Minutia Modelling and Secure Fingerprint Authentication with Applications to the IoT

Submitted by

Aseel BEDARI

B.S., University of Technology, 2009
M.S., La Trobe University, 2017

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

in the

Department of Engineering

School of Computing, Engineering and Mathematical Sciences

LA TROBE UNIVERSITY

Victoria
Australia

August, 2022

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

Name: Aseel BEDARI
Date: 16 August 2022

Abstract

Fingerprint authentication systems have been widely used in a range of military and civil applications for the distinctiveness and stability that fingerprints can provide. However, fingerprint biometrics have security and privacy concerns. The research behind this thesis aims at investigating these concerns and developing effective models and algorithms in the area of fingerprint template protection, specifically, designing cancelable fingerprint templates.

The existing fingerprint cancelable templates are unable to achieve satisfactory recognition accuracy due to the uncertainty presented in each fingerprint image. Despite a variety of approaches to detecting deformations in fingerprint images, there is currently no available method for capturing minutiae variations between two impressions of the same finger in a unified model. In this thesis, a Möbius transformation-based model is used to represent fingerprint minutiae variations between fingerprint scans and formulate the changes to minutiae feature patterns.

Minutia Cylinder Code (MCC) is an effective, high-quality representation of local minutia structures. MCC templates demonstrate fast and excellent fingerprint matching performance, but if compromised, they can be reverse-engineered to retrieve minutia information. To this end, this thesis proposes an alignment-free cancelable MCC-based template design based on a dynamic random key model, named the dyno-key model. The proposed method exhibits competitive performance in comparison with state-of-the-art cancelable fingerprint templates, as evaluated over five public databases and satisfies all the requirements of biometric template protection.

The applications of biometric authentication systems to Internet of Things (IoT) devices is the third problem investigated in this thesis. Energy-efficient data storage and low computational costs are critical issues when designing a secure authentication system for many IoT applications. In this thesis, a two-stage feature transformation scheme is developed to protect user privacy for authentication on IoT devices. The proposed authentication system provides energy-efficient data storage and low computational costs, thus making the proposed scheme highly suitable for resource- constrained IoT devices.

Publications

A number of papers have been published in various international journals based on the discussion and material in this thesis. The publications are listed as follows:

- J. Moorfield, S. Wang, W. Yang, **A. Bedari**, and P. Van Der Kamp, "A Möbius transformation based model for fingerprint minutiae variations," *Pattern Recognition*, vol. 98, 107054, 2020.
- **A. Bedari**, S. Wang, and W. Yang, "Design of cancelable MCC-based fingerprint templates using Dyno-key model," *Pattern Recognition*, vol. 119, 108074, 2021.
- **A. Bedari**, S. Wang, and J. Yang, "A two-stage feature transformation-based fingerprint authentication system for privacy protection in IoT," *IEEE Transactions on Industrial Informatics*, vol.18, no. 4, pp. 2745-2752, 2021.
- W. Yang , S. Wang, J. Kang, M. N. Johnstone, and **A. Bedari**, "A linear convolution-based cancelable fingerprint biometric authentication system," *Computers and Security*, vol. 114, 102583, 2022.

Acknowledgements

This work was supported by a La Trobe University Full Fee Research Scholarship and a La Trobe University Postgraduate Research Scholarship. This thesis is the product of a four-year journey. Collaboration with many researchers made it possible and the thesis is shaped by their contribu-tions and generous help.

First and foremost, my deepest gratitude goes to my supervisor, Dr Song Wang. Song's advice, guidance, help, ideas, insights, encouragement, regular reminders of "keep working hard" and enquiries of "any new breakthroughs?" were instrumental in making this thesis possible and shaped my research skills in solving real-world problems that expanded my horizons.

I am also grateful to Dr Wencheng Yang for his advice, guidance, and deep insights that helped me at various stages of my research. I really appreciated his useful suggestions which enabled me to improve my research and writing skills.

I extend my thanks to Prof. Jucheng Yang for his advice and guidance. I greatly appreciated his valuable support in relation to my research work.

I also would like to thank Dr Guang (Dennis) Deng for supervising my Master's thesis and for being my PhD co-supervisor. Dennis's passion and deep knowledge inspired me and honed my interest in this research field.

Finally, this work would not have been possible without the tireless support and encouragement of my family and my husband, Benjamin Shamoon, who always reminded me of the most important things in life when I was feeling lost. They gave me the resilience to face all difficulties.

Contents

List of Figures

List of Tables

List of Abbreviations

FAR	False Acceptance Rate
FRR	False Rejection rate
EER	Equal Error Rate
FMR	False Match Rate
FNMR	False Non-Match Rate
ARM	Attack via Record Multiplicity
IoT	Internet of Things
MCC	Minutia Cylinder-Code
FTP	Fingerprint Template Protection
FC	Fingerprint Cryptosystem
FV	Fuzzy Vault
FE	Fuzzy Extractor
MRC	Minutiae Relation Code
CIRF	Correlation Invariant Random Filtering
RMQ	Random Multispace Quantization
MVD	Minutia Vicinity Decomposition
MDG	Minimum Distance Graphs
IoM	Index-of-Maximum
GRP-IoM	Gaussian Random projection Index-of-Maximum
URP-IoM	Uniformly Random Permeation Index-of-Maximum
SC-IoM	Sparse Combined Index-of-Maximum
KPCA	Kernel principal component analysis
IMM	Indexing-Min-Max hashing
NMHS	Minimum Hash Signature
SEFV	Secure Extended Feature Vector
EFV	Extended Feature Vector
MLC	Multi-Line Code
DFT	Discrete Fourier Transform
BSI	Blind System Identification
FIR	Finite Impulse Response
PUFs	Physically Unclonable Functions
K-NNS	K-Nearest neighbourhood Structure
FVC	Fingerprint Verification Competition
DCT	Discrete Cosine Transform
DET	Detection Error Trade-off
ROC	Receiver Operating Characteristics

Chapter 1

Introduction

1.1 Fingerprint authentication system

Biometrics is an identification procedure that uses the unique behavioural and physiological individualities of the human body as identifiers [1]. Biometrics provide reliable authentication as they cannot be easily shared, misplaced, or forged compared to traditional token- or knowledge-based methods, e.g., keys, ID cards, passwords or PINs. There are several biometric traits such as fingerprints, faces, iris, finger veins, palm and hand geometry. Each trait has its own strengths and weaknesses, where the selection of a specific trait usually relies on the application itself.

Fingerprint-based authentication is one of the most reliable biometric technologies, due to its distinctiveness and stable characteristics. Each person's fingerprints are unique. Even identical twins, who share the same DNA sequence, have slightly different fingerprints. Therefore, fingerprint authentication has been used in a wide range of applications, such as law enforcement, commercial, civilian and financial applications [2]. In a typical fingerprint image, there are unique shapes and patterns that are formed by ridges called minutiae. The location of these patterns on the surface of the fingerprints is used for identification purposes. It is highly unlikely for two individuals to share the exact same kind of minutiae in the exact same location. This unlikeliness grows exponentially with each minutia added for comparison. Figure 1.1 illustrates different types of minutiae showing the various ways ridges tend to be discontinuous at a local level. Ridge ending and bifurcation are the most widely used features to represent a fingerprint pattern in biometric systems. A set of minutiae points $\mathbf{M}$

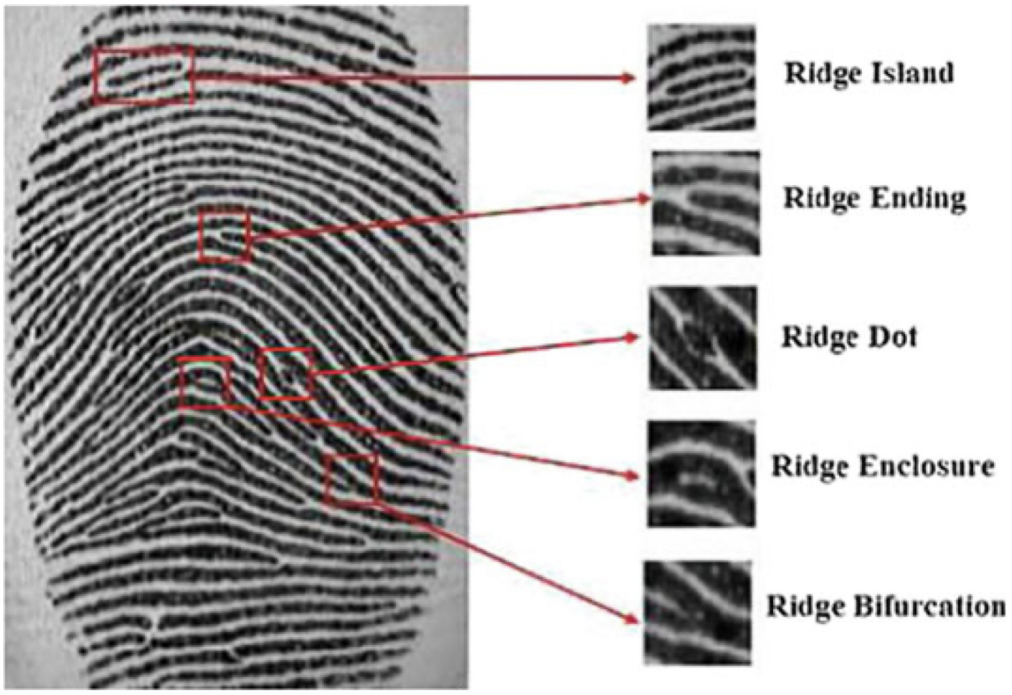

FIGURE 1.1: A fingerprint with multiple kinds of minutiae highlighted [3]

extracted from a fingerprint image can be presented as

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

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

Fingerprint authentication usually consists of two stages, the enrolment stage and recognition stage. During the enrolment stage, feature data is extracted from a captured fingerprint image as a template which is stored in central database whereas the recognition stage is further divided into two phases: identification and verification phases.

In the identification process, the query feature data, obtained in the same way as the template feature data, is compared with all the fingerprints which are stored in the database. This is known as one-to-many (1:N) matching to establish a user's identify. This process is widely used in crime scene situations.

In the verification process, the query feature data is verified from the database using matching algorithms, known as one-to-one (1:1) matching. This is to compare query fingerprint and an enrolled fingerprint stored as a template in the

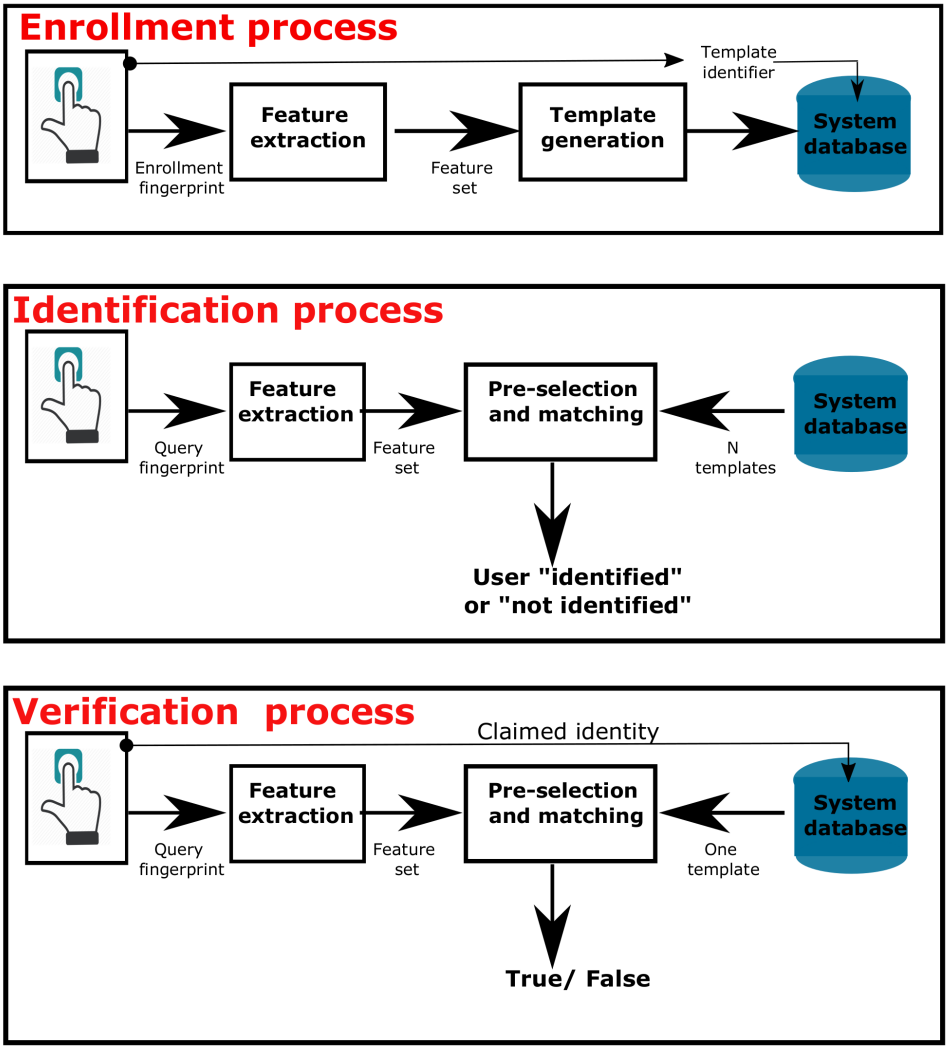

FIGURE 1.2: Enrolment, identification and verification processes of an insecure fingerprint recognition system (adapted from [4])

database. Figure 1.2 illustrates the enrolment, identification and verification process of an unsecured fingerprint recognition system.

1.2 Motivation and objectives

Despite the development in the fingerprint authentication sector during recent years and the significant achievements in the unencrypted domain, developing a fingerprint authentication system is a non-trivial task. This is due to three major factors: fingerprint uncertainty, security and privacy concerns; the need for energy-efficient storage and the need to keep computational costs low when using a fingerprint authentication system on resource-constrained IoT devices.

Firstly, fingerprint uncertainty, caused by rotation, translation, and non-linear distortion at each fingerprint image acquisition, is an obstacle in the design of a fingerprint authentication system. During the fingerprint acquisition process, a fingerprint sensor or scanner acquires fingerprint images using some means of contact sensing. The quality of the acquired images can be affected by several physiological, behavioural and environment factors, e.g., the amount of pressure applied by the person, the elasticity of their finger skin, the disposition of the person (sitting or standing), the moisture content of their finger skin (dry, wet or oily), the motion of their finger, the ambient temperature and light. As a result, fingerprint images contain a fair amount of uncertainty and variability, giving rise to intra-class variations and inter-class similarity [1]. In minutiae-based matching methods where minutia's x and y coordinates are used, registration is required to rotate and translate the query image with respect to the template image. However, an accurate registration to the singular point (core and delta) is difficult to perform as a small change in the singular point coordinators may significantly affect the coordinates of the minutiae. Therefore, a low-quality fingerprint image results in a loss of accuracy in matching two fingerprints. Figure

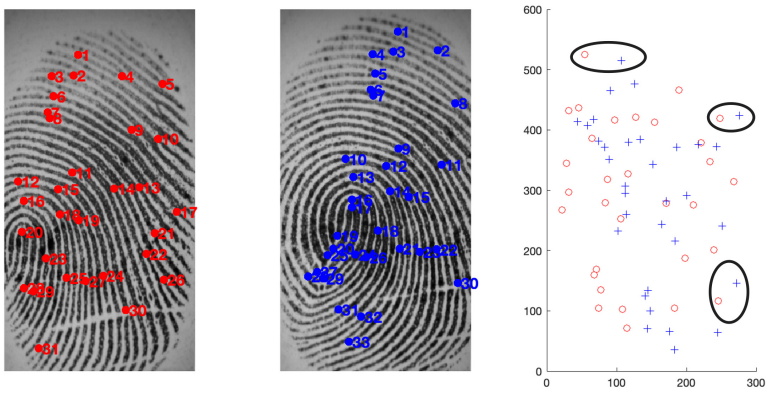

FIGURE 1.3: An example of two fingerprints from the same finger, one with distortion.

1.3 shows two impressions of the same finger. Due to non-linear distortion, after registration, several corresponding minutiae, e.g., in the circular region, are stretched more than a set threshold value.

Secondly, the security and privacy of fingerprint templates are critical concerns when designing a fingerprint authentication system. Fingerprint templates, which store users' original fingerprint information, are vulnerable if unprotected, as biometric traits are irreplaceable if stolen. Moreover, adversaries can use stolen

fingerprint templates to commit identity fraud or theft using various applications. This may lead to serious security breaches and privacy threats when a template is hacked. Researchers have been working on developing different template protection techniques, e.g., bio-cryptosystems and cancelable biometrics to secure biometric systems. The focus of this PhD thesis is on cancelable templates which are discussed in detail in Chapter 2 (along with a brief description in Section 1.3.2).

Thirdly, although the IoT environment has resulted in encouraging advances making daily life more convenient, ensuring the security and privacy of personal information is a challenge in IoT development. Authentication problems present a serious threat to IoT devices due to the massive number of connected objects resulting in a huge volume of exchanged/collected data in the IoT network. In addition to the aforementioned challenges, the IoT environment faces another challenge that stands in the way of IoT development. Resource-constrained (e.g., limited computing capacity and battery life) IoT devices often malfunction due to the excessive computational requirements in cryptography and are subject to high energy consumption.

The use of biometric-authentication systems is becoming a more prevalent solution over traditional password-based authentication methods. However, biometric information stored in central databases or smart devices is vulnerable since an individual's biometric traits cannot be altered or reissued. If a biometric template is compromised, it is compromised forever, enabling privacy and security breaches to occur. If an imposter gains access to IoT devices using stolen biometric templates, there are serious risks to the stored data. Hence, it is crucial to protect biometric data to protect the user's identity and to ensure that the original biometric information cannot be accessed by imposters.

On the other hand, energy-efficient data storage and low computational costs are critical when designing a secure biometric authentication system for many IoT applications. The existing preventive and security countermeasure solutions are inadequate and insufficient to successfully address these problems and mitigate threats. In fact, most biometric authentication systems are slow, have a limited database storage capacity and experience data transmission problems.

1.3 Fingerprint template protection

Fingerprint template protection (FTP) is a collective term for a variety of methods that aim to preserve privacy and ensure the secure storage of fingerprint data. Various algorithms have been developed which can produce diverse unlinkable and non-invertible references from biometric data. Biometric cryptosystems and cancelable biometrics are emerging technologies to ensure the secure protection of fingerprint templates. In this section, we briefly introduce both approaches: biometric cryptosystems and cancelable biometrics, and provide an overview of the performance metrics, databases and the existing types of performance evaluation protocols.

1.3.1 Biometrics cryptosystems

Biometric cryptosystems combine biometrics with a cryptographic key and merges the advantages of both biometrics and cryptosystems. Biometric cryptosystems can output a key by either combining the biometric features, such as fuzzy commitment (FC) and fuzzy vault (FV) or by generating the key from the biometric features, for instance, fuzzy extractor (FE).

1.3.2 Cancelable biometrics

A cancelable template is a privacy-preserving authentication method. Instead of storing raw biometric data as a template, it applies systematic distortion by a one-way transformation technique in the enrolment stage and in the verification stage. The transformed template and query are matched in the transformed domain. If a database is compromised and a stored template is stolen, an adversary cannot retrieve the original template and a new version of it can be reproduced by changing the transformation parameter(s). There are five important properties that should be possessed by cancelable templates.

Non-invertibility: It should be computationally difficult to retrieve the raw biometric data from the transformed biometric template.

Accuracy: The accuracy of the recognition system should not degrade in the transformed domain. A trade-off between recognition accuracy and security is one of the main challenges when a cancelable template is designed. A well-designed transformation function is needed to preserve the discriminatory features of a fingerprint as well as ensure recognition accuracy.

Diversity: To protect user privacy, the cancelable template must be able to generate a huge number of unrelated protected template from the same raw template to be used in different applications.

Revocability: A new template should be generated from raw biometric data in case the protected template is compromised.

Unlinkability: This property states that the protected templates from the same fingerprint for various applications should not be able to be cross-matched. No existing method should be able to determine if two templates generated from the same fingerprint are related.

1.3.3 Performance metrics

The trade-off between security and recognition accuracy presents a fundamental challenge associated with cancelable template design. Therefore, the accuracy and security of the designed fingerprint authentication system needs to be measured. In a secure fingerprint authentication system, the matching module yields a matching score between the enrolled template and the query template in the range [0,1]. A score that is closer to 1 indicates that the query fingerprint is derived from the same enrolled finger template. A score threshold is used to regulate the final decision in the form of "identified / accepted" or "not-identified / rejected".

Two types of errors can be identified in the matching module: TYPE 1 is to mistake the query fingerprint and the enrolled template which are from two different fingers as being from the same finger, namely false acceptance. TYPE 2 is to mistake the query fingerprint and the enrolled template which are from the same finger as being from different fingers, namely false rejection. Based on the false acceptance and false rejection generated by the system, the performance can be measured 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 refers to the probability of mistaking two fingerprints from different fingers as being from the same finger.

False rejection rate (FRR): FRR is the probability of mistaking two fingerprints from the same finger as being from different fingers.

Equal error rate (EER): EER is the error rate when FAR=FRR. Genuine testing and imposter testing were carried out to obtain these performance measures.

ZeroFMR: ZeroFMR refers to the minimum FRR at which the system achieves a FAR equal to zero.

FMR1000: FMR1000 refers to the minimum FRR at which the system achieves a FAR equal to 0.1%.

1.3.4 Databases

The cancelable template scheme proposed in this thesis is evaluated on eight public databases, namely FVC2002 DB1, DB2 and DB3 [5], FVC2004 DB1, DB2 and DB3 [6] and FVC2006 DB2 and DB3 [7]. These databases consist of fingerprint images with different qualities. Figure 1.4 shows some examples of

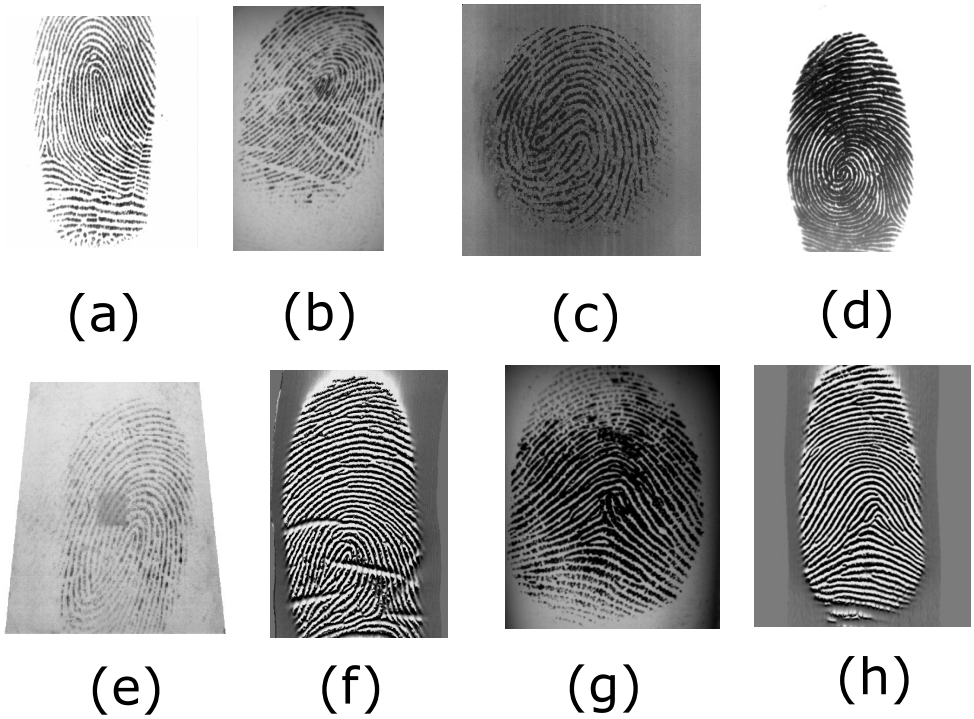

FIGURE 1.4: Example fingerprint images: (a) FVC2002DB1-Impression 2 of finger 3, (b) FVC2002DB2-Impression 7 of finger 14, (c) FVC2002DB3-Impression 1 of finger 65, (d) FVC2004DB1-Impression 3 of finger 59, (e) FVC2004DB2- Impression 6 of finger 80, (f) FVC2004DB3- Impression 5 of finger 99, (g) FVC2006DB2-Impression 1 of finger 13, (h) FVC2006DB3- Impression 7 of finger 19

fingerprint images and Table 1.1 provides information on the eight databases.

Commercial fingerprint recognition software VeriFinger SDK [8]] is employed to extract minutia points from the fingerprint images in these databases.

TABLE 1.1: Database information

Database	FVC2002			FVC2004		FVC2006	
	DB1	DB2	DB3	DB1	DB2	DB2	DB3
No. of fingers	100	100	100	100	100	150	150
Images per finger	8	8	8	8	8	12	12
Resolution	500 dpi	569 dpi	500 dpi	500 dpi	500 dpi	569 dpi	500 dpi
Sensor type	Optical	Optical	Capacitive	Optical	Optical	Optical	Thermal
Image size	388×374	296×560	300×300	640×480	328×364	400×560	400×500
Image quality	Good – Medium	Medium	Medium – Low	Extremely low	Very low	Good – Medium	Very low

1.3.5 Performance evaluation protocols

To evaluate the performance of the cancelable templates, two protocols, namely the 1v1 protocol and the FVC protocol, are used to produce a genuine score distribution. Each database (Table 1.1) has 800 fingerprint impressions from 100 different fingers and 8 impressions for each finger. The imposter scores are computed by comparing the first impression of each finger to the first impression of the other fingers in a non-redundant fashion. Therefore, for each database, there are $4950 = \frac{100(100-1)}{2}$ imposter scores. On the other hand, genuine scores can be calculated as follows:

1vs1 protocol: The first impression of each finger is compared with the second impression of the same finger. There are 100 genuine scores resulting from 100 different fingers for each database.

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

For each finger, the quality of the fingerprint continuously reduces from impression 1 to impression 8. Therefore, the performance under the 1vs1 protocol is better than the FVC protocol because the 1vs1 protocol compares only the first two impressions while the FVC protocol uses all 8 impressions for genuine testing. However, the robustness of any cancelable template method should reflect both protocols to verify whether the algorithm works successfully on both good and bad quality fingerprint images.

1.4 Summary of contributions

This thesis focuses on the development and design of a secure fingerprint authentication system that can overcome the impact of fingerprint uncertainty and provide reliable biometric template protection. Furthermore, it can provide energy-efficient storage and ensure low computational costs, which is important for resource-constrained IoT devices.

The contributions of the thesis are summarized as follows:

1. We designed a unified model to represent minutiae variations between fingerprint scans and formulate the changes to minutiae feature patterns. We identify the Möbius transformation as a good candidate for modelling minutiae translation, rotation, and non-linear distortion, that is, different types of minutiae variations are described in a single model. Not only do we mathematically prove that the Möbius transformation-based model is a unified model for capturing minutiae variations, we also experimentally verify the effectiveness of this model using a public database.

2. We developed an alignment-free cancelable MCC-based template based on designing a dynamic random key model, called the Dyno-key model. The Dyno-key model dynamically extracts elements from MCC's binary feature vectors based on randomly generated keys. Those extracted elements are discarded after the block-based logic operations to increase security. Leveling with the performance of the unprotected, reproduced MCC templates, the proposed method exhibits competitive performance in comparison with state-of-the-art cancelable fingerprint templates.

3. We proposed a secure fingerprint authentication system to protect user privacy for authentication on IoT devices. The proposed system applies a two-stage feature transformation scheme. Specifically, a weight-based fusion mechanism is designed in the first stage, while in the second stage a linear convolution-based transformation with element removal from the convolution output is designed to increase security and protection. The proposed authentication system exhibits highly competitive performance when compared with the existing cancelable fingerprint templates. Moreover, its energy-efficient storage and low computational costs make the proposed scheme highly suitable for resource-constrained IoT devices.

1.5 Thesis organisation

The thesis comprises six chapters, including this chapter. Chapter 2 reviews the related work in the literature survey based on minutiae modelling, fingerprint template protection and using a fingerprint authentication system with IoT devices and their applications. Chapter 3 describes how a Möbius transformation is used to model fingerprint minutiae variations, e.g., translation, rotation and non-linear distortion. Chapter 4 presents an alignment-free cancelable fingerprint template based on a dyno-key model. Chapter 5 describes a two-stage feature transformation scheme which is used to design a fingerprint authentication system utilised in resource-constrained IoT devices. Chapter 6 discusses the conclusions and future research based on the current work.

