Privacy-Preserving Biometric Authentication

QUANG NHAT TRAN

A thesis submitted in partial fulfillment of the requirements
for the degree of Doctor of Philosophy at the
School of Engineering & Information Technology
University of New South Wales at
Australian Defence Force Academy

🎓 Welcome to the Research Alumni Portal, Quang Tran!

You will be able to download the finalised version of all thesis submissions that were processed in GRIS here.

Please ensure to include the **completed declaration** (from the Declarations tab), your **completed Inclusion of Publications Statement** (from the Inclusion of Publications Statement tab) in the final version of your thesis that you submit to the Library.

Information on how to submit the final copies of your thesis to the Library is available in the completion email sent to you by the GRS.

Thesis submission for the degree of Doctor of Philosophy

Thesis Title and Abstract | **Declarations** | **Inclusion of Publications Statement**

Corrected Thesis and Responses

ORIGINALITY STATEMENT

☑ I hereby declare that this submission is my own work and to the best of my knowledge it contains no materials previously published or written by another person, or substantial proportions of material which have been accepted for the award of any other degree or diploma at UNSW or any other educational institution, except where due acknowledgement is made in the thesis. Any contribution made to the research by others, with whom I have worked at UNSW or elsewhere, is explicitly acknowledged in the thesis. I also declare that the intellectual content of this thesis is the product of my own work, except to the extent that assistance from others in the project's design and conception or in style, presentation and linguistic expression is acknowledged.

COPYRIGHT STATEMENT

☑ I hereby grant the University of New South Wales or its agents a non-exclusive licence to archive and to make available (including to members of the public) my thesis or dissertation in whole or part in the University libraries in all forms of media, now or here after known. I acknowledge that I retain all intellectual property rights which subsist in my thesis or dissertation, such as copyright and patent rights, subject to applicable law. I also retain the right to use all or part of my thesis or dissertation in future works (such as articles or books).

For any substantial portions of copyright material used in this thesis, written permission for use has been obtained, or the copyright material is removed from the final public version of the thesis.

AUTHENTICITY STATEMENT

☑ I certify that the Library deposit digital copy is a direct equivalent of the final officially approved version of my thesis.

Thesis submission for the degree of Doctor of Philosophy

UNSW is supportive of candidates publishing their research results during their candidature as detailed in the UNSW Thesis Examination Procedure.

Publications can be used in the candidate's thesis in lieu of a Chapter provided:

- The candidate contributed **greater than 50%** of the content in the publication and are the "primary author", i.e. they were responsible primarily for the planning, execution and preparation of the work for publication.
- The candidate has obtained approval to include the publication in their thesis in lieu of a Chapter from their Supervisor and Postgraduate Coordinator.
- The publication is not subject to any obligations or contractual agreements with a third party that would constrain its inclusion in the thesis.

The candidate has declared that **some of the work described in their thesis has been published and has been documented in the relevant Chapters with acknowledgement**.

A short statement on where this work appears in the thesis and how this work is acknowledged within chapter/s:

> My literature review includes a partial work of a survey paper that I contributed to. This paper was published in the IEEE Open Journal of the Computer Society. Parts of the work presented in Chapter 3 and Chapter 4 were published in the IEEE Transactions on Information Forensics and Security. Finally, parts of Chapter 5 were published in the IEEE Open Journal of Computer Society.

Candidate's Declaration

I declare that I have complied with the Thesis Examination Procedure.

Abstract

Biometric-based authentication provides a highly accurate means of authentication without requiring the user to memorize or possess anything. However, there are three disadvantages to the use of biometrics in authentication; any compromise is permanent as it is impossible to revoke biometrics; there are significant privacy concerns with the loss of biometric data; and humans possess only a limited number of biometrics, which limits how many services can use or reuse the same form of authentication.

As such, enhancing biometric template security is of significant research interest. One of the methodologies is called cancellable biometric template which applies an irreversible transformation on the features of the biometric sample and performs the matching in the transformed domain. Yet, this is itself susceptible to specific classes of attacks, including hill-climb, pre-image, and attacks via records multiplicity.

This work has several outcomes and contributions to the knowledge of privacy-preserving biometric authentication. The first of these is a taxonomy structuring the current state-of-the-art and provisions for future research. The next of these is a multi-filter framework for developing a robust and secure cancellable biometric template, designed specifically for fingerprint biometrics. This framework is comprised of two modules, each of which is a separate cancellable fingerprint template that has its own matching and measures. The matching for this is based on multiple thresholds. Importantly, these methods show strong resistance to the above-mentioned attacks. Another of these outcomes is a method that achieves a stable performance and can be used to be embedded into a Zero-Knowledge-Proof protocol. In this novel

method, a new strategy was proposed to improve the recognition error rates which is privacy-preserving in the untrusted environment. The results show promising performance when evaluated on current datasets.

Acknowledgement

I would like to take this opportunity to express my appreciation to the people who have supported me along the path of my PhD.

First and foremost, it would be never enough to say how much I am thankful having Professor Jiankun Hu and Associate Professor Benjamin Turnbull as my supervisors. Thank you both for all the training and lessons that I have actively or passively gained throughout the whole course and especially, for never having given up on me. Thank you, Professor Jiankun Hu for being a motivational and inspirational figure to whom I always look up and set my goal. Thank you, Associate Professor Benjamin Turnbull, for being not only a supervisor, but also a mentor, and a good friend of mine. Without you, this PhD would have never been possible.

Next, I want to send my thanks to all the staff in the School of Engineering and Information Technology, UNSW Canberra for all their help and support.

Importantly, I would like to express my gratitude to my family: My parents, my wife, my older brother, and my daughter. I am grateful to being one of my parents' sons as this day would never come without their caring and love. I thank my wife for having embarked on this journey with me. My brother deserves all the best credits for being not only a brother but also a great fellow throughout my whole PhD life. Finally, thank you, Angelina, for coming to my life as my daughter. You are the reason why I have never given up trying.

Finally, I thank myself for proving that some people were wrong and I am worthy.

Certificate of Originality

I hereby declare that this submission is my own work and that, to the best of my knowledge and belief, it contains no material previously published or written by another person, nor material which to a substantial extent has been accepted for the award of any other degree or diploma at UNSW or any other educational institution, except where due acknowledgement is made in the thesis. Any contribution made to the research by colleagues, with whom I have worked at UNSW or elsewhere, during my candidature, is fully acknowledged.

I also declare that the intellectual content of this thesis is the product of my own work, except to the extent that assistance from others in the project's design and conception or in style, presentation and linguistic expression is acknowledged.

Quang Nhat Tran

List of publications

[Journal articles]

1. Tran QN, Hu J. A Multi-Filter Fingerprint Matching Framework for Cancelable Template Design. IEEE Transactions on Information Forensics and Security. 2021 Mar 26;16:2926-40.

2. Tran QN, Turnbull BP, Wu HT, de Silva AJ, Kormusheva K, Hu J. A Survey on Privacy-Preserving Blockchain Systems (PPBS) and a Novel PPBS-Based Framework for Smart Agriculture. IEEE Open Journal of the Computer Society. 2021 Jan 20;2:72-84.

3. Tran QN, Turnbull BP, Hu J. Biometrics and Privacy-Preservation: How Do They Evolve?. IEEE Open Journal of the Computer Society. 2021 Mar 23;2:179-91.

4. Tran, Q., Turnbull, B., Wang, M. and Hu, J., 2021. A Privacy-preserving Biometric Authentication System with Binary Classification in a Zero Knowledge Proof Protocol. IEEE Open Journal of the Computer Society.

[Conference papers]

1. Tran QN, Hu J, Wang S. Alignment-free cancellable template with clustered-minutiae local structure. In 2018 IEEE Global Communications Conference (GLOBECOM) 2018 Dec 9 (pp. 1-6). IEEE.

Contents

List of Figures

List of Tables

List of Common Acronyms

Table 1: Abbreviated Terms used in this thesis

Abbreviated terms	Full terms
AI	Artificial Intelligence
ARM	Attack via Records Multiplicity
CNN	Convolutional Neural Network
DFT	Discrete Fourier Transform
ECC	Error Codes Correction
EER	Equal Error Rates
FAR	False Acceptance Rates
FRR	False Rejection Rates
GAR	Genuine Acceptance Rates
HMM	Hidden Markov Model
ICA	Independent Component Analysis
LBP	Local Binary Pattern
LDA	Linear Discriminant Analysis
LDP	Local Derivative Pattern
LPP	Locality Preserving Projections
LSH	Locality Sensitive Hashing
MLP	Multi-Layer Perceptron
PCA	Principal Component Analysis
SVM	Support Vector Machines
ZKP	Zero-Knowledge-Proof

Chapter 1

Introduction

1.1 Introduction to The Topic

Since the introduction of iPhone 5S with fingerprint authentication in 2013, biometric-based authentication has become a must-have feature in any smartphone since. Why is biometric authentication increasingly used more on personal handheld devices? Passwords and tokens based authentication methods rely on one's knowledge and possession, respectively. There exist some limitations for both of these approaches. Passwords that are easy to remember are also easy for an adversary to compromise while physical tokens can be stolen, lent, or cloned. On the other hand, for thousands of years, biometrics have been used to verify individuals [107] as they are the physical traits that constitute a human being. Over this period, biometrics have proven to be reliable for the recognition of people. The last several decades of advances in computing have seen the replacement of error-prone manual comparison to automated processes. There are numerous advantages to biometrics as an authentication mechanism; unlike passwords and tokens, biometrics cannot be forgotten or lost, and cannot be transferred or stolen. On a smartphone, presenting a biometric sample (such as scanning a fingerprint, showing a face) is far more convenient than

having to fill in a password. From the perspective of a malicious adversary, the effort expended to overcome a password is potentially significantly less than that for a biometric. Interestingly, biometrics have even been used within the Multifactor Authentication (MFA) to give a better access control [19]. The 'who you are' aspect of the MFA has distinct advantages for use in this paradigm, and is increasingly used.

Biometrics are often categorized into two classes: physiological biometrics and behavioral biometrics [150]. Each has its own advantages and disadvantages and depends on the context to be used effectively. For examples, smartphones usually integrate fingerprint, face, or iris recognition since the sensors for these biometrics are inexpensive and portable, allowing their use in handheld devices. Therefore, how good a biometric is depends on how it is used. Yet, fingerprint and face are still among the most widely used biometrics for authentication due to the explosive increase in smartphones.

However, biometrics do have disadvantages as a form of authentication. Chief amongst these is the concerns regarding privacy. What would happen if a biometric template is in the hands of a malicious adversary? First and foremost, all applications that use this template are potentially compromised. This is an issue as there are a finite number of unique biometrics for any given individual. The loss of a biometric is also important to note as biometrics are not revocable. A compromised biometric sample is considered lost permanently. As a result, there is a strong emerging research interest to devise the methods designated for securing biometric templates as a means of reducing the risk of accidental and malicious loss. One of the current approaches is the Cancellable Biometric Template.

Before detailing the research conducted in this thesis, this chapter is dedicated to framing the issues explored in this work. Some background knowledge is briefly reviewed in section 1.1.1, to frame the need for this work and to provide some context for key concepts. Afterward, the Research Question of the thesis will be presented in section 1.2. Finally, in section 1.2, the structure of the thesis is given.

1.1.1 Background Knowledge Framing the Research Need

The concept of the cancellable biometric template is one of the more actively researched methods for biometric template protection. Rather than a single definition, cancellable templates are often defined by their core characteristics. Ratha et al. [124] described the four characteristics of a cancellable biometric template as:

- Non-invertibility: The transformation that is applied on a biometric template is either non-invertible or computationally hard to be reversed. Later on, the ISO/IEC 24745 standard usually refers to this characteristic as *irreversibility*.
- Revocability: In case that a cancellable biometric template is compromised, it can be revoked while the original biometric data is still secure. A new cancellable biometric template is regenerated from it using a new set of parameter keys.
- Unlinkability: This term is also usually referred to as *Diversity*. It requires all the cancellable biometric templates generated from the same original biometric data with different set of parameter keys to have no correlation. This characteristic ensures that an attacker cannot use a compromised cancellable biometric template to cross authenticate another application.
- Accuracy: The non-invertible transformation, when applied, should not degrade the matching results in the transformed domain.

With the above characteristics, cancellable biometric templates provides a firm foundation as an appropriate approach to resolve the problems of traditional authentication methods. Importantly, it is a privacy-preserving methodology in the sense that it aims to protect the biometric with an irreversible transformation that avoids the necessity to store the original biometric template. However, there are emerging techniques that have been shown to weaken the protections given by cancellable biometric temples. One of these, Attacks via Records Multiplicity (ARM), have shown to be effective in reducing the privacy of users [100].

