against the brute force attack and the ARM. In particular, we show that the proposed method can prevent the adversary from reconstructing the original MP features from the resultant cancelable template in the lost-key scenario, where we assume that the adversary acquires the transformed feature vector $\tilde{\mathbf{y}}$, matrix $\mathbf{M}$, the RNG function $rand(.)$ and the permutation index key k_{indx}.

The brute force attack: There is no easy way for the adversary to determine the original feature vector b except through exhaustive guessing attempts, namely the brute force attack. In S_MP, the length of the binary feature vector b is $l = 30000$ in this work. Assume that there are $m = 40$ minutiae in a fingerprint image and the local structure formed by any two minutiae from these 40 minutiae is unique, the number of possible locations of 1s in the binary feature vector b can be calculated by $\begin{pmatrix} l \\ m(m\text{-}1)/2 \end{pmatrix}$, which yields an incredibly huge number.

Therefore, it is tremendously difficult for the adversary to determine the original feature vector **b** from brute force guesses.

The ARM: In this attack, if the proposed method is not used, the adversary can utilize multiple compromised templates, e.g., **y**, together with multiple copies of **M**, to build a full-rank linear equation system and thus find a unique solution to (4.5). However, the proposed feature-adaptive random projection method adapts projection matrix **M** in (4.5) to $\tilde{\mathbf{M}}_i$ in (4.8) based on local feature slots. The adapted projection matrix $\tilde{\mathbf{M}}_i$ is discarded after each random projection so it is unavailable and not publicly known. Moreover, the generation of matrix $\mathbf{R}_i$ is dependent on the feature vector **b** rather than any other parameters which are assumed to be public in the lost-key scenario. Therefore, the adversary is unable to work out $\tilde{\mathbf{M}}_i$ from **M** without knowledge of the original binary feature vector **b**. Without knowing $\tilde{\mathbf{M}}_i$, the adversary has no way of recovering original feature vector **b** via the ARM.

4.5 Summary

In this chapter, a feature-adaptive random projection-based cancelable fingerprint authentication system is proposed to provide user authentication and protect biometric template data simultaneously. The proposed method is applied to the fingerprint minutia feature descriptor MP, where the recognition performance of the protected system S_MP is evaluated on four public fingerprint databases. In the proposed method, projection matrices are generated from local feature slots, thereby adapting user-specific key **M** . The adapted projection matrices are discarded after each random projection. In this case, since the attacker has no knowledge about actual projection matrices, he/she is not able to launch the ARM even if the user-specific key **M** and the transformed feature vectors are both revealed. Hence, the proposed system is an enhancement of the existing random projection based cancelable biometric systems, many of which suffer from the ARM. The extensive experiments demonstrate that the proposed system achieves recognition

performance which is competitive enough against the existing random projection-based systems. For instance, the EER of the proposed method in the lost-key scenario under the 1vs1 protocol is 1%, 2%, 4% and 11.00% for FVC2002 DB1-DB3 and FVC2004 DB2, respectively which is better than most of the existing random projection-based systems.

Chapter 5

A lightweight and secure fingerprint authentication system for IoT applications

"If you stumble, make it part of the dance."

– Anon

5.1 Introduction

The capability of electronic devices to communicate with each other in the Internet of Things (IoT) environment is improving day-to-day life. It has a wide range of utility from medical applications to home automation and wearables to industrial applications. With user authentication being an important part of IoT devices, biometric traits such as fingerprints, provide an attractive alternative over traditional password- or token-based authentication since they are unique and cannot be forgotten or lost. Moreover, high recognition accuracy and good security make them effective candidates for identity verification and access control [1]. However,

biometric authentication in IoT comes with certain limitations and vulnerabilities. For instance, IoT devices are resource-limited in terms of power, computing capability and storage space. Moreover, ensuring secure user authentication to defend against possible attack vectors and attack resources is a great challenge which needs to be addressed [142].

To address the aforementioned limitations and security threats in IoT devices, a simple yet efficient fingerprint authentication system is proposed in this chapter. The proposed system adopts a robust pairwise-XOR approach on MCC's binary features in an intelligent way that results in reduced feature size (see section 5.4.3). Consequently, it requires significantly low resources in terms of storage space and computational power as well as provides protection against potential attacks. Using public databases FVC2002 DB1-DB3 and FVC2004 DB1-DB2, the performance of the proposed system is validated. A comprehensive security analysis of the system is presented using maximum aposteriori probability (MAP), which involves the estimate of an unknown based on given data [143].

5.2 Biometric authentication in IoT

In this section, we summarise the work done on the use of biometric authentication in IoT applications. For instance, Habib et al. [144] introduced a biometric-based authentication framework in patient health monitoring in an IoT environment by deploying on-body sensors. In [145], a multimodal biometric system is proposed for some IoT devices using iris and face images taken at the same time by a built-in high quality camera. In another multimodal biometric system proposed for access control and security defence on IoT devices [146], the authors used the user's hand geometry and a sequence of gestures. Prakash and Venkatram [147] proposed an efficient security scheme for home IoT devices equipped with fingerprint authentication. The authors used a Raspberry Pi 2 board for implementation along with relevant sensors and other sets of hardware. In [148], Karimian et al. proposed the use of an electrocardiogram signal (ECG) as a biometric trait for authentication

in an IoT system model. Roy et al. [149] proposed a secure and computationally efficient, remote user biometric authentication for the IoT environment. A more conceptual overview of the use of biometric authentication in IoT is presented in [150].

5.3 IoT constraints related to biometric authentication and its solution

The energy efficiency or the green issue in the IoT environment deals with the study of power consumption by sensor-loaded devices [151, 152]. The objective to study the green issue in the IoT-enabled smart world is to help reduce the greenhouse effect and develop energy-efficient processes at both hardware and software levels [152]. In [153], a reasonable characterization of IoT is provided in terms of the energy efficiency of IoT devices. Readers can refer to the following literature for a range of energy efficiency solutions in IoT, from the hardware architecture level to the software level [154–160].

Some work has already been done in the direction of developing energy-efficient biometric authentication systems for IoT applications. For instance, Dhillon et al. [161] proposed a scheme for developing light biometrics for remote user authentication for IoT devices. Recently, Punithavathi et al. [162] proposed a cloud-based framework for lightweight cancelable biometric authentication for smart IoT devices. Yang et al. [142] proposed a lightweight and privacy-preserving biometric system for IoT security which uses a block-logic operation on binary features of a fingerprint, which not only reduces its size but also ensures security of the template against attack vectors.

In this chapter, built upon minutia cylinder-code (MCC), a secure and light-weight biometric authentication system is proposed for IoT devices. As mentioned in earlier chapters, MCC representation is a state-of-the-art local minutia descriptor with proven recognition accuracy on public fingerprint databases [120]. Apart from exhibiting an excellent matching performance, the MCC fingerprint template

has a number of desirable properties such as rotation- and translation-invariance, resilience to elastic deformation and fixed-length feature vectors. However, MCC template in its original form is not suitable for IoT devices which have limited memory space and processing power.

In order to make MCC templates suitable for biometric authentication in IoT devices, we propose a pairwise-XOR logic operation and research contribution is two-fold. Firstly, pairwise-XOR significantly reduces the size of the MCC template to make it lightweight and provides considerable savings in relation to storage of IoT devices. Moreover, matching lightweight templates requires less computational power and matching time. Secondly, the proposed system is secured against attack vectors on IoT devices and protect the fingerprint in case of a security breach. We provide a computation and storage cost analysis as well as security analysis of the proposed system at the end of this chapter.

5.4 The proposed design for a secure and lightweight biometric system

This section presents the proposed design for an efficient and secure fingerprint authentication system which is effective in an IoT framework [142]. The overall processing flow of the proposed algorithm is depicted in Figure 5.1.

5.4.1 Extraction of minutiae features

In order to access an IoT device, the user needs to present his/her finger to a mobile device which is equipped with a fingerprint sensor. The fingerprint image acquired by the sensor is fed to a commercial software, VeriFinger of Neurotechnology [11] which extracts a set of M minutiae points from the image. As previously mentioned, each minutia in the set denotes a fingerprint feature, classified by ridge endings or bifurcations and is represented as a point in the cartesian coordinate system along with an orientation angle in the range of $[0, 2\pi]$ and the minutia type.

5.4.2 Generation of binary features using MCC

The minutiae set corresponding to a fingerprint image is input to the MCC algorithm [120]. The MCC minutia descriptor associates each minutia in a fingerprint image with a 3D local structure called a cylinder. The cylinder is constructed by aligning its base with the orientation of the reference minutia and encoding the relative relationships between the relative minutia and the neighbouring minutiae within a fixed radius. The cylinder is enclosed in a cuboid which is discretized into cells. The MCC calculates a numerical value to represent a cell in the cylinder. This value reflects the spatial and directional contributions of the neighbouring minutiae. Through a binarization step, all cell values in a cylinder are combined into a binary feature vector of fixed length $\bar{N}$. For M minutiae in the set, there are C corresponding feature vectors such that $C \leq M$.

Let's denote the c^{th} feature vector as $\mathbf{y}_c$ as shown in Figure 5.1, where $c = 1, 2, ..., C$ with C denoting the total number of feature vectors in an MCC template. Each $\mathbf{y}_c$ of length $\bar{N}$ has two parts, $\mathbf{m}_c$ and $\mathbf{S}_c$ in a fashion such as $\mathbf{y}_c = [\mathbf{m}_c \quad \mathbf{S}_c]$. $\mathbf{m}_c$ is called the mask which plays a pivotal role in matching. From one of the parameter sets provided in the MCC representation [120], the lengths of $\mathbf{m}_c$ and $\mathbf{S}_c$ are calculated to be 256 and 1280, respectively, such that $\bar{N} = 256 + 1280 = 1536$ for $\mathbf{y}_c$.