1.6 A note on the contribution of the collaborators

Several researchers contributed to the research presented in this thesis. Dr Song Wang (the author's supervisor) and Dr Dennis Deng (the author's co-supervisor) as well as Dr Wencheng Yang (a colleague from Edith Cowan University) provided valuable support and guidance (both theoretically and experimentally). The work in Chapter 1 and 2 presents the author's own knowledge and thoughts. Chapter 3 proposes the Möbius transformation-based model for fingerprint minutiae variations which was designed by Mr James Moorfield and Dr Song Wang. The the system was tested by the author to evaluate the effectiveness of the designed model, under the guidance of Dr Song Wang and Dr Wencheng Yang.

Chapter 4 discusses the development of the alignment-free cancelable template using the dyno-key model. The idea was developed and matured by the author and Dr Song Wang. Dr Wencheng Yang provided support in the analysis of the security of the system.

Chapter 5 presents a two-stage feature transformation-based fingerprint authentication system for privacy protection in IoT. The idea was developed and matured by the author and Dr Song Wang. Prof. Jucheng Yang provided support by reviewing the paper and analysing the security of the system.

Chapter 2

Literature Review

2.1 Introduction

This chapter aims to review the existing works related to fingerprint authentication systems in terms of modelling minutiae variations and their effects on fingerprint matching. The recent works in the field of template protection techniques are reviewed and finally, an overview is given of the existing fingerprint authentication systems with template protection to preserve privacy and security in IoT devices.

2.2 Modelling minutiae variations

The majority of fingerprint recognition systems rely on minutiae information to a degree, and these systems can only be as robust as the underlying minutiae information. Although reliable minutiae extraction is vital to a system's performance, minutiae variations can occur in different fingerprint scans including translation, rotation and non-linear distortion. Translation and rotation are due to changing fingerprint orientation and position shift when capturing a fingerprint, while non-linear distortion is caused by variable skin pressure.

In recent years, several techniques have been proposed to deal with the issue of minutiae variations (translation, rotation and non-linear distortion) that are inherited in fingerprint images, resulting in different approaches from different perspectives. Distortion can be modelled through different spatial transformations such as rigid and thin plate spline (TPS) [9]. Even though rigid transformation is not robust enough to model the complex properties of geometric distortion, combining a global rigid transform and a local tolerant window have shown improvements in matching distorted samples [10]. Bazen and Gerez [11,

12] used a thin-plate spline model to represent non-linear distortion as a non-rigid transformation, which compensates for elastic deformation to improve minutiae matching performance. But this model has to be fitted in rounds of iterations and the accuracy of this model is dependent on the size of the tolerance zone around a minutia. Bolle et al. [13] and Fujii [14] invented hardware-based methods to measure force and torque during fingerprint image capture. These hardware devices are expected to allow contact sensing of fingerprints to be completed with minimal distortion. Specifically, the mechanism designed by Bolle et al. [13] detects and measures excessive force and torque at image acquisition, while the fingerprint distortion detection unit devised by Fujii [14] detects the amount of movement of a finger on a fingerprint sensor through a transparent elastic film or a transparent board, which is mounted on or semi-fixed to the reading face of the fingerprint sensor. These hardware units restrict the application of force to be within a certain range during capturing. The hardware rejects distorted records and prompts the user to provide a new impression until the system requirements are satisfied. There are several drawbacks related to the use of hardware-based distortion detection methods: (a) specific sensors and/or additional instrumentation are required; (b) they cannot handle distorted fingerprint images from previously recorded samples; and (c) the system becomes weak against malicious users who fake their fingertips and ridge patterns.

Ross et al. [15, 16] proposed a rectification method based on learning distortion patterns from the correspondence of ridge curvatures of the same finger in different impressions. The parameters of the TPS transformation can be estimated by computing the average distortion based on the corresponding ridges. Despite enhancing the matching performance in the distorted samples, the performance of the ridge curve correspondence approach significantly relies on the number of impressions of the same finger. In a wide range of databases, there are not enough samples per class to provide such an estimation.

To study the dynamic behavioural of fingerprints, Dorai et al. [17] proposed the use of fingerprint video streams and applied joint temporal and motion analysis to structural distortion detection. Although the proposed approach can reliably detect the non-linear plastic distortion of fingerprint impressions and estimate fingerprint positions based on compressed fingerprint videos, the use of streamed video sequences is inefficient or infeasible in the mobile computing environment, where time and energy consumption is highly restrictive. In addition, researchers have come up with various models for non-linear distortion

in fingerprint images. Unlike the thin-plate spline model [11, 12], Cappelli et al. [18]] investigated distortion patterns in different parts of fingerprint images taken with online acquisition sensors. It was revealed in [18] finger pressure against the sensor surface was non-uniform, decreasing from the finger centre towards the outer area. Accordingly, a non-linear distortion model proposed in [18] was based on finger pressure variations in three distinct regions of a fingerprint: close-contact region (i.e., centre region), outer region and the region in between. Although this model explains the deformation of fingerprint images caused by improper finger positioning, estimating model parameters is difficult and unreliable. Chen et al. [19] developed a fuzzy theory-based algorithm to tackle non-linear distortion. The proposed algorithm can detect spurious minutiae and achieves good recognition accuracy for deformed fingerprints. However, image alignment is a prerequisite for the proposed algorithm, which means that if the pre-alignment is wrong, the proposed algorithm cannot perform well.

2.3 An overview of fingerprint template protection schemes

As discussed in Section 1.2, , the current fingerprint authentication systems are vulnerable to security attacks. An adversary can compromise an unprotected fingerprint template from the database during its transmission in the communication line. Therefore, many researchers have developed various methods and techniques to secure fingerprints and protect their information. Fingerprint template protection (FTP) is classified into fingerprint cryptosystems, cancelable templates, hybrid methods and homomorphic encryption [20]. Figure 2.1 shows the classification of FTP schemes.

Since the contribution of this thesis is based on a FTP cancelable template, an overview of each FTP category is highlighted and a comprehensive survey on cancelable templates by non-invertible transformations is presented.

2.3.1 Fingerprint cryptosystem

A fingerprint cryptosystem refers to binding a key to a biometric feature or generating a key from a biometric feature [21]. The biometric cryptosystems are categorised into key binding and key generation schemes based on how the helper

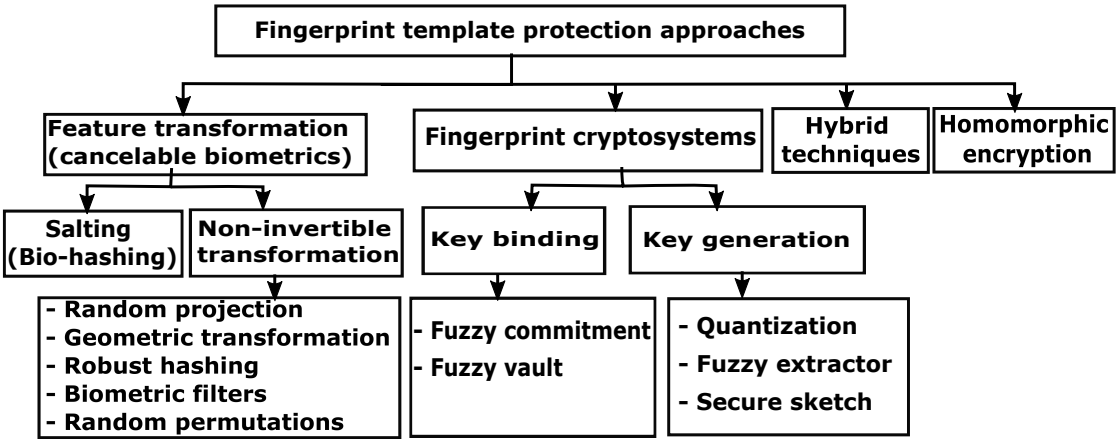

FIGURE 2.1: Classification of template protection schemes (adapted from [20])

data is derived. This helper data is a result of stored public information in reference to fingerprint template.

In a key binding cryptosystem, a fingerprint template is bound with a chosen user-specific key to obtain helper data. The secure template is generated by combining both a key and the fingerprint template bound. Using a suitable decoding method, the keys are obtained from the helper data [22]. Soutar et al. [23] developed the first key binding biometric cryptosystem named *BiometricEncryption*^{TM} for fingerprints. However, the fingerprint encryption used in this approach experienced a mismatch between security and accuracy. In addition, a key binding system does not satisfy revocability and diversity in the protected template [1]. To overcome these limitations, fuzzy commitment and fuzzy vault were developed to induce these two properties in the key binding systems.

A fuzzy commitment scheme was firstly proposed by Juels and Wattenberg [24] where a random codeword from an error correcting code is chosen. Helper data that contains the hashed codeword and the difference between the hashed codeword and the insecure biometric template are generated. In the authentication stage, a comparison between the recovered hashed codeword and the original hashed codeword is performed. Tong et al. [25] presented a system in which no biometric data need to be stored, and the current biometric data is used to decommit a secret value. This method demonstrated a practical use of a fuzzy commitment scheme on FingerCode [26]. Teoh and Kim [27] proposed a randomised dynamic quantization transformation technique to binarize fingerprint features

extracted from a multichannel Gabor filter. A fuzzy commitment scheme is constructed by applying Reed-Solomon codes on the extracted 375-bit feature vectors. The transformation includes a non-invertible projection based on a random matrix derived from a user-specific token. This token requires storage on a secure device. Nandakumar [28] employed a binary fixed-length minutiae representation obtained from quantizing the Fourier phase spectrum of a minutia set in a fuzzy commitment scheme. The alignment of minutiae features is achieved by a focal point of high curvature regions.

Another popular key binding biometric cryptosystem is the fuzzy vault scheme [29]. A fuzzy vault scheme is an order-invariant version of fuzzy commitment. It does not require the input of biometric features to be an ordered or fixed-length vector. The mechanism derives a polynomial from the minutiae set whilst adding random chaff points which do not lie on the polynomial to conceal it. The original polynomial is reconstructed by using error-correcting code indicating the amount of correlation between the query minutiae sets and the enrolled minutiae sets. The number of chaff points added provides a trade-off between the security and the robustness of the biometric cryptosystem. Following Juels and Sudan [29], Uludag et al. [30, 31] applied minutiae line-based representation scheme, where a 128-bit cryptographic key is bonded with fingerprint minutiae data that requires image alignment. Nandakumar et al. [32] proposed a further fingerprint minutiae fuzzy vault scheme, which utilized the high curvature points of the obtained field minutiae orientation as helper data for image alignment. This led to making the alignment more accurate without leaking any orientation information or minutiae position within the template data. Nagar et al. [33] introduced an approach to secure fingerprint template using a fuzzy vault. This approach uses minutiae descriptors containing a record of orientation and ridge frequency data in a minutia's neighbourhood to enable the polynomial evaluations to be locked in a fuzzy vault.

Unlike key binding cryptosystems, key generation cryptosystems directly produce a cryptographic key from a given fingerprint template. Hence, the helper data is derived from the fingerprint template to generate a cryptographic key [34]. Key generation models can be divided into quantization, secure sketch (SS) and fuzzy extractor (FE). Chang et al. [35] and Veilhauer et al. [36] introduced a biometric key generation based on user-specific quantization. Helper data is produced from stored information on quantization boundaries. Dodis et al. [37] proposed two biometric cryptographic key generation models, namely

the secure sketch and fuzzy extractor. The secure sketch is established from three distance metrics, that is Hamming distance, set difference and edit distance. The secure sketch can be treated as helper data that disclose limited information about the template (measured in terms of entropy loss), whereas the fuzzy extractor is a cryptographic primitive that is generated by combining the secure sketch with a randomness extractor. The key generation model has been utilised for encrypting different types of biometrics [35] such as a fingerprint [38, 39], face [40, 41], iris [42–44], voice [45] and palm vein [46], demonstrating that it can be adapted to many cryptographic applications. However, these methods display low discriminability. This means that it is extremely difficult to generate a key with high stability and entropy in the presence of intra-user variations in templates. Moreover, it is highly unlikely that the same key will be generated for different templates of the same user and there are very different keys for various users.

2.3.2 Feature transformation

Feature transformation uses a transformation function, characterized by a user-specific key to transform the fingerprint features to another domain. At the matching phase, the same transformation method is applied on the query fingerprint and is matched to perform in the transformed domain. Feature transformation can be classified into two categories i.e., salting and non-invertible transformation. In salting, unprotected fingerprint templates are transformed using an invertible function, defined by a user-specific key or password. The user-specific key needs to be securely saved or remembered by the user since the transformation is invertible to a large extent. This leads to an increase in the entropy of the fingerprint template and it is more difficult for the adversary to guess the template [34]. There are several advantages of salting techniques, such as low false accept rate and the ability to produce multiple secured templates using multiple user-defined keys. However, the salting mechanism has some significant limitations. For example, it is not robust since the original fingerprint template can be recovered if an adversary gains access to the key and the transformed template. Moreover, the recognition performance can be degraded due to the presence of intra-user variations. An example of the salting method was introduced by Teoh et al. [47]. This method is based on iterating a mix of pseudo-random numbers with fingerprint templates. The work is implemented in the stolen key scenario and was extended in Teoh et al. [48] for face

template and Teoh et al. [49] for speech recognition.

Unlike the salting method, non-invertible transformation secures the fingerprint template by applying a non-invertible transformation function. Non-invertible transformation is defined as a one-way function, f, which is easy to compute but is difficult to invert (given $f(x)$ as the probability of obtaining x in polynomial time is small). A key is used to define the parameters of the transformation function and it has to be available at the time of authentication to transform the query feature set. The main property of this method is that even though the key and/or the transformed template are known, it is computationally infeasible for the attacker to reconstruct the original fingerprint template. Diversity and revocability are another two important properties achieved by using application-specific and user-specific transformation functions, respectively. However, the robustness of this approach still relies on the trade-off between the discriminability and non-invertibility of the transformation function.

2.3.3 Hybrid techniques and homomorphic encryption

Hybrid techniques can be designed by combining two or more techniques to produce a cancelable fingerprint template, e.g., combination of fingerprint cryptosystem and feature transformation methods. Wong et al. [50] proposed a hybrid template protection method, called cancelable secure sketch (CaSS). The basic idea of this method is to combine the multi-line code (MLC) with the code-offset construction of the secure sketch. Feng et al. [51] introduced a three-step hybrid method based on random projection discriminability-preserving (DP) transform and the fuzzy commitment scheme. Nagar et al. [52] developed a hybrid cryptosystem by combining minutiae descriptors for fingerprints and both fuzzy vault and fuzzy commitment is used to build the cryptosystem. Sandhya and Prasad [53] proposed a hybrid method by constructing Delaunay triangles from fingerprint minutiae. Then, a cryptosystem was built using the fuzzy commitment scheme after transforming the acquired features.

On the other hand, homomorphic encryption technologies are an encryption method that allows computations to be held on encrypted data without first decrypting it. In other words, homomorphic encryption can be used to determine the distance between fingerprint vectors in the encrypted form. In the decryption stage, the results of the computations are held on the homomorphic encrypted data and the result is guaranteed to be the same as the result

of performing the same computations on plaintext data [54]. Homomorphic encryption schemes can be divided into two types, namely partially homomorphic encryption and fully homomorphic encryption. Partially homomorphic encryption authorises certain kinds of computations to be performed, while fully homomorphic encryption authorises any arbitrary computations to be performed. Barni et al. [55] developed a homomorphic encryption to filter bank-based fingerprint verification. The authors utilised two partially, additively homomorphic encryption methods. These two encryption methods are used to calculate the Euclidean distances between the encrypted fingerprint vectors. However, this step requires a template quantization to round the values of fingerprint vectors from double to integer digits. This decreases the accuracy of fingerprint recognition using the FingerCode template.

2.4 Cancelable templates using non-invertible feature transformation

Cancelable biometric template generation using non-invertible transformation has been a popular research area for the past two decades. The generation of cancelable fingerprint templates falls under two major categories, registration-based and registration-free methods. The registration-based techniques require the accurate detection of the singular points (core or delta) to align the feature vector before the transformation is performed [56]. Many previous works [56–60] addressed singular point detection and analysis in fingerprint images. However, locating singular points accurately is not a trivial task and it could lead to poor recognition accuracy results.

Unlike registration-based algorithms, registration-free or alignment-free cancelable templates use local features of minutiae structures for transformation. The local structures contain features that characterise the relative information between two or more minutiae, e.g., the distance between two minutiae, as these features are relatively invariant to global rotation and translation of the fingerprint images. Therefore, no prior alignment is required before matching. Moreover, alignment-free algorithms are computationally light and robust against non-linear distortion since there is no need for the pre-registration of the fingerprint image [61]. In the following section, we discuss the types of cancelable templates based on the different types of non-invertible transformations available.

2.4.1 Geometric transformation

Geometric transformation is one of the earliest methods for generating cancelable fingerprint templates. The basic idea of this transformation is to transform the original fingerprint templates by applying signal domain or feature domain transformation. Ratha et al. [62] were the first to introduce the concept of cancelable fingerprint template using three different geometric, non-invertible transformation functions, namely, Cartesian transformation, polar transformation, and functional transformation. The transformation functions are able to distort the fingerprint minutiae features into a new data format. This method is registration-based and hence depends on the accurate detection of the reference points, e.g., singular, core or delta points. In the Cartesian transformation, the minutiae positions are computed in rectangular coordinates with reference to the position of the singular points by aligning the x-axis with its orientation. All cells in the rigid transformation are translated based on the new position sets by the user key. Even if the transformation and the transformed patterns are exposed, it is infeasible to retrieve the original position of the minutiae.

In polar transformation, the minutiae positions are computed in polar coordinates with respect to the core position. The angles are computed with respect to the core orientation. Therefore, polar space is divided into polar regions. The non-invertible transformation is performed utilising a controlled key. This leads to a maintained consistency in the radial distance between the transformed region and the original position of the same region.

The main limitation of both Cartesian and polar transformations is instability, in the sense that a small change in minutiae positions in the original fingerprint can result in a significant change in minutiae positions after transformation. This leads to an increase in intra-user variations at the matching stage and hence reduces matching accuracy.

Yang et al. [63] proposed a non-invertible geometrical transformation to protect the minutiae-based fingerprint template. This is a registration-based method where the original minutiae-based template is mapped to protect the coordinate-based template using a combination of parameter-controlled, linear and nonlinear operations. By taking advantage of both linear and non-linear geometrical transformations, this algorithm can preserve good matching accuracy while providing strong non-invertibility compared to the non-invertible transformation-based cancelable fingerprint template proposed in [62].

Lee et al. [64] introduced an alignment-free cancelable fingerprint template using local minutiae information. In this approach, after processing the fingerprint image and minutiae extraction, translation and rotation, invariant values are extracted based on the orientation of its neighbouring regions and a user-specific random vector. In addition, a cancelable template is generated by moving the extracted minutiae by a distance as per the distance changing function. The direction of movement is measured by adding the original orientation of minutia and the rotational transformation value of the orientation changing function. The authors demonstrated that it is computationally difficult to extract the original data from the transformed template even though the attacker knows both the transformed template and the transformation function. However, the proposed algorithm does not perform well for low quality fingerprint images which is a significant drawback.

In [65], Ahn et al. presented a scheme to generate secure minutiae information for fingerprint templates by applying geometrical properties of local rotation from minutiae triplets to hide minutiae information. Although the idea is promising, the method has insignificant matching accuracy.

In [66], Yang and Butch developed a geometric alignment-free method for fingerprint template protection, which accomplishes self-alignment based on minutia vicinity instead of using the core point for pre-alignment. The algorithm proposed in [66] generates the final protected minutia vicinity by superimposing all self-aligned minutiae groups. Despite the high performance of this method, there is no discussion about how to revoke and replace a compromised template. Yang et al. [67] extended the work presented in [66] by extracting a binary minutia hash bit string encrypted with a randomly generated key.

Yang et al. [68] developed a cancelable fingerprint template based on local structures of Delaunay triangulation in polar-coordinate space followed by a polar transformation approach to achieve non-invertibility. The polar transformation is applied to every triangle in the local structure by altering their positions through transformation matrices. However, the implementation of the method proposed in [68] is limited to fingerprint modality and its applicability is not defined for other modalities. Sandhya et al. [69] developed a non-invertible cancelable fingerprint template using two methods to construct a feature set from the Delaunay triangle.

2.4.2 Filter-based methods

A cancelable biometric filter is a convolution-based technique where multiple transformed templates are generated using a random convolution method. Bloom filtering is a simple space-efficient data structure for supporting membership query sets. Bloom filter-based transformation has been successfully used to generate irreversible cancelable fingerprint templates. Two approaches to protecting fingerprint data were proposed in [70, 71]. These methods transform fingerprint feature vectors to an irreversible representation, i.e., Bloom filters. In [70], Li et al. applied Bloom filters to variable length binary fingerprint templates based on minutiae vicinities. The experiment results of this method showed no degradation if fingerprints are of good quality. Abe et al. [71] proposed a method to generate cancelable fingerprint templates by combining Minutiae Relation Code (MRC), which can represent the minutiae information efficiently and Bloom filters. The experiment results show that this method can maintain fingerprint performance as well as quickly compare the compact protected templates.

Correlation invariant random filtering (CIRF) is another instance of a cancelable biometric filter. CIRF is an elemental technique of cancelable biometrics with provable security for correlation-based matching. Hirata et al. [72] introduced a method of cancelable biometrics for correlation-based matching. The authors used numeric theoretic transform to enable the transform to be masked using random filters. Following from [72], Takahashi et al. [73] proposed registration-based cancelable templates based on CIRF and the chip algorithm for authentication. This method can extract two versions of cancelable templates i.e., a basic version and a minutia hiding version. However, both versions provide foolproof security in terms of the irreversibility of the cancelable templates.

Tran et al. [74] proposed a dynamic multifilter-based fingerprint matching scheme to enhance the accuracy of cancelable fingerprint templates. The multi-filtering framework consists of two layers of cancelable template design. The first layer is the KNN minutia descriptor that is equipped with multivariate polynomial transformation. This transformation depends on the power of the multivariate polynomial equation system. The second layer is the enhanced version of MCC which is protected by irreversible order-based encoding transformation. The authors proposed a multi-layer fingerprint matching technique where the decision-making process no longer relies wholly on a singular threshold. Despite the good matching performance and promising anti-attacking properties

of this approach, the performance on two low-quality datasets (FVC2004 DB1 and DB3) was not analysed.

2.4.3 Random projection

Another non-invertible transformation method that is widely used for generating cancelable fingerprint templates is random projection. The key concept of this technique is to project the extracted fingerprint features onto a random space. The dimension of the fingerprint template is reduced in Euclidean space. Given that feature vector $x \in \mathbb{R}^n$ extracted from a fingerprint image and projected onto a random subspace $\mathbf{A} = [\mathbf{a}_{ij}]$ where $\mathbf{A} \in \mathbb{R}^{n*N}$ with $n < N$. Each entry of $\mathbf{a}_{ij}$ of $\mathbf{A}$ is an independent realization of a random variable. This process is stated in (2.1).

$$\mathbf{y} = \mathbf{A}\mathbf{x} \tag{2.1}$$

where $\mathbf{y}$ is the resultant n dimensional vector.

BioHashing is one of the well-known random projection schemes, introduced by Teoh et al. [75] and has been applied to many biometric characteristics. In this approach, the iterated inner product is determined between a tokenised pseudo-random number and a user-specific fingerprint feature. The fingerprint feature vector is generated from the integrated wavelet and Fourier-Mellin transform. Then, a random user-specific token is used to create orthogonal vectors. The cancelable template is extracted by finding the inner dot product of the feature vector and the orthogonal pseudo-random vector. Teoh et al. [48] further improved the original BioHashing method using random multi-space quantization (RMQ) which extends the single ransom subspace formulation to multiple subspaces. The proposed methods in [48, 75] have significant advantages such as zero equal error rate point and clean separation of the genuine and imposter populations. This eliminates the false accept rate without suffering from an increased occurrence of the false reject rate.

In [76, 77], Jin et al. proposed a cancelable fingerprint template based on two-dimensional random projections using a minutia local structure named minutia vicinity decomposition (MVD).

Yang et al. [78] developed a method for generating cancelable templates using both the local and global features of a fingerprint. The first step in the implementation of this method was drawing a circle of a certain radius where the core point acts as the centre of the circle. A pair of minutiae points in the circle

are connected with a line and both points are mapped to the circle in the perpendicular direction. For local feature extraction, triangular properties which consist of the angle between two minutiae and the angle between two lines connecting two minutiae pairs, are computed. The local features are robust to the non-linear and geometric distortions that may occur during fingerprint acquisition. The method is irreversible since multiple minutiae pairs are mapped at the same points in the circle.

Although random projection provides a good diversification effect for biometric template protection, there are security concerns under lost-key attacks. As noted in [79], a two-factor cancelable formulation is constructed using multi-space random projections. In addition, a security threat is raised since random projection is a linear operation that preserves the distance very well. Yang et al. [80] introduced a dynamic random projection mechanism to overcome the security concerns due to a stolen key or token by adding an additional computational complexity to the search of the unprotected biometric features. In this method, a non-linear projection process is performed by relating the random matrix's assembly to the biometric feature itself. The dynamic random matrices are achieved by making several random vector slots publicly available, with each slot containing multidimensional random real-valued vectors. For each slot, one of the random vectors is selected for projecting the biometric features. Therefore, the attacker has no knowledge which random vector out of many in a slot is selected for projection.

Ahmad et al. [81] proposed an alignment-free cancelable template using pair-polar minutiae vectors in a polar space. This method utilises the relative relationship of minutiae in a rotation and shift-free pair-polar coordinate system. In addition, a many-to-one mapping-based non-invertible transformation is designed. But the reported recognition accuracy is particularly low over low-quality fingerprint images, which is undesirable for practical fingerprint authentication applications.

Yang et al. [82] proposed a feature-adaptive random projection-based approach to generate cancelable fingerprint templates. In this method, the projection matrices are generated from one basic matrix together with local feature slots and discarded after use, thus making it difficult for adversaries to gather enough information to launch attacks.

Alam et al. [83] introduced an alignment-free cancelable template scheme to secure fingerprint minutiae. The proposed method enhanced the non-invertibility by using bit-toggling strategy to inject noise into the proposed fingerprint template. Furthermore, cancelability is also achieved by incorporating discrete Fourier transform and random projection on the proposed template.

2.4.4 Robust hashing

Robust hashing is another method to generate non-invertible transformation using hash functions. A robust hash function is a one-way transformation tailored specifically for each user based on their biometrics. A secured biometric authentication system based on a robust hash function was introduced by Sutcu et al. [84]. In this method, the hash function is designed as a combination of various Gaussian functions with a secure cryptographic hash function which is utilised to satisfy both non-invertibility and security requirements.

In [85], Tulyakov et al. developed symmetric hash functions to secure fingerprint templates. The symmetric hash functions are invariant to the order of the input pattern. The algorithm does not rely on the singular points (core and delta) and does not need pre-alignment between the query and reference fingerprint templates. During the matching, all localized sets corresponding to the query pattern are compared with all the localized sets in the reference pattern. The matching score is determined by selecting the matches with the highest confidence. Although the developed fingerprint hash functions are cancelable and demonstrate reasonable performance, the weights incorporated in the error function are empirically set. This leads to difficulties implementing the method in real applications. The work proposed in [85] was extended in [86] to enhance the security of the system against brute force attacks and retain a reasonable performance.

Das et al. [87] proposed an alignment-free fingerprint hashing technique based on minimum distance graphs (MDG). The MDG hash function is composed of a set of connected nodes formed by calculating the distance between the core and the next nearest minutia. Then, the distance between the next closest minutia and its predecessor is calculated and so on. The MDG is further extended to a cancelable template by applying the minutia perturbation model proposed in [64]. Despite its good security strength against brute force attack, the method depends on the accurate detection of the core point.