ARM was first proposed in [136]. With this attack, the malicious adversary reverses the irreversible transformation applied on the biometric template by gathering samples from multiple biometric authentication systems that employ the same method. In detail, given a raw biometric template x, multiple sets of parameters k_i $(i = 1, 2, ..., n)$, and the transform function F, multiple transformed templates are generated as y_i $(i = 1, 2, ..., n)$ where each transformation follows the one-time-pad model such that each individual y_i is infeasible to be linked back to x. For convenience, such transformation will be referred as the One-Time-Pad (OTP) model.

Being deployed in multiple locations, these y_i's are not linked. However, assuming the OTP transformation function F and parameter set k_i $(i = 1, 2, ..., n)$ are known, an adversary can launch the ARM if he/she can determine the original biometric data x through solving the acquired system of equations as shown in several research publications 1.1. For example, a cancellable design with an OTP-based transformation such as many-to-one linear mapping is exposed to the ARM [100] because a unique solution can be determined through solving a well-defined system of linear equations.

$$\begin{bmatrix} y_1 = F(x, k_1) \\ y_2 = F(x, k_2) \\ y_3 = F(x, k_3) \\ \vdots \\ y_n = F(x, k_n) \end{bmatrix} \tag{1.1}$$

Therefore, the ARM can cripple a privacy-preserving biometric authentication system, making the cancellable biometric methods no longer privacy-preserving. This has consequences that are potentially far-reaching, as it can expose the original biometric, which may in use elsewhere and is non-revocable. It is important to find the irreversible transformations that are resistant to the ARM but does not affect the performance of the authentication systems. This leads us to the Research Question, which is detailed in the next section.

1.2 Research Question and Contributions

1.2.1 Thesis Research Question

As noted above, there is a need to progress the field of biometric authentication with privacy preservation. Specifically, cancellable biometric template needs to be defended against the ARM. As such, the major research question for this thesis is as follows:

> *How can we develop biometric authentication frameworks that can address major security and privacy threats while retaining a good authentication performance?*

This is a non-trivial research problem as security strength and high authentication performance are conflicting goals. To best answer this research question, there are multiple sub-processes required.

The first stage of this work is to understand the current state of the art in the field, both from an offensive and defensive perspective. What are the current biometric processes used, and what is their performance? What are the current threats and attacks on privacy and security, and how effective are these? What are the current research opportunities in this area? All of these responses are necessary to best explore the research question that is the central point of this work.

The second stage of answering this question is to evaluate, irrespective of performance, whether it is possible to mitigate the current and emerging attacks. If so, can performance then be improved or considered to be competitive with other current approaches? This may require the development or redevelopment of multiple approaches.

1.2.2 Novel Research Contributions of This Work

In order to answer the research question, this thesis contains the following contributions:

- A taxonomy for the current and emerging biometric authentication systems, especially the privacy-preserving technique, is devised.
- Two sets of robust local-structure-based fingerprint features are designed with the capability to deliver stable performance even in noisy conditions.
- Along with the features mentioned above, two irreversible transformations are proposed to incorporate in a multi-filter cancellable template framework that is able to defend against the current attacks such as the ARM, Hill-climb, and Pre-image.
- A light-weight biometric authentication that utilizes the power of Artificial Intelligence (AI) with high performance is embedded in a Zero Knowledge Proof Protocol to be ready for use in a subsequent cryptography-based security system.

1.3 Thesis Structure

The research in this thesis employs privacy-preserving biometric authentication as its theme. It is structured into six chapters: Chapter 1 introduces the topic of this thesis along with briefing some of the background knowledge in the field. Chapter 2 gives a taxonomy of the emerging related work and also functions as a comprehensive review of the literature in the field. Chapter 3 presents a local-structure-based design for a cancellable fingerprint template. Chapter 4 combines the work in Chapter 3 with a newly proposed cancellable fingerprint design based on the MCC to devise a Multi-filter Cancellable Fingerprint Template framework. This framework is proven to have successfully defended against the current attacks with the best performance

when compared with the current state of the art. Chapter 5 is dedicated to the integration of a light-weight biometric authentication in a Zero-Knowledge-Proof Protocol to be used in a subsequent cryptography-based security system. Finally, chapter 6 concludes this thesis and suggests future research directions.

Chapter 2

Literature Review

A subset of the work reported in this chapter (mostly from Section 2.2 to Section 2.4) has been published in the following article: Tran QN, Turnbull BP, Hu J. Biometrics and Privacy-Preservation: How Do They Evolve?. IEEE Open Journal of the Computer Society. 2021 Mar 23;2:179-91.

2.1 Overview

In addition to reviewing the related work in biometric authentication from a privacy-preserving perspective, this chapter is also dedicated to present a comprehensive taxonomy for privacy-preserving biometric authentication system. The well-designed taxonomy can structure the vast knowledge in the field which helps an in-depth understanding of the complicated relationships among various concepts and existing works.

Biometrics are traits of human body characteristics and behaviour. From a cryptographic perspective, biometrics possess properties that make them suitable as an authentication factor; they cannot be forgotten like a password or pin, and they cannot be lost or stolen like a token. Biometrics can help address the inherent security weakness of cryptography in identifying a genuine user. However, biometrics themselves are limited and will be a permanent loss if compromised. Also, the privacy of biometrics are subject to the protection of legal regulations. Therefore, there is a paradigm shift towards privacy-preserving biometric authentication technology,

which has the potential to address these concerns.

Due to their uncertain nature, biometrics cannot be protected by simply applying conventional encryption. This leaves them exposed to various threats. As a result, there exists an immediate necessity to devise methods that not only preserve the privacy of biometric data but also ensure the performance of biometric authentication systems. According to the standard set by ISO/IEC FCD 24745:2011 [55], a biometric protection scheme must be: (i) irreversible, that is computationally infeasible to reconstruct the original biometric data from the encrypted template; and (ii) unlinkable, whereby the encrypted templates generated from the same biometric data are not correlated such that a cross-matching attack is successful.

As many biometric matching techniques in the unprotected domain are integrated into the privacy-preserving biometric authentication systems, a taxonomy and summary of the state-of-art biometric matching techniques in the unprotected domain are also provided. Such system-level knowledge organization will help produce excellent self-contained contents of reference materials for researchers from both the biometric community and the cryptography community who would otherwise have difficulty in understanding the relevant materials from the other side. Additionally, it provides a structured approach to the understanding of the domain and its areas of the current and emerging research and development.

2.2 A Taxonomy of Biometrics and Privacy-preserving Techniques

Privacy-preserving mechanisms for biometrics are designed to ensure the security of biometrics when used in any authentication system. They are normally categorized into cancellable biometrics template and biometric cryptosystem [128]. This work presents a new perspective on the classification of privacy-preserving techniques in addition to the categorization of the biometrics genres. A privacy-preserving biometric security system consists of biometric component and privacy-preserving

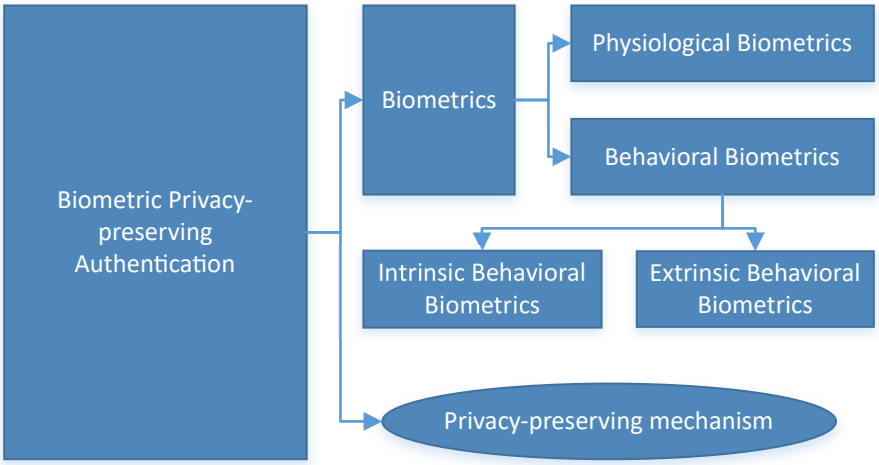


Figure 2.1: Privacy-preserving Biometric-based Authentication System

mechanisms.

Due to the characteristics of the biometrics, they are categorized into two main types: behavioral biometrics and physiological biometrics. Behavioral biometrics are the types of biometrics that are focused on the actions of the owner. The behavioral biometrics are categorized into two sub-categories: extrinsic and intrinsic behavioral biometrics. The reactions that correspond to certain events are extrinsic behavioral biometrics (typing, keystrokes, touchscreen usage patterns, driving styles, and so on) meanwhile those that come from the routine activities of a person are intrinsic behavioral biometrics (gait, voice, and many others). Being the actions of a person, behavioral biometrics are countless, resulting in more studies proposed on the new types being used in an authentication system.

Traditionally, privacy-preserving mechanisms for biometrics have always been categorized as cancellable biometrics and biometric cryptosystems. Cancellable biometrics are the application of a non-invertible transformation onto the biometric data, and biometric cryptosystems rely on cryptographic techniques to encrypt the biometric data. However, as the field continues expanding, more recent studies that have been proposed require a more complicated and specific categorization. Hence, this work proposes a novel taxonomy in which each class or sub-class is better spec-

ified based on its characteristics:

- Non-invertible Transformation: methods that applies a non-invertible transformation on the biometric data. Biometric matching is performed in the transformed domain. For instance: cancellable biometrics, Hashing, or Homomorphic Encryption.
- Direct Biometrics Key Generation: methods that generate a cryptographic key based on a biometric data.
- Information Hiding Techniques: techniques that, given public information, make it hard to find the corresponding original information.
- Protocol-based Protection: methods in which protection is achieved by deploying a protocol that usually involves multiple parties.

The taxonomy provides an overall structured level of biometrics and mechanisms. Fig 2.1 provides an overview of the interconnection between the privacy-preserving mechanisms. This relationship will be discussed in the next sections.

An abstraction-level taxonomy overview is presented in Figure. 2.1. In this taxonomy, the whole Biometric Privacy-preserving Authentication is comprised of Biometrics and privacy-preserving mechanisms. Biometrics are categorized into Physiological Biometrics and Behavioral Biometrics where Privacy-preserving mechanims are categorized into: Non-invertible Transformation. Direct Biometrics Key Generation, Information Hiding Techniques, and Protocol-based Protection. The details for each component are discussed in the following sections.

2.3 Biometric Authentication Systems

Biometrics are the traits of human body characteristics and behavior. They are excellent attributes for identity management.

2.3.1 Behavioral Biometrics

Behavioral biometrics focus on recognizing the individual based on the nature of their actions. As indicated in Figure 2.1, behavioral biometrics can be categorized into either extrinsic or intrinsic behavioral biometrics. Each of these is discussed separately.

2.3.1.1 Extrinsic Behavioral Biometrics

Extrinsic behavioral biometrics are those that occur based on the uniqueness of an individual's behaviour in dealing with specific situations. For example, the identification of typing or touchscreen usage patterns [152, 186].

The implementation and use of touchscreen has seen rapid expansion of use owing to the wide expansion of smartphones in the digital age. Consequently, touchscreen input has been extensively considered as an extrinsic behavioral biometric to identify users [56]. However, in general, touchscreen biometric authentication is user friendly but has a high error rate, potentially making it one factor of authentication in support of less error-prone techniques. Another important extrinsic behavioral biometric is patterns produced in typing. However, as pointed out in [118], the assumption that typing pattern is stable over time does not hold, meaning that it can change over time for multiple reasons. It has been shown that the accuracy of a typing-based behavioral biometric authentication is not reliable. In addition, the user's level of familiarity with the language to be typed also affects the identification process. Typing time latency relative order feature and clustering can help improve the system performance [74] [173].

2.3.1.2 Intrinsic Behavioral Biometrics

Intrinsic behavioral biometrics come from the natural activities of the body. These include, for instance, gait and voice. Intrinsic behavioral biometrics are normally used for distant individual identification and are cooperation agnostic.