5.4.3 Pair-wise XOR logic operation

In order to produce lightweight MCC templates, we perform the pairwise-XOR operation to $\mathbf{S}_c$. Let's express $\mathbf{S}_c$ as:

$$\mathbf{S}_c = [S_c(0), S_c(1), ..., S_c(N-1)] \tag{5.1}$$

where $N = 1280$ is the length of $\mathbf{S}_c$ and $S_c(n) = 0$ or 1, for $0 \leq n \leq N-1$. Take a fingerprint image with 50 minutiae as an example, where we assume that a valid cylinder can be created for each minutia. Then, the total size of the MCC

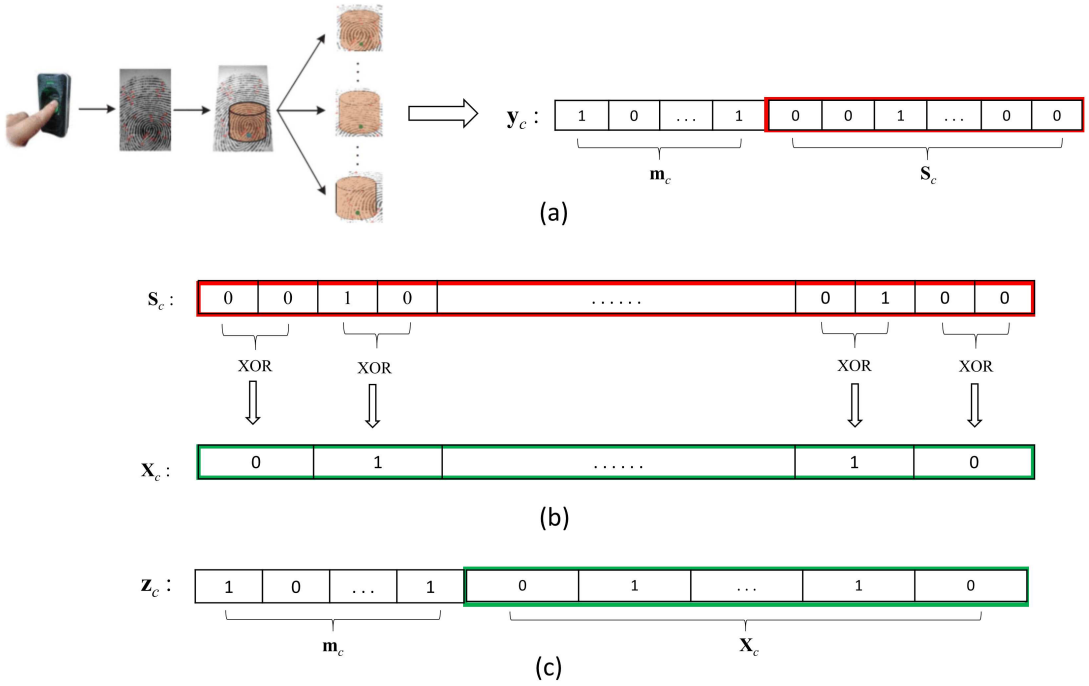

FIGURE 5.1: The proposed lightweight and secure biometric system: a) minutiae extraction and binary feature vector generation by MCC; b) pairwise-XOR operation on the non-mask segment $\mathbf{S}_c$ and the resultant vector $\mathbf{X}_c$; c) protected and lightweight vector.

template is $50 \times 1536 = 76,800$ bits, which is a sizable amount. In order to make the existing MCC template lightweight, we perform a pairwise-XOR logic operation on $\mathbf{S}_c$. The Boolean algebra XOR is an efficient logic function with low computational intensity [163]. Note that we have excluded $\mathbf{m}_c$ from the pairwise-XOR operation due to its essential role at the matching stage. The proposed pairwise-XOR operation produces a new binary vector of length $K = \frac{N}{2}$, i.e., half of the length of $\mathbf{S}_c$.

Let $\mathbf{X}_c$ be the new (post-XOR) binary vector, written as

$$\mathbf{X}_c = [X_c(0), X_c(1), ..., X_c(K-1)] \tag{5.2}$$

The elements of $\mathbf{X}_c$ are obtained by the XOR logic operation between the consecutive pairs of $\mathbf{S}_c$, i.e.,

$$X_c(k) = S_c(2k) \oplus S_c(2k+1) \tag{5.3}$$

where $\oplus$ represents the XOR operation and $k = 0, 1, ..., \frac{N}{2} - 1$ as shown in Figure 5.1. A final, shortened feature vector $\mathbf{z}_c$ as a result of pairwise-XOR in (5.3) is obtained by concatenating $\mathbf{m}_c$ and $\mathbf{X}_c$ as follows:

$$\mathbf{z}_c = [\mathbf{m}_c \;\; \mathbf{X}_c] \tag{5.4}$$

Figure 5.1 dictates that the length of $\mathbf{X}_c$ is strictly half of the length of $\mathbf{S}_c$, thanks to the pairwise-XOR Boolean algebra. This size reduction applies to $\mathbf{S}_c$, for $c = 1, 2, ..., C$, of each binary vector.

5.4.4 Fingerprint matching

Biometric authentication in all applications, as well as in the IoT environment, fundamentally comprises two stages, the enrolment stage and the verification stage. Hence, during enrolment, the proposed system allows a fingerprint to follow the steps discussed in sections 5.4.1 - 5.4.3 and the resultant lightweight template is stored in the IoT devices before deployment. At the verification stage, a query fingerprint of an authorised user who needs to access an IoT device, undergoes the same steps 5.4.1 - 5.4.3. Matching occurs between the query and the stored template as in [120] and completes this in two steps.

Step-I: In the first step, a score matrix is obtained by comparing each binary vector in the query with all binary vectors in the stored template. To differentiate the enrolled template and the query, we use letter $'t'$ and $'q'$, respectively. Suppose that there are C_q valid cylinders in the query, each generating $\mathbf{z}_{c_q}$ in (5.4), for $c_q = 1, 2, ..., C_q$, and there are C_t valid cylinders in the enrolled template with each generating a valid cylinder $\mathbf{z}_{c_t}$, for $c_t = 1, 2, ..., C_t$. The query and the template usually have a different number of minutiae and corresponding valid cylinders, hence $C_q \neq C_t$.

In practice, the vector $\mathbf{m}_c$, as shown in Figure 5.1, is used as a bit-mask to choose the valid bits in $\mathbf{X}_c$. Using bit-masks $\mathbf{m}_c^q$ and $\mathbf{m}_c^t$ from the query and template, respectively, an intersection between two masks is generated as $\mathbf{m}_c^{qt} = \mathbf{m}_c^q \otimes \mathbf{m}_c^t$,

where $\otimes$ represents bit-wise AND between two vectors. Two matchable vectors are generated by

$$\mathbf{z}^c_{q|t} = \mathbf{X}^q_c \otimes \hat{\mathbf{m}}^{qt}_c, \quad \mathbf{z}^c_{t|q} = \mathbf{X}^t_c \otimes \hat{\mathbf{m}}^{qt}_c \tag{5.5}$$

where $\hat{\mathbf{m}}^{qt}_c$ is derived from $\mathbf{m}^{qt}_c$ in the following fashion:

$$\hat{\mathbf{m}}^{qt}_c = [\mathbf{m}^{qt}_c \quad \mathbf{m}^{qt}_c \quad \mathbf{m}^{qt}_c(1:128)] \tag{5.6}$$

where $\mathbf{m}^{qt}_c(1:128)$ represents the first 128 bits in $\mathbf{m}^{qt}_c$. The vector $\hat{\mathbf{m}}^{qt}_c$ has the same length as $\mathbf{X}^q_c$ and $\mathbf{X}^t_c$, i.e., $K = \frac{N}{2} = 640$. Finally, the matching score between $\mathbf{z}^c_{q|t}$ and $\mathbf{z}^c_{t|q}$ is calculated as follows:

$$S(\mathbf{z}^c_{q|t}, \mathbf{z}^c_{t|q}) = 1 - \frac{||\mathbf{z}^c_{q|t} \oplus \mathbf{z}^c_{t|q}||_2}{||\mathbf{z}^c_{q|t}||_2 + ||\mathbf{z}^c_{t|q}||_2} \tag{5.7}$$

Here $S(\mathbf{z}^c_{q|t}, \mathbf{z}^c_{t|q})$ represents the matching score which is strictly in the range [0, 1] with 0 as no match and 1 as fully matched. Since the comparison between $\mathbf{z}_{c_q}$ and $\mathbf{z}_{c_t}$ is conducted for all $c_q = 1, 2, ..., C_q$ and $c_t = 1, 2, ..., C_t$, the result of (5.7) is a $C_q \times C_t$ score matrix.

Step-II: In the second step, a global matching score is obtained from the score matrix using local greedy similarity (LGS) algorithm as explained in [120]. This global score is bounded between 0 and 1 representing a no-match and full-match, respectively. A match is considered as successful if the global score is higher than a pre-defined threshold.

5.5 Experimental results

The proposed lightweight, MCC based biometric system is evaluated over public fingerprint databases FVC2002 DB1-DB3 [9] and FVC2004 DB1 and DB2 [10] using both 1vs1 and FVC protocols (see Chapter 1).

5.5.1 Performance metrics and analysis

The performance measures adopted in our experiments are the EER, FAR and FRR. As mentioned in Chapter 1, the FAR is the probability of mistaking the impression from two different fingers to be from the same finger. The FRR is the probability of mistaking two impressions from the same finger to be from two different fingers. The EER denotes the error rate when FAR = FRR. Table 5.1

Table 5.1: EER (%) comparison under the 1vs1 protocol

Methods	FVC2002 DB1	FVC2002 DB2	FVC2002 DB3	FVC2004 DB1	FVC2004 DB2
Reproduced MCC	0.01	0	1.41	7	5
Proposed method	0.04	0	2	8	5

Table 5.2: EER (%) comparison under the original FVC protocol

Method	FVC2002 DB1	FVC2002 DB2	FVC2002 DB3	FVC2004 DB1	FVC2004 DB2
Reproduced MCC	1.54	1.29	4	8.60	7.64
Proposed method	1.67	1.57	4.64	9.57	8.01

and Table 5.2 show the performance comparison of the proposed method with the existing MCC template in terms of the EER. Under both protocols, it is clear from Table 5.1 and Table 5.2 that the proposed method achieves equivalent or close performance to the baseline (reproduced MCC templates), but with more implementational efficiency and security. We also plotted the ROC curves for all databases under 1vs1 and original FVC protocols in Figure 5.2 and 5.3, respectively.