Jin et al. [88, 89] proposed cancelable templates based on locality sensitive hashing, named Index of Max (IoM) hashing. In this paper, random parameters are externally generated, and IoM hashing transforms a real-valued biometric feature vector into a discrete index (max ranked) hashed code. Two types of the IoM hashing for fingerprint biometrics are presented, namely Gaussian random projection-based (GRP-IoM) and uniformly random permutation-based (URP-IoM) hashing methods. This method achieves good accuracy performance with respect to its before-transformed counterparts. However, Ghammam et al. [90] argued that both GRP-IoM and URP-IoM methods are extremely vulnerable against authentication and linkability attacks.

Moreover, , a new cancelable biometric scheme [91], named sparse combined Index-of Maximum (SC-IoM), was designed on top of the IoM hashing method. Unlike IoM hashing, SC-IoM hashing extracts the indices of the largest and the second largest user-specific randomly projected biometric features.

Sadhya et al. [92] introduced a cancelable fingerprint template by randomly sampling bits from binary features. The binary features are extracted from binarizing MCC features using the KPCA and zero-thresholding schemes. The method achieved a low equal error rate (EER) in the stolen-key scenario. However, this method is not practical for use in real-world applications because the minutiae points were extracted by a manual tool [93].

Abdullahi et al. [94] designed a robust and a secure fingerprint hash using Fourier-Mellin transform and fractal coding. The proposed method employs the Fourier Mellon transform for feature alignment and generates a fixed-length minutiae representation. After this, fractal coding is utilised to exploit texture compression and dimensionality reduction to generate a compact and robust hash to enhance recognition and security. The proposed method satisfies the revocability and unlinkability criteria with fulfilling the recognition performance. In [95], Abdullahi and Sun introduced a non-invertible fingerprint hash code using vector permutation and a shift-order process. The dimension of feature vectors is reduced using KPCA prior to randomly permuting the extracted vector features. A shift-order process is then applied to enhance the security mechanism against non-invertibilty and similarity-based attacks.

Li et al. [96] designed cancelable fingerprint templates based on Indexing-Min-Max (IMM) hashing. The proposed method securely embeds the explicit fixed-length fingerprint feature vector non-linearly into implicit ordering space. Unlike the original IoM method, the IMM hashing model collects implicit indices of the maximum and the minimum values computed from multiple random tokenized partial Hadamard transforms to simultaneously ensure high-level security and satisfactory recognition performance.

Li and Wang [97] proposed a one-factor cancelable fingerprint authentication scheme based on Minimum Hash Signature (NMHS) and Secure Extended Feature Vector (SEFV). The NMHS algorithm was developed to produce the hash codes of the binary fingerprint templates and the XOR operation in the hashing process was utilised to enhance the stability of the performance. To get the encryption string in the form of a fuzzy vault, the XOR operation is carried out between the hash codes and the random binary string. The SEFV is then used to get the pseudo identifier. In the authentication stage, the pseudo identifier is produced with genuine queries using the auxiliary data provided by the system. This is then employed to classify the utilising hamming distance. The authors introduced a fusion rule to improve the performance during the authentication stage. The proposed system shows a good matching performance.

Li et al. [98] presented a cancelable fingerprint binary code generation scheme based on one permutation hashing. The transformed feature is bitwise uniformly distributed and offers fast matching. The proposed method also applies the partial Haar transform to strengthen the security of the cancelable fingerprint template.

Lee et al. [99] proposed a one-factor cancelable fingerprint template, called extended feature vector (EFV) hashing. The EFV hashing utilizes a permutation key separate from the fingerprint feature data to yield the cancelable template. With XOR encryption, the key is not stored in its original form.

2.4.5 Random permutations

Random permutation is another common method used to generate cancelable biometric templates. The key concept of this method is the shuffling of feature vector values using a permuted key followed by non-invertible transformation. Farooq et al. [100] presented a permutation-based method to produce cancelable fingerprint templates. The concept of the proposed method is to generate

cancelable bit strings from fingerprints by extracting translation and rotation invariant minutia triplets. This means that fingerprints can be represented by a set of triangles derived from sets of three minutiae. The set of triangles can be represented in a binary space by keeping only the triangles that occur once. The construction of anonymous fingerprint representation comprises two stages. The first stage is the selection of invariant fingerprint features that are utilised to compute binary strings from fingerprint images. The second stage is performing the non- invertible key-based transform on these binary strings by issuing a key to each user. This can be revoked and replaced resulting in a different binary string.

Similar to the method in [100], Lee and Kim [101] proposed a cancelable fingerprint template using minutiae-based bit strings. In this method, the protected template is generated by mapping the minutiae into a predefined three-dimensional array, which contain small cells and discovers which cells include minutiae. One of the minutiae is chosen as a reference minutia point and other minutiae are translated and rotated to map the minutiae into cells based on the position and orientation of the reference minutia. Next, each cell consisting of more than one minutia is set to 1 (otherwise 0). Hence, a one-dimensional bit string is generated by sequentially visiting the cells in 3D array. Finally, the bit-string is permuted using a specific PIN or the permutation matrices to achieve revocability. This method performs well in different PIN situations. However, the performance degrades when the PIN key is compromised.

Jin et al. [102, 103] introduced another bit-string based template generation method using minutiae pairs to obtain invariant features. The invariant features attached to a pair are the Euclidean 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, quantization, histogram binning and binarization operations are applied to generate a bit-string. Finally, by incorporating the helper data that is generated from the resultant bit strings, a user's key-based permutation procedure is used to generate a revocable and non-invertible binary bit-string as a template. Although the revocability in this method is achievable, a security threat may occur when the helper data and external token are known by the attacker. Therefore, the attacker may access the system by using the bit-string recovered from the helper

data and external token. In [104], Jin et al. used polar grid-based 3-tuple quantization to build binary string cancelable templates. Despite its efficiency in storage and matching, the derived binary templates exhibit suboptimal matching performance.

Wong et al. [105] proposed a feature extraction approach called Multi-Line Code (MLC), which involves the inspection of minutiae distributions along a straight line constructed based on each reference minutia. Then, a cancelable template is generated according to a user-specific key that produces the permutation order of MLC. To improve the performance of MLC, Wong et al. [106] proposed an enhancement method using different measures on minutiae contribution and learning-based binarization. Unfortunately, this latter method requires large storage capacity.

In the process of developing a cancelable template, performance preservation is a significant challenge which is addressed in [107]. Kho et al. developed a minutia descriptor based on partial local structures and formulated a non- invertible transformation using randomized non-negative least square optimization. This method achieves good performance as well as strong security. However, matching between two cancelable templates is a complex and computationally expensive process.

2.4.6 Other non-invertible transformation functions

Wang et al. [108–112] proposed various works on designing non-invertible transformation functions from the perspective of digital signal processing. In 2012, Wang and Hu [108] designed an alignment-free cancelable template with pair-minutiae vectors by extracting invariant features from a pair of minutiae. These feature vectors are subsequently converted into fixed-length binary vectors through quantization and bin-indexing. The binary vectors are then converted to complex vectors via the Discrete Fourier Transform (DFT). Lastly, a many-to-one mapping is implemented to achieve non-invertibility. This method achieved EER of 3.5%, 5%, 7.5% for FVC2002 DB1-3, respectively. In 2014, they used the curtailed circular convolution as a non-invertible transform to build alignment-free cancelable templates [109]. The method is based on extracting features and bin-indexing them to generate binary representation. Next, the features were converted to a frequency domain with DFT, and part of the resultants are removed to get the cancelable templates. This method managed to bring down

the EER of the good quality FVC2002 DB1 and FVC2002 DB2 to 2% and 3% and when dealing with lower quality images from FVC2002 DB3, it is still reached 6.12%.

By countering the identifiability condition of blind system identification (BSI), Song and Hu [110] applied the BSI approach to the design of alignment-free cancelable templates. In this method, the same approach proposed in [109] is used to extract features, generate a binary string, and convert the output to a frequency domain using DFT. Then, a cancelable template is generated using the Finite Impulse Response (FIR) vector of the moving average model. The transformation method in [110] is non-invertible when the length of the FIR vector is within a specified range.

Wang et al. [111, 112] proposed a partial Hadamard transform-based non-invertible transformation to generate cancelable fingerprint templates. The binary fingerprint feature vector is extracted by the pair-minutiae vectors used in [108] to a dense complex vector by means of Fourier transform. A cancelable fingerprint template is generated by adopting non-invertible mapping with partial Hadamard matrix. The Hadamard matrix has an interesting property, this being, it is always column rank deficient. Hence, the original template can be protected by hiding the true solution among many other solutions. Despite the clever design of various non-invertible transformations, the extracted features in these methods are not discriminative enough to render a strong matching performance, especially on databases with low quality fingerprint images, e.g., FVC2004 DB2.

Taking advantage of the Minutia Cylinder-Code (MCC) performance, various non-invertible transformations have been proposed to protect the templates. MCC is a well-known local minutia descriptor, which is based on a 3D-local structure associated with each minutia, as shown in Figure 2.2. Ferrara et al. [113] proposed a template protection method, named P-MCC. This method performs a KL transformation on the MCC feature representation. However, this method is not revocable. To make P-MCC templates revocable, the authors [114] combined a user-specific secret key and the non-invertible P-MCC representation to put forward a two-factor protection scheme, called 2P-MCC. While 2P-MCC templates are cancelable, the matching performance on FVC2002 databases is less satisfactory. Zhang et al. [115] designed a cancelable template using a combo plate and functional transformation built upon MCC. Arjona et al.

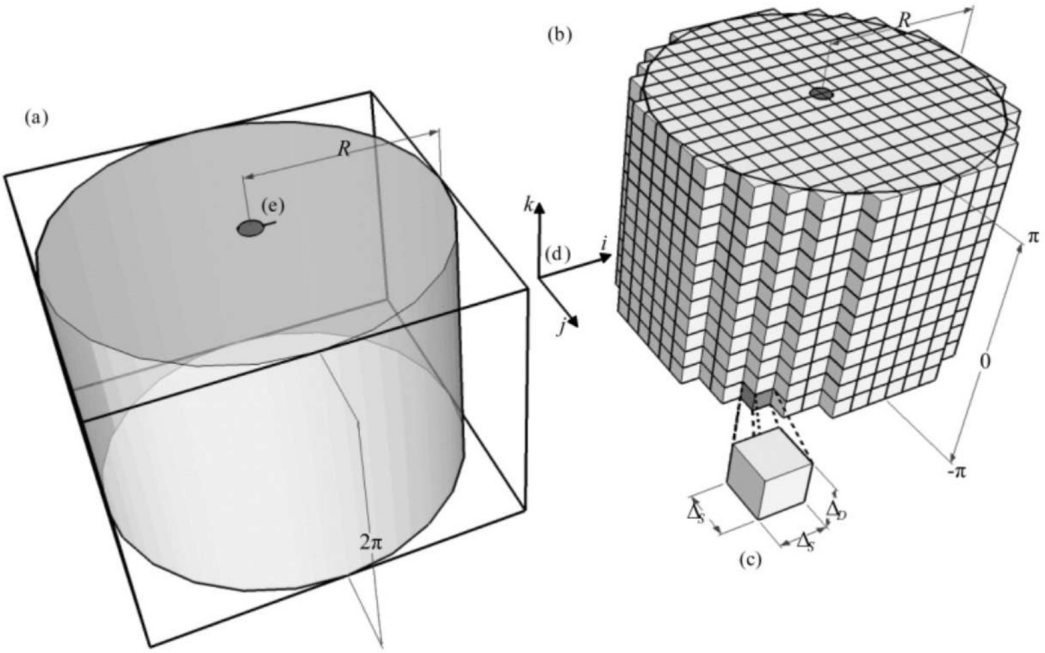

FIGURE 2.2: (a) The cylinder with the enclosing cuboid (b) Discretization of the cuboid into cells [117]

[116] proposed Physically Unclonable Functions (PUFs) to apply on P-MCC and named it P-MCC-PUFs.

Sandhya et al. [118] introduced a K-nearest neighbourhood structure (K-NNS) by means of relative spatial and directional information between each reference minutia and its k-nearest neighbours. The K-NNS structure is quantized and mapped into a 2D array to produce a fixed-length binary vector. Next, a complex vector is generated by applying DFT. Then, the complex vector is transformed by adopting a user-specific random matrix generated from a user's key. However, the performance of the proposed method in [118] is not sufficient to show the feasibility of using it in real fingerprint applications. Nhat et al. [119] proposed an alignment-free cancelable template using the KNN clustering method in conjunction with partial discrete Fourier transform.

Wang et al. [120] designed alignment-free cancelable templates by zoning minutia pairs for the construction of local invariant structures. In this method, all the minutiae in the fingerprint image are allocated into multiple circular zones with radius r while considering each and every minutia as the centre of the zone. Next, minutiae pairs were formed by considering the centre minutia and all

other minutiae of each zone. The features collected were expressed through distance, orientation, and difference between angles to make recognition resilient towards rotational and transnational invariances. After this, these collected features were quantized by selecting a certain step size. The quantized value obtained for zoned minutia pairs were mapped to various locations of cubicles with 1 and 0. All the values of 0's and 1's stored in cubicles were concatenated to form a binary string. To reduce the risk of ARM attack, modulo operation was applied to the index of the generated binary string which produces a new shortened binary string. Next, they applied partial DFT generated using a parameter key to the new shortened binary string. The variable utilised for modulo-operation and the parameter key were both user-specific.

Trivedi et al. [121] introduced a non-invertible cancelable fingerprint template based on the information extracted from the Delaunay triangulation of minutia points. A user key of a random binary template is utilized to generate a cancelable template.

Shahzad et al. [122] designed alignment-free cancelable templates with dual protection, which is composed of the window-shift-XOR model, and the partial discrete wavelet transform. Due to the dual protection, the security of the proposed cancelable template is enhanced.

A comparison of the most recent cancelable fingerprint template protection approaches is reported in Table 2.1.

TABLE 2.1: The comparison of cancelable biometrics for fingerprint template protection.

Cancelable fingerprint template design	**Feature transformation**	**Databases**	**Best Performance**
Wang and Hu [108]	Infinite-to-one mapping	FVC2002 DB1 FVC2002 DB2 FVC2002 DB3	EER=3.50% EER=4.00% EER=7.50%
Wang et al. [109]	Curtailed circular convolution	FVC2002 DB1 FVC2002 DB2 FVC2002 DB3	EER=2.00% EER=2.50% EER=6.12%

Wang et al. [110]	Blind system identification	FVC2002 DB1 FVC2002 DB2 FVC2002 DB3	EER=3.00% EER=2.00% EER=7.00%
Wang el at. [112]	Partial Hadamard transform	FVC2002 DB1 FVC2002 DB2 FVC2002 DB3	EER=1.00% EER=2.00% EER=5.20%
Wang et al. [120]	Zoned minutia pairs	FVC2002 DB1 FVC2002 DB2 FVC2002 DB3	EER=0.19% EER=1.00% EER=4.29%
Ferrara et al. [114]	2P-MCC	FVC2002 DB1 FVC2002 DB2 FVC2002 DB3 FVC2002 DB4 FVC2004 DB1 FVC2006 DB2	EER=2.00% EER=1.20% EER=4.40% EER=3.10% EER=3.00% EER=0.10%
Jin et al. [89]	IoM hashing	FVC2002 DB1 FVC2002 DB2 FVC2002 DB3 FVC2004 DB1 FVC2004 DB2 FVC2004 DB3	EER=0.22% EER=0.47% EER=3.07% EER=4.74% EER=4.10% EER=3.99%
Kim et al. [91]	SC-IoM hashing	FVC2002 DB1 FVC2002 DB2 FVC2004 DB1 FVC2004 DB2	EER=0.55% EER=0.93% EER=5.81% EER=6.85%
Abdullahi et al. [94]	Fourier-Mellin transform and fractal coding	FVC2002 DB1 FVC2002 DB2 FVC2002 DB3 FVC2004 DB1 FVC2004 DB2 FVC2004 DB3	EER=0.36% EER=0.54% EER=2.40% EER=2.35% EER=5.93% EER=2.37%
Shahzad et al [122]	Window-shift-XOR and partial discrete wavelet transform	FVC2002 DB1 FVC2002 DB2 FVC2002 DB3 FVC2004 DB1 FVC2004 DB2	EER=1.57% EER=1.50% EER=7.93% EER=10.49% EER=8.62%

2.5 Security on the Internet of Things

2.5.1 Overview of Internet of Things

In our modern world, the Internet of Things (IoT) provides a new paradigm that works on connecting objects, intelligent systems, and applications to collect data from physical world and offer IoT services to IoT consumers [123]. The IoT considers as a distinguished solution that allows anyone to access anything from anywhere and at any time. This means that several physical objects can be allowed to collect data through sensing and actuation capabilities, and process and exchange the data over the network transparently and seamlessly [124]. With the remarkable increase in the number of IoT devices, these interconnected smart devices can be used in different fields and their applications include but are not limited to smart homes, smart cities, environment, agriculture, the smart grid, industry, healthcare, and transport. According to [125], there are about 50 billion IoT devices connected at the present and it will probably increase to 75.44 billion devices by 2025.

Despite the attractive promises of the developing IoT networks, there are no sophisticated security policies on IoT devices. The large number of interconnected IoT devices encourages a rapid increase in attacks from imposters. In fact, consumers' inadequate awareness of IoT devices on the topic of IoT security results in them being a source of potential risks. The US Intelligence Community classifies the IoT as a significant cyber technology that can compromise data privacy, integrity, and service availability. An imposter can gain access to certain internal and open environments by accessing and probing into IoT devices. For instance, in healthcare applications, life-threatening cyberattacks can target medical devices (such as insulin pumps attacks, baby monitors). This can cause serious security issues for healthcare IoT applications [126].

Given the aforementioned security risks of IoT devices, it is important to have proper access control to protect user privacy and prevent on-device data leakages. Although passwords are commonly used for user authentication in IoT devices, the rapid development of biometric technology in the past decade has swiftly spread to almost every corner of our daily lives as a more reliable method of authentication. The combination of smartphones and biometrics in consumer

markets resulted in biometric authentication becoming more widely accepted. The use of biometric recognition has expanded rapidly since Apple started using biometric recognition with its smartphones, named Touch ID and face recognition [127].

2.5.2 Biometrics authentication on IoT devices

As discussed previously, authentication is the fundamental security protocol in the IoT environment. Therefore, in this section, we examine the existing biometric-based authentication solutions in IoT presented in the literature. Wilkins [128] reviewed how biometrics can be utilized to better secure manufacturing protocols and processes. The author discussed the options of choosing correct technologies to improve safety and security in factories. Since hackers continue to find new ways to gain information, the author stated that it is necessary to make systems adaptable, as security is a moving objective.

Habib et al. [129] developed a novel authentication framework based on biometric modalities and wireless device radio fingerprinting for IoT in healthcare. The proposed method can verify the monitored health data from the correct patient, whilst also ensuring the integrity of the data. Kantarci et al. [130] proposed a cloud-centric biometric identification architecture. This approach protects mobile applications from unauthorised access by combining the biometric and context-aware technique. Maček et al. [131] introduced a multimodal method for authentication. In this approach, high-quality cameras (e.g., laptops, smartphones and tablets) are used to build face and iris templates. However, the authors indicated that there is a privacy concern surrounding the stored face and iris templates.

Shahim et al. [132] developed an authentication system with users' hand geometry scans and a series of gestures on a Raspberry Pi platform. Dhillon and Kalra [133] presented a lightweight multi-factor remote user authentication method based on a computationally less expensive hash function and XOR operations. Yang et al. [134] developed a privacy-preserving lightweight fingerprint authentication system for resource-limited IoT devices. The proposed method uses a block logic-based algorithm to minimise the template size and achieve good performance.

Yang et al. [135] applied the binary decision diagram (BDD) to the design of a deep learning-based finger-vein system for template protection. The original

finger-vein template is transformed irreversibly by the BDD and further processed by a multilayer extreme learning machine. When compared with the existing non-machine learning and machine learning-based finger-vein recognition methods, the proposed finger-vein cancelable template achieves competitive performance.

Zheng et al. [136] proposed a Fingerprint based Insulin Pump security (FIPsec) scheme which employs a fingerprint authentication scheme to verify any access request to the pump. A cancelable Delaunay triangle-based fingerprint matching algorithm for the insulin pump is presented, which has capabilities to resist nonlinear fingerprint image distortion and the influence of missing or spurious minutiae.

Ayub et al. [137] introduced a lightweight secure three-factor biometric-based authentication protocol for e-Healthcare applications in the IoT using 5G technology. The proposed protocol is cost-effective in terms of computational and communication costs compared to many existing e-Health cloud authentication protocols. Security analyses show that the protocol can resist attacks such as user anonymity, offline password guessing, impersonation and stolen smartcard attacks, but is vulnerable to man-in-the-middle and replay attacks [138].

Yin et al. [139] introduced an IoT-oriented lightweight, privacy-preserving fingerprint authentication system. The proposed approach is built upon the MCC-based cancelable binary template where a random projection and Boolean operation XOR is used to transform the MCC binary feature vectors. A prototype of the proposed system is developed using a popular open-source platform (i.e., Open Virtual Platforms™) in the IoT setting.

2.6 Chapter summary

This chapter presents a comprehensive survey of research work on fingerprint authentication systems in terms of modelling minutiae variations and their effects on fingerprint matching. Then, the recent work in the field of fingerprint template protection (FTP) schemes is presented. FTP is classified into four categories i.e., fingerprint cryptosystems, feature transformation, hybrid methods and homomorphic encryption. Three categories were summarised in Section 2.3 and an exposition on the feature transformation category is presented in Section 2.4. Feature transformation or cancelable templates have been classified

based on the transformation methods. The most commonly used transformation methods are geometric, robust hashing, random projection, biometric filters, random permutation, and non-invertible transformation functions. A comprehensive survey on the security of IoT is presented in Section 2.5. An overview of IoT is given first and the recent work on using biometric fingerprint authentication systems with IoT is presented in Section 2.5.2.

Chapter 3

A Möbius Transformation-Based Model for Fingerprint Minutiae Variations

3.1 Introduction

With good recognition accuracy and strong security, fingerprint-based biometric recognition [1] is becoming an appealing alternative to traditional passwords and token-based authentication. During fingerprint acquisition, a fingerprint sensor or scanner acquires fingerprint images through some means of contact sensing. The quality of the acquired images can be affected by a number of physiological, behavioural and environment factors. As a result, fingerprint images contain a fair amount of uncertainty and variability, giving rise to intra-class variations and inter-class similarity [1]. How to extract more useful information from noisy (or even poor-quality) fingerprint images has attracted intense research interest in the areas of image processing and pattern recognition for many years.

In a fingerprint image, apart from the global fingerprint pattern, such as ridge line flow, at the local level, minutiae points provide salient information about an individual's fingerprint features [1] and play an important role in the design of fingerprint recognition systems. In particular, in recent years researchers have successfully applied minutia-based local structures [140] to the popular research topic of fingerprint template protection (see Chapter 2). These minutia-based local structures have some desirable properties; they are stable and alignment-free. However, in the fingerprint acquisition process, when a person presses his/her fingertip against the plain surface of a fingerprint scanner, the resultant

fingerprint image is produced through a three-dimension(3D)-to-two-dimension(2D) mapping. In this process, minutiae variations occur between different scans, because minutiae points are affected by linear transformations like translation and rotation. Moreover, due to skin elasticity compression or stretch, minutiae are subject to elastic deformation [11] or non-linear plastic distortion. The ideal way to cope with minutiae variations is to invert the 3D-to-2D mapping and compare minutiae in 3D, but how to invert this mapping has not yet been ascertained.

Despite the aforementioned software and hardware-based approaches to detecting deformations in fingerprint images (refer to Section 2.2), currently there is no existing method available for capturing minutiae variations in a unified model. None of the existing models can deal with rigid transformations (e.g., minutiae translation and rotation) and non-rigid transformations (e.g., non-linear distortion) in a comprehensive manner so that they can be described in a single model. In this chapter, we address this issue by proposing a unified model which is able to represent minutiae variations between fingerprint scans and formulate the changes to minutiae feature patterns. By observing the similarity between the process of pressing one's fingertip bulging outwards on a fingerprint scanner and taking objects on a curved surface and mapping them to a plane, we derive a simple model, namely inversion, for non-linear distortion using the Riemann sphere [141]. In addition, we use complex functions to express minutiae translation, rotation and inversion. Furthermore, we identify the Möbius transformation [142] as a candidate for modelling minutiae translation, rotation and non-linear distortion, that is, different types of minutiae variations are described in one, unified model. Not only do we mathematically prove that the Möbius transformation-based model is a unified model for capturing minutiae variations, we also experimentally verify the effectiveness of this model using the public database FVC2002 DB2 [5].

This chapter is organized as follows. Section 3.2 presents the complex functions to describe minutiae translation, rotation and inversion and it also describes the inversion model for non-linear distortion. Section 3.3 proposes the Möbius transformation-based model and demonstrates why it can be used to model minutiae variations. Section 3.4 evaluates the efficacy of the Möbius transformation-based model through experiments conducted over the public database FVC2002 DB2 [5]. The chapter summary is given in Section 3.5.

3.2 Minutiae translation, rotation and non-linear distortion

Minutiae variations that occur to different fingerprint scans include translation, rotation and non-linear distortion. Translations and rotations are due to changing finger orientation and position shift at fingerprint capturing time, while non-linear distortion is introduced by variable skin pressure. In this section, we propose inversion as a simple model for non-linear distortion.

Minutiae translation, rotation and inversion can be described by complex-valued functions. In order to use these functions, a minutia's position is represented by a complex number z, which means that the co-ordinates (x, y) of the minutia are given by $x = \mathrm{Re}(z)$ and $y = \mathrm{Im}(z)$, where $\mathrm{Re}(z)$ is the real part of z and $\mathrm{Im}(z)$ is the imaginary part of z. We now introduce the complex functions that express these mappings.

Proposition 1 *A translation in the complex plane is represented by a function of the form*

$$f(z) = z + \gamma \tag{3.1}$$

where $\gamma \in \mathbb{C}$.

Proof: Observe that $\mathrm{Re}(\gamma)$ displaces z along the real axis and $\mathrm{Im}(\gamma)$ displaces along the imaginary axis, giving the desired results. **Proposition 2** Rotation is described by

Proposition 2 *Rotation is described by*

$$f(z) = \alpha z \tag{3.2}$$

where $\alpha \in \mathbb{C}$.

Proof: It is straightforward to prove the result when we express z and α in polar form.

Non-linear distortion is inevitable during fingerprint capture. However, we note that pressing a fingerprint on a scanner is similar to mapping points of a curved surface, e.g., a sphere, to a plane. Motivated by this observation, we propose a model for non-linear distortion based on projecting points in the x-y plane to the surface of the Riemann sphere [141]. Consider the surface of the Riemann

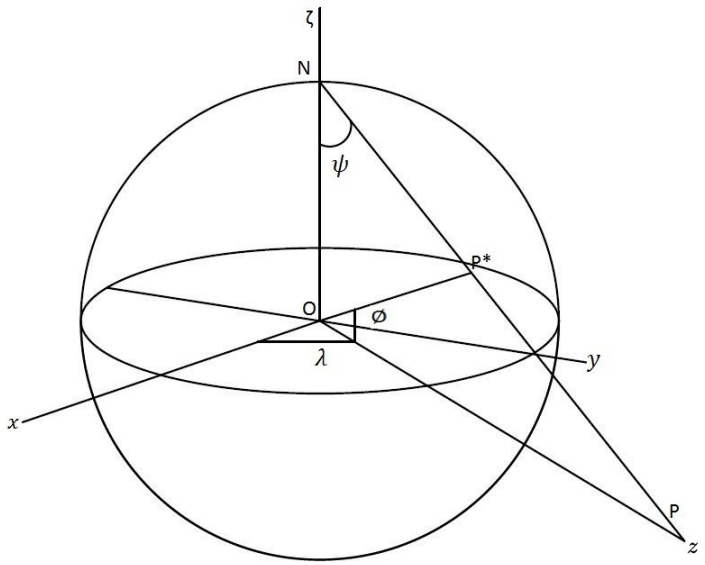

FIGURE 3.1: *Projection of point P (i.e., $z = x + iy$) to the Riemann sphere.*

sphere Σ of unit radius, centred at the origin in $\mathbb{R}^3$. Let Π be the x-y plane and N denote the point $(0, 0, 1)$. The complex number $z = x + iy$ can be represented by the point $P = (x, y)$ in Π. P can be mapped uniquely to the point P^* by taking the intersection of the line segment NP with Σ, or its extension for P inside Σ. The point P^* can be represented by overlaying a spherical co-ordinate system, where $\lambda \in (-\pi, \pi]$ and $\phi \in (-\pi/2, \pi/2)$. This arrangement is shown in Figure 3.1.