Tao et al. [143] proposed General Tensor Discriminant Analysis (GTDA) as a pre-processing step for LDA and applied this with gait recognition for evaluation. Aside from this, three Gabor-function-based decomposition techniques have also been devised to recognize the walking figure. Experimental results from this work indicated good performance when compared with other state-of-the-art methods of gait recognition, based on the University of South Florida HumanID Database. Specifically focusing on gait recognition without cooperation in different conditions, Bashir et al. [15] proposed Gait Entropy Image (GEnI) for auto feature selection on which an Adaptive Component and Discriminant Analysis (ACDA) is formulated for matching with the selected features. On the other hand, Zhang et al. [197] focused on devising a solution for the degraded performance when confounding variables are present by proposing AutoEncoder framework, which is capable of automatically disentangling gait features from appearance. The authors also generated a more challenging gait database that contains only frontal view gaits (FVG) with variations. Chao et al. [26] considered each gait as a set of independent frames and used a network called GaitSet for learning from this set. This method is said to be immune to frames permutation and able to integrate frames from other videos. Evaluations on the OU-MVLP gait database and CASIA-B gait database reached an average of 87.1% and 95.0% recognition rate. Wang and Yan [166] proposed a cross-view gait recognition system with ensemble learning in which multiple gait learners are taken into consideration. Recognition rate when evaluated with CASIA dataset A and B is 95.5% and 96.1%, respectively. Zou et al. [200] utilized a CNN and an RNN to learn the gait biometric of each individual from walking data, which is collected using smartphones in the wild with no constraints about speed or path. From the two datasets of 118 individuals collected by smartphones, this algorithm reached 93.5% and 93.7& accuracy rate in identification and authentication, respectively.

2.3.2 Physiological Biometrics

Physiological biometrics are the traits that belong to a human, including fingerprints, palmprints and finger veins. They are usually unchangeable and are consistent for an individual throughout their life. However, the collection of physiological biometrics is subject to multiple external factors, such as the pressure on the collection device, surface collection cleanliness, and other environmental factors. In this section, the physiological biometric authentication is categorized into the partitions of fingerprint, face, others, and multimodal.

2.3.2.1 Fingerprint

The fingerprint has long been applied as a reliable tool for individual identification. This section will review the proposed key advances on fingerprint matching techniques where most of them are integrated with the various privacy-preserving mechanisms in forming privacy-preserving biometric authentication systems.

Ridge-based Matching: One of the most common fingerprint matching methodologies is ridge-based matching. This method has been developed to deal with low-quality images generated from low-resolution sensors. In 1986, Isenor and Zaky [76] introduced a unique method to match two fingerprints by representing the images using connected graphs in which each node is a level number given to a ridge after adjusting the orientation of all ridges. Matching is performed between two graphs in three phases: partitioning, refining, and scoring. This technique has been proven to correctly identify corresponding minutiae. Marana and Jain [111] proposed a ridge-based fingerprint matching method using Hough Transform for low-quality fingerprint images captured by solid state sensors, achieving FRR of 1.7% at FAR of 0.1%. Feng et al. [48] presented a ridge-based matching method that constructed the ridge and minutia correspondences between two fingerprints. Choi et al. [27] also employed the concept of combining ridge features with minutiae.

Image-based Matching: An image-based methodology uses feature vectors to

represent an image. From a bio-cryptographic perspective, it is used to create images from fingerprints that can then be compared. Almansa and Cohen [11] presented a thin-plate spline model to match fingerprint images, relying on the geometric transformations between two images. Ito et al. [77] specifically sought to work with low-quality fingerprints, and overcame many of the challenges with a phase-based image matching process that uses phase components in 2D DFT. In general, a fingerprint image-based matching scheme is a global feature based matching scheme. Such features are not as accurate as local features, such as minutia representation. However, with the great success of Deep Learning mechanisms in image processing, such fingerprint image-based methods have found new applications in fingerprint presentation attack detection [28, 62].

Minutia-based Matching: A minutia is the point of either ridge bifurcation or a ridge ending on a fingerprint, which is described by its coordinates and orientation. Jain et al. [78] proposed a point pattern matching scheme for fingerprint comprising of two stages: alignment and matching. In alignment stage, the differences caused by translation, rotation, and scaling between the template and query is estimated such that the query minutiae are aligned with the template minutiae. In the matching stage, the minutiae from both are converted to polygons in a polar coordinate and matched using an elastic string matching algorithm from which an analysis of the accuracy and distribution of the genuine and impostor matching are provided. Minutia-based fingerprint matching is the major fingerprint matching mechanism in use today, and many fingerprint matching schemes are derived from the minutia feature. Many use minutia feature processes and add additional features, such as ridge count, to increase effectiveness [188]. In general, such methods can produce very high matching performance and are widely deployed in practical systems.

Local Structure-based Matching Methodology: Local structure matching is a process widely used for not only fingerprint matching but also for matching of other biometrics, since it limits the influence of external factors that cause noise and distortion to a biometric object. Minutia Cylinder Code (MCC), introduced by Cappelli et al. [24] is the current state-of-the-art algorithm. It is a hybrid between

local structure-based matching and minutia-based matching methodology, as each of the local structures constructed is based on a minutia. Given a minutia $m = \{x_m, y_m, \theta_m\}$, the MCC representation of m's is the cylinder whose bases' centered at m with a pre-defined radius R and a height of 2π. A cuboid encloses the cylinder such that the cylinder's bases are aligned with vector θ_m. The cuboid is divided into small cells with an associated value calculated by feeding the minutiae's spatial and directional contribution into a sigmoid function. Each of the cell values is assessed their validity to evaluate the cylinder's matchability before calculating the cylinder similarity. In addition, the authors also provide four global scoring methods to consolidate all pairs of cylinder similarity into a matching score as the means to determine whether two fingerprint match or not. MCC was evaluated with dataset FVC2006 DS2[a-e] under the traditional FVC protocol. The matching performance of this method is still considered the state-of-art today due to its low EER and FMR (0.15% and 0.18%, respectively).

2.3.2.2 Face

In parallel with fingerprints, facial recognition has been in development for a significant period of time. Unlike fingerprints, facial recognition does not require complex hardware, and a modern inexpensive camera can produce a face image of suitable quality, even from a distance. The art of facial recognition lies in the algorithm that enhances the image and extracts reliable features from a face to successfully verify or classify it.

Image-based facial matching: Facial recognition systems that use image-based matching techniques rely on input image or images of faces to extract features. There are primarily two types of systems in this category: feature-based and holistic. The difference between these two techniques is that feature-based approaches use local structure features and holistic approaches rely on global structure features, respectively. These are discussed separately below.

Feature-based Facial Recognition: Feature-based Facial Recognition takes the in-

put image and identifies the face area to extract individual facial features, such as the eyes, nose, lips, etc. Yuille et al. [190] proposed the deformable templates approach that describes the features extracted from a face using a parameterized template; Tan and Triggs [142] introduced Local Ternary Patterns (LTP), which is a generalized version of the LBP local texture descriptor to improve the recognition accuracy under uncontrolled lighting conditions. This method achieves state-of-the-art performance when evaluated with the Extended Yale-B, the CAS-PEAL-R1, and the (FRGC-204) datasets. A new development expanding on this technique has been proposed to retrieve local binary features via unsupervised machine learning, which has the potential to learn the binary codes and the codebook for local face patches in a single stage [43, 104].

There are a myriad of methods based on the use of profiles. Bhanu and Zhou [18] have proposed curvature values to extract fiducial points from faces, and used a dynamic time warping method to match them. There are two databases that are considered best-practice for use in profile-based facial recognition experiments. The first database, which is from the University of Bern [1], contains profile views of 30 people with three big gray-level profiles each, yielding accuracy of 90%. The second database, which is from the University of Stirling [2], has 311 images from 35 people, having 78.4% accuracy. Efraty et al. [45] expanded the angles of the profile such that various rotations having their own feature space with the aid of 3D models. Various experiments with two publicly available face databases have been conducted. Recent works are on facial landmark localization and alignment [39, 199].

Holistic Facial Recognition Holistic-based (or global features) facial recognition systems are designed to establish the features based on the whole image, rather than specific points or regions as feature-based methods do. Holistic face recognition systems can be categorized into two approaches: statistical approaches and AI-based approaches. In its most basic form, a holistic-based face recognition takes an image as input and treats it as a matrix of intensity values. In order to match, an input face is compared against the faces the system stored in memory or an existing database. As one might have thought, this method is not only complex

in terms of computational power but also prone to errors due to external condition changes. For this system to work with stability, several conditions regarding lighting, pose angle, and distance to camera must be met. In reality, this is rarely the case with face recognition. Therefore, to reduce the matching complexity, there exists a necessity to match less features. This would ideally only search for and match features that are meaningful or discriminative. This is described as the curse of dimensionality, and is common across several fields. Most works in this space focus on addressing the dimensional issue by using PCA [137], and LDA [105] to reduce dimensionality. These earlier works are mostly statistically-based approaches. Recently, a topology-preserving structural matching was proposed in [44]. Due to the success in the application of AI, significant attention has been directed toward AI-based face recognition approaches.

AI-based Facial Recognition With the integration of Artificial Intelligence, facial recognition has met its next chapter of development. This is at a time when existing methods such as PCA, LDA, and ICA methods are beginning to saturate and yield less improvements over time. AI-based face recognition offers multiple approaches to minimise the impact of the curse of dimensionality in the context of face recognition. Neural networks are one widely used approach to achieve this. Recently, Yin and Liu [187] devised a multi-task learning model in which a Convolutional Neural Network (CNN) was given a main task along with multiple side tasks. In this approach, pose variation is learned by a pose-directed multi-task CNN. This method reports comparable or even better performance than state-of-art methods on the LFW, CFP and IJB-A datasets. Meanwhile, Cocskun et al. [31] improved the performance of a face recognition system by adding two normalization operations to two of the eight layers (four convolutional and four max pooling layers) in a CNN-based system.

Multiple Classifier Facial Recognition Each classifier has its own advantages and disadvantages, and there is active research in the use of multiple classifiers to overcome these limitations. With integration, the result can be a single complex system comprised of complementary classifiers. In practice, Multiple Classifier Systems (MCS) are a powerful solution for solving pattern recognition problems, especially

those that involve noisy data and large class variations [72]. Toygar, Acan Chawla and Bowyer [145] embraced a divide-and-conquer design to introduce a multiple classifier face recognition system using appearance-based statistical methods in which a facial image is segmented into multiple horizontal regions where a particular statistical method (PCA, LDA, or ICA) is used to extract features. This technique was evaluated with the FERET dataset, and was shown to provide improvements in not only storage and computational complexity but also recognition rates.

Video Sequence Facial Recognition: With the growth of surveillance cameras for security purposes, combined with the increase in power and quality of smartphone video, the ability to perform facial recognition from video sequences in real-time has become an active research field. Early works in this space attempted to extend techniques used in still-image recognition to video, but these were met with limited success [68,196]. Recently, systems that are explicitly designed for facial recognition against video inputs have been devised. The most successful of these use neural networks. Ding and Tao [40] implemented a Convolutional Neural Network for their facial recognition system. This system proposed a Trunk-Branch Ensemble CNN model to extract complementary information from holistic face images and patches cropped around facial components. This method achieved state-of-art performance on three databases: PaSC, COX Face, and YouTube Faces. Yang et al. [177] proposed a facial recognition using a Neural Aggregation network (NAN), which takes a video or set of face images as input and produces a fixed-dimension feature representation for recognition. Experiments were conducted on IJB-A, YouTube Face, and Celebrity-1000 benchmarks, and the outcomes highlights its competitive performance against state-of-art naive aggregation methods at the time. In 2018, Li et al. [102] presented a Recurrent Regression Neural Network (RRNN) framework to solve the problem of cross-pose facial recognition on both still images and videos. MultiPIE and YouTube Celebrities databases have been used to evaluate the performance of this framework with different angle poses, achieving 95.6% and 84.6% on average, respectively.

Sensory Data-based Facial Recognition In parallel with the growth in the

number of facial recognition techniques based on 2D images or videos, facial recognition based on sensory data has recently attracted significant attention. With appropriate sensors, facial characteristics are captured and modelled accordingly. Based on the types of facial data, it can be categorized as infrared facial recognition and 3D model facial recognition. Each of these is independently discussed, as follows.

Infrared Facial Recognition Thermal infrared has been used as a tool for detection of facial features. Unlike images captured by cameras, infrared pictures are not easily affected by lighting variation. More importantly, Cutler [33] stated that infrared sensors are even capable of detecting veins underneath the skin, leading to the exposure of more discriminative features. Thus, thermal infrared sensors tend to deliver more stable data, especially in facial recognition. However, there are several reasons that infrared is not that popular for facial recognition; thermal cameras are more expensive and therefore have a higher deployment cost, they do not work with glasses and other facial coverings, and are temperature sensitive. Hence, in some situations, visible light facial recognition systems will outperform infrared ones [89].