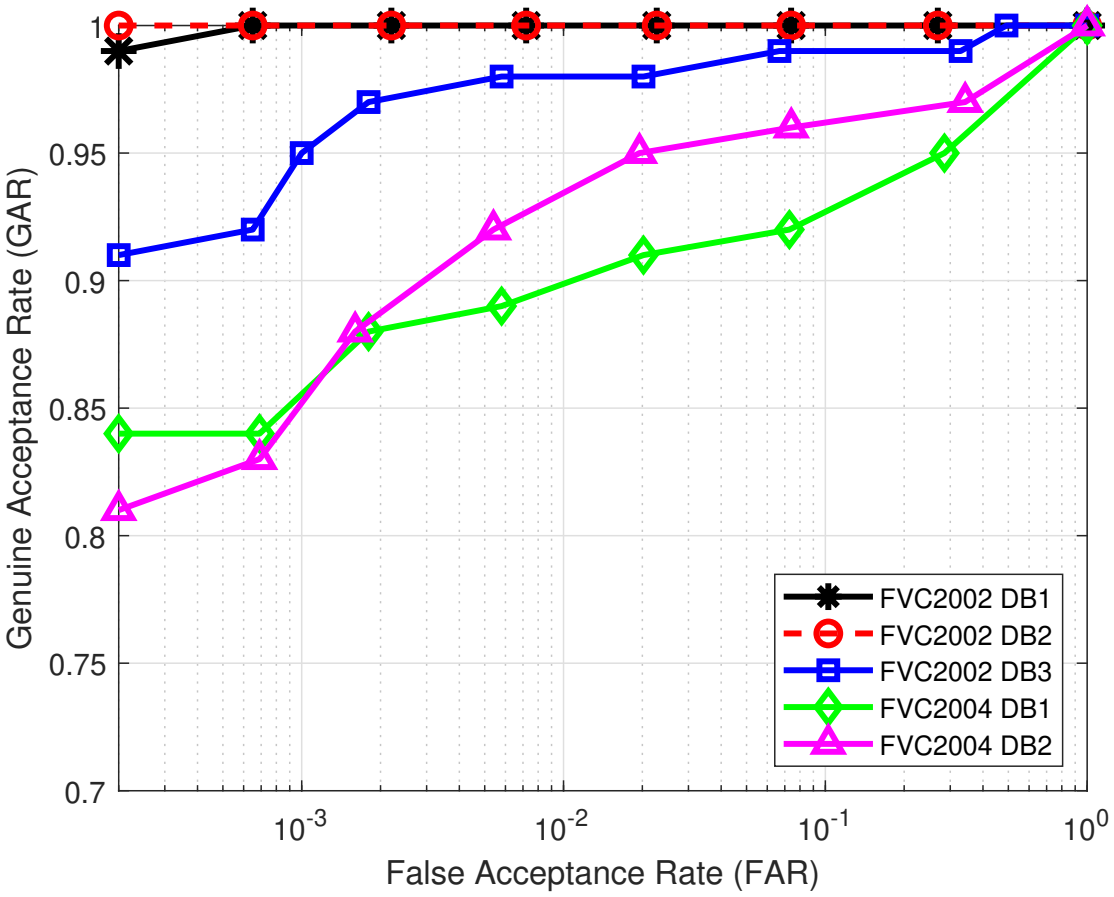

FIGURE 5.2: ROC curves for FVC2002 DB1-DB3 and FVC2004 DB1-DB2 under the 1vs1 protocol.

5.5.2 Security analysis

The proposed biometric system is designed for IoT devices with enhanced security. A biometric system is necessary to provide secure authentication to access an IoT device because a compromised biometric system may compromise the device itself. Moreover, a stolen template may reveal sensitive information, which may be used to reconstruct the original fingerprint image. Since biometrics are unchangeable, a reconstructed fingerprint may compromise all IoT devices on which a user is enrolled.

The proposed system adopts a pairwise-XOR approach at the binary MCC template and induces robust changes, as shown in Figure 5.1. As a result, a fingerprint template stored in an IoT device is considered protected. If an adversary steals the protected template by attacking the device and attempts to revert the robust

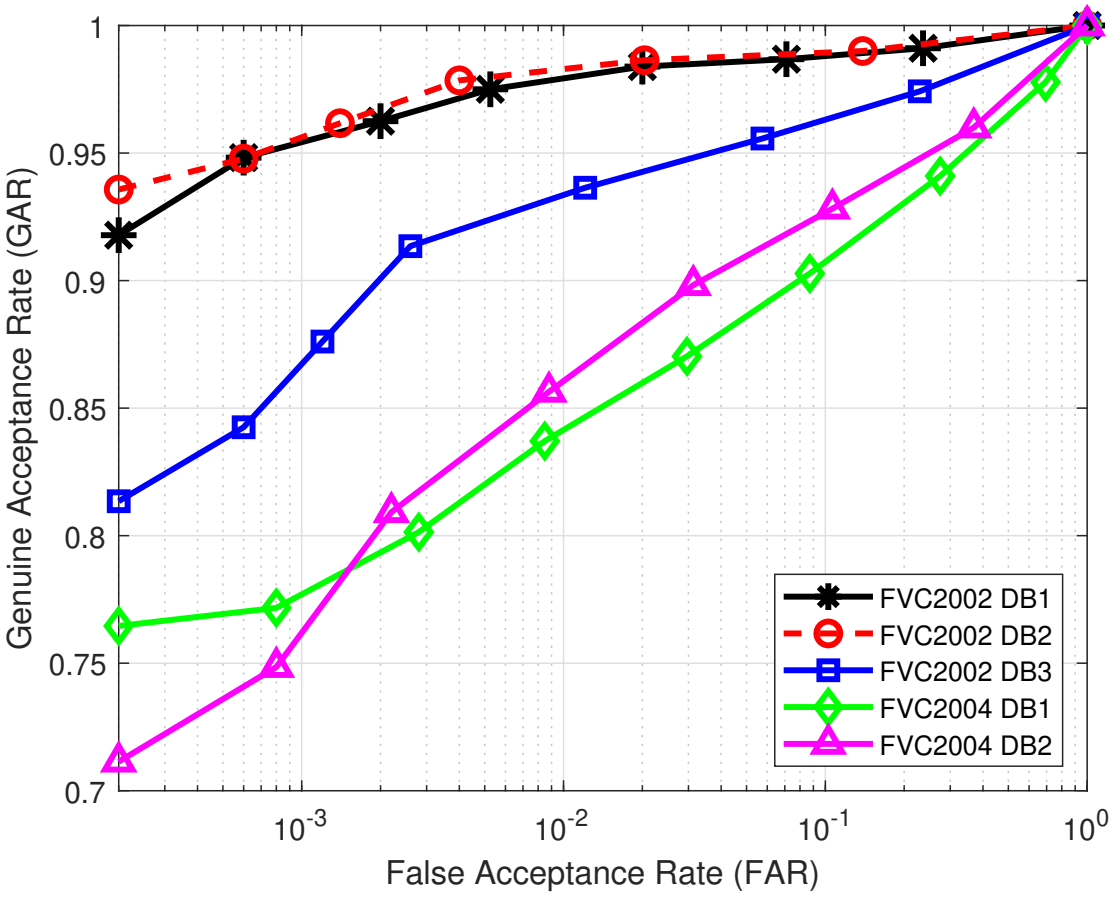

FIGURE 5.3: ROC curves for FVC2002 DB1-DB3 and FVC2004 DB1-DB2 under the original FVC protocol.

changes made to the original MCC template, it is computationally infeasible. As shown in Figure 5.1, proposed pairwise XOR is applied to vector $\mathbf{S}_c$ which transforms it into a shortened vector $\mathbf{X}_c$. To restore $\mathbf{S}_c$ from $\mathbf{X}_c$, the adversary must decode each bit in $\mathbf{X}_c$ to the accurate respective pair in $\mathbf{S}_c$.

To elaborate the analysis, we denote the bit-pairs in $\mathbf{S}_c$ as A = 00, B = 11, C = 01 and D = 10. An XOR operation can be regarded as a lossy process in which pairs A and B yield 0 while C and D yield 1. This implies that one can't predict if a 0 in $\mathbf{X}_c$ has originated from a bit-pair A or B in $\mathbf{S}_c$. Similarly, a 1 in $\mathbf{X}_c$ may have originated either from a bit-pair C or D. From a Bayesian point of view, the adversary has to make a decision rule for decoding all the bits in $\mathbf{X}_c$ based on the posterior probability. In this case, the posterior probabilities p_A and p_C are

calculated as

$$\begin{aligned} p_A = p(A|0) &= \frac{p(0|A)p(A)}{p(0)} \\ p_C = p(C|1) &= \frac{p(1|C)p(C)}{p(1)} \end{aligned} \tag{5.8}$$

where $p(A)$ and $p(C)$ are the probabilities of pairs A and C in $\mathbf{S}_c$, respectively. Since the pairwise-XOR process in (5.3) is deterministic, $p(0|A) = 1$ as well as $p(1|C) = 1$. We can assume that bit-pairs are independent such that

$$\begin{aligned} p(0) &= p(A) + p(B) \\ p(1) &= p(C) + p(D) \end{aligned} \tag{5.9}$$

We can rewrite (5.8) as:

$$\begin{aligned} p_A &= \frac{p(A)}{p(A) + p(B)} \\ p_C &= \frac{p(C)}{p(C) + p(D)} \end{aligned} \tag{5.10}$$

With p_A and p_C, we can derive the other two posterior probabilities p_B and p_D as:

$$\begin{aligned} p_B &= 1 - p_A \\ p_D &= 1 - p_C \end{aligned} \tag{5.11}$$

Using database FVC2002 DB2, we estimated the average of posterior probabilities i.e. p_A, p_B, p_C and p_D, and obtained $p_A = 0.9956$ and $p_B = 0.0044$. Since $p_A >> p_B$, it can be inferred that the adversary can make a decision rule to decode a 0 in $\mathbf{X}_c$ as 00 with a probability of error of 0.0044, which is very small. On the other hand, $p_C = 0.5105$ and $p_D = 0.4895$. Since $p_C > p_D$, the adversary can decode a 1 in $\mathbf{X}_c$ as 01 with a probability of error of 0.4985, which is very high.

It is noted from the experiments that $p(A) + p(B) = \frac{14}{15}$ while $p(C) + p(D) = \frac{1}{15}$. Since the length of $\mathbf{S}_c$ is $N = 2K$, where K is the length of $\mathbf{X}_c$, on average, the number of 00 and 11 is $\frac{14K}{15}$ and the number of 01 and 10 is $\frac{K}{15}$. Since $K = 640$, $\frac{K}{15} \approx 43$. In other words, there are approximately 43 bits of binary 1 in $\mathbf{X}_c$. Because

both 01 (i.e., bit-pair C) and 10 (i.e., bit-pair D) are independent (figuring out one pair does not give any information about the other pair), with $p_C = 0.5105$ and $p_D = 0.4895$, we can see that C and D bit-pairs are almost equally probable for any bit 1 in $\mathbf{X}_c$. Thus, the number of possibilities of decoding C and D bit-pairs in $\mathbf{S}_c$ from 43 bit 1s in $\mathbf{X}_c$ is 2^{43}. Assuming that there are 50 minutiae in a fingerprint image, even if we ignore the possible errors in decoding A and B bit-pairs in $\mathbf{S}_c$, it would take $2^{43\times 50} = 2^{2150}$ attempts to figure out C and D bit-pairs in $\mathbf{S}_c$. Clearly, it is highly unlikely for an attacker to correctly restore $\mathbf{S}_c$ from $\mathbf{X}_c$. Based on this analysis, we can infer that the security of the proposed system is strong.

5.5.3 Matching time and storage analysis

The proposed technique shortens the length N of $\mathbf{S}_c$ in (5.1) to $K = \frac{N}{2}$, i.e., the length of $\mathbf{X}_c$ in (5.2). As $N = 1280$, a reduction in size is $K = \frac{N}{2} = \frac{1280}{2} = 640$ bits. For 50 binary strings in an MCC template, a reduction in feature size is 32000($= 50\times 640$) bits which is a substantial savings in the memory consumption of IoT devices. As cylinder building and other feature extraction related procedures in [120] are not carried out in real time on IoT devices, the proposed pairwise-XOR operation doesn't impose an additional computational load. With a reduction in template size, the fingerprint matching process is accelerated.