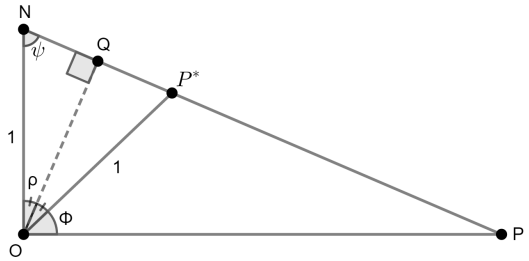

FIGURE 3.2: *Triangle NOP*

Figure 3.2 shows the triangle NOP, where O is the origin. Let $\psi = \angle ONP$ and Q be the point that bisects the line segment NP^*. As NOP^* is an isosceles triangle by construction, the line segment QO bisects $\angle P^*ON$. Let $\rho = \angle NOQ = (\angle P^*ON)/2$. As NOP is a right-angled triangle, we have $\rho = \pi/4 - \phi/2$. We

now derive ψ in terms of ϕ as follows:

$$\begin{aligned}\psi &= \frac{\pi}{2} - \rho \\ &= \frac{\pi}{4} + \frac{\phi}{2}\end{aligned}$$

We can now express the point P, represented by $z = x + iy$, with respect to our spherical co-ordinates λ and ϕ. Observe $\arg z = \lambda$ and $|z| = \tan\psi$. Therefore,

$$z = \tan(\frac{\pi}{4} + \frac{\phi}{2})e^{i\lambda} \tag{3.3}$$

Proposition 3 *Let g denote the function that rotates the sphere Σ by angle π about the x-axis. Let h map the points in the $x-y$ plane Π to the sphere Σ, as discussed above. Inversion is described by $f(z) = h^{-1} \circ g \circ\ h(z)$, where the symbol $\circ$ denotes function composition, and*

$$f(z) = 1/z \tag{3.4}$$

Proof: Observe that the rotation about the real axis corresponds to the rotation about the x-axis in Figure 3.1. After the rotation of the sphere, $\phi \to -\phi$ and $\lambda \to -\lambda$. Using (3.3), we have

$$\begin{aligned}f(z) &= \tan(\frac{\pi}{4} - \frac{\phi}{2})\, e^{-i\lambda} \\ &= \frac{\sin(\frac{\pi}{4} - \frac{\phi}{2})}{\cos(\frac{\pi}{4} - \frac{\phi}{2})}\, e^{-i\lambda} \\ &= \frac{\sin\frac{\pi}{4}\cos\frac{\phi}{2} - \cos\frac{\pi}{4}\sin\frac{\phi}{2}}{\cos\frac{\pi}{4}\cos\frac{\phi}{2} + \sin\frac{\pi}{4}\sin\frac{\phi}{2}}\, e^{-i\lambda} \\ &= \frac{\cos\frac{\pi}{4}\cos\frac{\phi}{2} - \sin\frac{\pi}{4}\sin\frac{\phi}{2}}{\sin\frac{\pi}{4}\cos\frac{\phi}{2} + \cos\frac{\pi}{4}\sin\frac{\phi}{2}}\, e^{-i\lambda} \\ &= \frac{\cos(\frac{\pi}{4} + \frac{\phi}{2})}{\sin(\frac{\pi}{4} + \frac{\phi}{2})}\, e^{-i\lambda} \\ &= \frac{1}{\tan(\frac{\pi}{4} + \frac{\phi}{2})\, e^{i\lambda}} \\ &= \frac{1}{z}\end{aligned}$$

We have shown that inversion corresponds to projection from a rotation of the Riemann sphere. Figure 3.3 and Figure 3.4 illustrate the effect of inversion on a

collection of example points in $\mathbb{C}$ that lie in a square.

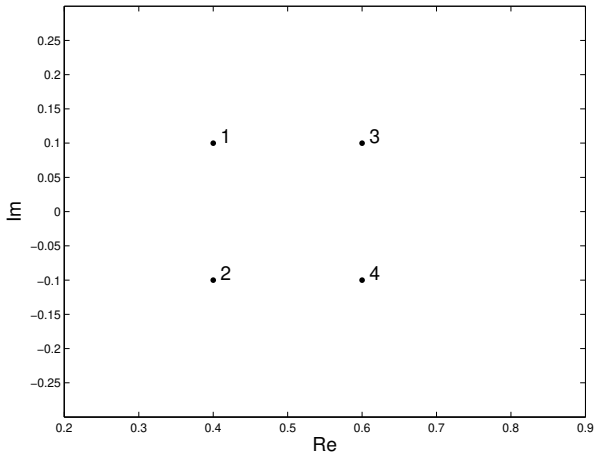

FIGURE 3.3: *Before inversion*

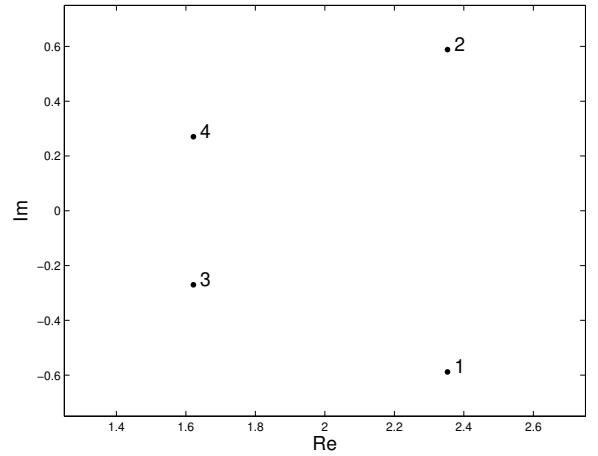

FIGURE 3.4: *After inversion*

Remark: In practice, since fingerprint acquisition is normally a monitored process, the amount of non-linear distortion should be less drastic than that shown in Figure 3.3 and Figure 3.4.

3.3 The Möbius transformation-based model

Based on the above analysis, we now introduce the Möbius transformation and show that is a good candidate for modelling minutiae variations between two impressions of the same finger.

Definition *A mapping of the form*

$$f(z) = \frac{az + b}{cz + d} \tag{3.5}$$

is called a Möbius transformation [143], where $a, b, c, d \in \mathbb{C}$*, and* $ad - bc \neq 0$*.*

Note that the assumption $ad - bc \neq 0$ is necessary [142] because if $ad - bc = 0$, the mapping $f(z)$ in (3.5) becomes a constant mapping, sending every point z to the same image point a/c.

Despite its seemingly simplicity, the Möbius transformation has abundant applications in fields such as computer vision and biological image analysis, thanks to its useful properties and its ability to work with non-Euclidean geometry. For example, in order to identify possible transformations in different images of the same object, Marsland and Mclachlan [144] presented Möbius invariants for both curves and images as well as developed invariant signatures, by which shapes can be recognised. In the context of building a model for fingerprint minutiae variations, we will prove that the Möbius transformation (3.5) can represent minutiae translation, rotation and non-linear distortion.

Theorem *The Möbius transformation is composed of translation, rotation and inversion.*

Proof: Let $f(z)$ be a Möbius transformation as defined in (3.5).

Case 1: $c = 0$. This implies $f(z) = (a/d)z + b/d$. Let $f_1 = (a/d)z$ and $f_2 = z + b/d$. Thus,

$$f_2 \circ f_1 = (a/d)z + b/d = f(z)$$

In this case, it follows from Proposition 1 and Proposition 2 that f is composed of translation and rotation.

Case 2: $c \neq 0$. According to [143], suppose $f_1(z) = z + d/c$, $f_2(z) = 1/z$, $f_3(z) = \frac{(bc-ad)}{c^2}z$ and $f_4(z) = z + a/c$. Based on Propositions 1, 2 and 3, these functions

describe translation, rotation and inversion.

$$
\begin{aligned}
f_2 \circ f_1 &= 1/(z + d/c) \\
\implies f_3 \circ f_2 \circ f_1 &= \frac{bc - ad}{(cz + d)c} \\
\implies f_4 \circ f_3 \circ f_2 \circ f_1 &= \frac{bc - ad}{c(cz + d)} + \frac{a(cz + d)}{c(cz + d)} \\
&= \frac{c(az + b)}{c(cz + d)} \\
&= f(z)
\end{aligned}
$$

Therefore, $f(z)$ is composed of translation, rotation and inversion as required.

Our proof above also echoes the statement made by Needham in [142] that the Möbius transformation can be decomposed into the following fundamental transformations:

i. $z \longmapsto z + \frac{d}{c}$, which is a translation.

ii. $z \longmapsto \frac{1}{z}$, which is inversion.

iii. $z \longmapsto -\frac{ad-bc}{c^2}z$, which is a rotation.

iv. $z \longmapsto z + \frac{a}{c}$, which is another translation.

In addition, it is shown [142] that there exists a unique Möbius transformation mapping any three given points to three other given points. Three points form a triangle and we know that triangles play a special role in Euclidean geometry, which is underpinned by similarity transformations. However, for similarities to exist in the realm of Euclidean geometry, the image points must form a triangle that is similar to the triangle formed by the original points, so this is considered as a type of rigid transformation. On the other hand, such similarities can be expressed by complex functions of the form $f(z) = az + b$, which is exactly a simplified version of the Möbius transformation (3.5). It is noted that minutiae translation and rotation can be dealt with by rigid transformations using Euclidean geometry, whereas non-linear distortion is caused by finger skin elasticity and such elastic deformation has to be treated by more flexible, non-Euclidean geometries through non-rigid transformations. The Möbius transformation fulfills this role. In other words, the Möbius transformation suits both rigid and non-rigid transformations.

The Möbius transformation possesses some nice properties [142] that are beneficial for modelling minutiae variations. These properties are:

- The Möbius transformation is conformal because it preserves local angles.
- The Möbius transformation preserves symmetry. Here, symmetry means that if two points are symmetric with respect to a circle, then their images under the Möbius transformation are symmetric with respect to the image circle.
- The Möbius transformation is bijective (i.e., one-to-one and onto). This property can be shown by finding the inverse function of (3.5):

$$f^{-1}(z) = \frac{dz - b}{-cz + a}$$

  It follows that $f^{-1}(z)$ is also a Möbius transformation.

We have proved mathematically that the Möbius transformation is a suitable candidate for modelling minutiae translation and rotation as well as non-linear distortion described by inversion. In the next section, we detail the experiments which were conducted using the public database FVC2002 DB2 [5] to test the effectiveness of the proposed Möbius transformation-based model.

3.4 Experimental results and discussion

To evaluate how effective the Möbius transformation-based model is when modelling minutiae variations, we conducted experiments on the public database FVC2002 DB2 [5], a standard database widely used in fingerprint-based biometrics research. We assume that the first impression of each finger is the template T and the second impression of the same finger is the query Q.

In order to test whether the proposed model can capture minutiae variations accurately enough, we take the following steps in our experiments:

1. Find the matching minutiae between two impressions of the same finger so that we obtain the reference positions of matching minutiae for subsequent comparisons.
2. From the matching minutiae found in Step 1, work out the amount of minutiae variations between the template fingerprint T and the query fingerprint Q. Specifically, determine the coefficients a, b, c, d of the Möbius

transformation (3.5) by using three randomly selected minutiae in T and their matching minutiae in Q.

3. Based on the values of a, b, c, d, use the minutiae in T to calculate their position-varied minutiae counterpart in Q, or equivalently, the matching minutiae in Q modelled by the Möbius transformation.

4. Compare the modelled minutiae's positions against the minutiae's actual (reference) positions in Q to assess the performance of our Möbius transformation-based model.

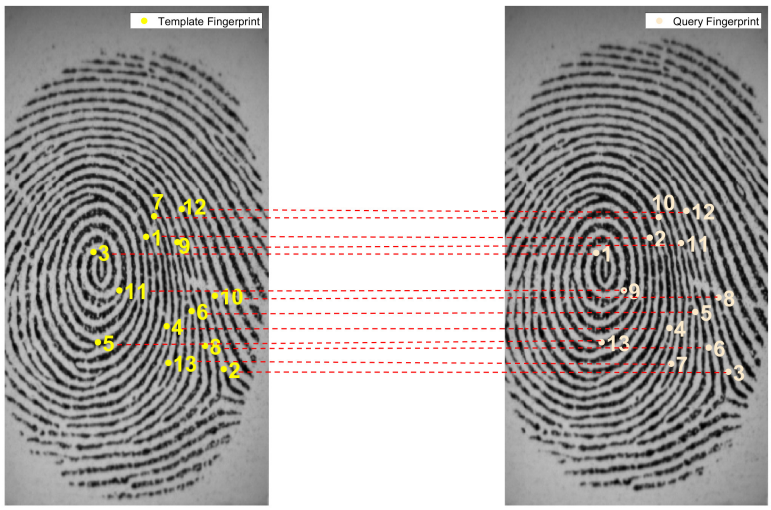

FIGURE 3.5: *Examples of matching minutiae between the template T and the query Q of Finger 7. (Note: For the sake of clarity, this figure only shows a portion of the minutiae in Finger 7.)*

For Step 1, to determine the matching minutiae between two impressions of the same finger, we applied the pair-minutiae vector based matching method in [109]; refer to Section 3.3 of [109] for the details on matching score calculation. For convenience, we use Finger 7 and Finger 40 to demonstrate our test results. The first impression of Finger 7 and Finger 10, respectively, is considered as the template T and the second impression of the same finger as the query Q.

Although it seems that in order to determine the coefficients a, b, c, d of the Möbius transformation (3.5), we would need four distinct minutiae (i.e., four different complex numbers) in the template T and the four matching minutiae in the query Q, it turns out that multiplying the coefficients by an arbitrary constant k,

where $k \neq 0$, yields the same mapping:

$$\frac{az+b}{cz+d} = f(z) = \frac{kaz+kb}{kcz+kd}$$

Therefore, the coefficients a, b, c, d of the Möbius transformation are non-unique – only the ratios of the coefficients matter [142] and three matching minutia pairs are sufficient to pin down the ratios. This is why in Step 2, we randomly selected only three minutiae rather than four in the template T and their three matching minutiae in the query Q to seek the coefficients a, b, c, d.

TABLE 3.1: Matched minutia pairs of Finger 7 and comparison of the modelled minutiae (last column) with the actual query minutiae (second last column).

Template T		Matched Query Q		Modelled
Minutia pair	Minutia position	Minutia pair	Minutia position	minutia pair
1	$159+260i$	2	$\mathbf{164+261i}$	$\mathbf{164.2+261.0i}$
2	$246+408i$	3	$\mathbf{252+411i}$	$\mathbf{252.4+411.2i}$
2	$246+408i$	3	$\mathbf{252+411i}$	$\mathbf{252.4+411.2i}$
6	$210+343i$	5	$\mathbf{215+344i}$	$\mathbf{215.3+344.1i}$
9	$194+266i$	11	$\mathbf{199+267i}$	$\mathbf{198.8+266.8i}$
8	$225+382i$	6	$\mathbf{230+384i}$	$\mathbf{230.6+384.1i}$
3	$100+277i$	1	$\mathbf{104+278i}$	$\mathbf{106.1+277.2i}$
11	$129+320i$	9	$\mathbf{135+320i}$	$\mathbf{134.1+320.1i}$
12	$199+229i$	12	$\mathbf{205+231i}$	$\mathbf{203.3+230.2i}$
4	$182+360i$	4	$\mathbf{186+362i}$	$\mathbf{186.6+361.3i}$
9	$194+266i$	11	$\mathbf{199+267i}$	$\mathbf{198.8+266.8i}$
6	$210+343i$	5	$\mathbf{215+344i}$	$\mathbf{215.3+344.1i}$
7	$168+237i$	10	$\mathbf{174+238i}$	$\mathbf{173.1+238.4i}$
8	$225+382i$	6	$\mathbf{230+384i}$	$\mathbf{230.6+384.1i}$
9	$194+266i$	11	$\mathbf{199+267i}$	$\mathbf{198.8+266.8i}$
10	$236+326i$	8	$\mathbf{241+328i}$	$\mathbf{241.7+326.7i}$
6	$210+343i$	5	$\mathbf{215+344i}$	$\mathbf{215.3+344.1i}$
5	$105+378i$	13	$\mathbf{110+378i}$	$\mathbf{108.4+377.5i}$
1	$159+260i$	2	$\mathbf{164+261i}$	$\mathbf{164.2+261.1i}$
11	$129+320i$	9	$\mathbf{135+320i}$	$\mathbf{134.1+320.1i}$
12	$199+229i$	12	$\mathbf{205+231i}$	$\mathbf{203.3+230.2i}$
13	$184+401i$	7	$\mathbf{188+402i}$	$\mathbf{188.1+403.2i}$

First, we report the experimental results of Finger 7. Figure 3.5 shows some examples of matching minutiae from Finger 7. By employing the matching mechanism in [109], we found the matching minutia pairs. Some of the matched pairs are listed in Table 3.1; for example, pairs $1-2$, $3-11$, $6-5$ and $9-6$ in

the template T match with pairs $2-3$, $1-9$, $5-13$ and $11-5$ in the query Q, respectively.

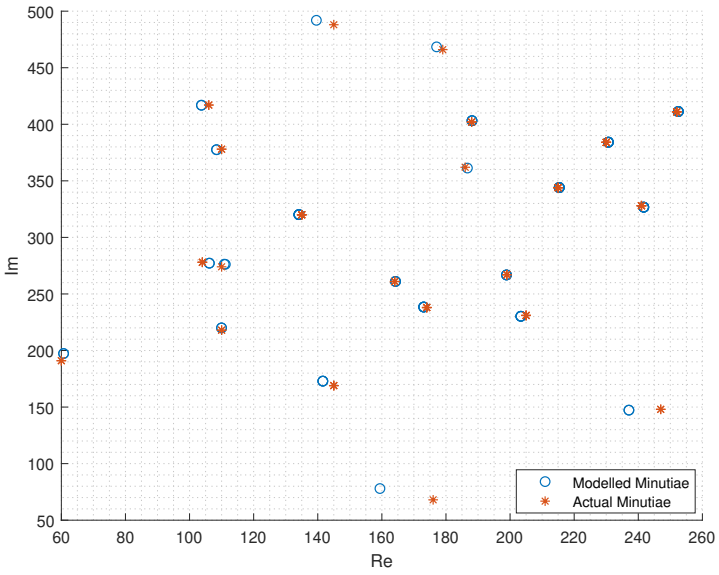

FIGURE 3.6: *Comparison of the modelled minutiae with the actual query minutiae of Finger 7.*

The matching minutiae could be readily obtained from those matched minutia pairs. After identifying the matched pairs, we should be able to work out the minutiae variations between two matching minutiae through the Möbius transformation. Equation (3.5) was used to numerically calculate the amount of variations occurred between the matching minutiae in the template T and the query Q. That is, we should determine the coefficients a, b, c and d in (3.5), where $f(z)$ is set as the minutia position in Q and z as the minutia position in T. If we refer to Table 3.1, the minutiae's positions of the first two pairs (containing three distinct minutiae 1, 2 and 6) in T and their corresponding matching minutiae (2, 3 and 5) in Q are used to find a, b, c and d, which yield $a = 0.8851 - 0.0019i$, $b = 14.9744 + 18.1392i$, $c = 0.000087467 + 0.00013611i$, $d = 1$. We then substitute these values of a, b, c and d into (3.5) and use the minutiae in T from Table 3.1 to calculate the modelled minutiae $f(z)$. The comparison between $f(z)$ and the actual query minutiae's positions in Q should reveal the performance of the proposed model. This comparison is shown by the last two columns of Table 3.1, from which we can see that $f(z)$ obtained from the Möbius transformation-based model is quite close to the actual query minutiae.

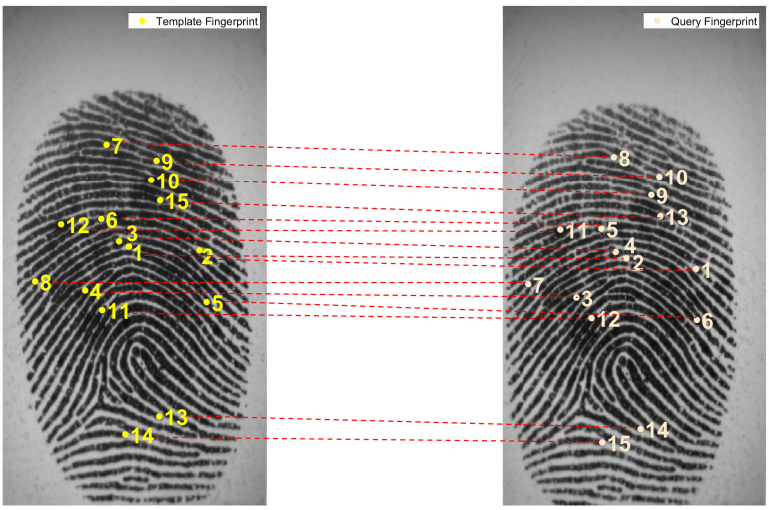

FIGURE 3.7: *Examples of matching minutiae between the template T and the query Q of Finger 40. (Note: For the sake of clarity, this figure only shows a portion of the minutiae in Finger 40.)*

In Figure 3.6, we plot the minutiae's positions modelled by the Möbius transformation, in comparison with the actual minutiae in the query Q of Finger 7. It is clear that a majority of minutiae calculated from the Möbius transformation-based model fall in the proximity of actual query minutiae. These results demonstrate that the Möbius transformation can model minutiae variations effectively between two impressions of the same finger.

Next, we report the test results of Finger 40. Figure 3.7 shows some matching minutiae between the template T and the query Q of this finger. The matching minutiae were obtained from the matched minutia pairs, which followed the same method in [109] as used for Finger 7. Table 3.2 lists some of the matching minutia pairs of Finger 40; for example, pairs $15-3$, $3-4$, $13-14$ and $7-8$ in the template T match with pairs $13-4$, $4-3$, $14-15$ and $8-7$ in the query Q, respectively. By randomly selecting the second and third minutia pairs in T (consisting of minutiae 3, 4 and 5) and their matching minutiae 4, 3 and 6, the same procedure for Finger 7 was applied to Finger 40 to find the coefficients a, b, c and d in the Möbius transformation, resulting in $a = 0.9450 + 0.1934i$, $b = 40.8843 + 1.3577i$, $c = 0.00010239 + 0.00012495i$ and $d = 1$. After substituting these values of a, b, c and d into (3.5), we calculated the modelled minutiae $f(z)$ by setting z in (3.5) as the minutiae in the template T from Table 3.2. It can be observed from the last two columns of Table 3.2 that the modelled minutiae

through the Möbius transformation are very similar to the actual query minutiae in terms of minutia position. This similarity is also exhibited clearly in Figure 3.8.

TABLE 3.2: Matched minutia pairs of Finger 40 and comparison of the modelled minutiae (last column) with the actual query minutiae (second last column).

Template T		Matched Query Q		Modelled
Minutia pair	Minutia position	Minutia pair	Minutia position	minutia pair
1	$142 + 271i$	2	$\mathbf{140 + 284i}$	$\mathbf{138.8 + 284.4i}$
2	$221 + 275i$	1	$\mathbf{218 + 296i}$	$\mathbf{216.7 + 295.8i}$
3	$131 + 265i$	4	$\mathbf{128 + 277i}$	$\mathbf{128.4 + 277.3i}$
4	$93 + 320i$	3	$\mathbf{84 + 328i}$	$\mathbf{84.0 + 328.6i}$
3	$131 + 265i$	4	$\mathbf{128 + 277i}$	$\mathbf{128.4 + 277.3i}$
5	$229 + 333i$	6	$\mathbf{219 + 353i}$	$\mathbf{220.1 + 354.0i}$
6	$111 + 240i$	5	$\mathbf{112 + 251i}$	$\mathbf{111.5 + 250.1i}$
5	$229 + 333i$	6	$\mathbf{219 + 353i}$	$\mathbf{220.1 + 354.0i}$
7	$117 + 156i$	8	$\mathbf{126 + 170i}$	$\mathbf{127.9 + 168.5i}$
8	$37 + 310i$	7	$\mathbf{30 + 313i}$	$\mathbf{28.0 + 311.6i}$
9	$173 + 174i$	10	$\mathbf{177 + 192i}$	$\mathbf{179.8 + 192.8i}$
4	$93 + 320i$	3	$\mathbf{84 + 328i}$	$\mathbf{84.0 + 328.6i}$
10	$167 + 196i$	9	$\mathbf{168 + 213i}$	$\mathbf{171.5 + 213.5i}$
11	$112 + 342i$	12	$\mathbf{101 + 351i}$	$\mathbf{101.1 + 353.1i}$
9	$173 + 174i$	10	$\mathbf{177 + 192i}$	$\mathbf{179.8 + 192.8i}$
11	$112 + 342i$	12	$\mathbf{101 + 351i}$	$\mathbf{101.1 + 353.1i}$
15	$177 + 219i$	13	$\mathbf{178 + 237i}$	$\mathbf{178.8 + 236.9i}$
3	$131 + 265i$	4	$\mathbf{128 + 277i}$	$\mathbf{128.4 + 277.3i}$
7	$117 + 156i$	8	$\mathbf{126 + 170i}$	$\mathbf{127.9 + 168.5i}$
12	$66 + 246i$	11	$\mathbf{66 + 252i}$	$\mathbf{65.8 + 250.5i}$
13	$176 + 461i$	14	$\mathbf{156 + 475i}$	$\mathbf{157.6 + 481.1i}$
14	$138 + 481i$	15	$\mathbf{113 + 490i}$	$\mathbf{116.1 + 499.9i}$

The main computations incurred by the proposed method are: (i) calculating the coefficients a, b, c, d of the Möbius transformation (3.5); and (ii) determining the modelled minutiae based on a, b, c, d and the (known) minutiae in the template. One way to quantify the amount of arithmetic involved is to count flops. A flop [145] is a floating point add, subtract, multiply or divide. The values of a, b, c, d are obtained by calculating the determinants of four 3×3 matrices [142], amounting to 56 flops in total. After a, b, c, d are found, using the template minutiae, we can calculate the modelled minutiae according to (3.5). To acquire a modelled minutia only requires 5 flops. Obviously, the total amount of arithmetic work in the proposed method is low. All of these results are obtained

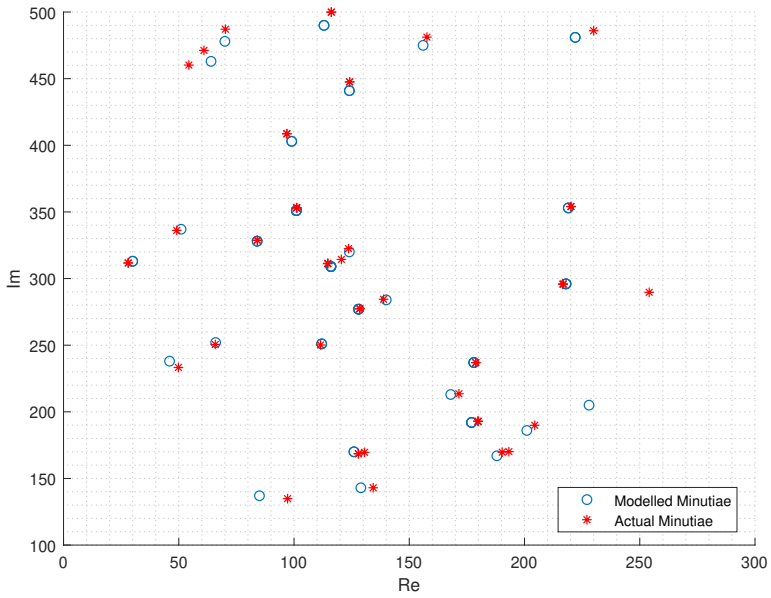

FIGURE 3.8: *Comparison of the modelled minutiae with the actual query minutiae of Finger 40*

using MATLAB, which is run on a PC with Core i7, 3.41 GHz CPU and operating system of 64-bit Win 10. It takes 0.0057 second to calculate a, b, c, d for all of 100 fingers in the database FVC2002 DB2 [5]. It takes 0.0539 second to determine the modelled minutiae for 100 fingers of the same database. Thus, the proposed method is computationally inexpensive.

According to [146], the forensic guidelines state to determine if two fingerprints are the same, the minimum number of matching minutiae should be 12. From Table 3.1 and Table 3.2, which only include a portion of the matched minutia pairs, we can see that the number of matching minutiae is much greater than 12 and that our Möbius transformation-based model accurately captures minutiae variations between two impressions of the same finger.