Despite these limitations, there is significant work in this space, and many advantages for doing so. One particular area of research in this space has been the generation of infrared face databases [106, 192]. Recently, Rodriguez et al. [130] proposed a Long Wave Infrared (LWIR) image facial recognition framework and an infrared facial recognition system based on the complex wavelet structural similarity (CW-SSIM) index. The authors also generated two new LWIR facial image databases with variations in poses, expressions, and illumination conditions. Abd El-Rahiem et al. [3] proposed an infrared facial recognition system that uses Convolutional Neural Network (CNN) that includes five convolutional layers and five max-pooling layers. Terravic Facil IR Database (TFIRDB) has been used for evaluation of the method, reaching accuracy of 99%.

3D Model Facial Recognition Constructing a three-dimensional model of the face for recognition brings an obvious benefit - it provides a greater number of discrim-

inative features from the curves and shapes on the face, resulting in improvements to the performance of the developed system. However, it also increases the computational complexity of the system. Computing developments are such that this cost will largely be irrelevant, making systems employing such technology more popular over time. There are several well-known techniques in this area. Sharma and Kumar [138] proposed a Voxel-based 3D face reconstruction technique and applied it in facial recognition along with sequential deep learning. Bosphorus, UMBDB and KinectFaceDB datasets have been used for evaluation, achieving competitive recognition rates.

Targeting the pose variation, He et al. [71] recently proposed a Deformable Face Net (DFN) in which a deformable convolution module learns the alignment and identity-preserving feature extraction. This method has been evaluated on multiple benchmarks, yielding superior performance in comparison with other state-of-art at the time. Recently, Al-Obaydy and Suandi [10] presented an automatic pose normalization technique that automates the process of facial landmark detection in a facial recognition system. Experiments evaluated on FERET database show comparable or better performance than the state-of-the-art pose normalization approaches.

2.3.2.3 Iris

The iris, considered as biometric with the highest reliability, has been widely used to identify individuals. In order to use the iris as a method of recognition, a sensor is required to scan the iris, from which the feature vectors are generated and matched according to a process. Iris recognition methods can be categorized based on the following stages; image acquisition, region segmentation, feature extraction, and matching. Iris recognition systems are categorized into two different types based on their methodology; features-based and AI-based.

Features-based Iris Recognition: One of the most and first phase-based iris recognition algorithms used in commercial systems was proposed by Daugman [36, 37]. In this work, the feature vectors of an iris are extracted by applying the 2D

Gabor filters. After quantization, these feature vectors are called the 'iriscode'. The Hamming distance is calculated between a pair of iriscodes, reporting best performance with FAR of 1/151000 and FRR of 1/128000. Tan and Kumar [141] proposed a solution to improve iris recognition when comparing images taken from different distances. This process used a Zernike moment-based phase to encode the local iris features and combine it with global features in a joint strategy. The proposed algorithm was evaluated with public iris databases, UBIRIS.v2, FRGC, and CASIA.v4-distance, providing an average improvement in EER of 54.3%, 32.7%, and 42.6%, respectively, in comparison with other state-of-the-art methods at the time. Kaur et al. [88] based their method on moment invariants to extract local and global features with their invariance properties and tolerance to noise from localized iris region until 15th order.

AI-based Iris Recognition: The use of AI in iris recognition is still in its relative infancy, but has yielded significant success. Of note, Ahmadi et al. [8] devised a new method that is developed by neural network and genetic algorithm for iris recognition. Proencca and Neves [122] proposed to use deep learning classification models to construct a segmentation-less and non-holistic iris recognition system. Separately, Dua et al. [42] utilized a feed-forward neural network with a k-means clustering algorithm in which iris segmentation is conducted with circular Hough transform that helps separating the iris region from other parts. Targeting post-mortem iris recognition in deceased forensic identification, Trokielewicz et al. [151] used deep learning to segment the iris texture area with Gabor-based recognition method. In addition, a new database of post-mortem iris images from 42 subjects is established.

2.3.2.4 Other biometrics

Apart from the fingerprint, face, and iris, there are other types of biometrics that have been used to perform recognition. Although some of these biometrics are not as popular, largely due to the level of inconvenience and deployment cost when com-

pared with other biometrics. For example, palmprints are a unique biometric, but require a physically larger scanner for collection when compared with a fingerprint, and EEG recognition systems provide explicit uniqueness, but require much more complex signal capturing devices than many other systems. This section reviews some eminent works that have been proposed for other biometrics.

Palmprint: Although similar to fingerprints, due to having a bigger area, palmprint contains more discriminative features that can be used for individual identification. There are several algorithms proposed to utilize features for matching two palmprints, and several of the works designed for fingerprint analysis may be translated. However, palmprints have unique issues, and are susceptible to the curse of dimensionality problem. Fei et al. [47] made good use of the direction information of the palmprint by proposing a three-phase feature extraction procedure; first, the surface direction of the palmprint is extracted; then its energy map layer is used to retrieve the latent direction features, and finally, applying multiplication and addition schemes, the apparent direction and latent direction features are combined in a histogram feature descriptor, which is used for the process of recognition. As with other areas of biometrics, AI is also being utilized in the identification of palmprints. Motivated by the desire to construct an scenario-adaptive palmprint recognition system, Zhao et al. [198] proposed a generic framework that is capable of extracting high-level discriminative features using a discriminative deep convolutional network that is trained with limited palmprint data. Upon being evaluated with PolyU Multi-spectral database, IITD, and CASIA, this method reported significant results.

Finger Vein: One advantage to using finger veins as a unique attribute is that, unlike many other personal attributes, it is non-obvious and not subject to easy retrieval by adversaries. However, the use of finger veins does induce complexity for deployment. There has been significant work in the use of finger veins for biometrics. In 2017, Lu et al. [178] proposed a finger vein recognition framework in which the anatomy structure is exploited to construct a more reliable vein network and vein

backbone. Matching is performed by first using the vein backbone to align the finger. Experimental results on Hong Kong Polytechnic Database and Shandong University database shows the effectiveness of this framework with EER of 0.38% and 1.39% for HKPD and SDU database, respectively.

Hong el al. [73] utilized NIR image sensors with a convolutional neural network to improve the quality of the image and the process of matching two finger veins, respectively. Their method was evaluated with the SDU database in addition to the two databases that the authors constructed themselves, showing better performance in comparison with the conventional methods. Xi et al. [174] proposed to perform finger vein recognition using discriminative binary codes (DBC). The process for this is as follows; firstly, the relation between subject was illustrated by a subject relation graph, from which binary templates were transformed to describe the characteristics of each vein, then SVMs were trained to serve the matching process. This method has been evaluated with PolyU and MLA databases, showing better performance when compared with other methods at the time. Another work that also employs binary representation for finger vein recognition is [103] in which Liu et al., motivated by the LBP, proposed a personalized binary code (PBC) to exploit the structure of the binary feature corresponding to each class. This method shows leading performance on SDU and HKPU in terms of EER.

Palm Vein: The relationship between the palm vein and finger vein is similar to the relationship of the palmprint and fingerprint. Palm vein recognition provides another way to identify individual based on the features underneath the human skin. As a result, a palm vein recognition system requires more complicated hardware setup in addition to the growth in dimensionality. Hence, it is only appropriate to be deployed with systems that require higher level of security or where deployment cost is less of a factor.

Although less active than many other areas of biometric research, palm vein research has still made significant improvements in the last decade. Van et al. [154] proposed to deal with contactless palm vein by a combination of enhanced center-

symmetric LBP (ECS-LBP) and SIFT. Aberni et al. [5] used multi-scale LBP for features extraction and ant colony optimization for the preprocessing of palm vein images towards the recognition of palm vein. Verification rate achieved in this method is 99.64% while EER is 0.00078%, outperforming state-of-the-art methods. Kilian et al. [92] focused on the pre-processing stage to generate high-resolution image by using multiframe super-resolution (MSR) from multiple images of the same scene. According to the authors, this method shows a promising path for low-cost yet effective imaging devices by outperforming most classical methods.

Ear Recognition: The ear has emerged as one of the newest biometrics for recognition, and has only been actively researched in the last decade. An empirical study has shown that the ear possesses certain features that are distinct even for identical twins [117]. Based on the unique shape of the ear, one's identity can be verified with an inexpensive camera that captures the image of the ear from afar. Ear acquisition does not require contact or cooperation. Although it has received significant research interest, the commercial deployment of this kind of biometric as a unimodal biometric recognition is not as wide as others due to its variation with age, imaging modalities, and lack of datasets. Instead, the ear can be a supplemental tool used in parallel with other primary biometric(s) in a multimodal biometrics recognition system. Recently, Ganapathi et al. [60] based their method on geometric statistics for a 3D ear recognition. In this process, feature keypoints were first extracted from 3D data through the use of surface variations. Then, each descriptor vector for each keypoint was defined by three components. Experiments conducted with the UND-J2 database illustrated the effectiveness with best recognition rate of 100% and EER of 1.5%.

Electroencephalography: Electroencephalography (EEG) is a test that tracks the brain wave patterns using small metal discs with wires placed on the scalp. Brain signals are captured through these sensors and sent back to a computer. This method is well established in the medical field. There are normally five main brain

oscillation patterns: Delta (0.5 - 4Hz), Theta (4 - 8Hz), Alpha (8 - 14Hz), Beta (13 - 30Hz), and Gamma (over 30Hz) [155]. Although it has been shown that EEG carries genetic information [155], it also has the applicability as a biometric recognition resolution. From the perspective of privacy preservation, the EEG possesses some advantages over other biometrics. It is a secret biometric, which is even harder to retrieve than vein-family biometrics, making it robust against spoofing attacks as an attacker cannot acquire EEG signals, and is inherently present in all humans and less susceptible to the physical loss that other biometrics are. However, EEG also has limitations when used in a biometric recognition system: First, it requires deep cooperation of the user, as EEG signals cannot be distantly recorded. Second, the deployment of EEG equipment is more expensive than other biometrics. Third, acquiring EEG is an inconvenient and time-consuming process. Last but not least, in comparison with other biometrics, EEG contains health data of the user. Thus, to some extent, it still potentially leaks health information if retrieved by an adversary.

There are several significant works in the research space of EEGs as biometrics. Das et al. [35] investigated the use of EEG under different frequency bands, visual stimuli, and subsets of time intervals after the stimuli presence. The experiments were conducted on a set of 50 healthy subjects and each sample was acquired twice, which the second one week after the first. Various results have been acquired with the best being 13.55% of EER in a non-target vs non-target scheme. Fraschini et al. [57] presented a phase synchronization-based approach for an EEG recognition system, resulting in an EER of 0.044% for EEGMMIDB. Nakamura et al. [115] aimed at applying EEG in real-world application by resolving the two issues; collectability and reproducibility. This EEG system is designed by using a "one-fits-all" viscoelastic generic in-ear EEG sensor to collect data over multiple days with multiple objects. Autoagressive model and spectral features are supported by LDA and used with SVM classifiers. This method showed a 95.7% accuracy rate on a dataset from 15 subjects.

Wang et al. [158] have proposed some works on the advances of EEG recognition systems. They presented a deep Gaussian Mixture-HMM for EEG Signals classifi-

cation [158] that contains two components: the first serves as the automatic feature extraction by utilizing an autoregressive-deep variational autoencoder model while the second is built for EEG classification by incorporating the Gaussian mixture-HMM. In [159], the authors proposed an EEG recognition system that used convolutional neural networks on EEG signals collected during a diverse set of tasks while recently, in [160], a graph-based method consisting of a network estimate module and a graph analysis module for EEG biometric identification.

2.3.2.5 Multimodal

Multimodal biometric recognition systems combine multiple, different biometrics to deliver more stable performance than unimodal biometric systems in terms of recognition [140]. The features from each biometric are extracted and used for the process of matching. Multimodal biometric systems have the advantage of accuracy at the expense of complexity. Depending on the system used, fusion is performed between biometric responses at a system level, to calculate identity. The most popular method of fusion is at matching score level.

In 2000, Dialog Communication Systems (DCS) developed BioID, a commercial multimodal biometric recognition system combining a physiological biometric (face) with two other behavioral biometrics (voice and lip movement). This system is outlined in [58]. In the wake of EEG's increasing applicability as an identification system, Min et al. [157] incorporated face recognition with EEG to a trusted autonomous system in which the presence of a user is continuously verified. Recently, Zhang et al. [195] introduced DeepKey as a multimodal biometric authentication system for gaits and brainwaves. DeepKey is comprised of two components; an invalid ID filter model that blocks unauthorized personnel, and an attention-based Recurrent Neural Network for parallel subject matching. This system achieved 1% FRR while maintaining FAR at 0%.