To compare the matching speed between two original MCC templates and their respective lightweight versions, we use a stored template with 52 minutiae and a query template with 58 minutiae. A matching time comparison is presented in Table 5.3 and by running MATLAB on a desktop computer with Core i7 and a 3.41 GHz CPU. With comparable recognition performance, we observe that the proposed method takes significantly less storage and provides faster matching than the original MCC template.

TABLE 5.3: Template size and matching time comparison between the original MCC template and the lightweight template

Template	Template size(bits)	Matching time (second)
Original MCC	76,800	0.4057
Lightweight	44,800	0.2997

5.6 Summary

This chapter presents a fingerprint-based biometric authentication system suitable for use in the IoT environment. It is specifically designed to address the limitations of IoT devices such as limited computational power and memory space. The proposed system is built on the state-of-the-art MCC algorithm and uses a pairwise-XOR logic operation enabling its computational and storage compatibility with an IoT device as well as ensuring energy efficiency. The pairwise-XOR operation not only reduces the size of an MCC template and makes the system lightweight, but it also enhances security, while maintaining high recognition accuracy. The proposed system is tested on three publicly available fingerprint databases from FVC 2002. The results show that proposed system helps address the energy efficiency issues of IoT devices. Moreover, there is negligible deterioration in the recognition accuracy of the proposed system i.e., the EER of the proposed system for 1vs1 protocol is 0.04%, 0%, 2%, 8% and 5% which nearly equals the baseline performance 0.01%, 0%, 1.41%, 7% and 5% for FVC2002 DB1-DB3 and FVC2004 DB1-DB2, respectively.

Chapter 6

Conclusion

"The power of imagination makes us infinite."

– John Muir

The aim of the thesis is to develop new fingerprint template protection schemes in the form of cancelable templates. Over the past few years, researchers found the inadequacies in the existing designs for cancelable templates. Some of the recently explored security threats include attacks via record multiplicity, masquerade attacks and pre-image attacks. Many existing cancelable template schemes are unable to withstand these attacks. This thesis presents two novel schemes for cancelable templates with the goal of achieving in-built security against all or some of these security threats while attaining good recognition performance. Another aim of this thesis is to design a secure fingerprint authentication system which suits resource-constrained IoT devices.

The three main research contributions of the thesis are summarized as follows:

Alignment-free cancelable templates with dual protection

The first idea for cancelable fingerprint templates, presented in Chapter 3, addresses the several security threats, i.e., the ARM, masquerade attacks and preimage attacks. The proposed algorithm achieves the desired security by introducing two layers of protection. The first layer has a window-shift-XOR model which is implemented on the binary features of the MCC template using XOR logic. As a consequence, uncertainties are added to the resultant template which are hard to reverse in computationally bound attacks such as the ARM. However, window-shift-XOR only involves simple operations like window segmentation, window shifting and XOR logic. So, the second layer of protection is added. It is achieved via partial DWT which preserves the recognition accuracy with good denoising tendency of DWT and facilitates fast implementation by fast wavelet transform (FWT). This layer enables the algorithm to produce cancelable templates with the required properties such as revocability, diversity, accuracy and unlinkability. Extensive experiments verify that the proposed algorithm can withstand the aforementioned security threats. Moreover, the scheme also meets the latest and strict unlinkability requirements.

Cancelable biometric system based on feature-adaptive random projection

Of the various existing one-way transformations, random projection is a well-known privacy-preserving method to produce cancelable templates. The key to the transformation is a user-defined random projection matrix which transforms the original template feature vector into another vector with lower dimensions. The user-specified key and other transformation parameters are required to be public in biometrics which, if compromised, may lead to ARM attack.

The random projection-based cancelable templates presented in Chapter 4 are designed to address the aforementioned ARM limitations. It is a feature-adaptive random projection based method, in which the projection matrixes, which are key to the ARM, are generated from one basic matrix in conjunction with local feature slots. The generated projection matrixes are discarded after use, thus making it difficult for the adversary to launch the ARM. Moreover, the random projection in

the proposed method is performed on a local feature basis. This feature-adaptive random projection can mitigate the negative impact of biometric uncertainty on recognition accuracy, as it limits the error to part of the transformed feature vector rather than the entire vector. The proposed method is evaluated on four publicly available databases FVC2002 DB1-DB3 and FVC2004 DB2. The experimental results and security analysis show the validity of the proposed method.

A secure fingerprint system for resource-limited IoT devices

Fingerprint-based recognition is an emerging technology for personal authentication in IoT devices. However, IoT devices are resource-constrained in terms of limited storage space and computational capability and is powered by limited-life batteries, known as the green issue for IoT devices. Moreover, a secure biometric authentication is a challenge against attack vectors and attack sources.

Chapter 5 presents a light-weight and secure fingerprint authentication system implemented in the IoT environment. The proposed system addresses the aforementioned green-issue by reducing the size of the MCC templates in a simple and robust manner. The system adopts a pairwise-XOR process on MCC's binary feature vectors which significantly reduces their size as well as adding uncertainties while preserving recognition accuracy. As a consequence, the processed MCC templates require less memory storage and offer enhanced matching speed. The proposed scheme ensures the security of the system against attack vectors and attack sources. The efficiency of the proposed algorithm is analysed in terms of savings on storage space and improved matching speed. Moreover, the in-depth security analysis of the proposed system is presented which proves its safety against possible aforementioned attacks.

Chapter 7

Future Work

"If you would not be forgotten, as soon as you are dead and rotten, either write things worth reading, or do things worth writing."

– Benjamin Franklin

The research presented in this thesis contributes to the field of fingerprint template protection. In this regard, two novel schemes are introduced to develop cancelable fingerprint templates. In addition, a lightweight fingerprint authentication system is designed specifically for resource-limited IoT devices. In this chapter, possible future directions are presented related to the proposed method (discussed in Chapter 3) and the current research trends in biometric template protection.

Discrete Wavelet Transform (DWT) and Cancelable Templates

In Chapter 3, partial DWT (refer to (3.12)) is used to produce cancelable templates. DWT is implemented using the transformation matrix $\mathbf{A}$ in (3.4). However, partial DWT is enabled by a rank deficient rectangular matrix $\bar{\mathbf{A}}$ made by selecting a portion of the rows of $\mathbf{A}$ using a user-specific key. The proposed method uses partial DWT for cancelable transformation, exploiting the excellent properties of DWT such as its fast implementation using FWT and denoising property which preserves recognition accuracy [128]. Moreover, FWT is asymptotically faster than FFT and Hadamard transform requiring only $O(N)$ computations.

The DWT is susceptible to shift variance in which even a small shift in the input signal causes a significant change in the energy distribution of DWT coefficients [164–168] which also complicates processing in the wavelet domain. Furthermore, DWT suffers from shortcomings such as oscillations of the wavelet coefficients around singularities, aliasing and a lack of directionality [169]. These shortcomings can be overcome using complex wavelets in a redundant fashion instead of using real-valued wavelets. The transformation now becomes a complex wavelet transform (CWT) and its well-known redundant frameworks are dual-tree CWT, double-density DWT and dual-tree double-density DWT. These redundant frameworks need to be investigated for further improvement in biometric recognition accuracy in the transformed domain.

The Dual-Tree CWT

The implementation of DWT is made possible by filter banks (refer to Figure 3.1). An equivalent implementation of dual-tree CWT is achieved using two real DWTs. However, it requires new sets of filter pairs which ensure close Hilbert transform pair approximation for corresponding complex wavelets. The dual-tree CWT implementation using two real DWTs with corresponding sets of filter banks is depicted in Figure 7.1.

The Double-Density DWT

Double-density DWT is somewhat similar to dual-tree CWT with respect to their ability to achieve shift-invariance. Unlike DWT, double-density DWT uses two wavelets (and hence equivalent filters for implementation) (see Figure 7.2) to achieve narrow wavelet spacing within the same scale, making it less shift sensitive [170].

Dual-Tree Double-Density DWT

This framework possesses the properties of the dual-tree CWT and double-density DWT simultaneously (see design in 7.3). Apart from being shift invariant, this framework is an excellent candidate for image denoising applications and allows

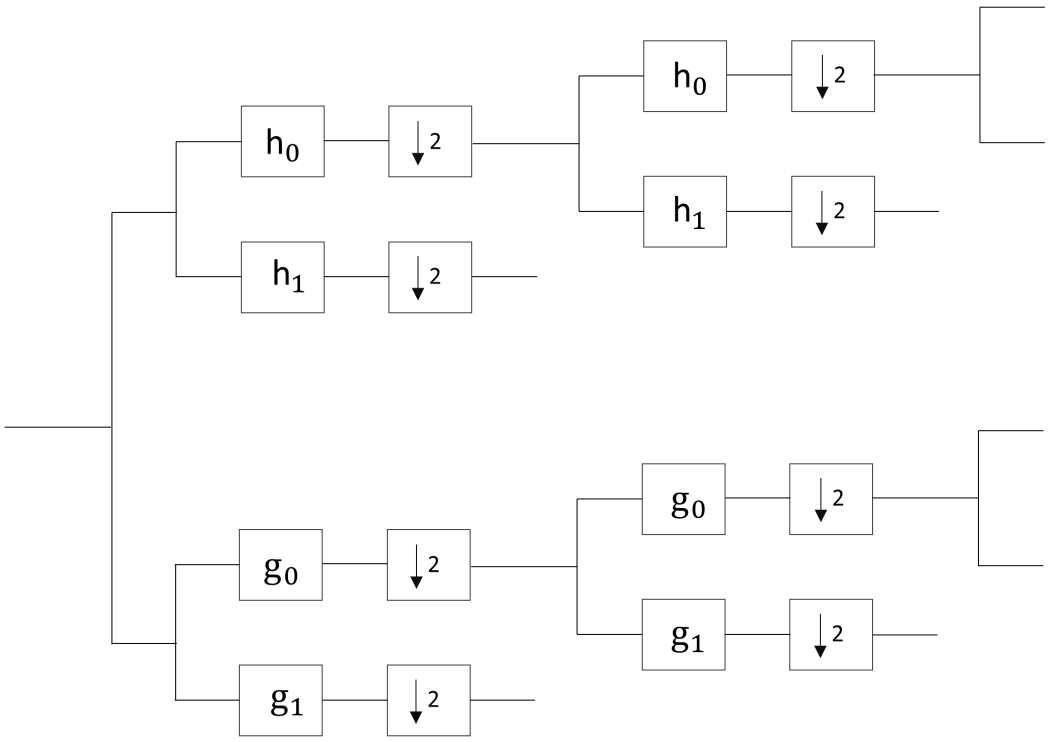

FIGURE 7.1: Analysis filter bank for dual-tree CWT (adapted from [169]).