To thoroughly evaluate the proposed method, we conducted further testing over the entire database FVC2002 DB2 [5] with a total of 100 fingers. The forensic guidelines [146] require at least 12 mated pairs to make a 'match' verdict on two fingerprints, so we found the 12 best matched minutia pairs between the template (i.e, the first impression) and the query (i.e., the second impression of the same finger) for each finger in the database FVC2002 DB2 [5] by

applying the matching approach in [109]. We then calculated the Euclidean distance between the actual and modelled minutiae. That is, the Euclidean distance between the actual minutia (x_1, y_1) and its modelled minutia (x_2, y_2) is $d = \sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2}$. The average Euclidean distance between these actual and modelled minutiae is reported in Table 3.3. From the Euclidean distance in Table 3.3, it is clear that the modelled and actual minutiae are very close to each other. Therefore, we have experimentally verified the validity of the proposed model.

TABLE 3.3: The average Euclidean distance (in pixels) between the actual and modelled minutiae of each finger in the database FVC2002 DB2 (100 fingers).

Finger 1	Finger 2	Finger 3	Finger 4	Finger 5	Finger 6	Finger 7
1.235	1.365	1.429	1.297	1.334	2.256	0.559
Finger 8	Finger 9	Finger 10	Finger 11	Finger 12	Finger 13	Finger 14
1.813	1.903	0.674	1.433	1.707	1.425	2.658
Finger 15	Finger 16	Finger 17	Finger 18	Finger 19	Finger 20	Finger 21
0.891	6.464	1.636	1.616	1.535	2.592	1.050
Finger 22	Finger 23	Finger 24	Finger 25	Finger 26	Finger 27	Finger 28
1.209	0.729	1.023	0.772	1.874	1.957	3.661
Finger 29	Finger 30	Finger 31	Finger 32	Finger 33	Finger 34	Finger 35
1.256	0.440	0.925	1.013	0.646	1.134	1.073
Finger 36	Finger 37	Finger 38	Finger 39	Finger 40	Finger 41	Finger 42
3.053	0.976	1.209	1.065	0.800	0.966	1.150
Finger 43	Finger 44	Finger 45	Finger 46	Finger 47	Finger 48	Finger 49
0.891	0.787	1.159	0.895	0.950	0.678	1.185
Finger 50	Finger 51	Finger 52	Finger 53	Finger 54	Finger 55	Finger 56
0.779	0.641	1.142	0.527	2.938	0.940	0.652
Finger 57	Finger 58	Finger 59	Finger 60	Finger 61	Finger 62	Finger 63
2.415	1.414	0.531	1.861	0.699	0.885	1.118
Finger 64	Finger 65	Finger 66	Finger 67	Finger 68	Finger 69	Finger 70
1.341	0.708	0.417	1.285	1.547	1.325	0.414
Finger 71	Finger 72	Finger 73	Finger 74	Finger 75	Finger 76	Finger 77
0.756	0.354	4.409	0.763	0.578	0.803	0.649
Finger 78	Finger 79	Finger 80	Finger 81	Finger 82	Finger 83	Finger 84
0.831	1.724	0.984	0.512	0.404	1.397	1.336
Finger 85	Finger 86	Finger 87	Finger 88	Finger 89	Finger 90	Finger 91
1.927	0.794	0.918	1.474	2.576	0.463	1.121
Finger 92	Finger 93	Finger 94	Finger 95	Finger 96	Finger 97	Finger 98
1.306	0.990	0.811	2.425	0.918	3.021	1.024
Finger 99	Finger 100					
0.984	1.194					

3.5 Chapter summary

It is well known that minutiae variations occur in relation to different impressions of the same finger. How to capture these variations between fingerprint scans is a research problem of theoretical and practical importance, yet a unified model for describing minutiae variations has not been available. In this chapter, we proposed the Möbius transformation-based model as a unified model to

express minutiae variations – translation, rotation and non-linear distortion. We proved mathematically that the Möbius transformation-based model is a unified model for representing different types of minutiae variations. In addition, we used the the public database FVC2002 DB2 [5] to evaluate the effectiveness of the proposed model. The experimental results show that the modelled minutiae through the Möbius transformation are very close to the actual minutiae in terms of minutia position, which verifies the efficacy of the proposed model.

Chapter 4

Design of Cancelable MCC-Based Fingerprint Templates Using Dyno-Key Model

4.1 Introduction

As discussed in Chapter 1, fingerprints are one of the most studied biometric traits and fingerprint-based biometric authentication has been widely used in a variety of modern-day applications, such as access control and financial transactions on mobile devices. While fingerprint recognition has numerous advantages over traditional password or token-based authentication, e.g., convenience and good security, fingerprint templates, which store users' original fingerprint information, are vulnerable if unprotected, because adversaries can use stolen fingerprint templates to commit privacy invasion and identity theft. To ensure the safety and integrity of users' raw fingerprint data, it is crucial to protect fingerprint templates.

Cancelable biometrics is an important technique for biometric template protection (refer to Section 2.4). Designing cancelable fingerprint templates involves using a non-invertible transformation to convert raw fingerprint data in an intentionally distorted manner such that the original fingerprint information cannot be retrieved from the transformed template. Moreover, if a cancelable template is compromised, a new template can be generated by changing transformation parameters. Due to security considerations, matching between template and query fingerprints takes place in the transformed domain, where the same transformation is applied to the query fingerprint.

Although cancelable fingerprint templates have spurred great interest among researchers in the last decade, how to design well-functioning cancelable templates faces challenges, such as the extraction of discriminative and robust local features and how to achieve strong security while maintaining good recognition accuracy. Minutia Cylinder Code (MCC) [117] is commonly recognized to be an effective, high-quality representation of local minutia structures. The MCC fingerprint templates demonstrate fast and excellent matching performance over a number of databases, e.g., FVC2002 DB1-DB4 [5]. However, despite a satisfactory level of accuracy, if compromised, MCC templates can be reverse-engineered to reconstruct original minutiae values.

In this chapter, we propose alignment-free cancelable MCC-based templates built on top of the MCC feature extraction and representation. The core component of our design is a dynamic random key model, called the Dyno-key model. The Dyno-key model uses randomly generated keys to dynamically take elements out of MCC's binary feature vectors. In a bid to increase security and uncertainty, those extracted elements are discarded after the block-based logic operations. Since the keys are random, user-specific and can be set differently for different applications, different keys extract different elements from MCC's binary vectors and yield different post-XOR results. The produced length-shortened, post-XOR binary vectors give rise to cancelable templates. We highlight the features and contributions of the proposed method as follows.

1. The Dyno-key model offers an efficient and effective way to transform MCC's binary feature vectors non-invertibly. Not only does the Dyno-key model significantly enhance the security of the MCC representation, but it also makes MCC templates revocable.

2. The proposed cancelable MCC-based templates are equipped with unlinkability and diversity through the Dyno-key model, performing tasks such as the dynamic extraction of MCC cell values, block-based logic operations and the removal of extracted elements.

3. The cancelable MCC-based templates designed have high recognition accuracy. When evaluated over seven public databases, FVC2002 DB1-DB3 [5], FVC2004 DB1 and DB2 [6], and FVC2006 DB2 and DB3 [7], under two testing protocols, the 1vs1 protocol and the original FVC protocol [113], the matching performance of the proposed method levels with that of the

unprotected, reproduced MCC templates. Compared with the state-of-the-art cancelable fingerprint templates, the proposed method also shows competitive performance. For example, the equal error rate (EER) of the proposed method in the lost-key scenario under the 1vs1 protocol is 0 for FVC2002 DB1 and DB2, 0.99% for FVC2002 DB3 and 3.01% for FVC2004DB2.

The rest of this chapter is organized as follows. Section 4.2 presents the proposed scheme, including a detailed description of the Dyno-key model. Section 4.3 discusses the experimental results of the proposed cancelable MCC-based templates in comparison with the state of the art. Security analysis is also given in Section 4.3.4. Finally, the summary is provided in Section 4.4.

4.2 Proposed cancelable template design

MCC [117] is a high-performing minutia descriptor for fingerprint recognition. Building upon MCC's feature extraction and representation, we develop the Dyno-key model, the core component in our design of cancelable MCC-based templates. The resulting protection strategy secures the original MCC features. The proposed scheme is made up of three parts:

1. MCC-based feature extraction and representation
2. The Dyno-key model
3. Fingerprint matching in the transformed domain

4.2.1 MCC-based feature extraction and representation

In a fingerprint image, each minutia is expressed as a triplet (x_m, y_m, θ_m), where m is the minutia index, (x_m, y_m) denotes the x, y coordinates of minutia m and $\theta_m \in [0, 2\pi]$ denotes the orientation of minutia m. In the MCC reprersentation [117], a 3D local structure, referred to as 'cylinder', is constructed for each minutia. The cylinder encodes both spatial and directional relationships between a reference minutia and its neighbourhood of radius R. The MCC builds a cylinder set which includes cylinders corresponding to all minutiae with a sufficient number of neighbours. As each cylinder is a local descriptor, it is invariant to minutiae translation and rotation, robust against skin distortion and has a fixed length given by the total number of cells in the cylinder. Figure 4.1 shows a graphical representation of an MCC cylinder.

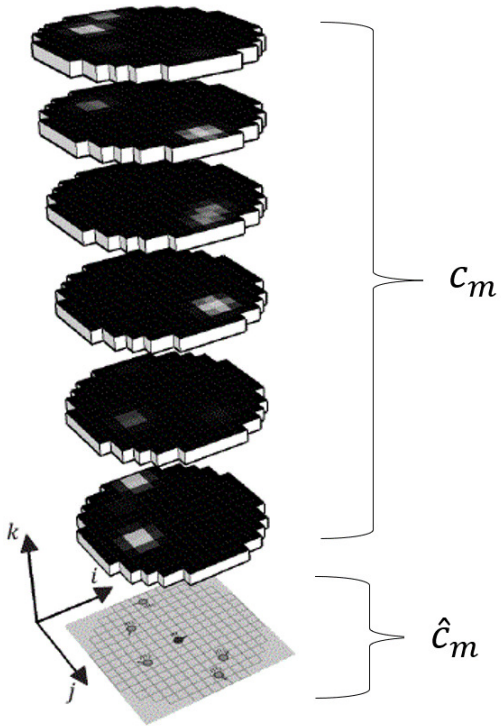

FIGURE 4.1: A graphical representation of an MCC cylinder (adapted from [117]). Cell validity is given by $\hat{c}_m$ and cell values are contained in c_m (lighter areas represent higher values).

A bit-based implementation in [117] renders a binary representation for MCC templates. Specifically, each valid cylinder contains the following information: a sequence of 0 and 1, indicating the validity of each cell of the cylinder base and the binary sequence of the cell values. Thus, all the information about a valid cylinder of minutia m can be expressed by the binary vector $\mathbf{C}_m$ as

$$\mathbf{C}_m = [\hat{c}_m \; c_m] \tag{4.1}$$

where

$$\hat{c}_m = [\hat{c}_m(1), \hat{c}_m(2), \cdots, \hat{c}_m(S)] \tag{4.2}$$

$$c_m = [c_m(1), c_m(2), \cdots, c_m(N)] \tag{4.3}$$

In the above expressions, $\hat{c}_m(i)$ denotes cell validity – 0 means 'Invalid cell' and 1 'Valid cell', for $i = 1, 2, \cdots, S$ with $S = (N_s \times N_s)$, and $c_m(j)$ stores the cell value, for $j = 1, 2, \cdots, N$ with $N = (N_s \times N_s \times N_D)$. The parameters N_s and N_D are the number of cells on the cylinder base and the number of cylinder sections, respectively.

Although MCC templates are considered one of the most robust in dealing with fingerprint uncertainties, they are insecure. This is because the cylinders can be reversed to rebuild the minutiae (see the reconstruction of minutiae from MCC cylinders in [113]). Therefore, to prevent cylinders from being reversed while taking advantage of MCC's high-quality feature extraction, we propose the Dyno-key model to create new, irreversible binary feature vectors.

4.2.2 The Dyno-key model

In this section, we present the Dyno-key model, which is key to generating cancelable templates by transforming MCC's binary vector $\mathbf{C}_m$ non-invertibly. The central idea of the Dyno-key model is the use of dynamic random keys for feature transformation purposes. Based on randomly generated keys, elements of MCC's binary feature vectors are dynamically picked to perform block-based logic operations. These elements are discarded afterwards so as to increase security of the resultant binary feature vectors. This also adds uncertainty to the original MCC features. By transforming MCC's binary features in an irreversible manner, the Dyno-key model gives rise to new binary vectors of reduced lengths. It has a similar effect to dimensionality reduction but is guided by dynamic random keys. A block diagram of the Dyno-key model is illustrated in Figure 4.2.

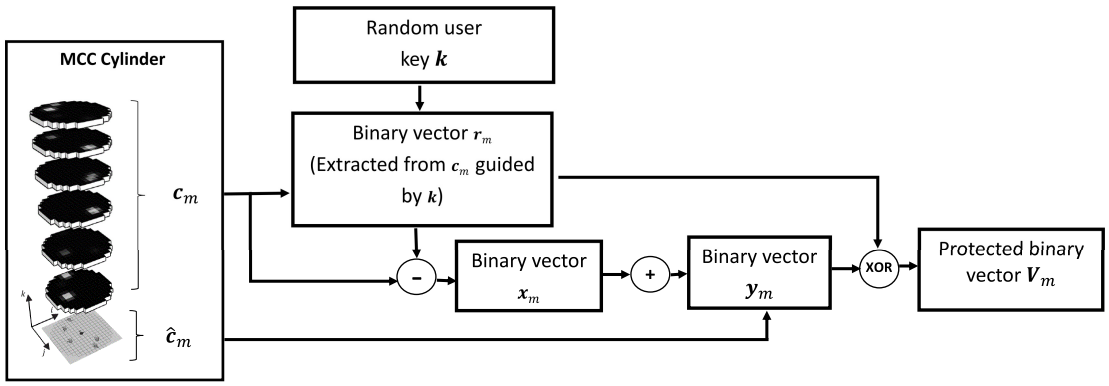

FIGURE 4.2: Block diagram of the Dyno-key model.

It follows from MCC's binary vector $\mathbf{C}_m$ that the bit-vector $\hat{c}_m$ in (4.2) stores cell validity, while the bit-vector c_m in (4.3) stores cell values, containing minutia-related information. Hence, it is important to protect these bit-vectors, especially c_m. To this end, the Dyno-key model consists of three steps.

Step 1: Generate a random vector $\boldsymbol{k}$ of length L, written as

$$\boldsymbol{k} = [k_1, k_2, \cdots, k_L] \tag{4.4}$$

where $1 < L < N$, and all entries k_j of $\boldsymbol{k}$, for $j = 1, 2 \cdots, L$, are strictly positive integers with $k_m \neq k_n$ for all $m \neq n$. The random vector $\boldsymbol{k}$ acts like an index vector, responsible for picking those cell values out of the bit-vector $\boldsymbol{c}_m$ which have the same indexes as values of k_j in $\boldsymbol{k}$, for $j = 1, 2 \cdots, L$. This process is detailed in Step 2.

Step 2: Construct binary vectors $\boldsymbol{r}_m$ and $\boldsymbol{y}_m$. The binary vector $\boldsymbol{r}_m$ is formed by extracting those elements from $\boldsymbol{c}_m$ in (4.3), whose indexes are k_j, for $j = 1, 2 \cdots, L$. In other words, the entries of binary vector $\boldsymbol{r}_m$ are made up of $c_m(k_j)$, for $j = 1, 2 \cdots, L$. So the binary vector $\boldsymbol{r}_m$ is of length L, given by

$$\begin{aligned} \boldsymbol{r}_m &= [r_m(1), r_m(2), \cdots, r_m(L)] && (4.5) \\ &= [c_m(k_1), c_m(k_2), \cdots, c_m(k_L)] && (4.6) \end{aligned}$$

The binary vector $\boldsymbol{r}_m$ will be discarded after the block-based logic operation in Step 3. The binary vector $\boldsymbol{y}_m$ is constructed by

$$\boldsymbol{y}_m = [\hat{\boldsymbol{c}}_m \; \boldsymbol{x}_m] \tag{4.7}$$

where $\hat{\boldsymbol{c}}_m$ is given in (4.2), and $\boldsymbol{x}_m$ contains the remaining entries of $\boldsymbol{c}_m$ after those elements indexed by k_j, for $j = 1, 2 \cdots, L$, are taken out of $\boldsymbol{c}_m$. It follows from (4.7) that the binary vector $\boldsymbol{y}_m$ is of length $S + N - L$.

Step 3: Divide $\boldsymbol{y}_m$ into L blocks and perform block-based logic operation with $\boldsymbol{r}_m$, after which $\boldsymbol{r}_m$ is discarded.

When $\boldsymbol{y}_m$ is divided into L blocks, we get $\boldsymbol{y}_m = [\boldsymbol{y}_m^{(1)} \; \boldsymbol{y}_m^{(2)} \; \cdots \; \boldsymbol{y}_m^{(L)}]$. Block $\boldsymbol{y}_m^{(j)}$, for $j = 1, 2, \cdots, L$, can be expanded as

$$\boldsymbol{y}_m^{(j)} = [y_m^{(j)}(1), y_m^{(j)}(2), \cdots, y_m^{(j)}(W)] \tag{4.8}$$

where the length of block $\boldsymbol{y}_m^{(j)}$ is $W = \lceil (S + N - L)/L \rceil$. Then we perform the block-based XOR between block $\boldsymbol{y}_m^{(j)}$ and $\boldsymbol{r}_m$, given by

$$v_m^{(j)}(i) = y_m^{(j)}(i) \oplus r_m(j) \tag{4.9}$$

where the symbol $\oplus$ denotes the XOR operation, $i = 1, 2, \cdots, W$ and $j = 1, 2, \cdots, L$. Upon completion of (4.9), we discard $\boldsymbol{r}_m$ for security purposes (refer to the security analysis in Section 4.3.4). Finally, to compactly express the post-XOR results in the vector form, we concatenate all $v_m^{(j)}(i)$, for $i = 1, 2, \cdots, W$ and $j = 1, 2, \cdots, L$, to obtain

$$\boldsymbol{V}_m = \left[v_m^{(1)}(1), v_m^{(1)}(2), \cdots, v_m^{(1)}(W), \cdots, v_m^{(L)}(1), v_m^{(L)}(2), \cdots, v_m^{(L)}(W) \right] \quad (4.10)$$

The binary vector $\boldsymbol{V}_m$ is of length $S + N - L$.

Remarks:

1. Compared to MCC's binary representation $\mathbf{C}_m$ in (4.1), the length of $\boldsymbol{V}_m$ is shortened by L and $\boldsymbol{V}_m$ constitutes a cancelable template. Due to the uncertainty added by the block-based logic operation in (4.9) and the deliberate deletion of $\boldsymbol{r}_m$, whose entries come from MCC's binary vector $\mathbf{c}_m$ in (4.3), the Dyno-key model transforms MCC's original features irreversibly into the new binary vector $\boldsymbol{V}_m$ for every minutia m (see more detail in Section 4.3.4 – Security analysis).
2. The random vector $\boldsymbol{k}$ in (4.4) serves as user-specific parameter keys. As these parameter keys are generated at random, different keys result in different $\boldsymbol{V}_m$, thus fulfilling the requirement of revocability for cancelable biometrics.
3. Apart from serving as parameter keys, the random vector $\boldsymbol{k}$ in (4.4) plays the role of dynamically extracting elements from MCC's binary vector $\boldsymbol{c}_m$ to construct $\boldsymbol{r}_m$ (see (4.6)). Since $\boldsymbol{r}_m$ is discarded afterwards, the Dyno-key model heightens the security of the resultant vector $\boldsymbol{V}_m$, making the original MCC features hard to restore.

In summary, the proposed algorithm for the generation of cancelable templates is as follows.

Step 1: Generate the random vector $\boldsymbol{k}$ in (4.4).

Step 2: Use (4.6) to form the binary vector $\boldsymbol{r}_m$ and construct the binary vector $\boldsymbol{y}_m$ according to (4.7).

Step 3: Divide $\boldsymbol{y}_m$ into L blocks, i.e., $\boldsymbol{y}_m = [\boldsymbol{y}_m^{(1)} \ \boldsymbol{y}_m^{(2)} \ \cdots \ \boldsymbol{y}_m^{(L)}]$. Perform block-based XOR operation between $\boldsymbol{r}_m$ and block $\boldsymbol{y}_m^{(j)}$, for $j = 1, 2, \cdots, L$ (refer

to (4.9)). After the block-based logic operation, discard $\boldsymbol{r}_m$ and use (4.10) to obtain the resultant vector $\boldsymbol{V}_m$.

4.2.3 Fingerprint matching in the transformed domain

In cancelable biometrics, fingerprint matching is conducted in the transformed domain for security reasons. Therefore, a query fingerprint goes through the same transformation procedures as the template fingerprint. For clarity, we use superscripts t and q to distinguish between the template and query fingerprints, so $\boldsymbol{V}_m^t$ and $\boldsymbol{V}_n^q$ represent the transformed template and query binary vectors, respectively derived from cylinder $\boldsymbol{C}_m^t$ in the template and cylinder $\boldsymbol{C}_n^q$ in the query (see (4.1)).

After obtaining the protected binary vectors using the Dyno-key model, similar to splitting $\boldsymbol{C}_m$ into $\hat{\boldsymbol{c}}_m$ in (4.2) and $\boldsymbol{c}_m$ in (4.3), we separate $\boldsymbol{V}_m^t$ ($\boldsymbol{V}_n^q$) into two bit-vectors $\hat{\boldsymbol{v}}_m^t$ ($\hat{\boldsymbol{v}}_n^q$) and $\boldsymbol{v}_m^t$ ($\boldsymbol{v}_n^q$). The length of $\hat{\boldsymbol{v}}_m^t$ and $\hat{\boldsymbol{v}}_n^q$ is S and the length of $\boldsymbol{v}_m^t$ and $\boldsymbol{v}_n^q$ is $N - L$. In practice, bit-vectors $\hat{\boldsymbol{v}}_m^t$ and $\hat{\boldsymbol{v}}_n^q$ act as bit-masks to select valid bits from $\boldsymbol{v}_m^t$ and $\boldsymbol{v}_n^q$, respectively. We follow a similar procedure to the bit-based implementation process in [117] to get

$$\boldsymbol{v}_m^{t|q} = \boldsymbol{v}_m^t \wedge \hat{\boldsymbol{v}}_{m,n}, \;\; \boldsymbol{v}_n^{q|t} = \boldsymbol{v}_n^q \wedge \hat{\boldsymbol{v}}_{m,n} \tag{4.11}$$

where the symbol $\wedge$ denotes the bitwise AND and $\hat{\boldsymbol{v}}_{m,n} = \hat{\boldsymbol{v}}_m^t \wedge \hat{\boldsymbol{v}}_n^q$.

The similarity score between $\boldsymbol{V}_m^t$ and $\boldsymbol{V}_n^q$ is calculated by

$$S(\boldsymbol{V}_m^t, \boldsymbol{V}_n^q) = 1 - \frac{\|\boldsymbol{v}_m^{t|q} \oplus \boldsymbol{v}_n^{q|t}\|_2^2}{\|\boldsymbol{v}_m^{t|q}\|_2^2 + \|\boldsymbol{v}_n^{q|t}\|_2^2} \tag{4.12}$$

where the symbol $\oplus$ denotes the bitwise XOR and $\|\cdot\|_2$ represents the 2-norm of a vector. The similarity score $S(\boldsymbol{V}_m^t, \boldsymbol{V}_n^q)$ in the range of $[0, 1]$ indicates the local similarity between a valid cylinder in the template and a valid cylinder in the query. When the local similarities between all valid cylinders in the template and query fingerprints are calculated using (4.12), a global score representing the overall similarity between the template and query fingerprints is determined according to the Local Greedy Similarity algorithm in the MCC SDK [117].

4.3 Experiment results and analysis

Experiments were carried out on seven public databases (FVC2002 DB1 – DB3 [5], FVC2004 DB1 and DB2 [6], and FVC2006 DB2 and DB3 [7]) to evaluate the proposed cancelable template design. The details of these databases are given in Table 1.1. All of the tests are designed to evaluate whether the proposed method fulfills the requirements of cancelable biometrics. We also analyze to what extent the proposed cancelable templates strengthen security, thus protecting the original MCC features. In light of these, this section focuses on:

- Performance evaluation
- Revocability and diversity
- Unlinkability
- Security analysis

The performance measures used in our experiments are false match rate (FMR), false non-match rate (FNMR) and error equal eate (EER). Two testing protocols, the 1vs1 protocol and the original FVC protocol [113], were employed to report the experiment results of the proposed scheme.

4.3.1 Performance evaluation

The matching performance of the proposed method was evaluated under the lost-key scenario. This scenario represents the worst case in practice where the adversary knows a user's key. In the experiments, for both genuine and imposter testing, all the transformed templates were built using the same random vector $\boldsymbol{k}$ of length L (see (4.4)). That is, all the users of a database were assigned the same $\boldsymbol{k}$.

The proposed method is controlled by the randomly generated parameter key $\boldsymbol{k}$, which is responsible for dynamically extracting elements from the bit-vector $\boldsymbol{c}_m$ to create $\boldsymbol{r}_m$ in (4.6). The length L of $\boldsymbol{k}$ has an impact on the matching performance. A smaller value of L renders a larger block size W of $\boldsymbol{y}_m^{(j)}$; see (4.8). In this case, if one bit of $\boldsymbol{r}_m$ is in error, it would affect more bits as a result of the XOR operation in (4.9), compared to a larger value of L leading to a smaller block size W of $\boldsymbol{y}_m^{(j)}$. This is shown in Tables 4.1 and 4.2, which illustrate the effect of different key lengths on the matching performance. It can be observed from Table 4.2 that the EER keeps decreasing as the key length L increases; however,

this trend reverses when the value of L gets large enough, e.g., $L = 640$. This is because if the key is too long, i.e., L too large, it would cause more information loss as more elements are taken out of $\boldsymbol{c}_m$ to go into $\boldsymbol{r}_m$, but $\boldsymbol{r}_m$ is discarded afterwards, leading to performance degradation.

TABLE 4.1: EER(%) with different key lengths in the lost-key scenario under the 1vs1 protocol

Key length L	**FVC2002**			**FVC2004**		**FVC2006**	
	DB1	DB2	DB3	DB1	DB2	DB2	DB3
Unprotected MCC	0.01	0	1.21	5.99	4.99	0.81	8.57
$L = 128$	0	0	0.99	5.99	4.00	2.87	10.01
$L = 300$	0	0	0.99	6.00	4.00	1.42	9.21
$L = 500$	0	0	0.99	6.00	3.01	1.42	7.86
$L = 640$	0	0	0.99	5.23	3.01	1.72	8.57

TABLE 4.2: EER(%) with different key lengths in the lost-key scenario under the original FVC protocol

Key length L	**FVC2002**			**FVC2004**		**FVC2006**	
	DB1	DB2	DB3	DB1	DB2	DB2	DB3
Unprotected MCC	1.54	1.33	4.03	7.92	7.65	0.93	6.92
$L = 128$	2.04	1.72	5.36	10.10	8.90	2.14	9.55
$L = 300$	1.67	1.42	4.11	9.04	7.92	1.22	7.83
$L = 500$	1.38	1.35	4.21	8.89	7.63	1.14	7.06
$L = 640$	1.53	1.39	4.31	8.87	7.78	1.21	7.60

Tables 4.1 and 4.2 also show the comparison in terms of EER between the unprotected, reproduced MCC templates and the proposed method with different key lengths. It is evident that the proposed scheme preserves the recognition accuracy of MCC templates.

With $L = 500$, we plotted the detection error trade-off (DET) curves in the lost-key scenario for all databases according to the 1vs1 and original FVC protocols in Figure 4.3 and Figure 4.4, respectively. We can see from Figure 4.3 and Figure 4.4 that the matching performance of the proposed scheme drops from high on FVC2002 DB1 and DB2 to low on FVC2004 DB1, DB2 or FVC2006 DB3 under both protocols. This comes as no surprise since the image quality in these databases is very poor. It is worth noting that under the 1vs1 protocol, the proposed method achieves outstanding matching performance in the lost-key scenario, as evidenced by EER $= 0$ for FVC2002 DB1 and DB2 and EER $= 0.99$ for FVC2002 DB3.