The methods to fuse outcomes at a systemic level is a major research focus for multimodal biometrics systems. In a multimodal biometric system, fusion is a crit-

ical factor that influences the overall matching performance. In [129], Rodrigues et al. proposed two fusion schemes. The first of these was the extension of the likelihood ratio-based fusion, and the second was based on fuzzy logic. The authors claimed that their proposed methods are more robust against spoof attacks than other fusion methods. Walia et al. [156] performed fusion at the score level in a multimodal biometrics system comprised of iris, finger vein, and fingerprints. This fusion worked by first applying Backtracking Search Optimization Algorithm (BSA) on each classifier, then using proportional conflict redistribution rules (PCR-6) to resolve the conflicts among classifiers. This system was tested to produce a 1.5.% EER and 98.43% accuracy rate. Gupta et al. [67] proposed a score fusion method that is adaptive, where the matching scores are boosted or suppressed based on the situation. This method is said to be capable of distinguishing noisy inputs from spoofing attacks. Accuracy rate of the proposed method reached 99.5% with 0.5% EER.

Aside from a matching score fusion process, there are several other methods designed to fuse multimodal biometrics at different levels. Believing a feature set is more informative than matching score or the decision output, Haghighat et al. [69] introduced Discriminant Correlation Analysis (DCA) to perform feature-level fusion in a multimodal biometric system. With the same assumption, Joseph et al. [84] proposed a multimodal biometric system for the improvement in security in cloud environments. This system fused the features of fingerprint, iris scans, and palmprint to generate a unique key, which is the outcome of the fusion.

In addition to the development of recognition methods, researchers have also worked on generating benchmark databases for multimodal biometrics. The majority of these databases provide a combination of physiological and behavioral biometrics that are acquired with different sensors or views to ensure the presence of variations. In 2007, Fierrez et al. [54] generated BioSec, a multimodal biometrics database containing fingerprint images, frontal face images, iris images, and voice utterances. The data was recorded from 200 individuals over two sessions. Fierrez et al. [53] constructed another multimodal biometric database named BiosecurID. This

database includes different unimodal biometrics sub-databases; speech, handwritten signature and handwritten text, keystrokes, iris, face, fingerprints, and hand. Yin et al. [189] generated the SDUMLA-HMT database for multimodal biometrics, containing face images, finger vein and fingerprint images, iris images, and gait videos.

2.4 Privacy-preserving Techniques

This section introduces a new perspective on the categorization of the privacy-preserving mechanisms for biometric system. An overview of the classes is presented in Figure 2.2.

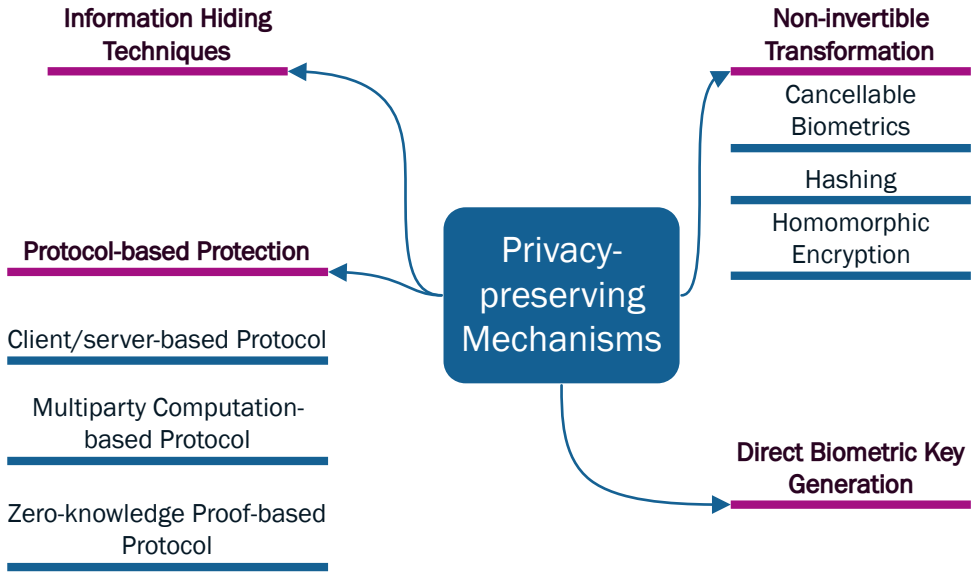


Figure 2.2: Privacy-preserving Mechanisms

The privacy-preserving mechanisms are categorized into the following categories:

- Non-invertible Transformation.
- Direct Biometrics Key Generation.
- Information Hiding Techniques.
- Protocol-based Protection.

Each of these is discussed separately.

2.4.1 Non-invertible Transformation

Non-invertible Transformation techniques are comprised of one-way transformations applied on the biometrics data such that an adversary cannot retrieve the original biometric data. Comparison of two biometrics is performed in the transformed domain to ensure no information about the original data is leaked.

2.4.1.1 Hashing

Cryptographic hashing generates a hash value from an input data. However, applying it on biometric induces variation, as cryptographic hashing requires the input data to be exactly the same every time. Any slight change to the input completely changes the hash produced. In 2004, Jin et al. [80] proposed a two-factor authentication method named BioHashing. This work used an iterative inner product operation to combine the tokenized data with fingerprint data. The resultant data is a separate feature set, which is then binarized using a predefined threshold. This work achieved 0% as its best EER when working with FVC2002 DB1-4 at the time. In 2017, Jin et al. [81] proposed an Index of Max (IoM) Hashing as the non-invertible transformation for cancellable fingerprint template with MCC. MCC was used as the fingerprint vector, which is fed into the process of generating template by finding the IoM codes with different approaches (Gaussian Random Projection based IoM and Uniformly Random Permutation based IoM). FVC2002 DB1-3 and FVC2004 DB1-3 were chosen to test this method. Approaching from the BioHashing concept, Meetei and Begum [113] combined the iris features with a tokenized pseudo-random number. One of the most famous works that have been proposed in protecting the palmprint template is by Connie et al. [30] in which a set of pseudo-random keys is used to generate palmhash code, functioning as the protection layer for palmprint template.

2.4.1.2 Cancellable Biometric Templates

Ratha et al. [124] first proposed the idea of cancellable biometrics in 2001 as a method to protect biometric data. To be considered as a cancellable template, the following four characteristics are required [124]:

- Non-invertibility: cancellable biometric template cannot be, or is computationally hard to be, reverted to retrieve the original biometric data given the corresponding parameter is exposed to the adversary. Irreversibility is a more accurate term that is used in the ISO/IEC 24745 standard.
- Revocability: If a cancellable biometric template is compromised, the original biometric data is still safe and able to be used with new sets of parameters to generate new transformed templates. The template generated with the old parameters is no longer valid and is revoked.
- Diversity: Different cancellable biometric templates generated by different set of parameters should have no correlation such that a cross-template attack is not possible.
- Accuracy: Transformation of the biometric data should not degrade the matching process.

Lee et al. [96] used each minutia in a fingerprint as a reference point whose invariant features are derived from its neighboring area. The transformation applied on each of the minutiae is determined by two changing functions of the distance of the orientation, leading to a new position of the minutiae. The proposed method yields EER of 3.4%. A separate work that also employed a minutia-matching methodology, Ahn et al. [9] extracted the features from a triplet of minutiae and applied a shifting transformation on the geometrical properties of the tripplet. Being evaluated with good quality dataset FVC2002 DB2, the proposed work reached EER of 3.61%.

Approaching from the direction of applying two-factor key generated by splitting the projection matrix to produce biometric template, Yang et al. [175] project

the biometric features as the transformation in the sense that a dynamic random projection is applied on the feature vectors of the local minutia. The projection's content is determined by the feature vectors. In 2011, Ahmad et al. [7] designed a cancellable fingerprint template whose features are constructed based on the relative interaction between two minutiae in a pair polar coordinate system. Yang et al. [176] utilized both local and global structures to extract features to which a perpendicular projection is applied as the non-invertible transformation. Yang et al. [182] used the Delaunay triangulation method to construct triangles from three minutiae from which local features are extracted. Each element in the set of triangles (also referred to as the set of local structures) is applied with the non-invertible Polar Transformation defined in [124]. Two fingerprint images are deemed match or non-match based on the number of corresponding triangles. Due to this inflexible tolerance, this method's performance when evaluated with good quality dataset FVC2002 DB1 and FVC2002 DB2 is comparatively poor with 5.93% and 4.0%, respectively. Binary representation has been widely used in designing cancellable fingerprint templates due to its simplicity and lightweight in implementation. Recently, Yang et al. [181] proposed a cancellable fingerprint template method using random projection. The remarkable novelty in this work is the decorrelation algorithm, which provides protection against the ARM.

In recent years, Wang et al. [162–164] have proposed various works on designing non-invertible transformation functions from the perspective of digital signal processing. In 2012 [162], they proposed an infinite to one mapping approach in which the binary strings representation of features are first mapped to the frequency domain by applying the Discrete Fourier Transform (DFT). Afterward, the resultant vectors are multiplied with a parameter matrix whose number of rows equals the number of binary values from the string and number of columns is less that the number of rows. This method achieved EER of 3.5%, 5%, 7.5% for FVC2002 DB1-3, respectively. In 2014, they proposed another alignment-free cancellable template method that uses curtailed circular convolution as the non-invertible transformation [163]. After extracting features and bin-indexing them to produce binary rep-

resentation, the authors converted them to frequency domain with DFT and remove part of the resultants to get the cancellable templates. This method managed to bring down the EER of the good quality FVC2002 DB1 and FVC2002 DB2 to 2% and 3% but when dealing with lower quality images from FVC2002 DB3, it still reached 6.12%. In 2016 [164] , Song and Hu proposed to protect the template of the fingerprint using a non-invertible transformation based on blind system identification concept. Using the same method to extract features, generate a binary string, and convert the output to frequency domain using DFT as the previously mentioned method, the authors then used a Finite Impulse Response (FIR) vector of the moving average model to generate cancellable template. They also showed that under certain circumstances, as long as the length of the FIR vector is within a specified range, the transformation is non-invertible. Both One versus One and FVC protocols have been evaluated with FVC2002 DB1-3 and shown competitive performance against the state-of-art methods at the time. Song et al. designed partial Hadamard transformations and partial DFT in [161] and [165], respectively. Both works employ a vector as a parameter key to select certain rows of the output matrix accordingly as the cancellable templates of the binary string representation of features. The difference lies in the fact that the former method was used with Hadamard transformation meanwhile the latter method utilized the Discrete Fourier Transformation. Recently, Yang et al. [185] proposed a feature-adaptive random projection cancellable biometric template. The projection matrices are determined by a basic matrix that is associated with local features. The four fingerprint databases FVC2002 DB1-3 and FVC2004 DB2 are used to evaluate this approach. Although the authors claimed that the projection matrices are destroyed after use, this method is still not resistant to the ARM.

Taking advantage of the MCC's performance, various non-invertible transformations have been proposed to protect the templates. The authors of MCC proposed P-MCC [50] as a template protection scheme in which a KL projection [59] is applied on the MCC vector. However, this projection is not revocable. Hence, in 2014, the authors proposed 2P-MCC [51] with the ability to reissue a compromised template

by incorporating a partial permutation-based scheme. In the meantime, Zhang et al. [194] proposed two non-invertible transformation to generate cancellable fingerprint templates from MCC: Combo Plate Transformation and Functional Transformation. In 2018, Arjona et al. [12] designed Physically Unclonable Functions (PUFs) to apply on P-MCC and named it P-MCC-PUFs.

Similar to fingerprints, cancellable biometric templates have also been applied to the iris. Recently, Yang et al. [183] proposed a cancellable iris system by employing steganography to hide the user's key, decreasing the chance of losing the key to adversary and improving the security of the system. Having been evaluated on CASIA-IrisV3-Interval, MMU-V1, and UBIRIS-V1-Session 1 databases, this method achieved EER of 1.66%, 4.75%, and 3%, respectively. Importantly, by incorporating steganography to hide the user's key in an image, which is not detectable with human eyes, the authors made this method less exposed to the ARM. However, a machine learning technique or a simple method that scans the stego-images's pixels may give knowledge about a secret being hidden. Hence, further analysis may be employed to retrieve the secret.