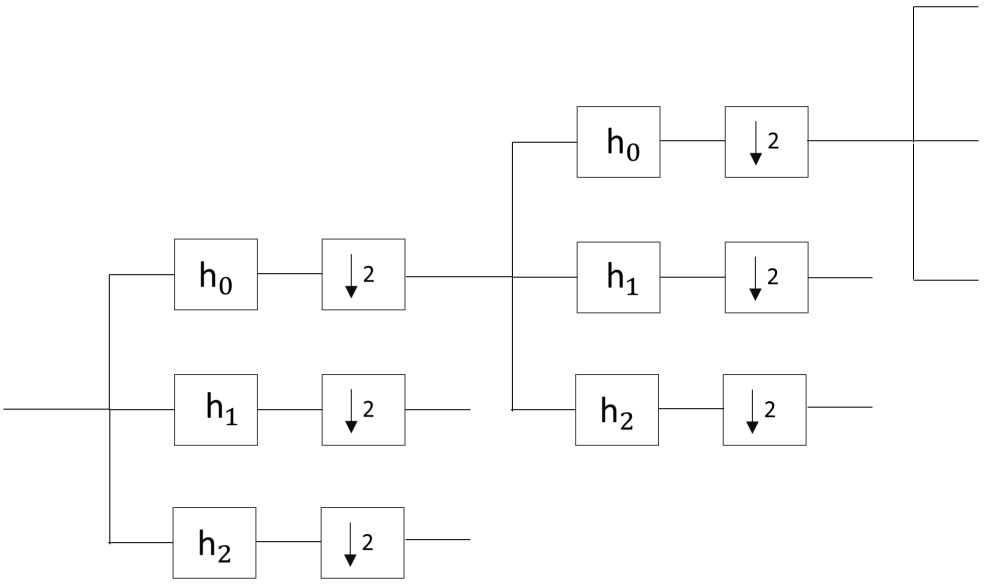

FIGURE 7.2: Analysis filter bank for double-density DWT (adapted from [170]).

better Hilbert transform pair approximation [170]. It also confirms its good candidacy for developing cancelable templates with superior recognition accuracy.

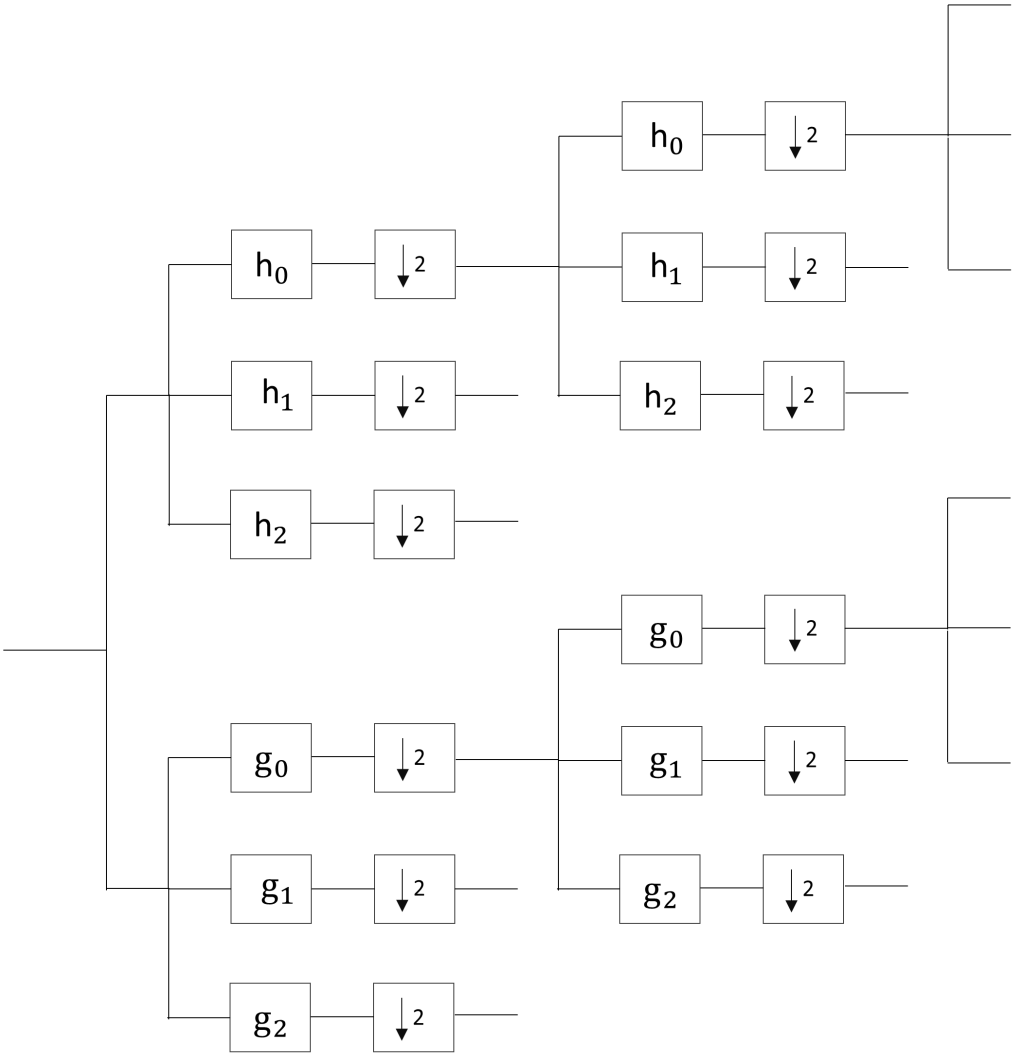

FIGURE 7.3: Iterative filterbank for dual-tree double-density DWT (adapted from [170]).

While artificial intelligence (AI) has achieved remarkable success in biometric applications, how to protect the template data of AI-based biometric systems is an open area and an abundance of work awaits. Although some progress has been made on securing deep-learning-based finger vein biometrics [171], we will investigate template protection for AI-based fingerprint biometric systems. More recently, a fixed-length fingerprint representation of only 200 bytes, named DeepPrint [70], demonstrated superior authentication accuracy in the encrypted domain using fully homomorphic encryption. Given the importance of fingerprint feature extraction and representation in the scheme of things, this novel, compact fingerprint representation lays a great foundation for the future development of

fingerprint template protection methods. In addition, homomorphic encryption is worthy of further study as to how to apply it to fingerprint matching with protected (transformed) templates.

Bibliography

[1] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, *Handbook of fingerprint recognition*. Springer Science & Business Media, 2009.

[2] N. K. Ratha, J. H. Connell, and R. M. Bolle, "Biometrics break-ins and band-aids," *Pattern Recognition Letters*, vol. 24, no. 13, pp. 2105–2113, 2003.

[3] R. Cappelli, D. Maio, A. Lumini, and D. Maltoni, "Fingerprint image reconstruction from standard templates," *IEEE transactions on pattern analysis and machine intelligence*, vol. 29, no. 9, pp. 1489–1503, 2007.

[4] J. Feng and A. K. Jain, "Fingerprint reconstruction: from minutiae to phase," *IEEE transactions on pattern analysis and machine intelligence*, vol. 33, no. 2, pp. 209–223, 2010.

[5] Y. Wang and J. Hu, "Global ridge orientation modeling for partial fingerprint identification," *IEEE transactions on pattern analysis and machine intelligence*, vol. 33, no. 1, pp. 72–87, 2010.

[6] N. K. Ratha, J. H. Connell, and R. M. Bolle, "Enhancing security and privacy in biometrics-based authentication systems," *IBM systems Journal*, vol. 40, no. 3, pp. 614–634, 2001.

[7] R. M. Bolle, J. H. Connell, and N. K. Ratha, "Biometric perils and patches," *Pattern recognition*, vol. 35, no. 12, pp. 2727–2738, 2002.

[8] K. Simoens, B. Yang, X. Zhou, F. Beato, C. Busch, E. M. Newton, and B. Preneel, "Criteria towards metrics for benchmarking template protection algorithms," in *2012 5th IAPR International Conference on Biometrics (ICB)*. IEEE, 2012, pp. 498–505.

[9] "Fingerprint verification competition," http://bias.csr.unibo.it/fvc2002/, accessed: 2020-06-12.

[10] "Fingerprint verification competition," http://bias.csr.unibo.it/fvc2004/, accessed: 2020-08-01.

[11] "Verifinger s. d. k. neuro technology," http://www.neurotechnology.com/verifinger.html, accessed: 2020-06-12.

[12] A. Siswanto, N. Katuk, and K. R. Ku Mahamud, "Fingerprint template protection schemes: A literature review," *Journal of Theoretical and Applied Information Technology*, vol. 96, no. 10, pp. 2764–2781, 2018.

[13] U. Uludag, S. Pankanti, S. Prabhakar, and A. K. Jain, "Biometric cryptosystems: issues and challenges," *Proceedings of the IEEE*, vol. 92, no. 6, pp. 948–960, 2004.

[14] A. K. Jain, K. Nandakumar, and A. Nagar, "Biometric template security," *EURASIP Journal on advances in signal processing*, vol. 2008, pp. 1–17, 2008.

[15] A. Vetro and N. Memon, "Biometric system security," in *Tutorial presented at Second International Conference on Biometrics, Seoul, South Korea*, 2007.

[16] K. Nandakumar, A. K. Jain, and S. Pankanti, "Fingerprint-based fuzzy vault: Implementation and performance," *IEEE transactions on information forensics and security*, vol. 2, no. 4, pp. 744–757, 2007.

[17] A. Juels and M. Sudan, "A fuzzy vault scheme," *Designs, Codes and Cryptography*, vol. 38, no. 2, pp. 237–257, 2006.

[18] M. Khalil-Hani, M. N. Marsono, and R. Bakhteri, "Biometric encryption based on a fuzzy vault scheme with a fast chaff generation algorithm," *Future Generation Computer Systems*, vol. 29, no. 3, pp. 800–810, 2013.

[19] T. C. Clancy, N. Kiyavash, and D. J. Lin, "Secure smartcardbased fingerprint authentication," in *Proceedings of the 2003 ACM SIGMM workshop on Biometrics methods and applications*, 2003, pp. 45–52.

[20] T. H. Nguyen, Y. Wang, Y. Ha, and R. Li, "Improved chaff point generation for vault scheme in bio-cryptosystems," *IET biometrics*, vol. 2, no. 2, pp. 48–55, 2013.

[21] C. Örencik, T. B. Pedersen, E. Savaş, and M. Keskinöz, "Improved fuzzy vault scheme for fingerprint verification," 2008.

[22] Y. Chung, D. Moon, S. Lee, S. Jung, T. Kim, and D. Ahn, "Automatic alignment of fingerprint features for fuzzy fingerprint vault," in *International Conference on Information Security and Cryptology*. Springer, 2005, pp. 358–369.

[23] M. Fouad, A. El Saddik, J. Zhao, and E. Petriu, "A fuzzy vault implementation for securing revocable iris templates," in *2011 IEEE International Systems Conference*. IEEE, 2011, pp. 491–494.

[24] Y. J. Lee, K. R. Park, S. J. Lee, K. Bae, and J. Kim, "A new method for generating an invariant iris private key based on the fuzzy vault system," *IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics)*, vol. 38, no. 5, pp. 1302–1313, 2008.