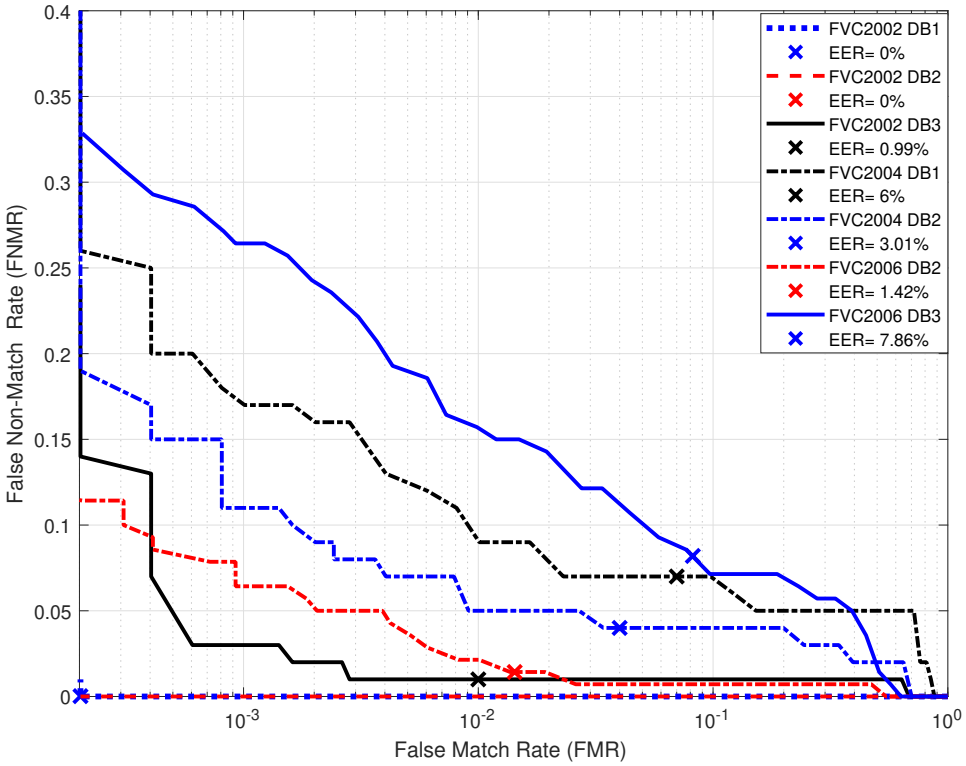

FIGURE 4.3: DET curves for FVC2002 DB1-DB3, FVC2004 DB1 and DB2, and FVC2006 DB2 and DB3 in the lost-key scenario under the 1vs1 protocol.

Table 4.3 and Table 4.4 compare the EER between the proposed method (with $L = 500$) and state-of-the-art cancelable fingerprint templates in the lost-key scenario under the 1vs1 and original FVC protocols, respectively. It is clear from Tables 4.3 and 4.4 that the proposed cancelable templates exhibit superior performance under the 1vs1 protocol and achieve a competitive performance under the original FVC protocol.

4.3.2 Revocability and diversity

Revocability and diversity are fundamental properties of cancelable biometrics. In case a stored template is compromised, it should be replaced by a new template, which must be different to the old one. That is, there should be no correlation between them although they come from the same biometric data. To assess the revocability and diversity of the proposed method, we produced 100 transformed templates from the first impression of each finger in FVC2002 DB2

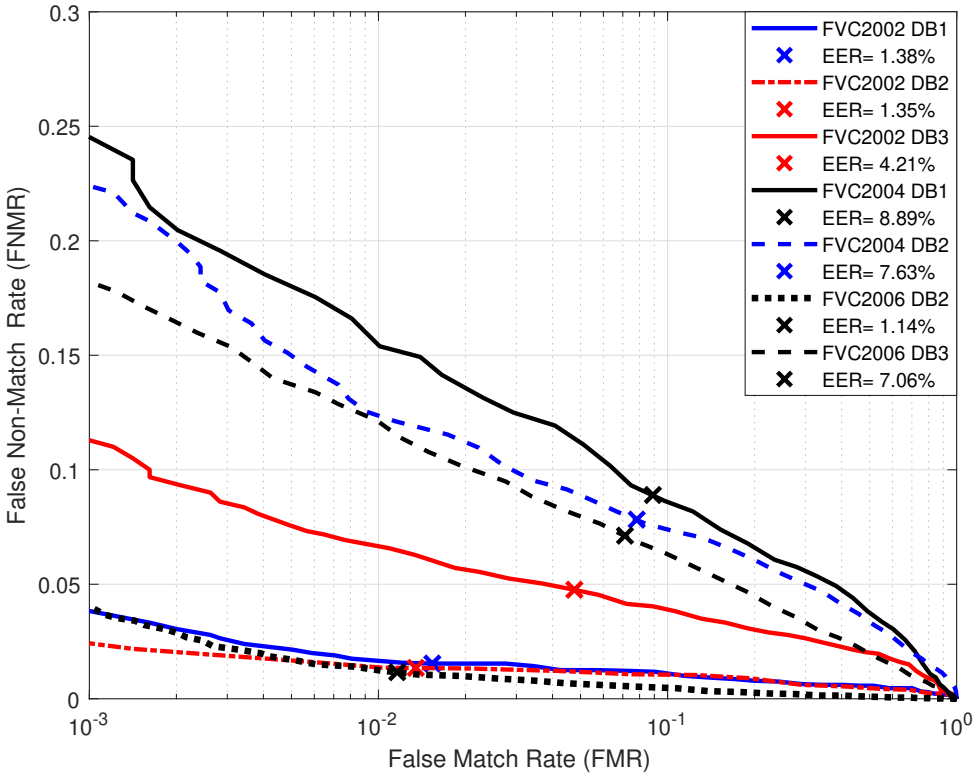

FIGURE 4.4: DET curves for FVC2002 DB1-DB3, FVC2004 DB1 and DB2, and FVC2006 DB2 and DB3 in the lost-key scenario under the original FVC protocol.

by randomly generating different user keys $\boldsymbol{k}$. Then these pseudo-imposter templates were matched against the original ones. Figure 4.5 shows the genuine, imposter and pseudo-imposter distributions, where it can be seen that the pseudo-imposter and imposter distributions are overlapping. Their mean and standard derivation are very close to each other, given by the mean 0.2606 (pseudo-imposter) and 0.2513 (imposter), and standard derivation 0.0275 (pseudo-imposter) and 0.0207 (imposter). The results demonstrate that despite the pseudo-imposter templates being generated from the same fingerprint, they are different and uncorrelated as if they were from different fingers.

4.3.3 Unlinkability

Unlinkability is considered one of the most important properties of protected templates. It guarantees user privacy and prevents cross-matching when a user is registered in different applications with the same biometric trait. In order to evaluate the level of unlinkability offered by the designed cancelable templates,

TABLE 4.3: EER(%) comparison in the lost-key scenario under the 1vs1 protocol.

Cancelable fingerprint template design	FVC2002			FVC2004		FVC2006	
	DB1	DB2	DB3	DB1	DB2	DB2	DB3
Ahmad et al. [81]	9	6	27	–	–	–	–
Jin et al. [104]	5.19	5.65	–	–	11.64	–	–
Wong et al. [106]	1.97	2.54	–	–	9.2	–	–
Ferrara et al. [114]	2	1.1	4.4	3	–	–	–
Wang and Hu [108]	3.5	4	7.5	–	–	–	–
Wang and Hu [109]	2	2.3	6.12	–	–	–	–
Wang and Hu [110]	3	2	7	–	–	–	–
Wang et al. [112]	1	2	5.2	–	–	–	–
Wang et al.[120]	0.19	1	4.57	–	9.01	–	–
Yang et al. [147]	0.32	0.64	4.57	–	9.9	–	–
Kho et al. [107]	0	0	2	–	4	–	–
Trivedi et al. [121]	1.2	2.1	–	–	–	–	–
Shahzad et al. [122]	0	0	1.63	7.35	4.69	–	–
Yang et al. [82]	1	2	4	–	11.00	–	–
Proposed method	0	0	0.99	6.00	3.01	1.42	7.86

TABLE 4.4: EER(%) comparison in the lost-key scenario under the original FVC protocol.

Cancelable fingerprint template design	FVC2002			FVC2004		FVC2006	
	DB1	DB2	DB3	DB1	DB2	DB2	DB3
Ferrara et al. [114]	3.3	1.8	7.8	6.3	–	0.3	–
Wang and Hu [110]	4	3	8.5	–	–	–	–
Yang et al. [147]	5.75	4.71	10.22	–	12	–	–
Kho et al. [107]	2.28	1.25	6.4	–	7	–	–
Shahzad et al. [122]	1.57	1.50	7.93	10.49	8.62	–	–
Proposed method	1.38	1.35	4.21	8.89	7.63	1.14	7.06

we follow the methodology provided in [148], [149]. Two types of score distributions, named mated and non-mated sample score distributions [148], need to be measured for the assessment of unlinkability. Mated sample scores refer to the scores computed by matching templates generated from the same impression of a finger using different keys. Non-mated sample scores are yielded by comparing templates generated from different fingers using different keys.

Gomez-Barrero et al. [148] proposed two measures of unlinkability: score-wise linkability $D_{\leftrightarrow}(s)$ and system overall linkability $D_{\leftrightarrow}^{sys}$. The score-wise linkability $D_{\leftrightarrow}(s) \in [0,1]$ measures the level of linkability of protected templates for each specific matching score s of mated and non-mated sample score distributions. Thus, for a specific score s, $D_{\leftrightarrow}(s) = 0$ means that both templates are

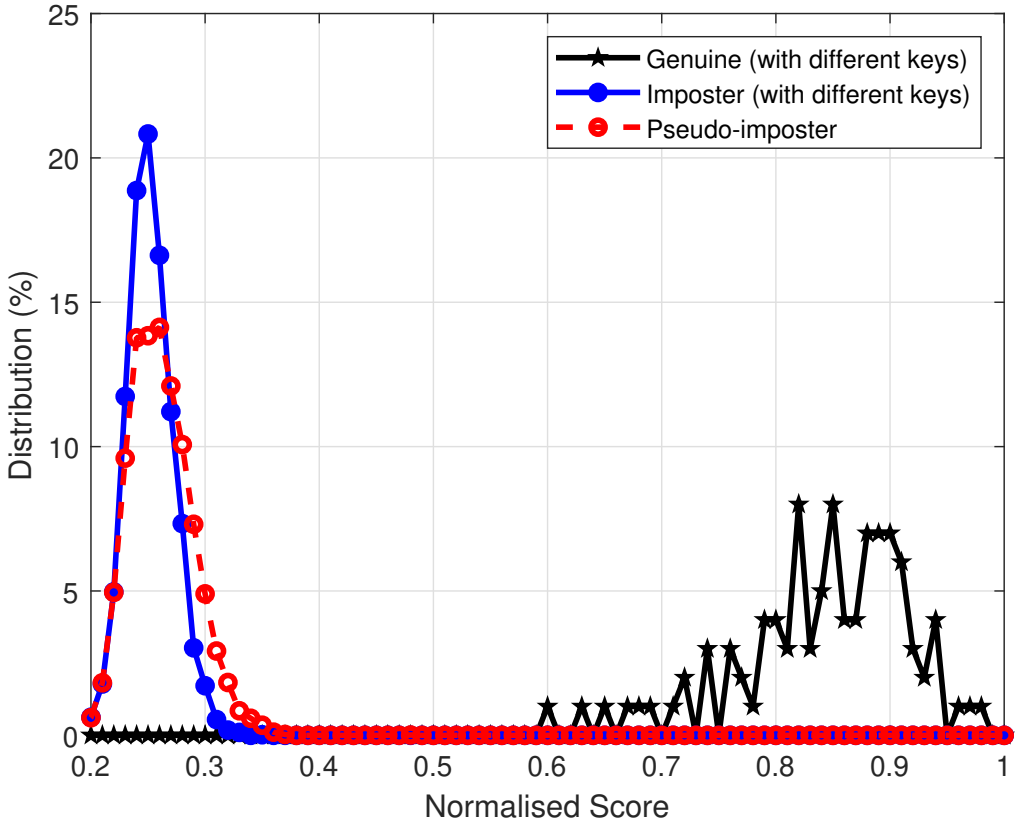

FIGURE 4.5: Genuine, pseudo-imposter and imposter distributions over FVC2002 DB2.

fully unlinkable, while $D_{\leftrightarrow}(s) = 1$ shows that both templates are fully linkable. Any intermediate values between 0 and 1 indicate the degree of linkability corresponding to specific matching scores. In contrast, the system overall linkability $D_{\leftrightarrow}^{sys} \in [0,1]$ provides an estimation of linkability for the entire system, independently of the scores. When $D_{\leftrightarrow}^{sys} = 0$ (or $D_{\leftrightarrow}^{sys} = 1$), the template protection system is fully unlinkable (or fully linkable).

To test unlinkability of the proposed cancelable templates, we produced 100 transformed templates of the first impression of each finger in FVC2002 DB2 with randomly generated user keys $\boldsymbol{k}$, with each key of length $L = 500$. The mated sample scores were obtained by matching each transformed template with 100 newly produced templates using different user keys, resulting in 10000 mated scores. On the other hand, 4950 non-mated sample scores were generated by comparing the transformed template of each finger with that of all other different fingers in FVC2002 DB2.

According to the unlinkability framework proposed by Gomez-Barrero et al. [148], the parameter ω controls the ratio between the prior probabilities of the mated

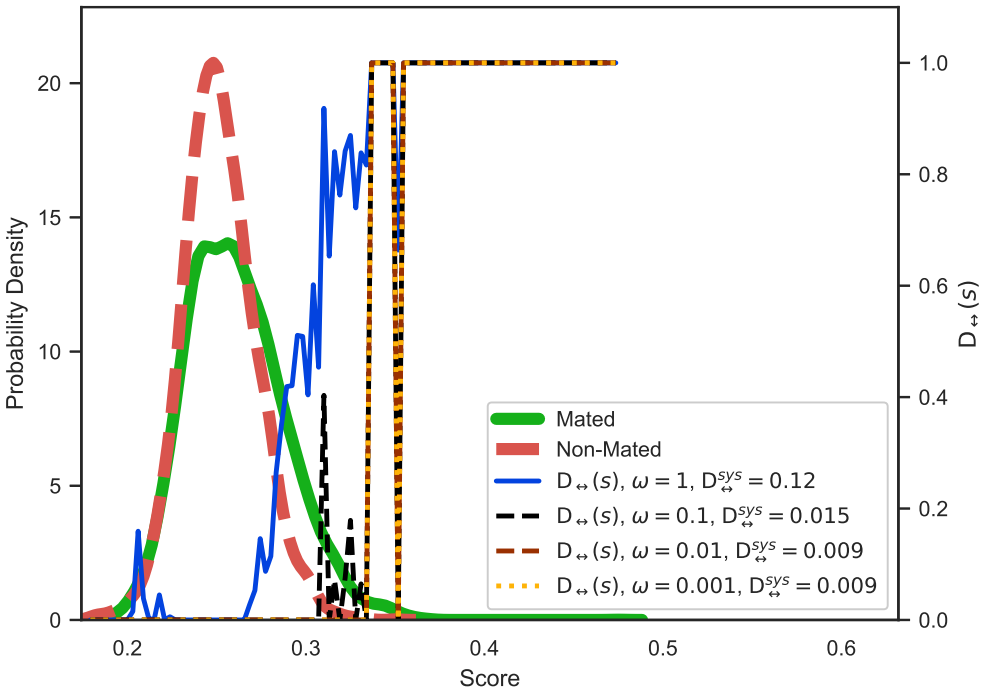

FIGURE 4.6: Unlinkability analysis of the proposed cancelable templates using mated and non-mated score distributions and different values of ω.

and non-mated sample distributions. If the prior probabilities are known, they should be used to calculate ω. Otherwise, it is assumed that mated and non-mated samples are equally probable, i.e., $\omega = 1$, which is the worst-case scenario in the unlinkability analysis. In the unlinkablity test of the proposed system, we set ω to four different values: $\omega = \{0.001, 0.01, 0.1, 1\}$. We plotted the mated and non-mated sample score distributions in Figure 4.6, where it is shown that both distributions have a substantial overlap. From Figure 4.6, we can also observe that a larger value of ω leads to a higher $D_{\leftrightarrow}(s)$ for each linkage score s, which in turn increases $D^{sys}_{\leftrightarrow}$. This is because when ω has a bigger value, it means that samples are more likely to come from mated instances than non-mated instances, increasing the probability of linking the two subjects. When $\omega = 1$, $D^{sys}_{\leftrightarrow}$ reaches its maximum value. It is clear from Figure 4.6 that $D^{sys}_{\leftrightarrow} = 0.12$ for $\omega = 1$, so the designed template protection system is almost fully unlinkable.

4.3.4 Security analysis

In this section, we conduct the security analysis of the proposed method. We first analyse how the non-invertibility requirement of cancelable biometrics is met. Then we evaluate whether the proposed cancelable templates can defend against revoked template attacks and masquerade attacks.

4.3.4.1 Non-invertibility analysis

Non-invertibility is a core requirement for cancelable biometrics as this property ensures the security of raw biometric data. The proposed method achieves non-invertibility through the Dyno-key model. The model dynamically extracts elements from $\boldsymbol{c}_m$ in (4.3) based on the randomly generated key $\boldsymbol{k}$ in (4.4) and then deletes the extracted elements, after performing the block-based XOR operation with $\boldsymbol{y}_m$ in (4.7). By this means, the Dyno-key model makes it hard for the adversary to restore the original MCC features $\mathbf{C}_m$ in (4.1) from the transformed vector $\boldsymbol{V}_m$ in (4.10). This is because to retrieve $\mathbf{C}_m$ in (4.1), or equivalently $\boldsymbol{y}_m$ in (4.7), the adversary needs to figure out the deleted or discarded elements, namely $\boldsymbol{r}_m$ in (4.6). Only when these elements are recovered can $\boldsymbol{y}_m$ be known. For example, if the discarded element in $\boldsymbol{r}_m$ is a 0 and the post-XOR bit in $\boldsymbol{V}_m$ is 1, then the corresponding bit in $\boldsymbol{y}_m$ should be 1. But if the discarded element in $\boldsymbol{r}_m$ is a 1 and the post-XOR bit in $\boldsymbol{V}_m$ is also 1, then the corresponding bit in $\boldsymbol{y}_m$ must be 0. We can see that the Dyno-key model increases uncertainty in two ways. Firstly, the block-based XOR operation creates more possibilities for the input to produce the same output. Secondly, entries in the vector $\boldsymbol{r}_m$ are dynamically selected by the random key $\boldsymbol{k}$ and are discarded afterwards, thus increasing the difficulty to recover them. Without finding out $\boldsymbol{r}_m$, the adversary cannot restore $\mathbf{C}_m$.

From the above analysis, we can see that it boils down to how difficult it is to work out $\boldsymbol{r}_m$. The MCC's cell values $\boldsymbol{c}_m$ in (4.3) contain more 0s than 1s. Moreover, the distribution of 0s and 1s in $\boldsymbol{c}_m$ is not uniform. For example, if the random key $\boldsymbol{k}$ is of length $L = 500$, assuming that there are 5% of 1s in $\boldsymbol{r}_m$, i.e., 25 bits, to find these 1s, the adversary has to make $\begin{pmatrix} 500 \\ 25 \end{pmatrix} = 1.0439 \times 10^{42} \approx 2^{140}$ attempts. As there are 30-60 minutiae in each fingerprint image and each minutia is represented with one $\mathbf{C}_m$, this results in a total of $2^{4200} (= 2^{140 \times 30})$ attempts to reconstruct all $\mathbf{C}_m$. Clearly, it is computationally infeasible. Therefore, the Dyno-key model transforms $\mathbf{C}_m$ in an irreversible manner.

4.3.4.2 Revoked template attacks

Since the proposed method allows the protected MCC templates to be revoked and re-issued, we assess if the renewed templates can resist attacks from adversaries using the revoked templates. We consider two attack scenarios [114]:

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

Each attack scenario was assessed at two different security levels [**2pmcc**]:

1. Medium security – the matching threshold is set to 0.1% FMR.
2. High security – the matching threshold is set to 0% FMR.

Both attack scenarios were tested over FVC2002 DB2. For the Type-I attack, there was a total of $800 (= 8 \times 100)$ revoked template attacks. For the Type-II attack, there were $2800 (= ((8 \times 7)/2) \times 100)$ attacks. Table 4.5 reports the percentage of successful attacks at both security levels. We can see from Table 4.5 that the proposed method can resist revoked template attacks.

TABLE 4.5: Percentage of successful revoked template attacks at medium and high security levels

Security level	Type-I attack	Type-II attack
Medium security	0%	0.1%
High security	0%	0%

4.3.4.3 Masquerade attacks

In masquerade attacks, the adversary forges a synthetic input which can be very similar to the actual template. We simulated masquerade attacks using a fake binary input that resembles the MCC binary vector $\mathbf{C}_m$ in (4.1). Specifically, with $\mathbf{C}_m$ of length $N = 1536$ in our experiments, we fabricated the synthetic input by randomly flipping a small number of bits, e.g., 20 bits, in $\mathbf{C}_m$. That is, a 0 bit becomes 1 and vice versa. By doing so, the fake input shares a lot of similarity with $\mathbf{C}_m$.

We assess the robustness of the proposed method against masquerade attacks under Type-I and Type-II attack scenarios at medium and high security levels

using FVC2002 DB2. The test results are reported in Table 4.6, where it is observed that the proposed method is robust enough against masquerade attacks, even when the synthetic input is very similar to $\mathbf{C}_m$; for example, it is only different in 20 (out of 1536) bits to $\mathbf{C}_m$, or 98.7% of bits are identical.

TABLE 4.6: Percentage of successful masquerade attacks at medium and high security levels

Bits different to $\mathbf{C}_m$	Medium security		High security	
	Type-I attack	Type-II attack	Type-I attack	Type-II attack
20	0.1%	0.07%	0%	0%
30	0.1%	0.07%	0%	0%
45	0%	0.04%	0%	0%

4.4 Chapter summary

In this chapter, we have described the design of alignment-free cancelable MCC-based templates, which hinge upon the Dyno-key model. Not only does the Dyno-key model transform original MCC feature vectors non-invertibly, it also offers revocability and unlinkability, while maintaining the satisfactory performance of MCC templates. The proposed method shows high recognition accuracy and outperforms the majority of the existing alignment-free cancelable fingerprint templates.

Chapter 5

A Two-Stage Feature Transformation-Based Fingerprint Authentication System for Privacy Protection in IoT

5.1 Introduction

The Internet of Things (IoT) is defined as a network of physical objects, such as cars, mobile phones and home appliances embedded with electronics, sensors and actuators. All objects in the IoT utilize the Internet to connect, communicate and exchange data with each other [124]. Using applications like smart healthcare monitoring device, medical practitioners can rely on IoT devices to evaluate their patients' health conditions [150]. Since IoT devices transfer information via an open channel (i.e., the Internet), security and privacy are challenging issues [151]. For example, unauthorised access to IoT devices may threaten the user's identity and data confidentiality. User authentication is key to providing reliable services between IoT users and devices, as well as preventing unauthorized access. A secure authentication system can ensure that the received data come from legitimate users and IoT devices [134].

Biometric-based authentication overcomes the disadvantages of traditional password-based authentication because biometric traits cannot be lost and do not require memorization. Biometric authentication is gaining popularity (e.g., using face ID or touch ID on iPhones). There are many biometric traits that can be utilized in biometric authentication, such as fingerprints, iris, face and palm prints. In

comparison with other biometrics, fingerprint-based authentication is highly reliable with well-developed feature extraction algorithms and remarkable recognition accuracy. For instance, a real-valued, fixed-length feature vector [152] extracted from the state-of-the-art Minutia Cylinder-Code (MCC) [117] shows a strong matching performance.

However, there is largely no protection for fingerprint data, stored as templates on IoT devices [134]. Furthermore, many IoT devices have resource constraints (e.g., limited computing capacity and battery life). To address these issues, in this chapter we propose a secure fingerprint authentication system that applies a two-stage feature transformation scheme. Specifically, a weight-based fusion mechanism is designed in the first stage, while the second stage is featured by a linear convolution-based transformation with element removal from the convolution output to increase security. The proposed method employs the real-valued, fixed-length MCC feature vectors presented in [152] as the input. The contributions of this chapter are highlighted as follows:

1. The proposed two-stage feature transformation scheme is innovative in that it enables our system to achieve superior recognition accuracy. As a prelude to the weight-based fusion in the first stage, a finite impulse response (FIR) high-pass filter is designed. FIR high-pass filters are known for their stability and denoising effect which helps preserve recognition accuracy.

2. The proposed system is best suited to user authentication on IoT devices due to its energy efficiency on savings in memory space and low computational costs. With recognition accuracy maintained, the cancelable fingerprint template can be designed to be smaller in size than the original real-valued, fixed-length feature vector, thus saving memory usage and matching time.

The rest of this chapter is organised as follows. Section 5.2 reviews the fixed-length MCC minutia descriptor. Section 5.3 details the proposed secure fingerprint authentication system. The experiment results are reported and discussed in Section 5.4. The summary is given in Section 5.5.

5.2 Review of the fixed-length MCC minutia descriptor

Jin et al. [152] proposed a generic point-to-string conversion framework for minutia representation based on kernel learning. This framework works on a fixed number of selected training samples and a projection matrix produced by kernels. As a result, a discriminative real-valued, fixed-length feature vector is obtained from the variable-sized MCC binary features.

We briefly review how to generate the real-valued, fixed-length feature vector [152]. The state-of-the-art MCC minutia descriptor is a 3D local structure [117], known as a 'cylinder'. First, a kernel matrix is computed using a kernel function with a number of selected MCC training samples. Then, a projection matrix $\mathbf{P}$ is generated from the kernel matrix. Based on the matching scores between the training samples of the query and the enrolled template, vector $\bar{\mathbf{v}}$ is obtained. Finally, the real-valued, fixed-length feature vector $\mathbf{x}$ can be computed by projecting $\bar{\mathbf{v}}$ using the projecting matrix $\mathbf{P}$:

$$\mathbf{x} = \bar{\mathbf{v}}\mathbf{P} \tag{5.1}$$

According to the results in [152], the matching performance of the kernel method is better than that of the MCC. However, the new fixed-length feature vector is phase-sensitive and insecure since there is no protection over it. To address this, we design a cancelable template and the proposed fingerprint authentication system is intended for privacy protection in IoT.

5.3 Proposed system

The proposed system builds upon the real-valued, fixed-length feature vector $\mathbf{x}$ in (5.1), which is deemed as the original feature vector to be protected. We develop a two-stage feature transformation scheme to generate a cancelable fingerprint template. In the first stage, a weight-based feature fusion mechanism produces a temporary feature vector by fusing an FIR high-pass filter with partial elements selected from the original feature vector through a random user key. In the second stage, the temporary feature vector is linearly convolved with the original feature vector and the resultant cancelable template is formed by

keeping part of the convolution output through another random user key. The proposed scheme comprises the following steps:

1. FIR high-pass filter design
2. Cancelable template generation
3. Fingerprint matching in the transformed domain

5.3.1 FIR high-pass filter design

FIR filters are basic but widely used filters. They are primarily used in digital communication (e.g., digital radio). An FIR filter acts as a signal conditioner where it accepts an input signal, blocks pre-specified frequency components, and passes to the output the original signal without the pre-specified frequency components [153]. A high-pass filter is a filter that allows only high frequency signals (below a specified cut-off frequency) through to its output and is used to eliminate low frequencies. The main characteristic of an FIR high-pass filter [154] is its stability and freedom from limit cycles that occur due to finite wordlength representations of multiple constants and signal values. An FIR high-pass filter can be designed easily to be of linear phase. This means that the filter will transmit all frequencies with the same level of delay without any phase distortion and the input signal will be delayed by a constant when it is transmitted to the output [154]. These properties are particularly useful for dealing with a phase-sensitive feature vector, such as the real-valued, fixed-length feature vector $\mathbf{x}$ in (5.1).