In addition to fingerprints, iris, and face, the cancellable template design has also been applied to protect other biometrics. These are less common, but there has still been significant enhancements in this area. Palmprints are one of the hidden biometrics that needs to be protected as a person only has 2 palmprints. Due to the large area of the palmprint, more complicated and costly sensor is required, leading to less interest in comparison to other biometrics. Qiu et al. [123] proposed to generate a cancellable palmprint template by utilizing Anisotropic Filter to extract the orientation information and applying chaotic matrix to measure it. Evaluation of the method's performance is conducted on Hong Kong PolyU database and Tongji Contactless Palmprint Dataset, achieving EER of 0%. One of the recently published works on palm vein is by Ahmad et al. [6] in which the authors used a wave atom transform (WAT) from which the features are extracted. In order to protect the feature, with a user-specific key, a randomization and quantization are applied to generate the palm vein templates. Under four databases: PolyU, PUT, VERA, and

their own database, this method achieved 1.98%, 0%, 3.05%, and 1.49%, respectively.

2.4.1.3 Homomorphic Encryption-based Biometric Matching

Homomorphic Biometric Encryption though conceptually is similar to cancellable biometric as the former performs matching in encrypted domain while the latter performs in transformed domain, it is a type of bio-cryptosystem as it modifies and applies traditional encryption techniques on biometric data instead of using a non-invertible transformation. Barrero et al. [64] utilized homomorphic probabilistic encryption to construct a general framework for multi-biometric template protection with fusions in three levels and achieved EER of 0.12% while the templates storage requires only 200KB. Recently, Morampudi et al. [114] protected the iris used in an authentication system with fully homomorphic encryption. Evaluated with CASIA-V1 database, this method reached an EER of 0.19%.

2.4.2 Direct Biometric Key Generation

Direct Biometric Key Generation takes a biometric data as input to generate helper data, from which digital keys are generated. Importantly, biometric key generation schemes do not require either of the biometric template or the private key to be stored in the system, mitigating the risk of them being exposed to adversary when there is an attack targeting the database.

One of the first biometric key generation schemes was proposed by Davida et al. [38] in which they used user-specific error correction to address the uncertainty in testing data. The authors demonstrated this method with iris biometric. Although applicability in iris was shown, whether or not this method is suitable for other biometrics is still doubtful as iris exhibits far less variation in comparison with face or fingerprint features.

Since then, there have been various key-generation designs proposed with different types of biometrics [16, 120, 126, 127, 131]. In general, direction biometric key gener-

ation methods tend to be unreliable due to the biometric data noise. The following sections of this work focuses on research designed to retrieve reliable keys from noisy data. It will focus on the concept of Fuzzy Extractor and its applications for being one of the breakthroughs that provides a firm foundation for other methods.

Fuzzy Extractor Fuzzy Extractor [41] is one of the famous biometric key generation schemes. This method differs from FVS (Fuzzy Vault Scheme which will be introduced in the next sections) in the sense that instead of using chaff points, high-degree polynomial is used. In their original paper, the authors proposed two primitives: secure sketches and a fuzzy extractor: A secure sketch is a probabilistic function that generates helper data about the noisy input w (w can be considered as, but is not limited to being a biometric input) without significantly revealing it, i.e., reducing its entropy. An exact recovery of w can be retrieved given the existence of some w' as input that is computationally close enough to w. Assuming M is the metric space to be used with the scheme and *dis* calculates the distance between two objects in M, a secure sketch is comprised of two phases: Sketch (SS) and Recover (Rec) such that: (i) SS takes the input w and returns a binary string s; (ii) Rec takes s and w' as input. If $dis(w, w') \leq t$, then w is recovered, i.e: $Rec(w', s) = w$ where t is the distance threshold or error tolerance. On the other hand, a fuzzy extractor is constructed from a secure sketch and a strong extractor (the reader can refer to the original text in [41] for further information). It can reproduce a nearly uniform random string R from the input w' when $dis(w, w') \leq t$. Additionally, a syndrome key generation scheme that is based on polynomial interpolation that requires low storage space is proposed and called PinSketch.

In the original text, fuzzy extractor is enabled to work with different metric spaces, such as Hamming distance, Set difference, and Edit distance. Hence, it has a wide range of applications to protect biometric template data. There is significant work in this space, especially focusing on fingerprints. Xi et al. [172] proposed an alignment-free fingerprint authentication system with fuzzy extractor. In details, rotation and shift free local structures derived from minutia are used to eliminate the alignment process. A near equivalent Dual Layer Structure Check (NeDLSC) is devised to

make it applicable to bio-crypgraphic constructions. Finally based on NeDLSC, fuzzy extractor is applied. The algorithm is evaluated on FVC2002 DB2, yielding EER of 4.5%. In 2012, Yang et al. [179] applied fuzzy extractor to protect the features in a fingerprint authentication system. In their design, Delaunay triangle-based local structures are extracted as registration-free features. The use of fuzzy extractor not only delivers the improvement in matching performance but also makes pre-alignment process unecessary. Upon having been evaluated on FVC2002 DB2, the algorithm achieved 13% of EER.

Various works from unimodal to multimodal biometrics have also employed fuzzy extractor. Chang et al. [25] incorporated cancellable multi-biometric with fuzzy extractor and a novel bit-wise encryption.

2.4.3 Information Hiding Techniques

Information Hiding Techniques are processes that hide or obfuscate biometric data by fusing it with another piece of data (known as a digital key) to produce public helper data. In an authentication phase, the digital key is recovered by applying a retrieval algorithm given the presence of a closely matched biometric query to the template that is used to generate the helper data.

Fuzzy Commitment Scheme: In 1999, Juels and Wattenberg [87] proposed the Fuzzy Commitment Scheme (FCS). Given a set C containing error correcting codewords c with length n, witness x being the biometric data with length n, in the enrolment phase, a function F is used to commit the codeword c and the biometric data x to create the helper data $F(c, x)$ by estimating and storing the difference vector δ between x and c where $\delta = x - c$. The hash value of the codeword c, denoted as $h(c)$ is stored along with δ. In the authentication phase, given that a biometric data x' is computationally close to x with respect to a pre-defined metric, c can be retrieved by using δ to perform a translation of x' toward x. Decision is made based when comparing the hash value of the result with $h(c)$.

Rathgeb et al. [125] used the FCS to protect the fusion at the feature level in

which two binary biometric templates are combined. This method was evaluated with the CASIA-v3-Interval iris database [193].

There have also been numerous methods that apply FCS in protecting fingerprint templates: Sandhya and Prasad have proposed quite some works in applying FCS to design a fingerprint-based authentication system: In 2016, the authors used FCS to protect the binary strings generated from the Delaunay neighbor structures [134] and achieved 1.43%, 1.79%, and 5.89% for datasets FVC2002 DB1-3, respectively. In the same year, they proposed a privacy-preserving system for fingerprint with Delaunay triangulation net features based on FCS. In 2017, they [135] combined the concept of cancellable biometrics with FCS to devise their cancellable fingerprint privacy-preserving authentication system using spiral curves, reaching EER of 1.17%, 2.46%, 8.51% when evaluated with datasets FVC2002 DB1-3, respectively. In 2013, Imamverdiyev et al. [75] built an FCS-based privacy-preserving biometric authentication system using different combinations of texture descriptors (such as Gabor filter-based FingerCode, local binary pattern, and local direction pattern). In details, the fingerprint texture descriptors, which is the result of the combination, is binarized by a biometric discretization method and protected with FCS. Upon being evaluated with FVC2002 DB2a fingerprint dataset, the results show improvement in the performance of texture-based fingerprints bio-cryptosystem with FCS.

Due to the variations presented in facial recognition, leading to a variant binary string representation, it has rarely been used in an FCS-based bio-cryptosystem. Feng et al. [49] combined the transform-based and bio-cryptosystem approach in a three-step hybrid algorithm based on random projection, discriminability-preserving transform, and FCS. Three face databases are used for the evaluation of this method, namely: FERET, CMU-PIE, and FRGC, giving estimated security of 206.3 bits, 203.5 bits, and 347.3 bits, respectively. In 2018, Nazari et al. [116] is one of the few who used FCS to protect face features. They integrated face recognition with binarization transformation, chaos feature permutation and FCS. The proposed work was evaluated in three face databases: CMU PIE, FEI, and Extended Yale B. Gilkalaye et al. [61] constructed FCS-based bio-cryptosystem with facial recognition by

proposing a real-value compatible FCS. Labeled Faces in the Wild (LFW) dataset was used for evaluation.

Recently, Yang et al. [184] used FCS to protect the biometric-based healthcare data and stored it along with the cancellable finger vein template on a smart card.

In addition to physiological biometrics, FCS has also been used with behavioral biometrics. Specifically, gait-based authentication systems are receiving increasing research interest. Recently, Elrefaei and Al-Mohammadi [46] extracted gait features from gait images with local ternary pattern and calculated the average of a gait cyle using gait energy image before having joined them together and produced feature vector. FCS is used to protected the data. This system achieved good results with 0% of FAR as well as FRR. However, the key length retrieved is only 45-50 bits.

The most obvious disadvantage of FCS is that it requires an ordered representation of the biometric features. As a result, it has limited application due to the difficulties in designing a biometric feature extraction scheme that produces ordered binary string from a noisy input. This problem is addressed by the next introduced work.

Fuzzy Vault Scheme In 2006, Juels and Sudan proposed one of the most well-known privacy-preserving biometric system concepts, the Fuzzy Vault Scheme (FVS) [86]. FVS uses error correcting code with polynomial encoding. In the enrolment phase, given the biometric feature set A and a polynomial p to encode the key k, $p(A)$ is calculated in addition to the adding of chaff points to hide the genuine points of p. This set of points T is the template. In authentication phase, assuming that A' is the input query biometric feature set, $p(A')$ is calculated. If a large portion of A overlaps with A', sufficient points lying on p are located. Hence, applying error code correction, k is successfully recovered. With this work, the authors enabled privacy-preserving biometric authentication system to work with an unordered set, which is one of biometrics' characteristics. In addition, it was proved that without having the same biometric, reconstruction of the polynomial is not possible with the presence of the chaff points.

Fingerprints are one of the hidden biometrics that urgently need protection. This

fact alone explains why there are countless studies on securing fingerprints, especially using FVS. Li et al. [101] proposed a topological structure-based fingerprint privacy-preserving biometric authentication system with FVS. This method requires the process of registration in order to identify the core though it does not reveal any information about the minutiae. The performance reported from evaluation with FVC2002 DB2 is 94% of GAR with FAR being 0.03%. In 2009, Xi and Hu [171] proposed an FVS-based Fingerprint based on composite features that requires no pre-alignment and evaluated this method with FVC2002 DB2 dataset, reporting GAR of 98.5% while FAR is 0.01%.

Iris is another hidden biometric that requires complex techniques in order to meaningfully and correctly capture. Lee et al. [98] presented an FVS-based privacy-preserving biometric authentication system with local iris features in which multiple local regions' iris features are extracted from the iris image. Clustering method is applied to generate exact values of the unordered set. The problem of alignment is addressed by using a shift-matching technique. Through experimental results, 128-bit private keys were generated using iris data with no prior registration.

Apart from fingerprints and iris, face has also been incorporated with the FVS. Wu and Yuan [169] proposed to apply FVS on a face online authentication system in which instead of using the original face template, a transformed face template is used with a key with FVS to provide revocability for the face template. However, because the face template is transformed and applied with FVS, it is expected that this method suffers from great degradation. Joshi and Sanghavi [85] integrated a Face FVS in Cloud Computing. Facial features are extracted from user's face image then converted to binary string to be bound with a secret key in FVS.

Beside unimodal privacy-preserving biometric authentication system and single-technique privacy-preserving, FVS has also been used as the protection layer for multimodal privacy-preserving biometric system or as one of the components in a multi-technique privacy-preserving scheme. Leng and Teoh [99] combined 2DPalmHash-Code, cancellable biometric, and Fuzzy Vault to protect palmprint templates. Re-

cently, Bobkowska et al. [21] combined iris, fingerprint, and face biometrics to construct a multibiometric privacy-preserving biometric authentication system with the purpose of preventing fraud in e-passports with FVS. Another security technique that is also incorporated in this method is the use of steganography in mapping biometric images to one another. The location map functions as the secret key, protected by FVS.

There have also been studies that incorporate multiple methodologies to construct a privacy-preserving biometric authentication system. For instance, Yang et al. [180] use bio-hashing algorithm to generate two transformed templates and apply FCS and Fuzzy Vault to generate two sketches, respectively. The sketches are then fused with two operations: 'AND' operation and 'OR' operation to switch the focus on performance or security.