[25] Y. J. Lee, K. Bae, S. J. Lee, K. R. Park, and J. Kim, "Biometric key binding: Fuzzy vault based on iris images," in *International Conference on Biometrics*. Springer, 2007, pp. 800–808.

[26] S. Kanade, D. Camara, E. Krichen, D. Petrovska-Delacrétaz, and B. Dorizzi, "Three factor scheme for biometric-based cryptographic key regeneration using iris," in *2008 Biometrics Symposium*. IEEE, 2008, pp. 59–64.

[27] X. Wu, N. Qi, K. Wang, and D. Zhang, "A novel cryptosystem based on iris key generation," in *2008 Fourth International Conference on Natural Computation*, vol. 4. IEEE, 2008, pp. 53–56.

[28] ——, "An iris cryptosystem for information security," in *2008 International Conference on Intelligent Information Hiding and Multimedia Signal Processing*. IEEE, 2008, pp. 1533–1536.

[29] E. S. Reddy and I. R. Babu, "Performance of iris based hard fuzzy vault," in *2008 IEEE 8th International Conference on Computer and Information Technology Workshops*. IEEE, 2008, pp. 248–253.

[30] V. Meenakshi and G. Padmavathi, "Securing iris templates using combined user and soft biometric based password hardened fuzzy vault," *arXiv preprint arXiv:1003.1449*, 2010.

[31] T. Frassen, X. Zhou, and C. Busch, "Fuzzy vault for 3d face recognition systems," in *2008 International Conference on Intelligent Information Hiding and Multimedia Signal Processing*. IEEE, 2008, pp. 1069–1074.

[32] Y. Wang and K. N. Plataniotis, "Fuzzy vault for face based cryptographic key generation," in *2007 Biometrics Symposium*. IEEE, 2007, pp. 1–6.

[33] L. Wu and S. Yuan, "A face based fuzzy vault scheme for secure online authentication," in *2010 Second International Symposium on Data, Privacy, and E-Commerce*. IEEE, 2010, pp. 45–49.

[34] L. Wu, P. Xiao, S. Yuan, S. Jiang, and C. W. Chen, "A fuzzy vault scheme for ordered biometrics," *Journal of Communications*, vol. 6, no. 9, pp. 682–690, 2011.

[35] A.-Y. Kim and S.-H. Lee, "Authentication protocol using fuzzy eigenface vault based on moc," in *The 9th International Conference on Advanced Communication Technology*, vol. 3. IEEE, 2007, pp. 1771–1775.

[36] Y. C. Feng and P. C. Yuen, "Protecting face biometric data on smartcard with reed-solomon code," in *2006 Conference on Computer Vision and Pattern Recognition Workshop (CVPRW'06)*. IEEE, 2006, pp. 29–29.

[37] V. Meenakshi and G. Padmavathi, "Security analysis of hardened retina based fuzzy vault," in *2009 International conference on advances in recent technologies in communication and computing*. IEEE, 2009, pp. 926–930.

[38] X. Wu, K. Wang, and D. Zhang, "A cryptosystem based on palmprint feature," in *2008 19th International Conference on Pattern Recognition*. IEEE, 2008, pp. 1–4.

[39] G. Lu, F. Shan *et al.*, "A novel template protection method based on palmprint feature," in *International Conference Image Analysis and Recognition*. Springer, 2013, pp. 80–88.

[40] A. Kumar and A. Kumar, "A palmprint-based cryptosystem using double encryption," in *Biometric technology for human identification V*, vol. 6944. International Society for Optics and Photonics, 2008, p. 69440D.

[41] O. P. Verma and D. Bharathan, "A new palm print based fuzzy vault system for securing cryptographic key," *International Journal of Information and Electronics Engineering*, vol. 2, no. 2, p. 289, 2012.

[42] H. Liu, D. Sun, K. Xiong, and Z. Qiu, "Palmprint based multidimensional fuzzy vault scheme," *The Scientific World Journal*, vol. 2014, 2014.

[43] A. Juels and M. Wattenberg, "A fuzzy commitment scheme," in *Proceedings of the 6th ACM conference on Computer and communications security*, 1999, pp. 28–36.

[44] F. Hao, R. Anderson, and J. Daugman, "Combining crypto with biometrics effectively," *IEEE transactions on computers*, vol. 55, no. 9, pp. 1081–1088, 2006.

[45] J. Bringer, H. Chabanne, G. Cohen, B. Kindarji, and G. Zemor, "Theoretical and practical boundaries of binary secure sketches," *IEEE Transactions on Information Forensics and Security*, vol. 3, no. 4, pp. 673–683, 2008.

[46] J. Bringer, H. Chabanne, G. Cohen, B. Kindarji, and G. Zémor, "Optimal iris fuzzy sketches," in *2007 First IEEE International Conference on Biometrics: Theory, Applications, and Systems*. IEEE, 2007, pp. 1–6.

[47] C. Rathgeb and A. Uhl, "Context-based texture analysis for secure revocable iris-biometric key generation," 2009.

[48] ——, "Adaptive fuzzy commitment scheme based on iris-code error analysis," in *2010 2nd European Workshop on Visual Information Processing (EUVIP)*. IEEE, 2010, pp. 41–44.

[49] A. B. J. Teoh and J. Kim, "Secure biometric template protection in fuzzy commitment scheme," *IEICE Electronics Express*, vol. 4, no. 23, pp. 724–730, 2007.

[50] K. Nandakumar, "A fingerprint cryptosystem based on minutiae phase spectrum," in *2010 IEEE International Workshop on Information Forensics and Security*. IEEE, 2010, pp. 1–6.

[51] M. Van Der Veen, T. Kevenaar, G.-J. Schrijen, T. H. Akkermans, and F. Zuo, "Face biometrics with renewable templates," in *Security, Steganography, and Watermarking of Multimedia Contents VIII*, vol. 6072. International Society for Optics and Photonics, 2006, p. 60720J.

[52] H. Lu, K. Martin, F. Bui, K. N. Plataniotis, and D. Hatzinakos, "Face recognition with biometric encryption for privacy-enhancing self-exclusion," in *2009 16th International Conference on Digital Signal Processing*. IEEE, 2009, pp. 1–8.

[53] Y. Dodis, L. Reyzin, and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," in *International conference on the theory and applications of cryptographic techniques*. Springer, 2004, pp. 523–540.

[54] Q. Li, Y. Sutcu, and N. Memon, "Secure sketch for biometric templates," in *International Conference on the Theory and Application of Cryptology and Information Security*. Springer, 2006, pp. 99–113.

[55] Y.-J. Chang, W. Zhang, and T. Chen, "Biometrics-based cryptographic key generation," in *2004 IEEE International Conference on Multimedia and Expo (ICME)(IEEE Cat. No. 04TH8763)*, vol. 3. IEEE, 2004, pp. 2203–2206.

[56] S. V. Gaddam and M. Lal, "Efficient cancelable biometric key generation scheme for cryptography." *IJ Network Security*, vol. 11, no. 2, pp. 61–69, 2010.

[57] R. Ranjan and S. K. Singh, "Improved and innovative key generation algorithms for biometric cryptosystems," in *2013 3rd IEEE International Advance Computing Conference (IACC)*. IEEE, 2013, pp. 943–946.

[58] B. Chen and V. Chandran, "Biometric based cryptographic key generation from faces," in *9th Biennial Conference of the Australian Pattern Recognition Society on Digital Image Computing Techniques and Applications (DICTA 2007)*. IEEE, 2007, pp. 394–401.

[59] L. Wu, X. Liu, S. Yuan, and P. Xiao, "A novel key generation cryptosystem based on face features," in *IEEE 10th International Conference on Signal Processing Proceedings*. IEEE, 2010, pp. 1675–1678.

[60] L. Zhang, Z. Sun, T. Tan, and S. Hu, "Robust biometric key extraction based on iris cryptosystem," in *International Conference on Biometrics*. Springer, 2009, pp. 1060–1069.

[61] C. Rathgeb and A. Uhl, "Privacy preserving key generation for iris biometrics," in *IFIP International Conference on Communications and Multimedia Security*. Springer, 2010, pp. 191–200.

[62] ——, "Context-based biometric key generation for iris," *IET computer vision*, vol. 5, no. 6, pp. 389–397, 2011.

[63] F. Monrose, M. K. Reiter, Q. Li, and S. Wetzel, "Cryptographic key generation from voice," in *Proceedings 2001 IEEE Symposium on Security and Privacy. S&P 2001.* IEEE, 2000, pp. 202–213.

[64] B. Prasanalakshmi and A. Kannammal, "A secure cryptosystem from palm vein biometrics," in *Proceedings of the 2nd International Conference on Interaction Sciences: Information Technology, Culture and Human*, 2009, pp. 1401–1405.

[65] T. S. Ong, A. T. B. Jin, and D. C. L. Ngo, "Application-specific key release scheme from biometrics." *IJ Network Security*, vol. 6, no. 2, pp. 127–133, 2008.

[66] K. Nandakumar, A. Nagar, and A. K. Jain, "Hardening fingerprint fuzzy vault using password," in *International conference on Biometrics*. Springer, 2007, pp. 927–937.

[67] S. Ye, Y. Luo, J. Zhao, and S.-C. Cheung, "Anonymous biometric access control," *EURASIP Journal on Information Security*, vol. 2009, no. 1, p. 865259, 2009.

[68] S. D. Rane, W. Sun, and A. Vetro, "Secure distortion computation among untrusting parties using homomorphic encryption," in *2009 16th IEEE international conference on image processing (ICIP)*. IEEE, 2009, pp. 1485–1488.

[69] M. Barni, T. Bianchi, D. Catalano, M. Di Raimondo, R. D. Labati, P. Failla, D. Fiore, R. Lazzeretti, V. Piuri, A. Piva *et al.*, "A privacy-compliant fingerprint recognition system based on homomorphic encryption and fingercode

templates," in *2010 Fourth IEEE International Conference on Biometrics: Theory, Applications and Systems (BTAS)*. IEEE, 2010, pp. 1–7.

[70] J. J. Engelsma, K. Cao, and A. K. Jain, "Learning a fixed-length fingerprint representation," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 2019.

[71] A. M. Bazen and S. H. Gerez, "Systematic methods for the computation of the directional fields and singular points of fingerprints," *IEEE transactions on pattern analysis and machine intelligence*, vol. 24, no. 7, pp. 905–919, 2002.

[72] M. Kawagoe and A. Tojo, "Fingerprint pattern classification," *Pattern recognition*, vol. 17, no. 3, pp. 295–303, 1984.

[73] K. Nilsson and J. Bigun, "Localization of corresponding points in fingerprints by complex filtering," *Pattern Recognition Letters*, vol. 24, no. 13, pp. 2135–2144, 2003.

[74] P. Ramo, M. Tico, V. Onnia, and J. Saarinen, "Optimized singular point detection algorithm for fingerprint images," in *Proceedings 2001 International Conference on Image Processing (Cat. No. 01CH37205)*, vol. 3. IEEE, 2001, pp. 242–245.