The first step in designing an FIR high-pass filter is to calculate the Fourier series coefficients c_{HP} and the finite series H_M of the filter, as shown in (5.2) and (5.3), respectively (see derivations in [154]).

$$c_{HP}(n) = \begin{cases} 1 - \dfrac{w_c}{\pi}, & n = 0 \\ -\dfrac{\sin(w_c n)}{\pi n}, & |n| > 0 \end{cases} \tag{5.2}$$

$$H_M(e^{jw}) = \sum_{n=-M}^{n=M} c_{HP}(n) e^{-jnw} \tag{5.3}$$

where the finite series of (5.3) contains $(2M+1)$ coefficients from $-M$ to M, as an approximation to the infinite series $\sum_{n=-\infty}^{n=\infty} c_{HP}(n) e^{-jnw}$.

Next, the filter contains oscillations, called ripples. A Hamming window $w_H(n)$ is used to reduce the effects of ripples.

Then, $c_{HP}(n)$ and $w_H(n)$ are multiplied to obtain $h_w(n)$.

Last, by delaying $h_w(n)$ by M samples to get $h(n)$ [i.e., $h_w(n-M) = h(n)$], a causal filter of finite length $N = 2M+1$ with coefficients $h(n)$ is obtained, where $n = 1, 2, ..., N$.

5.3.2 Cancelable template generation

In this section, we describe how the cancelable template is built.
Let $\mathbf{z} = [z(1), z(2), ..., z(d)]$ be the original real-valued, fixed-length feature vector, obtained in the same way as feature vector $\mathbf{x}$ in (5.1), so vector $\mathbf{z}$ contains the original MCC features that should be protected. We generate a random vector $\mathbf{r}$ of length n:

$$\mathbf{r} = [r_1, r_2, ..., r_n] \tag{5.4}$$

where $1 < n \leq d$, and the entries r_j of $\mathbf{r}$, for $j = 1, 2, \ldots, n$, are strictly positive integers with $r_i \neq r_k$ for all $i \neq k$. The random vector $\mathbf{r}$ works as an index vector to construct a new vector from vector $\mathbf{z}$. In other words, vector $\mathbf{r}$ is responsible for copying the elements in $\mathbf{z}$ that have the same indices as the value of r_j in $\mathbf{r}$, for $j = 1, 2, \ldots, n$. Thus, this yields a new vector $\mathbf{y}$ of length n, given by

$$\begin{aligned} \mathbf{y} &= [y(1), y(2), ..., y(n)] \\ &= [z(r_1), z(r_2), ..., z(r_n)] \end{aligned} \tag{5.5}$$

We now present the weight-based feature fusion mechanism. The mechanism utilizes a weight-based fusion between elements of vector $\mathbf{y}$ in (5.5) and the FIR high-pass filter coefficients $h(i), i = 1, 2, ..., n$ (see details of the FIR high-pass filter design in Section 5.3.1). The weight-based fusion, given by (5.6), produces vector $\mathbf{b} = [b(1), b(2), ..., b(n)]$, in which

$$b(i) = \alpha y(i) + (1-\alpha)h(i) \tag{5.6}$$

where α is a weighting factor and $0 \leq \alpha \leq 1$. Different $b(i)$ can be produced by adjusting α. To increase security, vector $\mathbf{y}$ is discarded after fusion. We then linearly convolve the fusion output (i.e., vector $\mathbf{b}$) with the real-valued, fixed-length feature vector $\mathbf{z}$. The linear convolution, expressed by (5.7), gives rise to

vector $\mathbf{w} = [w(1), w(2), ..., w(s)]$.

$$\mathbf{w} = \mathbf{z} \circledast \mathbf{b} \tag{5.7}$$

where $\circledast$ denotes the linear convolution operator. The length of vector $\mathbf{w}$ is $s = d + n - 1$.

Upon completion of the linear convolution and to further enhance security, a new user key $\mathbf{v} = [v_1, v_2, \cdots, v_t]$ is randomly generated with length t, where $n - 1 \leqslant t < s$. The entries v_j of $\mathbf{v}$, for $j = 1, 2, \ldots, t$, are strictly positive integers with $v_m \neq v_n$ for all $m \neq n$. Vector $\mathbf{v}$ is utilized to discard t elements from vector $\mathbf{w}$ that have the same indices as $v_j, j = 1, 2, ..., t$. The resultant vector $\mathbf{T}$ is obtained as

$$\mathbf{T} = [T_1, T_2, ..., T_k] \tag{5.8}$$

where k is the length of $\mathbf{T}$ and $k = s - t$. Deleting t elements from vector $\mathbf{w}$ heightens the security of the proposed authentication system, because the values of those discarded elements cannot be recovered. Moreover, the length k of the resultant vector $\mathbf{T}$ is shorter than the length d of the original (input) feature vector $\mathbf{z}$.

Remarks:

1. The stable characteristic and denoising effect of FIR high-pass filters plays a critical role in assisting the proposed system in achieving good recognition accuracy. Also, it is worth noting the flexibility of designing different high-pass filters by adjusting cut-off frequencies. A different filter produces a different resultant vector $\mathbf{T}$ (see the experiment results and analysis in Section 5.4.1).

2. Random vectors $\mathbf{r}$ and $\mathbf{v}$ act as parameter keys. Different $\mathbf{r}$ and $\mathbf{v}$ lead to different $\mathbf{T}$, making $\mathbf{T}$ a cancelable template.

3. The resultant cancelable template $\mathbf{T}$ can protect the original MCC features contained in vector $\mathbf{z}$. The protection is twofold. First, the original MCC features cannot be retrieved even if the stored (transformed) template $\mathbf{T}$ and the user-specific parameter keys $\mathbf{r}$ and $\mathbf{v}$ are acquired by an adversary. Second, if the stored template $\mathbf{T}$ is compromised, it can be replaced with a new one by simply changing the user keys. The new template is unrelated to the compromised template and can be made different from one application to another (see the unlinkability analysis in Section 5.4.4).

5.3.3 Fingerprint matching in the transformed domain

Biometric authentication consists of two stages, enrolment and verification. In the enrolment stage, by following the process presented in Section 5.3.2, a transformed feature vector is produced from the original real-valued, fixed-length feature vector. The transformed vector is stored on an IoT device as a template. In the verification stage, a transformed query feature vector is obtained by going through the same transformation procedure as in the enrolment stage. For clarity, we use superscript e to denote the template and superscript q to denote the query. The similarity score S between the template and the query is calculated in the transformed domain using the following equation adapted from Equation (32) in [152]:

$$S = \frac{\sum_{j=1}^{k}(T_j^e * T_j^q)}{\sum_{j=1}^{k}(T_j^e)^2 + \sum_{j=1}^{k}(T_j^q)^2} \tag{5.9}$$

where $*$ denotes element-wise multiplication.

5.4 Experiment results and analysis

The proposed authentication system is evaluated over six public fingerprint databases, namely FVC2002 DB1-DB3 [5] and FVC2004 DB1-DB3 [6]. Each of these databases contains 100 users with 8 impressions per user, so there are 800 $(= 100 \times 8)$ fingerprint images in total in each database. These databases contain fingerprint images with differing qualities. We designed our tests to assess whether the proposed system fulfils the requirements of cancelable biometrics (i.e., performance preservation, revocability and diversity, unlinkability and non-invertibility).

In the experiments, we adopted the real-valued, fixed-length feature vector (of length 299) proposed in [152] as the input to the proposed system. The performance measures used in our tests are the false acceptance rate (FAR), the false rejection rate (FRR) and equal error rate (ERR). Based on the method in [152], the 1^{st} to 3^{rd} samples of each finger served as the training samples to produce the fingerprint feature vectors; the remaining samples (i.e., 4^{th} to 8^{th}) of each finger were used in our experiments. The FVC protocol [113] was employed in our performance testing, resulting in 1000 genuine testing scores and 4950 imposter testing scores for each database.

5.4.1 Performance evaluation

The matching performance of the proposed system was evaluated under the lost-key scenario. This scenario is considered the worst case since the adversary knows the user's key. In these experiments, all users of a database were assigned the same FIR high-pass filter and the same user keys **r** and **v**. Figure 5.1 shows the matching performance of the proposed method for the FVC2002 DB1-DB3 and FVC2004 DB1-DB3 databases, where the parameters are set as $n = 29$, $w_c = \frac{\pi}{100}$, $\alpha = 0.2$ and $t = 50$. It can be seen from the receiver operating characteristic (ROC) curves in Figure 5.1 that the matching performance of the proposed system over the FVC2002 DB1-DB3 databases was higher than that over the FVC2004 DB1-DB3 databases due to the former's better image quality.

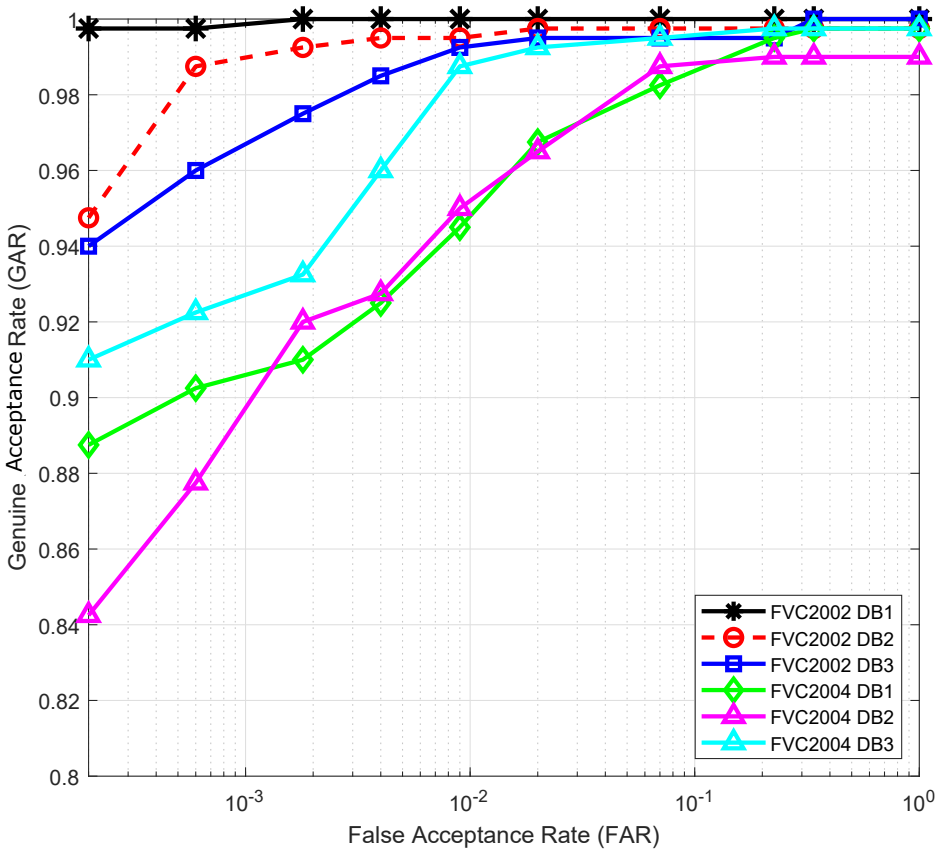

FIGURE 5.1: ROC curves for FVC2002 DB1-DB3, FVC2004 DB1-DB3 in the lost-key scenario under the FVC protocol.

5.4.1.1 Effects of different parameter settings

The proposed method is controlled by the following parameters: the FIR high-pass filter, the randomly generated keys **r** and **v**, and the weighting factor α. We analyse each parameter's effect on the matching performance. First, we compare the performance by setting the length n of **r** to 29, 49, 69, 89, and 299 with $w_c = \frac{\pi}{100}$, $\alpha = 0.2$ and $t = 50$. Table 5.1 shows that when the length n of **r** increases, the EER decreases throughout the majority of the databases, which indicates a performance improvement. Figure 5.2 illustrates the ROC curve for different lengths of user key **r** under the lost-key scenario.

TABLE 5.1: EER (%) of the proposed system when the length n of **r** varies (in this test, the FIR high-pass filter, α and **t** are fixed).

Key length n	**FVC2002**			**FVC2004**		
	DB1	DB2	DB3	DB1	DB2	DB3
Unprotected real-valued MCC	0.00	0.25	0.75	2.99	2.75	1.50
n=29	0.03	0.49	0.74	2.73	2.73	1.24
n=49	0.04	0.49	0.96	2.75	3.03	1.29
n=69	0.05	0.49	0.75	2.75	3.00	1.29
n=89	0.03	0.49	0.75	2.74	2.98	1.25
n=299	0.02	0.49	0.70	2.50	2.73	1.24

Next, the design of the FIR high-pass filter is controlled by two parameters: the filter length and the cut-off frequency w_c. The filter length must coincide with the length n of **r** so that the weight-based fusion mechanism can work. Therefore, we examined how w_c affects the matching performance. The parameters n, α and t were fixed to 29, 0.2 and 50, respectively. Table 5.2 shows that smaller values of w_c yield better performance than larger values. This is because when w_c is large, more values of the feature vector are filtered out.

Then we compared the matching performance by setting the length t of vector **v** to 28, 50, and 100 with $n = 29$, $\alpha = 0.2$ and $w_c = \frac{\pi}{100}$. Table 5.3 shows that smaller lengths of **v** yield better performance than larger lengths. The reason for this is that when the length t of **v** is large, more elements of the convolution output are deleted, causing more information loss.

Finally, we examined the matching performance using different values of the weighting factor α. The parameters w_c, n and t were fixed to $\frac{\pi}{100}$, 29 and 50, respectively. Table 5.4 shows that smaller values of α produce better performance

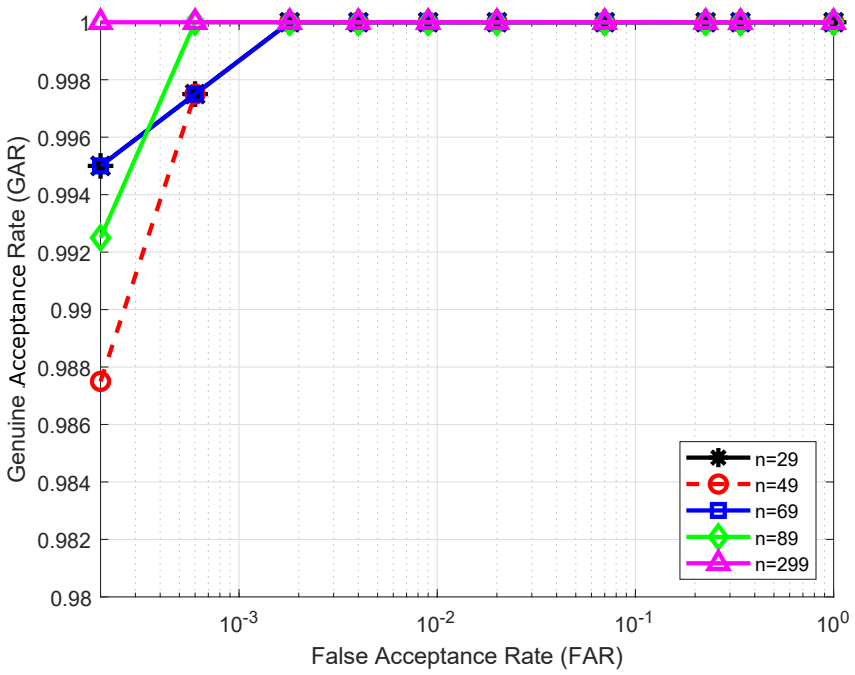

FIGURE 5.2: ROC curves for different lengths of user key **r** evaluated over FVC2002 DB1 in the lost-key scenario under the FVC protocol.

TABLE 5.2: EER (%) of the proposed system when the value of w_c varies (in this test, n, α and t are fixed).

Cut-off frequency w_c	**FVC2002**			**FVC2004**		
	DB1	DB2	DB3	DB1	DB2	DB3
Unprotected real-valued MCC	0.00	0.25	0.75	2.99	2.75	1.50
$w_c = \frac{\pi}{100}$	0.03	0.49	0.74	2.73	2.73	1.24
$w_c = \frac{\pi}{10}$	0.20	0.50	0.93	3.49	3.49	1.49
$w_c = \frac{3\pi}{10}$	0.26	0.73	1.57	3.24	4.01	2.23
$w_c = \frac{5\pi}{10}$	0.52	0.99	2.49	4.21	5.72	2.98

than larger values of α. In other words, when more weight is given to vector **y** than to filter coefficients, recognition accuracy improves. This makes sense because vector **y** contains part of the original feature vector **z**.

TABLE 5.3: EER (%) of the proposed system when the length t of $\mathbf{v}$ varies (in this test, the FIR high-pass filter, α and n are fixed).

Key length t	**FVC2002**			**FVC2004**		
	DB1	DB2	DB3	DB1	DB2	DB3
Unprotected real-valued MCC	0.00	0.25	0.75	2.99	2.75	1.50
$t = 28$	0.00	0.50	0.75	2.75	2.75	1.04
$t = 50$	0.03	0.49	0.74	2.73	2.73	1.24
$t = 100$	0.26	0.75	1.19	2.97	3.50	1.95

TABLE 5.4: EER (%) of the proposed system with different α values (in this test, the FIR high-pass filter and $\mathbf{r}$ and $\mathbf{v}$ are fixed).

Weight-based fusion mechanism	**FVC2002**			**FVC2004**		
	DB1	DB2	DB3	DB1	DB2	DB3
Unprotected real-valued MCC	0.00	0.25	0.75	2.99	2.75	1.50
$\alpha = 0.1$	0.03	0.49	0.74	2.70	2.74	1.31
$\alpha = 0.2$	0.03	0.49	0.74	2.73	2.73	1.24
$\alpha = 0.3$	0.06	0.49	0.76	2.74	2.99	1.37
$\alpha = 0.5$	0.06	0.49	0.75	2.73	3.01	1.36

5.4.1.2 Comparison with existing cancelable fingerprint templates

Table 5.5 depicts the EER comparison between the proposed system and state-of-the-art cancelable fingerprint templates under the lost-key scenario. It is clear from Table 5.5 that the proposed method outperforms the majority of the existing cancelable templates under the FVC protocol, except for being slightly inferior to [89] over the FVC2002 DB2 database and to [94] over the FVC2004 DB1 database.

5.4.2 Analysis of memory and computational cost savings

In this section, we present two reasons why the proposed scheme demonstrates energy efficiency and low computational costs for IoT devices. First, it uses the fixed-length feature vector extracted from MCC. The fixed-length feature vector only uses a very low amount of memory, as each fingerprint image is represented by only one fixed-length vector, unlike other feature representation methods (e.g., MCC) that have a variable number of local feature vectors for each fingerprint image. For example, if there is an average of N minutiae in a fingerprint image, the MCC will create N local feature vectors. By contrast, in

TABLE 5.5: EER (%) comparison in the lost-key scenario under the FVC protocol.

Cancelable fingerprint template design	**FVC2002**			**FVC2004**		
	DB1	DB2	DB3	DB1	DB2	DB3
Wang and Hu [110]	4	3	8.5	-	-	-
Ferrara et al. [113]	3.33	1.76	7.78	-	-	-
Jin et al. [89]	0.22	**0.47**	3.07	4.74	4.10	3.99
Kim et al. [91]	0.55	0.93	-	5.81	6.85	-
Abdullahi et al. [94]	0.36	0.54	2.40	**2.35**	5.93	2.37
Shahzad et al. [122]	1.57	1.50	7.93	10.49	8.62	-
Proposed method ($n = 29$, $w_c = \frac{\pi}{100}$, $\alpha = 0.2$ and $t = 50$)	**0.03**	0.49	**0.74**	2.73	**2.73**	**1.24**

the proposed system, only one feature vector (i.e., the cancelable template $\mathbf{T}$) is generated.

Second, the proposed system shortens the length of the original feature vector $\mathbf{z}$ from d to k. For example, with user keys $\mathbf{r}$ and $\mathbf{v}$, if we set their lengths to $n = 29$ and $t = 50$, then the transformed template $\mathbf{T}$ is of length 277, which is less than the length of the original feature vector (i.e., $d = 299$). Therefore, the computational cost of the fingerprint matching process on IoT devices will decrease due to the reduced template size. For instance, the running time of matching a transformed template $\mathbf{T}^e$ and a transformed query $\mathbf{T}^q$ of length $k = 277$ is about 6.6×10^{-6} second, while the running time of matching an original template vector $\mathbf{z}^e$ and an original query vector $\mathbf{z}^q$ of length $d = 299$ is about 1.07×10^{-5} second. The above results were obtained by running MATLAB on a computer with a 3.41 GHz Intel (R) Core (TM) i7-6700 CPU.

5.4.3 Revocability and diversity

Revocability and diversity are essential properties for designing a secure authentication system. When a stored template is compromised, a new template should be generated by simply changing the user key. The new template should be unrelated to the compromised template. To evaluate the revocability and diversity of the proposed method, we generated 100 transformed templates from the first impression of each finger in FVC2002 DB2 by randomly producing different user keys $\mathbf{r}$ and $\mathbf{v}$. These pseudo-imposter templates were then matched

against the original. Figure 5.3 shows the genuine, pseudo-imposter and imposter distributions. The pseudo-imposter and imposter distributions can be seen to overlap. The mean and standard derivation of the pseudo-imposter distribution are 0.4481 and 0.0546, respectively, compared with 0.4479 (mean) and 0.0580 (standard derivation) of the imposter distribution.

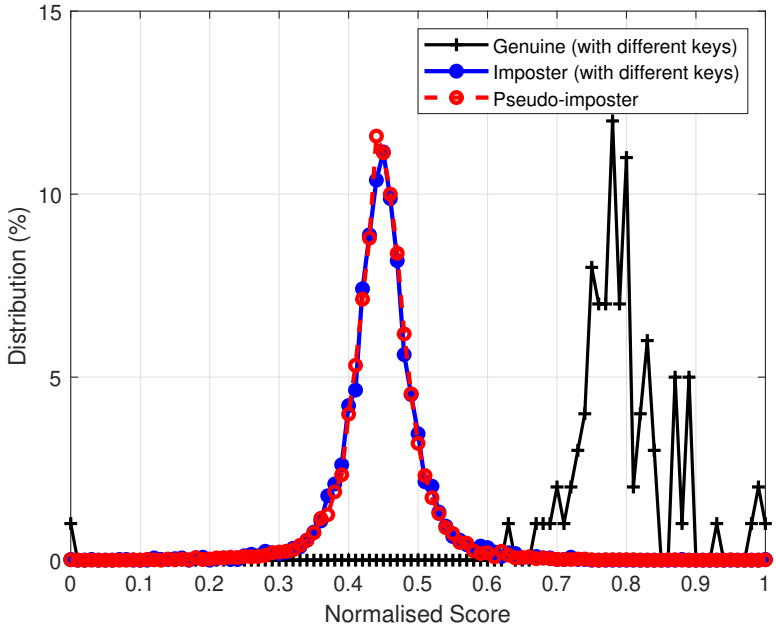

FIGURE 5.3: Genuine, imposter and pseudo-imposter distributions over FVC2002 DB2.

5.4.4 Unlinkability

Unlinkability is another fundamental property of a secure authentication system. This property requires that the generated templates of the same fingerprint in different applications cannot be cross-matched. To assess the level of linkability of the proposed method, we follow the methodology in [148]. In this framework, there are two types of score distributions that must be determined: mated and non-mated sample score distributions. Mated sample scores are defined as the scores extracted from comparisons of templates produced from the same impression of a finger using different keys. In contrast, non-mated scores are the scores calculated from matching templates generated from different fingers using different keys.

According to [148], there are two measures of unlinkability, score-wise linkability $D_{\leftrightarrow}(s)$ and system overall linkability $D_{\leftrightarrow}^{sys}$. The score-wise linkability

$D_{\leftrightarrow}(s) \in [0,1]$ measures the amount of linkability of protected templates for each specific matching score s of mated and non-mated sample score distributions. Therefore, for a specific score s, if $D_{\leftrightarrow}(s) = 0$, two templates are considered fully unlinkable, whereas if $D_{\leftrightarrow}(s) = 1$, two templates are considered fully linkable. Values between 0 and 1 indicate a certain level of linkability. The system's overall linkability $D_{\leftrightarrow}^{sys} \in [0,1]$ estimates the level of linkability for the whole system independent of matching scores. If $D_{\leftrightarrow}^{sys} = 0$ (or $D_{\leftrightarrow}^{sys} = 1$), the template protection system is fully unlinkable (or fully linkable).

To evaluate the unlinkability of the proposed system, we generated 100 transformed templates of the first impression of each finger in FVC2002 DB2 with randomly generated user keys $\mathbf{r}$ and $\mathbf{v}$. The mated scores were determined by comparing each transformed template with the 100 newly generated templates using different user keys, resulting in 10000 mated scores. The non-mated scores were obtained by matching the transformed template of each finger with all other different fingers in FVC2002 DB2, producing 4950 non-mated scores. The mated and non-mated sample score distributions are plotted in Figure 5.4, showing that the two score distributions mostly overlap with $D_{\leftrightarrow}^{sys} = 0.02$. Therefore, the designed authentication system is almost fully unlinkable.

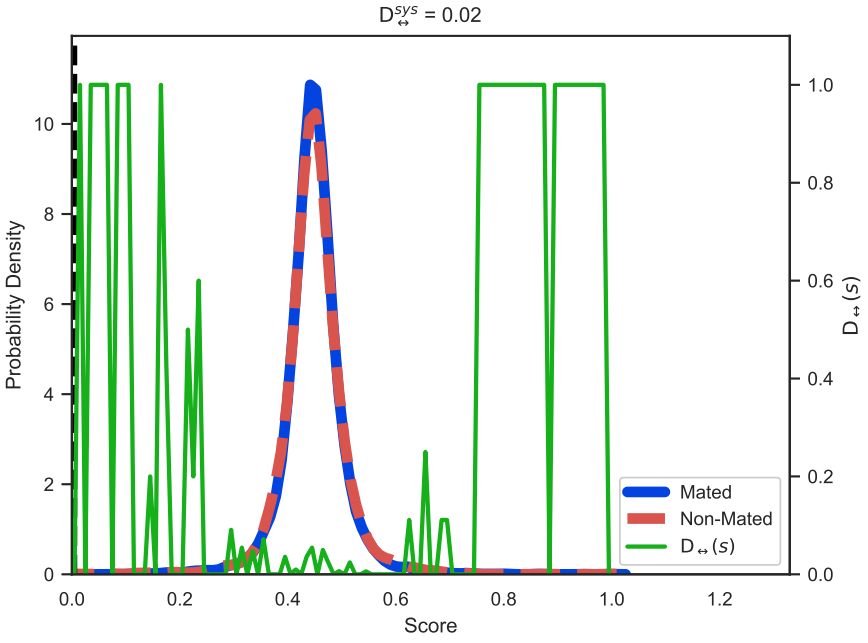

FIGURE 5.4: Unlinkability analysis of the proposed authentication system using mated and non-mated scores distributions.

5.4.5 Security analysis

In this section, the security analysis of the proposed authentication system is carried out by analysing non-invertibility first. Then, the ability of the proposed system to defend revoked template attacks and masquerade attacks is evaluated.

5.4.5.1 Non-invertibility analysis

Non-invertibility is a main requirement for secure authentication systems. It can be defined as the computational difficulty of restoring raw biometric data. The proposed system accomplishes non-invertibility through a two-stage feature transformation scheme: a weight-based feature fusion mechanism in the first stage and a linear convolution-based transformation with element removal in the second stage. The feature transformation in the proposed method is represented by Equations (5.5) to (5.8) in Section 5.3.2.

We analyze the worst-case scenario, where an adversary is able to compromise the stored template $\mathbf{T}$, the two user keys $\mathbf{r}$ and $\mathbf{v}$, the designed FIR high-pass filter and the transformation method. Even though the adversary has all this information, it is difficult to retrieve the original feature vector $\mathbf{z}$, as he/she needs to reverse the transformation method in sequence from Equations (5.8) to (5.5) to retrieve $\mathbf{z}$. Given that $\mathbf{T}$ is compromised, according to (5.7), the attacker needs to figure out $\mathbf{w}$ and $\mathbf{b}$. To get $\mathbf{w}$, the attacker has to guess the deleted t elements. To obtain $\mathbf{b}$, as the FIR high-pass filter and $\mathbf{r}$ are known to the attacker, from (5.6), the attacker must work out $\mathbf{y}$, which contains n elements selected from $\mathbf{z}$. Therefore, the adversary has to figure out the selected elements, namely $\mathbf{y}$ in (5.5) and the randomly deleted elements in $\mathbf{w}$. Only when these elements are recovered can $\mathbf{z}$ be known. Since the selected elements in vector $\mathbf{y}$ and the deleted elements from vector $\mathbf{w}$ are not stored, recovering them is infeasible. Therefore, the designed authentication system transforms the original feature vector $\mathbf{z}$ in an irreversible manner.