2.4.4 Protocol-based Protection

Bio-cryptosystem constructs biometric authentication system using encryption techniques at the protocol level, which plays an important role in ensuring the security of biometric data. With the rapid development of smart devices, bio-cryptosystem has become more and more crucial in protecting the user's privacy.

2.4.4.1 Client/server-based Biometrics Authentication Protocol

Assuming that the server is secure, Xi et al. [170] proposed a client/server protocol authentication system based on fingerprint in which the original features from fingerprint are protected by Elliptic Curve Cryptography (ECC) in the transferring from the client to the server. On the server side, biometric keys are generated and protected using FVS. The security of this protocol has been shown by analyses of several types of attack in addition to the details about memory and time usage. Experiments have been evaluated on the NIST Special Database 24 and FVC2002 DB2, yielding competitive results. Odelu et al. [119] showed that the multiserver

scheme in [70] is exposed to a threat with certain flaws then proposed an improve multi-server authentication protocol with biometric smart card and ECC. Various attack scenarios have been analyzed in addition to the simulation for formal security verification. Recently, dealing with the privacy of autonomous vehicle users, Jiang et al. [79] devised a cloud-centric three-factor authentication protocol for authentication and key agreement called CT-AKA in which biometrics, passwords, and smart cards are combined to control access. The authors synthesized three eminent biometric protection techniques FVS, FCS, and Fuzzy Extractor to ensure a leakage-free protocol in addition to two sessions keys being used in the protocol. Formal proof of this method is also provided to show its security strength.

2.4.4.2 Secure Multiparty Computation-based Biometric Security Protocol

Secure multiparty computation (SMC) is a powerful cryptography protocol which can protect the input privacy of each participant [23]. It has found some applications in privacy-preserving biometrics security systems [23, 29, 52, 144]. Bringer et al. [23] provided an overview of an early SMC application on privacy-preserving biometrics security. It focused on securing the face identification from a database, and distance computation of fingerprint and iris representations. Chun et al. [29] considered the privacy-preserving biometric authentication problem where the biometric authentication process is outsourced to the cloud and the biometric data is fully encrypted. An outsourceable privacy-preserving biometric authentication (O-PPBA) protocol was proposed. The proposed O-PPBA can take advantages from both homomorphic encryption and the garbled circuit. One drawback is the requirement for another independent cloud service provider. Tian et al. [144] stated that the existing biometric-based remote user authentication (BRUA) methods in the client-serve setting lack certain privacy considerations, e.g., authorized user's multiple sessions should not be linked while the user's identity remains anonymous to the cloud server. In addressing this issue, a privacy-preserving biometric-based remote

user authentication (PriBioAuth) proposed was proposed. Based on the SMC technique, secure biometrics matching protocol was proposed. One of the advantages is that no user interaction is required for the biometrics matching. Similar to [29], it requires two independent servers. A major issue with these works is that no matching/authentication performance evaluation has been conducted. In the biometrics community and in practice, matching performance is most important. The challenge is the conflicting goal of achieving high biometric authentication accuracy while maintaining high privacy protection.

2.4.4.3 Zero-knowledge proof-based Biometric Security Protocol

Zero-knowledge proof is a cryptography protocol where party A can prove to party B that part A has certain knowledge and yet without revealing any other additional information [52]. This nice property is well suited for privacy-preserving biometrics authentication and some interests have been made [20, 66]. In real-life security systems, authentication processes often involve many attributes/identifiers, e.g., password, login name, and biometrics etc. of a personal identity. In [20], a privacy-preserving scheme in addressing the problem of verification of multiple identifiers and proofs of identity was proposed. The proposed idea is to generate aggregate signatures on commitments which are then used for privacy-preserving identity proof via the zero-knowledge proof protocol. The security of the proposed scheme has been formally proved under the co-gap Diffie-Hellman assumption for groups with bilinear maps. The authors in [66] proposed a mobile phone-oriented privacy-preserving biometric authentication scheme. The proposed scheme used machine learning-based classifier to extract a revocable biometric identifier and then produced a cryptographic identify token encoding the biometric identifier. Finally, the cryptographic identity token is embedded into the zero-knowledge proof protocol for the privacy-preserving authentication. The proposed scheme was integrated with a key agreement mechanism to address the man-in-the-middle Mafia attack on the conventional zero-knowledge proof based identify verification protocol. Biometrics

matching performance has been provided.

2.5 Research Limitations and Opportunities

In addition to the fact that many of the existing works, although privacy-preserving mechanisms applied, are exposed to the ARM [100], there have been proofs that biometric authentication systems are compromised by the hill-climbing [110] and the pre-image attacks [95, 97]. While ARM is an exclusive attack in the field, hill-climbing and pre-image attacks are not. This means that there are more and more attacks that can be devised and launch to compromise a biometric authentication system. Hence, it is important that new privacy-preserving mechanisms must be able to protect the biometric authentication systems from these attacks. This is the main target of this thesis as it seeks to devise a privacy-preserving biometric authentication system that not only is resistant to the abovementioned attacks but also does not sacrifice its authentication performance for the security.

2.6 Chapter Summary

This chapter has reviewed the related work in biometric authentication and the privacy-preserving mechanisms then provided a systematic taxonomy that can be used for the current and emerging work in the field. It has also pointed out the need to defend current and emerging biometric authentication systems from popular attacks, including the ARM. The next chapters will present the design to achieve this goal.

Chapter 3

Cancellable Template Generation based on K-nearest-neighbor Local Structures

The work reported in this chapter (mostly from Section 3.2 to Section 3.4), has been partially published for publication in the following articles:

Tran QN, Hu J. A Multi-Filter Fingerprint Matching Framework for Cancelable Template Design. IEEE Transactions on Information Forensics and Security. 2021 Mar 26;16:2926-40.

Tran QN, Hu J, Wang S. Alignment-free cancelable template with clustered-minutiae local structure. In2018 IEEE Global Communications Conference (GLOBECOM) 2018 Dec 9 (pp. 1-6). IEEE.

3.1 Introduction

As presented in Chapters 1 and 2, there exists a need to provide secure biometric authentication in terms of template privacy while the performance is not sacrificed. This chapter first proposes a robust set of fingerprint features then evaluates it with the existing partial DFT as the transformation. However, due to the transformation's being exposed to the ARM, an ARM-resistant transformation is proposed. Specifically, the concept of using the KNN clustering algorithm to construct the local structures for the recognition of fingerprints will be presented. Employing the same concept from [146], this work first clusters the set of minutiae, then performs the

feature extraction. Specifically, extending the previous work, this newly proposed method significantly improves the performance by applying the KNN Clustering algorithm, making the outcome more usable and able to be implemented in real-world environments. To do this, the novel process first employs the partial Discrete Fourier Transform (pDFT) that was proposed in [165] to generate the biometric cancellable template and examine the performance of the proposed features. It then presents the Multivariate Polynomial Transformation (MPT) to enable ARM resistance for the set of features.

3.2 KNN-based Local Structure

3.2.1 KNN Clustering Algorithm

KNN is one of the most basic clustering techniques. The algorithm works by iterating through a finite set of data points and finding the k nearest points of the reference point by calculating the their distance to it. Based on the attributes of the dataset, an appropriate distance metric is chosen. As a result, one data point may belong to multiple clusters.

In the proposed process, the set of minutiae is clustered with the KNN based on their physical position on the fingerprint. For this work, the Euclidean distance metric has been used. The clusters will then be referred to as local structures in this work.

3.2.2 Feature Extraction

In this section, the details of the proposed scheme are presented.

Suppose that a set of N minutiae extracted from a fingerprint image is denoted as:

$$M = \{m_i\}_{i=1}^{N} \tag{3.1}$$

in which $m_i = (x_i, y_i, \theta_i, t_i)$ and x_i and y_i are the horizontal and vertical coordinate of the minutia, respectively; θ_i is the orientation of the minutia; and t_i indicates the type, whether an ending or a bifurcating minutia. In order to construct the local structures, the kNN algorithm is applied on the set M. Iterating through each of the minutiae in the fingerprint, kNN constructs a cluster that contains $k + 1$ minutiae, including the reference minutia itself. Each of the cluster is considered as a local structure. Connecting each of the minutiae a' in the local structure with the reference minutia a, the following features are extracted from each pair:

$$f = (l_{aa'}, \alpha, \beta, t_{a'}) \tag{3.2}$$

where:

- l is the Euclidean distance between the member minutiae and the reference minutia.
- α is the angle formed by minutia orientation vector and the line connecting.
- β is the angle formed by minutia's orientation vector and the line connecting.
- t is the type of minutiae.

This process results in a feature matrix of size $4 \times k$ for each local structure in the fingerprint image. There are totally N local structures, corresponding to N minutiae in the fingerprint.

After the feature extraction phase, a process of quantization is applied in order to compensate for the distortion caused by the elasticity of skin. In details, an appropriate stepsize for each of the feature (except the minutia type) is selected, denoting as: b_l, b_α, and b_β for l, α, β, respectively. Therefore, the total number of bits used to represent a local structure's feature matrix is: $b = b_l + b_\alpha + b_\beta$. This means that upon translating into decimal number, after quantization, the value of each feature vector in the feature matrix is a number ranging from 0 to 2^b (corresponding to string containing b 0 bits to b 1 bits). At this point, the feature matrix becomes

a vector of k decimal numbers. Those numbers that appear only once in the vector act as the index of the bins in a binary string that contains 2^b bits. These positions are assigned the values of 1's meanwhile the rest have value of 0's. At the end, each feature matrix is represented by a sparse 2^b binary string. This process is the same as bin-indexing process in [162].

The original features of the fingerprint are protected with bin-indexing since they are partially hidden after the process of choosing indices. However, as if an attacker were able to acquire the binary string of a local structure, the information leakage could lead to the expose of indices that appear once in the quantized feature vector. Therefore, it is vital that each of the binary strings are applied a non-invertible transformation to be protected.

3.3 Cancellable Template Generation with Partial DFT

First of all, a DFT matrix is expressed as follows:

$$U = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & W & W^2 & \cdots & W^{2^b-1} \\ 1 & W^2 & W^4 & \cdots & W^{2(2^b-1)} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 1 & W^{2^b-1} & W^{2(2^b-1)} & \cdots & W^{(2^b-1)(2^b-1)} \end{bmatrix} \tag{3.3}$$

where b is the number of elements in the binary string and $W = e^{-j2\pi/b}$. The DFT vector f_c of the binary string f_b that has 2^b elements is calculated as:

$$f_c = U f_b \tag{3.4}$$

where f_b is the original feature representation of a local structure in the form of a 2^b-column vector.

With U being used, the transformation applied is reversible. Hence, in order to satisfy the irreversibility characteristic, instead of using the full-rank matrix U, a submatrix of U, referred to as ω is used. In order to generate ω, a vector P that contains the index of the chosen row in U is randomly generated.

$$P = [p_1, p_2, p_3, \ldots, p_R] \tag{3.5}$$

Since ω is a submatrix of U, the length R of the vector P that determines ω's number of rows must be in the range $[1, 2^b - 1]$ where an ω with $2^b - 1$ rows is the matrix U itself. The greater R is, the more features are selected to be used for matching but the less secure the original features become. In this scheme, to balance between the performance and security, $R = 500$. On the other hand, each $p_i \leq 2^b - 1$ since p_i acts as the index of the row chosen in U. This is how ω is constructed from the original DFT matrix U. After this step, the partial DFT vector is calculated as follows:

$$f_{pDFT} = \omega f_b \tag{3.6}$$

From the equations 3.4 and 3.6, the relationship between f_{DFT} and f_{pDFT} can be drawn as:

$$f_{pDFT} = [f_{DFT}(k_1), f_{DFT}(k_2), \ldots, f_{DFT}(k_R)]^T \tag{3.7}$$

f_{pDFT} is a vector comprises of complex numbers, which represent the selected features based on the parameter key K in the frequency domain.

3.3.1 Matching in the Transformed Domain

In order to protect the privacy of the original fingerprint features, matching is performed in the transformed domain. The process of matching a query fingerprint is essentially the same as for a template: cluster the minutiae, extract and quantize the features, and apply non-invertible transformation.