[75] N. K. Ratha, S. Chikkerur, J. H. Connell, and R. M. Bolle, "Generating cancelable fingerprint templates," *IEEE Transactions on pattern analysis and machine intelligence*, vol. 29, no. 4, pp. 561–572, 2007.

[76] B. Yang, C. Busch, P. Bours, and D. Gafurov, "Non-invertible geometrical transformation for fingerprint minutiae template protection," in *2009 Proceedings of the 1st International Workshop on Security and Communication Networks*. IEEE, 2009, pp. 1–7.

[77] C. Lee, J.-Y. Choi, K.-A. Toh, S. Lee, and J. Kim, "Alignment-free cancelable fingerprint templates based on local minutiae information," *IEEE*

Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics), vol. 37, no. 4, pp. 980–992, 2007.

[78] S. Yang and I. Verbauwhede, "Automatic secure fingerprint verification system based on fuzzy vault scheme," in *Proceedings.(ICASSP'05). IEEE International Conference on Acoustics, Speech, and Signal Processing, 2005.*, vol. 5. IEEE, 2005, pp. v–609.

[79] J. Jeffers and A. Arakala, "Minutiae-based structures for a fuzzy vault," in *2006 Biometrics Symposium: Special Session on Research at the Biometric Consortium Conference*. IEEE, 2006, pp. 1–6.

[80] L. Hong, Y. Wan, and A. Jain, "Fingerprint image enhancement: algorithm and performance evaluation," *IEEE transactions on pattern analysis and machine intelligence*, vol. 20, no. 8, pp. 777–789, 1998.

[81] B. Yang and C. Busch, "Parameterized geometric alignment for minutiae-based fingerprint template protection," in *2009 IEEE 3rd International Conference on Biometrics: Theory, Applications, and Systems*. IEEE, 2009, pp. 1–6.

[82] B. Yang, C. Busch, P. Bours, and D. Gafurov, "Robust minutiae hash for fingerprint template protection," in *Media Forensics and Security II*, vol. 7541. International Society for Optics and Photonics, 2010, p. 75410R.

[83] W. Yang, J. Hu, S. Wang, and J. Yang, "Cancelable fingerprint templates with delaunay triangle-based local structures," in *Cyberspace Safety and Security*. Springer, 2013, pp. 81–91.

[84] S. Hirata and K. Takahashi, "Cancelable biometrics with perfect secrecy for correlation-based matching," in *International Conference on Biometrics*. Springer, 2009, pp. 868–878.

[85] K. Takahashi and S. H. Hitachi, "Generating provably secure cancelable fingerprint templates based on correlation-invariant random filtering," in *2009*

IEEE 3rd International Conference on Biometrics: Theory, Applications, and Systems. IEEE, 2009, pp. 1–6.

[86] A. T. B. Jin, D. N. C. Ling, and A. Goh, "Biohashing: two factor authentication featuring fingerprint data and tokenised random number," *Pattern recognition*, vol. 37, no. 11, pp. 2245–2255, 2004.

[87] A. B. Teoh, A. Goh, and D. C. Ngo, "Random multispace quantization as an analytic mechanism for biohashing of biometric and random identity inputs," *IEEE transactions on pattern analysis and machine intelligence*, vol. 28, no. 12, pp. 1892–1901, 2006.

[88] J. K. Pillai, V. M. Patel, R. Chellappa, and N. K. Ratha, "Sectored random projections for cancelable iris biometrics," in *2010 IEEE International Conference on Acoustics, Speech and Signal Processing*. IEEE, 2010, pp. 1838–1841.

[89] ——, "Secure and robust iris recognition using random projections and sparse representations," *IEEE transactions on pattern analysis and machine intelligence*, vol. 33, no. 9, pp. 1877–1893, 2011.

[90] Z. Jin, B.-M. Goi, A. Teoh, and Y. H. Tay, "A two-dimensional random projected minutiae vicinity decomposition-based cancellable fingerprint template," *Security and Communication Networks*, vol. 7, no. 11, pp. 1691–1701, 2014.

[91] S. Chikkerur, N. K. Ratha, J. H. Connell, and R. M. Bolle, "Generating registration-free cancelable fingerprint templates," in *2008 IEEE Second International Conference on Biometrics: Theory, Applications and Systems*. IEEE, 2008, pp. 1–6.

[92] H. Yang, X. Jiang, and A. C. Kot, "Generating secure cancelable fingerprint templates using local and global features," in *2009 2nd IEEE International Conference on Computer Science and Information Technology*. IEEE, 2009, pp. 645–649.

[93] A. B. J. Teoh and C. T. Yuang, "Cancelable biometrics realization with multispace random projections," *IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics)*, vol. 37, no. 5, pp. 1096–1106, 2007.

[94] B. Yang, D. Hartung, K. Simoens, and C. Busch, "Dynamic random projection for biometric template protection," in *2010 Fourth IEEE International Conference on Biometrics: Theory, Applications and Systems (BTAS)*. IEEE, 2010, pp. 1–7.

[95] T. Ahmad, J. Hu, and S. Wang, "Pair-polar coordinate-based cancelable fingerprint templates," *Pattern recognition*, vol. 44, no. 10-11, pp. 2555–2564, 2011.

[96] W. Yang, J. Hu, S. Wang, and Q. Wu, "Biometrics based privacy-preserving authentication and mobile template protection," *Wireless Communications and Mobile Computing*, vol. 2018, 2018.

[97] S. Wang and J. Hu, "Alignment-free cancelable fingerprint template design: A densely infinite-to-one mapping (ditom) approach," *Pattern Recognition*, vol. 45, no. 12, pp. 4129–4137, 2012.

[98] Z. Jin, A. B. J. Teoh, T. S. Ong, and C. Tee, "Generating revocable fingerprint template using minutiae pair representation," in *2010 2nd International Conference on Education Technology and Computer*, vol. 5. IEEE, 2010, pp. V5–251.

[99] Z. Jin, M.-H. Lim, A. B. J. Teoh, and B.-M. Goi, "A non-invertible randomized graph-based hamming embedding for generating cancelable fingerprint template," *Pattern Recognition Letters*, vol. 42, pp. 137–147, 2014.

[100] J. Zhe and A. T. B. Jin, "Fingerprint template protection with minutia vicinity decomposition," in *2011 International Joint Conference on Biometrics (IJCB)*. IEEE, 2011, pp. 1–7.

[101] S. Wang and J. Hu, "A hadamard transform-based method for the design of cancellable fingerprint templates," in *2013 6th International Congress on Image and Signal Processing (CISP)*, vol. 3. IEEE, 2013, pp. 1682–1687.

[102] S. Wang, G. Deng, and J. Hu, "A partial hadamard transform approach to the design of cancelable fingerprint templates containing binary biometric representations," *Pattern Recognition*, vol. 61, pp. 447–458, 2017.

[103] A. K. Jindal, S. R. Chalamala, and S. K. Jami, "Securing face templates using deep convolutional neural network and random projection," in *2019 IEEE International Conference on Consumer Electronics (ICCE)*. IEEE, 2019, pp. 1–6.

[104] S. Tulyakov, F. Farooq, P. Mansukhani, and V. Govindaraju, "Symmetric hash functions for secure fingerprint biometric systems," *Pattern Recognition Letters*, vol. 28, no. 16, pp. 2427–2436, 2007.

[105] G. Kumar, S. Tulyakov, and V. Govindaraju, "Combination of symmetric hash functions for secure fingerprint matching," in *2010 20th International Conference on Pattern Recognition*. IEEE, 2010, pp. 890–893.

[106] Z. Jin, J. Y. Hwang, Y.-L. Lai, S. Kim, and A. B. J. Teoh, "Ranking-based locality sensitive hashing-enabled cancelable biometrics: Index-of-max hashing," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 2, pp. 393–407, 2017.

[107] J. Kim and A. B. J. Teoh, "Sparse combined index-of-max hashing for fingerprint template protection," in *2019 12th International Congress on Image and Signal Processing, BioMedical Engineering and Informatics (CISP-BMEI)*. IEEE, 2019, pp. 1–6.

[108] S. M. Abdullahi, H. Wang, and T. Li, "Fractal coding-based robust and alignment-free fingerprint image hashing," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 2587–2601, 2020.

[109] F. Farooq, R. M. Bolle, T.-Y. Jea, and N. Ratha, "Anonymous and revocable fingerprint recognition," in *2007 IEEE conference on computer vision and pattern recognition*. IEEE, 2007, pp. 1–7.

[110] R. S. Germain, A. Califano, and S. Colville, "Fingerprint matching using transformation parameter clustering," *IEEE Computational Science and Engineering*, vol. 4, no. 4, pp. 42–49, 1997.

[111] Z. Jin, A. B. J. Teoh, T. S. Ong, and C. Tee, "Secure minutiae-based fingerprint templates using random triangle hashing," in *International Visual Informatics Conference*. Springer, 2009, pp. 521–531.

[112] ——, "A revocable fingerprint template for security and privacy preserving," *KSII Transactions on Internet & Information Systems*, vol. 4, no. 6, 2010.

[113] ——, "Fingerprint template protection with minutiae-based bit-string for security and privacy preserving," *Expert systems with applications*, vol. 39, no. 6, pp. 6157–6167, 2012.

[114] C. Lee and J. Kim, "Cancelable fingerprint templates using minutiae-based bit-strings," *Journal of network and computer applications*, vol. 33, no. 3, pp. 236–246, 2010.

[115] W. J. Wong, M. L. D. Wong, Y. H. Kho *et al.*, "A low complexity multi-line code for cancelable fingerprint template," in *2nd International Conference on Convergence Technology. Qingdao: Korea Convergence Society*, 2012, pp. 61–65.

[116] W. J. Wong, A. B. Teoh, M. D. Wong, and Y. H. Kho, "Enhanced multi-line code for minutiae-based fingerprint template protection," *Pattern Recognition Letters*, vol. 34, no. 11, pp. 1221–1229, 2013.

[117] J. B. Kho, J. Kim, I.-J. Kim, and A. B. Teoh, "Cancelable fingerprint template design with randomized non-negative least squares," *Pattern Recognition*, vol. 91, pp. 245–260, 2019.

[118] S. Wang and J. Hu, "Design of alignment-free cancelable fingerprint templates via curtailed circular convolution," *Pattern Recognition*, vol. 47, no. 3, pp. 1321–1329, 2014.

[119] M. Ferrara, D. Maltoni, and R. Cappelli, "A two-factor protection scheme for mcc fingerprint templates," in *2014 International Conference of the Biometrics Special Interest Group (BIOSIG)*. IEEE, 2014, pp. 1–8.

[120] R. Cappelli, M. Ferrara, and D. Maltoni, "Minutia cylinder-code: A new representation and matching technique for fingerprint recognition," *IEEE transactions on pattern analysis and machine intelligence*, vol. 32, no. 12, pp. 2128–2141, 2010.

[121] M. Ferrara, D. Maltoni, and R. Cappelli, "Noninvertible minutia cylinder-code representation," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 6, pp. 1727–1737, 2012.