5.4.5.2 Revoked template attacks

We assess whether the proposed system can defeat attacks from adversaries using a revoked template. In our experiment, two attack scenarios are considered [114]:

- *Type-I attack*: A compromised template is utilized to attack a system containing a renewed template generated from the same impression.

TABLE 5.6: Percentage of successful masquerade attacks at medium and high security levels.

Number of elements changed in **z**	Medium security		High security	
	Type-I attack	Type-II attack	Type-I attack	Type-II attack
10	0.2%	0.1%	0%	0%
20	0.2%	0.1%	0%	0%
30	0.2%	0.1%	0%	0%

- *Type-II attack*: A compromised template is utilized to attack a system containing a renewed template generated from another impression of the same finger.

There are two different levels of security to evaluate each attack scenario [114]:

1. Medium security: The matching threshold is set to 0.1% FAR.
2. High security: The matching threshold is set to 0% FAR.

We tested both attack scenarios on FVC2002 DB2. There are, in total, 500 ($= 100 \times 5$) Type-I attacks, and there are $1000 (= (5 \times 4)/2) \times 100)$ Type-II attacks. The test results show that the percentage of successful attacks for medium and high security levels is 0% for Type-I attacks and 0.1% for Type-II attacks, respectively. Therefore, the proposed method can resist revoked template attacks.

5.4.5.3 Masquerade attacks

Masquerade attacks occur when an adversary fakes a synthetic input that is very similar to the actual template. To perform masquerade attacks, we produced a fake real-valued input similar to the feature vector **z**. The fabricated input with length 299 was generated by randomly selecting a small number of elements (e.g., 20 elements) from the original feature vector **z** and replacing their values with different numbers but close to the original ones, thus making the fake input similar to **z**.

The robustness of the proposed system against masquerade attacks was evaluated under Type-I and Type-II attack scenarios at medium and high security levels using FVC2002 DB2. Table 5.6 reports the test results of the masquerade attacks. The results in Table 5.6 demonstrate that the proposed method is robust enough against masquerade attacks.

5.5 Chapter summary

In this chapter, we have proposed a secure fingerprint authentication system for user privacy protection on IoT devices. The proposed system applies a two-stage feature transformation scheme, in which a weight-based fusion mechanism is developed in the first stage, while in the second stage, we design a linear convolution-based transformation with some elements removed from the convolution output to increase security. The proposed fingerprint authentication system satisfies all the requirements of cancelable biometrics (i.e., accuracy, revocability and diversity, unlinkability and non-invertibility). The experiment results on six public fingerprint databases demonstrate the highly competitive performance of the proposed system, when compared with the existing cancelable fingerprint templates. Moreover, its efficiency in terms of saving memory space and reducing computational costs makes the proposed system suitable for resource-constrained IoT devices.

Chapter 6

Conclusion and Future Directions

6.1 Summary of the thesis chapters

Fingerprint authentication systems are widely utilised in various applications and dominate the biometric security market. However, fingerprint authentication over the encrypted domain is still a challenge due to the nature of biometric uncertainty presented at each fingerprint image during acquisition. Despite a variety of approaches to detect deformations in fingerprint images, there is currently no method available for capturing minutiae variations between two impressions of the same finger in a unified model. This thesis presented a unique unified model to represent minutiae variations between fingerprint scans and formulate the changes to minutiae feature patterns. Another fundamental objective of this thesis was to develop a new non-invertible fingerprint template protection method in the form of cancelable templates. Since many existing cancelable template methods are unable to withstand several security threats, such as attacks via record multiplicity, masquerade attacks and pre-image attacks, this thesis presented a novel scheme for cancelable templates with the aim of achieving in-built security against all or some of these security attacks while attaining good recognition performances. The third objective of this thesis was to design a secure fingerprint authentication system which is suitable for resource-constrained IoT devices.

The main research contributions of this thesis are summarised as follows:

A Möbius Transformation-Based Model for Fingerprint Minutiae Variations

In Chapter 3, we proposed a unified model to represent minutiae variations between fingerprint scans and formulate the changes to minutiae feature patterns. We identified the Möbius transformation as a suitable candidate for modelling

minutiae translation, rotation and non-linear distortion, where different types of minutiae variations are described in a single model. Not only do we mathematically prove that the Möbius transformation-based model is a unified model for capturing minutiae variations, we also experimentally verified the effectiveness of this model using a public database.

Design of Cancelable MCC-Based Fingerprint Templates Using Dyno-Key Model

The second scheme for cancelable fingerprint templates was proposed in Chapter 4. The core component of our design was to dynamically randomise key models, called the Dyno-key model. The Dyno-key model dynamically extracted elements from MCC's binary feature vectors based on randomly generated keys. These extracted elements are discarded after the block-based logic operations to enhance security levels. Leveling with the performance of the unprotected, reproduced MCC templates, the proposed method exhibited competitive performance in comparison with state-of-the-art cancelable fingerprint templates, as evaluated over seven public databases, FVC2002 DB1-DB3, FVC2004 DB1 and DB2, and FVC2006 DB2 and DB3. The proposed cancelable MCC-based templates satisfied all the requirements of biometric template protection.

A Two-Stage Feature Transformation-Based Fingerprint Authentication System for Privacy Protection in IoT

The significant and rapid development of the Internet of Things (IoT) in recent years has greatly benefited everyday activities. However, there are serious security and privacy concerns that need to be addressed when using the IoT for distributed authentication.

In Chapter 5, a secure fingerprint authentication system to protect user privacy for authentication on IoT devices is presented. The proposed system applied a two-stage feature transformation scheme. Specifically, a weight-based fusion mechanism is designed in the first stage, while the second stage is featured by a linear convolution-based transformation with element removal from the convolution output to increase security and protection. The proposed authentication system satisfied all the requirements of cancelable biometrics: accuracy, revocability and diversity, unlinkability and non-invertibility. Evaluated over six public fingerprint databases, the proposed authentication system exhibited highly

competitive performance when compared with the existing cancelable fingerprint templates. Moreover, its energy-efficient storage and low computational costs made the proposed scheme a good fit for resource-constrained IoT devices.

6.2 Future research directions

Despite the contributions of this thesis, from modelling minutiae variations to proposing new non-invertible transformation methods for secure fingerprint authentication with applications in the IoT, some aspects can be further explored and extended for a more secure fingerprint authentication system. Therefore, we devote this section to identifying various perspectives and possible future research directions.

1. The proposed unified model is based on using Möbius transformation to analyse and construct minutia-based local feature structures. However, in future work, we will continue to improve this model and investigate how to efficiently apply it to enhance the quality and accuracy of minutia extraction in modern-day fingerprint-based biometric applications, e.g., e-passports, mobile device authentication and mobile healthcare data protection.

2. The MCC representation is built with rich or even redundant information in terms of the spatial and directional relationships between each reference minutia and its neighbouring minutiae. It is this 'redundancy' that causes the Dyno-key model to work effectively in the design of cancelable MCC-based templates. For future work, we will investigate how to better use the silent information in the MCC representation in the development of suitable non-invertible transformations, thus further improving the matching performance.

3. In relation to the use of biometric authentication systems to preserve the privacy and security of the IoT, we designed a secure fingerprint authentication system that can protect IoT devices. Our proposed method can resist many attacks such as revoked template attacks and masquerade attacks while maintaining high recognition accuracy. However, it is necessary to explore how to design lightweight and robust biometric authentication schemes suitable for the IoT environment.

Bibliography

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

[2] 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.

[3] N. Sulaiman and Q. Tajul Ariffin, "Overview on fingerprinting authentication technology," *InECCE2019*, pp. 451–462, 2020.

[4] M. M. Ali, V. H. Mahale, P. Yannawar, and A. Gaikwad, "Overview of fingerprint recognition system," *International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT)*, pp. 1334–1338, 2016.

[5] *Fingerprint verification competition*, http://bias.csr.unibo.it/fvc2002/, 2002.

[6] *Fingerprint verification competition*, http://bias.csr.unibo.it/fvc2004/, 2004.

[7] *"fingerprint verification competition"*, http://bias.csr.unibo.it/fvc2006/, 2006.

[8] *Neurotechnology, verifinger sdk*, (http://www.neurotechnology.com/megamatcher.html).

[9] F. L. Bookstein, "Principal warps: Thin-plate splines and the decomposition of deformations," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 11, no. 6, pp. 567–585, 1989.

[10] N. K. Ratha, K. Karu, S. Chen, and A. K. Jain, "A real-time matching system for large fingerprint databases," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 18, no. 8, pp. 799–813, 1996.

[11] A. M. Bazen and S. H. Gerez, "Elastic minutiae matching by means of thin-plate spline models," *Object Recognition Supported by User Interaction for Service Robots*, vol. 2, pp. 985–988, 2002.

[12] A. M. Bazen and S. H. Gerez, "Fingerprint matching by thin-plate spline modelling of elastic deformations," *Pattern Recognition*, vol. 36, no. 8, pp. 1859–1867, 2003.

[13] R. M. Bolle *et al.*, *System and method for distortion control in live-scan inkless fingerprint images*, US Patent 6,064,753, May 2000.

[14] Y. Fujii, *Detection of fingerprint distortion by deformation of elastic film or displacement of transparent board*, US Patent 7,660,447, Feb. 2010.

[15] A. Ross, S. Dass, and A. Jain, "A deformable model for fingerprint matching," *Pattern Recognition*, vol. 38, no. 1, pp. 95–103, 2005.

[16] A. Ross, S. C. Dass, and A. K. Jain, "Fingerprint warping using ridge curve correspondences," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 28, no. 1, pp. 19–30, 2005.

[17] C. Dorai, N. K. Ratha, and R. M. Bolle, "Dynamic behavior analysis in compressed fingerprint videos," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 14, no. 1, pp. 58–73, 2004.

[18] R. Cappelli, D. Maio, and D. Maltoni, "Modelling plastic distortion in fingerprint images," *International Conference on Advances in Pattern Recognition*, pp. 371–378, 2001.

[19] X. Chen, J. Tian, and X. Yang, "A new algorithm for distorted fingerprints matching based on normalized fuzzy similarity measure," *IEEE Transactions on Image Processing*, vol. 15, no. 3, pp. 767–776, 2006.

[20] 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.

[21] M. Sandhya and M. V. Prasad, "Biometric template protection: A systematic literature review of approaches and modalities," *Biometric Security and Privacy*, pp. 323–370, 2017.

[22] 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.

[23] C. Soutar, D. Roberge, A. Stoianov, R. Gilroy, and B. V. Kumar, "Biometric encryption: Enrollment and verification procedures," *Optical Pattern Recognition IX*, vol. 3386, pp. 24–35, 1998.

[24] A. Juels and M. Wattenberg, "A fuzzy commitment scheme," *Proceedings of the 6th ACM Conference on Computer and Communications Security*, pp. 28–36, 1999.

[25] V. V. T. Tong, H. Sibert, J. Lecoeur, and M. Girault, "Biometric fuzzy extractors made practical: A proposal based on fingercodes," *International Conference on Biometrics*, pp. 604–613, 2007.

[26] A. K. Jain, S. Prabhakar, L. Hong, and S. Pankanti, "Filterbank-based fingerprint matching," *IEEE Transactions on Image Processing*, vol. 9, no. 5, pp. 846–859, 2000.

[27] 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.

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

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

[30] U. Uludag, S. Pankanti, and A. K. Jain, "Fuzzy vault for fingerprints," *International Conference on Audio-and Video-Based Biometric Person Authentication*, pp. 310–319, 2005.

[31] U. Uludag and A. Jain, "Securing fingerprint template: Fuzzy vault with helper data," *2006 Conference on Computer Vision and Pattern Recognition Workshop (CVPRW'06)*, pp. 163–163, 2006.

[32] 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.

[33] A. Nagar, K. Nandakumar, and A. K. Jain, "Securing fingerprint template: Fuzzy vault with minutiae descriptors," *19th International Conference on Pattern Recognition*, pp. 1–4, 2008.

[34] A. K. Jain, K. Nandakumar, and A. Nagar, "Biometric template security," *EURASIP Journal on Advances in Signal Processing*, vol. 2008, pp. 1–17, 2008.

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

[36] C. Vielhauer, R. Steinmetz, and A. Mayerhofer, "Biometric hash based on statistical features of online signatures," *Object Recognition Supported by User Interaction for Service Robots*, vol. 1, pp. 123–126, 2002.

[37] Y. Dodis, R. Ostrovsky, L. Reyzin, and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," *SIAM Journal on Computing*, vol. 38, no. 1, pp. 97–139, 2008.

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

[39] S. V. Gaddam and M. Lal, "Efficient cancelable biometric key generation scheme for cryptography.," *Int. J. Netw. Secur.*, vol. 11, no. 2, pp. 61–69, 2010.

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

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

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

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

[44] C. Rathgeb and A. Uhl, "Context-based biometric key generation for iris," *IET Computer Vision*, vol. 5, no. 6, pp. 389–397, 2011.

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

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

[47] A. B. Teoh and D. C. Ngo, "Biophasor: Token supplemented cancellable biometrics," *9th International Conference on Control, Automation, Robotics and Vision*, pp. 1–5, 2006.

[48] 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.

[49] A. B. J. Teoh and L.-Y. Chong, "Secure speech template protection in speaker verification system," *Speech Communication*, vol. 52, no. 2, pp. 150–163, 2010.

[50] W. J. Wong, M. D. Wong, and A. B. J. Teoh, "A security-and privacy-driven hybrid biometric template protection technique," *International Conference on Electronics, Information and Communications (ICEIC)*, pp. 1–5, 2014.

[51] Y. C. Feng, P. C. Yuen, and A. K. Jain, "A hybrid approach for generating secure and discriminating face template," *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 1, pp. 103–117, 2009.

[52] A. Nagar, K. Nandakumar, and A. K. Jain, "A hybrid biometric cryptosystem for securing fingerprint minutiae templates," *Pattern Recognition Letters*, vol. 31, no. 8, pp. 733–741, 2010.

[53] M. Sandhya and M. V. Prasad, "Cancelable fingerprint cryptosystem based on convolution coding," *Advances in Signal Processing and Intelligent Recognition Systems*, pp. 145–157, 2016.

[54] T. Kim, Y. Oh, and H. Kim, "Efficient privacy-preserving fingerprint-based authentication system using fully homomorphic encryption," *Security and Communication Networks*, vol. 2020, 2020.

[55] M. Barni *et al.*, "Privacy-preserving fingercode authentication," *Proceedings of the 12th ACM Workshop on Multimedia and security*, pp. 231–240, 2010.

[56] W. Zhang and Y. Wang, "Singular point detection in fingerprint image," *The 5th Asian Conference on Computer Vision*, pp. 23–25, 2002.

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

[58] J. Zhou, F. Chen, and J. Gu, "A novel algorithm for detecting singular points from fingerprint images," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 31, no. 7, pp. 1239–1250, 2008.

[59] H. K. Lam, Z. Hou, W.-Y. Yau, T. P. Chen, and J. Li, "A systematic topological method for fingerprint singular point detection," *10th International Conference on Control, Automation, Robotics and Vision*, pp. 967–972, 2008.

[60] L. Pang, J. Chen, F. Guo, Z. Cao, E. Liu, and H. Zhao, "Rose: Real one-stage effort to detect the fingerprint singular point based on multi-scale spatial attention," *Signal, Image and Video Processing*, vol. 16, no. 3, pp. 669–676, 2022.

[61] K. Nandakumar and A. K. Jain, "Biometric template protection: Bridging the performance gap between theory and practice," *IEEE Signal Processing Magazine*, vol. 32, no. 5, pp. 88–100, 2015.

[62] 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.

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

[64] 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.

[65] D. Ahn, S. G. Kong, Y.-S. Chung, and K. Y. Moon, "Matching with secure fingerprint templates using non-invertible transform," *Congress on Image and Signal Processing*, vol. 2, pp. 29–33, 2008.

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

[67] B. Yang, C. Busch, P. Bours, and D. Gafurov, "Robust minutiae hash for fingerprint template protection," *Media Forensics and Security II*, vol. 7541, pp. 274–282, 2010.

[68] W. Yang, J. Hu, S. Wang, and J. Yang, "Cancelable fingerprint templates with Delaunay triangle-based local structures," *International Symposium on Cyberspace Safety and Security*, pp. 81–91, 2013.

[69] M. Sandhya, M. V. Prasad, and R. R. Chillarige, "Generating cancellable fingerprint templates based on Delaunay triangle feature set construction," *IET Biometrics*, vol. 5, no. 2, pp. 131–139, 2016.

[70] G. Li, B. Yang, C. Rathgeb, and C. Busch, "Towards generating protected fingerprint templates based on bloom filters," *3rd International Workshop on Biometrics and Forensics*, pp. 1–6, 2015.

[71] N. Abe, S. Yamada, and T. Shinzaki, "Irreversible fingerprint template using minutiae relation code with bloom filter," *IEEE 7th International Conference on Biometrics Theory, Applications and Systems (BTAS)*, pp. 1–7, 2015.

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

[73] K. Takahashi and S. H. Hitachi, "Generating provably secure cancelable fingerprint templates based on correlation-invariant random filtering," *IEEE 3rd International Conference on Biometrics: Theory, Applications, and Systems*, pp. 1–6, 2009.

[74] Q. N. Tran and J. Hu, "A multi-filter fingerprint matching framework for cancelable template design," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 2926–2940, 2021.

[75] 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.

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

[77] 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.

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

[79] 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.

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

[81] 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.

[82] W. Yang, S. Wang, M. Shahzad, and W. Zhou, "A cancelable biometric authentication system based on feature-adaptive random projection," *Journal of Information Security and Applications*, vol. 58, p. 102 704, 2021.

[83] B. Alam, Z. Jin, W.-S. Yap, and B.-M. Goi, "An alignment-free cancelable fingerprint template for bio-cryptosystems," *Journal of Network and Computer Applications*, vol. 115, pp. 20–32, 2018.

[84] Y. Sutcu, H. T. Sencar, and N. Memon, "A secure biometric authentication scheme based on robust hashing," *Proceedings of the 7th Workshop on Multimedia and Security*, pp. 111–116, 2005.

[85] 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.

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

[87] 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.

[88] Z. Jin, Y.-L. Lai, J.-Y. Hwang, S. Kim, and A. B. J. Teoh, "A new and practical design of cancellable biometrics: Index-of-max hashing," *arXiv Preprint ArXiv*, vol. 1703, 2017.

[89] 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 Trans. Information Forensics and Security*, vol. 13, no. 2, pp. 393–407, 2017.

[90] L. Ghammam, K. Karabina, P. Lacharme, and K. Thiry-Atighehchi, "A cryptanalysis of two cancelable biometric schemes based on index-of-max hashing," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 2869–2880, 2020.

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

[92] D. Sadhya, Z. Akhtar, and D. Dasgupta, "A locality sensitive hashing based approach for generating cancelable fingerprints templates," *IEEE 10th International Conference on Biometrics Theory, Applications and Systems (BTAS)*, pp. 1–9, 2019.

[93] M. Kayaoglu, B. Topcu, and U. Uludag, "Standard fingerprint databases: Manual minutiae labeling and matcher performance analyses," *arXiv Preprint ArXiv:1305.1443*, 2013.

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

[95] S. M. Abdullahi and S. Shuifa, "Random hash code generation for cancelable fingerprint templates using vector permutation and shift-order process," *ArXiv Preprint ArXiv:2105.10227*, 2021.

[96] Y. Li, L. Pang, H. Zhao, Z. Cao, E. Liu, and J. Tian, "Indexing-min-max hashing: Relaxing the security-performance tradeoff for cancelable fingerprint templates," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 2022.

[97] H. Li and X. Wang, "One factor cancellable fingerprint scheme based on novel minimum hash signature and secure extended feature vector," *Multimedia Tools and Applications*, vol. 81, no. 9, pp. 13 087–13 113, 2022.

[98] Y. Li, H. Zhao, Z. Cao, E. Liu, and L. Pang, "Compact and cancelable fingerprint binary codes generation via one permutation hashing," *IEEE Signal Processing Letters*, vol. 28, pp. 738–742, 2021.

[99] M. J. Lee, Z. Jin, and A. B. J. Teoh, "One-factor cancellable scheme for fingerprint template protection: Extended feature vector (EFV) hashing," *IEEE International Workshop on Information Forensics and Security (WIFS)*, pp. 1–7, 2018.

[100] F. Farooq, R. M. Bolle, T.-Y. Jea, and N. Ratha, "Anonymous and revocable fingerprint recognition," *IEEE Conference on Computer Vision and Pattern Recognition*, pp. 1–7, 2007.

[101] 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.

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

[103] Z. Jin, A. B. J. Teoh, T. S. Ong, and C. Tee, "A revocable fingerprint template for security and privacy preserving," *KSII Transactions on Internet and Information Systems (TIIS)*, vol. 4, no. 6, pp. 1327–1342, 2010.

[104] Z. Jin, A. B. J. Teoh, T. S. Ong, and C. Tee, "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.

[105] W.-j. Wong, M.-l. D. Wong, and Y.-h. Kho, "Multi-line code: A low complexity revocable fingerprint template for cancelable biometrics," *Journal of Central South University*, vol. 20, no. 5, pp. 1292–1297, 2013.

[106] 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.

[107] 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.

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

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

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

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

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

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

[114] M. Ferrara, D. Maltoni, and R. Cappelli, "A two-factor protection scheme for MCC fingerprint templates," *Proc. Int. Conf. of the Biometrics Special Interest Group (BIOSIG)*, pp. 1–8, 2014.

[115] N. Zhang, X. Yang, Y. Zang, X. Jia, and J. Tian, "Generating registration-free cancelable fingerprint templates based on minutia cylinder-code representation," *IEEE Sixth International Conference on Biometrics: Theory, Applications and Systems (BTAS)*, pp. 1–6, 2013.

[116] R. Arjona, M. A. Prada-Delgado, I. Baturone, and A. Ross, "Securing minutia cylinder codes for fingerprints through physically unclonable functions: An exploratory study," *International Conference on Biometrics (ICB)*, pp. 54–60, 2018.

[117] R. Cappelli, M. Ferrara, and D. Maltoni, "Minutia cylinder-code: A new representation and matching technique for fingerprint recognition," *IEEE Trans. Pattern Analysis and Machine Intelligence*, vol. 32, no. 12, pp. 2128–2141, 2010.

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

[119] Q. N. Tran, J. Hu, and S. Wang, "Alignment-free cancellable template with clustered-minutiae local structure," *IEEE Global Communications Conference (GLOBECOM)*, pp. 1–6, 2018.

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

[121] A. K. Trivedi, D. M. Thounaojam, and S. Pal, "Non-invertible cancellable fingerprint template for fingerprint biometric," *Computers & Security*, vol. 90, p. 101 690, 2020.

[122] M. Shahzad, S. Wang, G. Deng, and W. Yang, "Alignment-free cancelable fingerprint templates with dual protection," *Pattern Recognit.*, vol. 111, 107735, 2021.

[123] Y. Series, *Global information infrastructure, internet protocol aspects and next-generation networks: Next generation networks-frameworks and functional architecture models. overview of the internet of things, recommendation itu-t y. 2060*, 2012.

[124] M. A. Ferrag, L. A. Maglaras, H. Janicke, J. Jiang, and L. Shu, "Authentication protocols for internet of things: A comprehensive survey," *Security and Communication Networks*, vol. 2017, 2017.

[125] A. Kumar, R. Saha, M. Conti, G. Kumar, W. J. Buchanan, and T. H. Kim, "A comprehensive survey of authentication methods in internet-of-things and its conjunctions," *Journal of Network and Computer Applications*, p. 103 414, 2022.

[126] S. Li, S. Zhao, G. Min, L. Qi, and G. Liu, "Lightweight privacy-preserving scheme using homomorphic encryption in industrial internet of things," *IEEE Internet of Things Journal*, 2021.

[127] W. Yang, S. Wang, N. M. Sahri, N. M. Karie, M. Ahmed, and C. Valli, "Biometrics for internet-of-things security: A review," *Sensors*, vol. 21, no. 18, p. 6163, 2021.

[128] J. Wilkins, "Can biometrics secure manufacturing?" *Biometric Technology Today*, vol. 2019, no. 1, pp. 9–11, 2019.

[129] K. Habib, A. Torjusen, and W. Leister, "A novel authentication framework based on biometric and radio fingerprinting for the IoT in ehealth," *Proc. 3rd Int. Conf. Smart Systems, Devices, and Technologies*, pp. 32–37, 2014.

[130] B. Kantarci, M. Erol-Kantarci, and S. Schuckers, "Towards secure cloud-centric internet of biometric things," *Proc. 4th Int. Conf. Cloud Networking (CloudNet)*, pp. 81–83, 2015.

[131] N. Maček, I. Franc, M. Bogdanoski, and A. Mirković, "Multimodal biometric authentication in IoT: Single camera case study," *Proc. 8th Int. Conf. Business Info. Security, Belgrade, Serbia*, 2016.

[132] L.-P. Shahim, D. Snyman, T. du Toit, and H. Kruger, "Cost-effective biometric authentication using leap motion and IoT devices," *Proc. 10th Int. Conf. Emerging Security Information, Systems and Technologies, Nice, France*, pp. 24–28, 2016.

[133] 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.

[134] 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.

[135] 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 Trans. Industrial Informatics*, vol. 15, no. 7, pp. 4244–4253, 2019.

[136] G. Zheng *et al.*, "Fingerprint access control for wireless insulin pump systems using cancelable Delaunay triangulations," *IEEE Access*, vol. 7, pp. 75 629–75 641, 2019.

[137] M. F. Ayub, K. Mahmood, S. Kumari, A. K. Sangaiah, *et al.*, "Lightweight authentication protocol for e-health clouds in IoT-based applications through 5G technology," *Digital Communications and Networks*, vol. 7, no. 2, pp. 235–244, 2021.

[138] M. Tanveer, H. Shah, S. A. Chaudhry, A. Naushad, *et al.*, "Paske-iod: Privacy-protecting authenticated key establishment for internet of drones," *IEEE Access*, 2021.

[139] X. Yin, S. Wang, M. Shahzad, and J. Hu, "An IoT-oriented privacy-preserving fingerprint authentication system," *IEEE Internet of Things Journal*, 2021.

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

[141] R. A. Silverman, *Introductory complex analysis*. Courier Corporation, 2013.

[142] T. Needham, *Visual complex analysis*. Oxford University Press, 1998.

[143] J. B. Conway, *Functions of one complex variable II*. Springer Science & Business Media, 2012, vol. 159.

[144] S. Marsland, R. I. McLachlan, *et al.*, "Möbius invariants of shapes and images," *SIGMA. Symmetry, Integrability and Geometry: Methods and Applications*, vol. 12, p. 080, 2016.

[145] G. H. Golub and C. F. Van Loan, *Matrix computations, fourth edition*, 2013.

[146] T.-Y. Jea and V. Govindaraju, "A minutia-based partial fingerprint recognition system," *Pattern Recognition*, vol. 38, no. 10, pp. 1672–1684, 2005.

[147] 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.

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

[149] 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.

[150] H. Qin, H. Wang, X. Wei, L. Xue, and L. Wu, "Privacy-preserving wildcards pattern matching protocol for IoT applications," *IEEE Access*, vol. 7, pp. 36 094–36 102, 2019.

[151] X. Wang, S. Garg, H. Lin, M. J. Piran, J. Hu, and M. S. Hossain, "Enabling secure authentication in industrial IoT with transfer learning empowered blockchain," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 11, pp. 7725–7733, 2021. DOI: 10.1109/TII.2021.3049405.

[152] Z. Jin, M.-H. Lim, A. B. J. Teoh, B.-M. Goi, and Y. H. Tay, "Generating fixed-length representation from minutiae using kernel methods for fingerprint authentication," *IEEE Trans. Systems, Man, and Cybernetics: Systems*, vol. 46, no. 10, pp. 1415–1428, 2016.

[153] S. Zahoor and S. Naseem, "Design and implementation of an efficient FIR digital filter," *Cogent Engineering*, vol. 4, no. 1, 1323373, 2017.

[154] B. A. Shenoi, *Introduction to Digital Signal Processing and Filter Design*. Wiley Online Library, 2006.