[122] M. Sandhya and M. V. Prasad, "k-nearest neighborhood structure (k-nns) based alignment-free method for fingerprint template protection," in *2015 International Conference on Biometrics (ICB)*. IEEE, 2015, pp. 386–393.

[123] S. Wang and J. Hu, "A blind system identification approach to cancelable fingerprint templates," *Pattern Recognition*, vol. 54, pp. 14–22, 2016.

[124] S. Wang, W. Yang, and J. Hu, "Design of alignment-free cancelable fingerprint templates with zoned minutia pairs," *Pattern Recognition*, vol. 66, pp. 295–301, 2017.

[125] A. K. Jain, K. Nandakumar, and A. Nagar, "Fingerprint template protection: From theory to practice," in *Security and privacy in Biometrics*. Springer, 2013, pp. 187–214.

[126] C. Li and J. Hu, "Attacks via record multiplicity on cancelable biometrics templates," *Concurrency and Computation: Practice and Experience*, vol. 26, no. 8, pp. 1593–1605, 2014.

[127] P. Das, K. Karthik, and B. C. Garai, "A robust alignment-free fingerprint hashing algorithm based on minimum distance graphs," *Pattern Recognition*, vol. 45, no. 9, pp. 3373–3388, 2012.

[128] G. Strang and T. Nguyen, *Wavelets and filter banks*. SIAM, 1996.

[129] A. V. Oppenheim, *Discrete-time signal processing*. Pearson Education India, 1999.

[130] G. H. Golub *et al.*, "Cf vanloan, matrix computations," *The Johns Hopkins*, 1996.

[131] W. Yang, S. Wang, J. Hu, G. Zheng, and C. Valli, "Security and accuracy of fingerprint-based biometrics: A review," *Symmetry*, vol. 11, no. 2, p. 141, 2019.

[132] M. Gomez-Barrero, J. Galbally, C. Rathgeb, and C. Busch, "General framework to evaluate unlinkability in biometric template protection systems," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 6, pp. 1406–1420, 2017.

[133] M. Gomez-Barrero, C. Rathgeb, J. Galbally, C. Busch, and J. Fierrez, "Unlinkable and irreversible biometric template protection based on bloom filters," *Information Sciences*, vol. 370, pp. 18–32, 2016.

[134] Y. Chen, Y. Wo, R. Xie, C. Wu, and G. Han, "Deep secure quantization: On secure biometric hashing against similarity-based attacks," *Signal Processing*, vol. 154, pp. 314–323, 2019.

[135] W.-H. Steeb and Y. Hardy, *Problems and solutions in introductory and advanced matrix calculus*. World Scientific Publishing Company, 2016.

[136] F. Quan, S. Fei, C. Anni, and Z. Feifei, "Cracking cancelable fingerprint template of ratha," in *2008 International Symposium on Computer Science and Computational Technology*, vol. 2. IEEE, 2008, pp. 572–575.

[137] W. Yang, "Local structure based fingerprint authentication systems with template protection." Ph.D. dissertation, University of New South Wales, Canberra, Australia, 2015.

[138] W. Yang, S. Wang, J. Hu, G. Zheng, and C. Valli, "A fingerprint and finger-vein based cancelable multi-biometric system," *Pattern Recognition*, vol. 78, pp. 242–251, 2018.

[139] P. L'ecuyer, "Tables of linear congruential generators of different sizes and good lattice structure," *Mathematics of Computation*, vol. 68, no. 225, pp. 249–260, 1999.

[140] E. J. Kelkboom, J. Breebaart, T. A. Kevenaar, I. Buhan, and R. N. Veldhuis, "Preventing the decodability attack based cross-matching in a fuzzy commitment scheme," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 1, pp. 107–121, 2010.

[141] W. Yang, S. Wang, G. Zheng, J. Chaudhry, and C. Valli, "Ecb4ci: An enhanced cancelable biometric system for securing critical infrastructures," *The Journal of Supercomputing*, vol. 74, no. 10, pp. 4893–4909, 2018.

[142] W. Yang, S. Wang, G. Zheng, J. Yang, and C. Valli, "A privacy-preserving lightweight biometric system for internet of things security," *IEEE Communications Magazine*, vol. 57, no. 3, pp. 84–89, 2019.

[143] B. V. Gnedenko, *Theory of probability*. Routledge, 2018.

[144] K. Habib, A. Torjusen, and W. Leister, "A novel authentication framework based on biometric and radio fingerprinting for the iot in ehealth," in *Proceedings of International Conference on Smart Systems, Devices and Technologies (SMART)*, 2014, pp. 32–37.

[145] N. Maček, I. Franc, M. Bogdanoski, and A. Mirković, "Multimodal biometric authentication in iot: Single camera case study," 2016.

[146] L.-P. Shahim, D. Snyman, T. du Toit, and H. Kruger, "Cost-effective biometric authentication using leap motion and iot devices," in *Proceedings of the*

Tenth International Conference on Emerging Security Information, Systems and Technologies (SECURWARE 2016), Nice, France, 2016, pp. 24–28.

[147] N. S. Prakash and N. Venkatram, "Establishing efficient security scheme in home iot devices through biometric finger print technique," *Indian Journal of Science and Technology*, vol. 9, no. 17, pp. 1–8, 2016.

[148] N. Karimian, P. A. Wortman, and F. Tehranipoor, "Evolving authentication design considerations for the internet of biometric things (iobt)," in *Proceedings of the Eleventh IEEE/ACM/IFIP International Conference on Hardware/Software Codesign and System Synthesis*, 2016, pp. 1–10.

[149] S. Roy, S. Chatterjee, and G. Mahapatra, "An efficient biometric based remote user authentication scheme for secure internet of things environment," *Journal of Intelligent & Fuzzy Systems*, vol. 34, no. 3, pp. 1403–1410, 2018.

[150] G. Meena and S. Choudhary, "Biometric authentication in internet of things: A conceptual view," *Journal of Statistics and Management Systems*, vol. 22, no. 4, pp. 643–652, 2019.

[151] C. Zhu, V. C. Leung, L. Shu, and E. C.-H. Ngai, "Green internet of things for smart world," *IEEE access*, vol. 3, pp. 2151–2162, 2015.

[152] F. K. Shaikh, S. Zeadally, and E. Exposito, "Enabling technologies for green internet of things," *IEEE Systems Journal*, vol. 11, no. 2, pp. 983–994, 2015.

[153] P. Sathyamoorthy, E. C.-H. Ngai, X. Hu, and V. C. Leung, "Energy efficiency as an orchestration service for mobile internet of things," in *2015 IEEE 7th International Conference on Cloud Computing Technology and Science (CloudCom)*. IEEE, 2015, pp. 155–162.

[154] A. Tzanakaki, M. P. Anastasopoulos, S. Peng, B. Rofoee, Y. Yan, D. Simeonidou, G. Landi, G. Bernini, N. Ciulli, J. F. Riera *et al.*, "A converged network architecture for energy efficient mobile cloud computing," in *2014 International Conference on Optical Network Design and Modeling*. IEEE, 2014, pp. 120–125.

[155] T. K. Kundu and K. Paul, "Improving android performance and energy efficiency," in *2011 24th Internatioal Conference on VLSI Design*. IEEE, 2011, pp. 256–261.

[156] P. Shu, F. Liu, H. Jin, M. Chen, F. Wen, Y. Qu, and B. Li, "etime: Energy-efficient transmission between cloud and mobile devices," in *2013 Proceedings IEEE INFOCOM*. IEEE, 2013, pp. 195–199.

[157] S. Nirjon, A. Nicoara, C.-H. Hsu, J. Singh, and J. Stankovic, "Multinets: Policy oriented real-time switching of wireless interfaces on mobile devices," in *2012 IEEE 18th Real Time and Embedded Technology and Applications Symposium*. IEEE, 2012, pp. 251–260.

[158] J. Tang, Z. Zhou, J. Niu, and Q. Wang, "An energy efficient hierarchical clustering index tree for facilitating time-correlated region queries in the internet of things," *Journal of Network and Computer Applications*, vol. 40, pp. 1–11, 2014.

[159] A. Venčkauskas, N. Jusas, E. Kazanavičius, and V. Štuikys, "An energy efficient protocol for the internet of things," *Journal of Electrical Engineering*, vol. 66, no. 1, pp. 47–52, 2015.

[160] B. Steigerwald and A. Agrawal, "Developing green software," *Intel White Paper*, vol. 9, 2011.

[161] P. K. Dhillon and S. Kalra, "A lightweight biometrics based remote user authentication scheme for iot services," *Journal of Information Security and Applications*, vol. 34, pp. 255–270, 2017.

[162] P. Punithavathi, S. Geetha, M. Karuppiah, S. H. Islam, M. M. Hassan, and K.-K. R. Choo, "A lightweight machine learning-based authentication framework for smart iot devices," *Information Sciences*, vol. 484, pp. 255–268, 2019.

[163] J. Wang, J. Sun, X. Zhang, D. Huang, and M. Fejer, "Ultrafast all-optical three-input boolean xor operation for differential phase-shift keying signals

using periodically poled lithium niobate," *Optics letters*, vol. 33, no. 13, pp. 1419–1421, 2008.

[164] P. L. Dragotti and M. Vetterli, "Wavelet footprints: theory, algorithms, and applications," *IEEE Transactions on Signal Processing*, vol. 51, no. 5, pp. 1306–1323, 2003.

[165] N. Kingsbury, "Image processing with complex wavelets," *Philosophical Transactions of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences*, vol. 357, no. 1760, pp. 2543–2560, 1999.

[166] N. Kingsbury and J. Magarey, "Wavelet transforms in image processing," in *Signal analysis and prediction*. Springer, 1998, pp. 27–46.

[167] J. Romberg, H. Choi, R. Baraniuk, and N. Kingbury, "Multiscale classification using complex wavelets and hidden markov tree models," in *Proceedings 2000 International Conference on Image Processing (Cat. No. 00CH37101)*, vol. 2. IEEE, 2000, pp. 371–374.

[168] H. Choi, J. Romberg, R. Baraniuk, and N. Kingsbury, "Hidden markov tree modeling of complex wavelet transforms," in *2000 IEEE International Conference on Acoustics, Speech, and Signal Processing. Proceedings (Cat. No. 00CH37100)*, vol. 1. IEEE, 2000, pp. 133–136.

[169] I. W. Selesnick, R. G. Baraniuk, and N. C. Kingsbury, "The dual-tree complex wavelet transform," *IEEE signal processing magazine*, vol. 22, no. 6, pp. 123–151, 2005.

[170] I. W. Selesnick, "The double-density dual-tree dwt," *IEEE Transactions on signal processing*, vol. 52, no. 5, pp. 1304–1314, 2004.

[171] W. Yang, S. Wang, J. Hu, G. Zheng, J. Yang, and C. Valli, "Securing deep learning based edge finger vein biometrics with binary decision diagram," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 7, pp. 4244–4253, 2019.