Assume that after clustering, the template image has N_t local structures, whereas

the query image has N_q local structures. Note that $N_t \neq N_q$ can happen due to the difference between two images. Extracting the features as in Eq. 3.2, followed by a quantization process, and finally using pDFT to apply non-invertible transformation, each local structure from the template and query is represented by a complex vector f_{pDFT} of length R. For a better illustration, each f_{pDFT} from the template and the query is referred to as h_{C_t} and h_{C_q}, respectively, for $C_t = 1, 2, ..., N_t$ and $C_q = 1, 2, ..., N_q$. The dissimilarity between two local structures from the template and query is calculated as follows:

$$d(h_{C_t}, h_{C_q}) = \frac{e^T * e}{(h_{C_t}^T * h_{C_t}) + (h_{C_q}^T * h_{C_q})} \tag{3.8}$$

in which:

$$e = h_{C_t} - h_{C_q}$$

The distance between two local structures ranges from 0 to 1, meaning absolutely identical or absolutely different, respectively. After the calculation of the distance between all pairs of local structures from template and query, the pair that has the least distance is selected as the dissimilarity score between the template and query. The matching is a match if this score is less than a pre-defined threshold.

3.3.2 Experimental Results and Analysis

The proposed scheme was implemented with the community-respected public databases FVC2002-DB1, FVC2002-DB2, FVC2002-DB3 [108], and FVC2004-DB2 [109]. Each of these databases has 100 fingerprints. Each of which contains eight impressions. More importantly, the resolution of the databases varies from one to another as indicated in Table 3.1.

The fingerprint recognition software *VeriFinger SDK* was used to extract minutiae from raw fingerprint image.

Each of the databases is tested with One versus One Matching Protocol. In detail,

Table 3.1: Database resolution details

Database	FVC2002DB1	FVC2002DB2	FVC2002DB3	FVC2004DB2
Number of fingerprints	100	100	100	100
Number of images/fingerprint	8	8	8	8
Resolution	500 dpi	569 dpi	500 dpi	500 dpi
Sensor Type	Optical	Optical	Capacitive	Optical
Image size	388×374	296×560	300×300	328×364
Image Quality	Good - Medium	Medium	Medium - Low	Very Low

the first impression of each fingerprint is used as the template. Genuine testing uses the second impression meanwhile impostor testing uses the first impression of other fingerprints in the database as the query to compare against the template. This results in having a total of 100 genuine tests and 4950 imposter tests. In order to evaluate the performance of the proposed methods, the Equal Error Rate (EER), the False Rejection Rate (FRR), and the False Acceptance Rate (FAR) are employed. FAR is the rate that the system mistakenly authenticates a fingerprint from different finger. FRR is the rate that indicates the system's probability to reject the fingerprint from the same finger. EER is the rate when FAR and FRR are equal.

3.3.2.1 Lost-key Scenario

As the user loses their personal key to an adversary, it can be used as a tool to penetrate the biometric authentication system. This scenario is simulated by using the same key to create templates for all users' fingerprint. The Receiver Operating Curve (ROC) of all databases evaluated under this scenario is shown in Figure 3.1. The resultant EERs are presented in the Table 3.2.

As shown in Figure 3.1, the best EERs that the algorithm can reach with keylength of 500 are: 0.2%, 0.04%, 4.78% and 7.64% for FVC2002 DB1, FVC2002 DB2, FVC2002 DB3, and FVC2004 DB2, respectively. Though observing a slight decrease of 0.01% and 0.49% comparing to the work proposed in [165] when working with FVC2002 DB1 and FVC2002 DB3, the algorithm tends to work well with all other the databases tested, even with very low-quality images in FVC2004 DB4. Moreover,

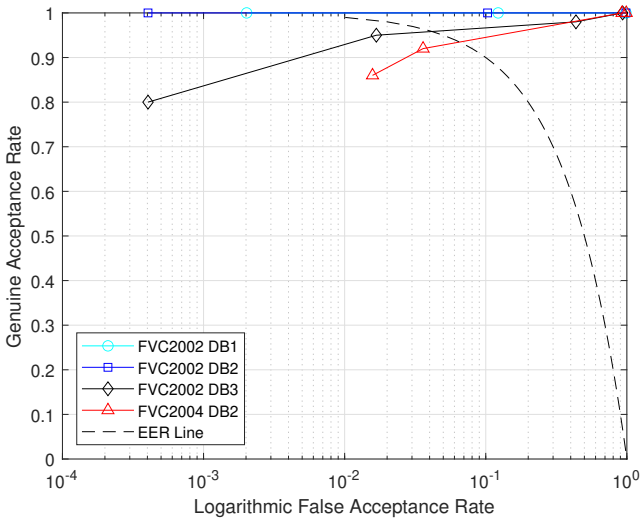


Figure 3.1: ROC Curves

the keylength parameter applied in this work is $R = 500$. Meanwhile in [165], the keylength evaluated was 1000. This means that a shorter vector of features is used, achieving a better result. At the same time, the shorter the keylength is, the more secure the system becomes.

3.3.2.2 Revocability and Diversity

Revocability and Diversity test evaluates a very important characteristic of a fingerprint cancellable template design. It is used to make sure that different templates generated with different keys from the same fingerprint are not related. In order to test the new method's revocability and diversity, the same direction as Wang et al. [165] is followed. In detail, the process goes as follows: 50 transformed templates were generated from the first impression of each fingerprint in FVC2002-DB2, each with a different set of parameter keys to match with the original. This test yields the pseudo-impostor score. On the other hand, each user is assigned different key to match to each other. This test produces real impostor score. The distribution of these scores is plotted in the Figure 3.2. A statistical analysis is performed to determine how similar the distribution of the impostor score to the pseudo-impostor score: To compare, the mean of impostor score compared with pseudo-impostor

Table 3.2: EER comparison (%)

	FVC2002DB1	**FVC2002DB2**	**FVC2002DB3**	**FVC2004DB2**
Ahmad et al. [7]	9	6	27	-
Jin et al. [83]	5.19	5.65	-	11.64
Yang et al. [182]	5.93	4	-	-
Jin et al. [82]	4.36	1.77	-	21.82
Das et al. [34]	2.27	3.79	-	-
Tulyakov et al. [153]	3	-	-	-
Wong et al. [168]	1.97	2.54	-	9.2
Kumar et al. [94]	-	4.98	-	-
Sandhya and Prasad [133]	4.71	3.44	8.79	-
Wang and Hu [162]	3.5	4	7.5	-
Wang and Hu [164]	3	2	7	-
Wang et al. [161]	1	2	5.2	13.3
Wang et al. [165]	0.19	1	4.29	9.01
Proposed method	**0.2**	**0.04**	4.78	**7.64**

score is: 0.1142 and 0.1141, respectively. Meanwhile, the standard deviation of impostor score and pseudo-impostor score is: 0.0107 and 0.0110, respectively. It is clear that they are very close to each other. This means that the reissued templates using different parameter keys are virtually impostor to the original template. Hence, a malicious adversary cannot perform a cross-template attack.

3.3.2.3 Security Analysis:

The proposed method translates the features extracted from fingerprint into binary string representation. Therefore, in order to secure the original features, the binary string is what needs protecting. To achieve this, a partial Discrete Fourier Transformation, serving as the non-invertible transformation, creates a security barrier using an underdetermined system of linear equations: As mentioned above, ω is the submatrix of D by selecting specific rows from D. This makes ω a full row rank but column rank-deficient. Since there are 2^b columns in D, ω has 2^b columns too. Moreover:

$$nullity(\omega) = 2^b - rank(\omega) \tag{3.9}$$

or equivalently:

$$nullity(\omega) = 2^b - R \tag{3.10}$$

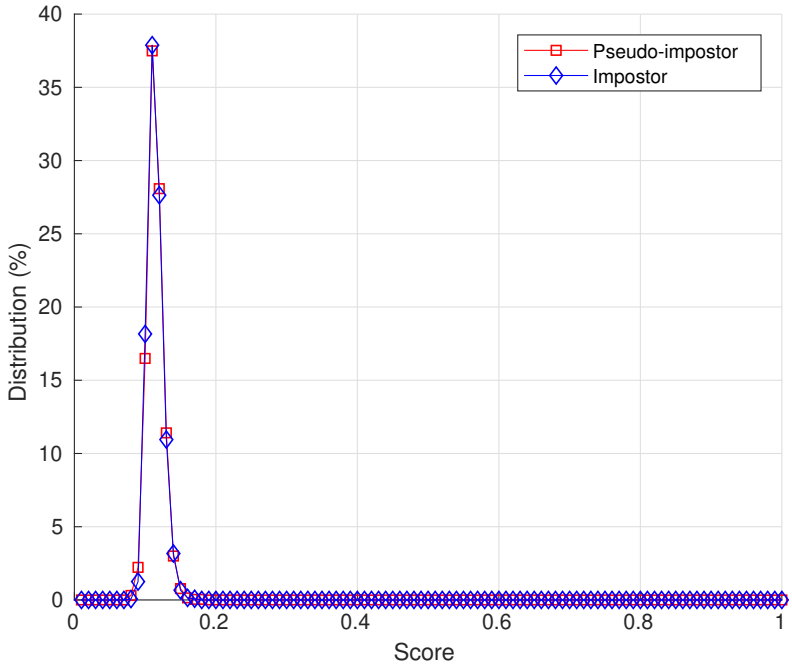


Figure 3.2: Normalized Score Distribution

In the experiments, the following parameters were set: $R = 500$ and $b = 16$. Therefore, there are $2^b - 500$ free variables in the equation system. Assuming that the malicious adversary launches an ARM into the algorithm, they must rebuild the full rank equation system by gathering enough equations. With keylength $R = 500$ and there are $2^{16} = 65536$ equations required in reaching a unique solution, each system compromised gives an adversary 500 equations. In order to get the user's original features, the adversary would need to successfully compromise approximately 132 applications.

Although this non-invertible transformation can mitigate the chance of a hacker successfully launching an ARM into the biometric system, it does not fully defend the original biometric data from this attack. Thus, an additional method is proposed to generate biometric cancellable template that can defend the biometric authentication system from ARM by leveraging the power of multivariate polynomial system of equations.

3.4 Cancellable Template Generation with the Multivariate Polynomial Transformation

In this section, the performance of the algorithm is improved by expanding the idea of using the KNN to construct the so-called KNN Minutia Extractor with the help of the Multivariate Polynomial Transformation (MPT), which also functions as an irreversible transformation. In other words, MPT is not only used for protection but also to contribute to generating the minutia descriptor.

3.4.1 Multivariate Polynomial Transformation (MPT)

Irreversible transformations have mostly been relied on underdetermined system of linear equations. However, this approach has been proved to be vulnerable to the Attack via Record Multiplicity [100]. Therefore, the non-linear Multivariate Polynomial Transformation (MPT) is proposed to utilize the power of non-linear system of polynomials to protect the raw fingerprint features. In [32], Courtois et al. claimed that solving large systems of quadratic multivariate polynomial equations is an NP-hard problem. In this case, a higher-degree multivariate polynomial is used to increase the complexity of finding the solutions.

Given the vector $f_b = (b_l, b_\alpha, b_\beta, t)$ and a multivariate polynomial equation is generated with the form:

$$\sum_{1}^{\mu} \prod_{1}^{\nu} x_j^{\chi} = \zeta \tag{3.11}$$

where μ, ν are the number of monomials and the number of variables in each monomial, respectively. Both are predefined as positive integers. χ is the degree corresponding to variable x_j; and x_j's are the components of vector f_b.

Upon plugging in the variables and evaluating the equation, the result ζ is retrieved. Repeating this process 4 times (which is also the number of components in

each vector f_b) gives us the Multivariate Polynomial System of Equations:

$$\left\{ \begin{array}{l} \sum_{1}^{\mu_1} \prod_{1}^{\nu_1} x_{j_1}^{\chi_1} = \zeta_1 \\ \sum_{1}^{\mu_2} \prod_{1}^{\nu_2} x_{j_2}^{\chi_2} = \zeta_2 \\ \sum_{1}^{\mu_3} \prod_{1}^{\nu_3} x_{j_3}^{\chi_3} = \zeta_3 \\ \sum_{1}^{\mu_4} \prod_{1}^{\nu_4} x_{j_4}^{\chi_4} = \zeta_4 \end{array} \right\} \tag{3.12}$$

This is a well-defined Multivariate Polynomial System of Equations and solving such system is an NP-hard problem. Security of the system can be enhanced by introducing more variables to the system. In other words, security is improved by adding more *virtual features* to each vector f in Eq. 3.2. In this case, a hash function can be applied that takes the features as input. In more detail, each feature from a feature vector is fed into the hash function SHA224 to create 28 8-bit hash values. After all four features have been hashed, there are a total of 112 hash values, which are to be used as input for the MPT. However, this also increases the computation that needs to be done in order to perform matching. Therefore, the balance between the number of variables in an MPT and the time to perform matching is an optimization problem. A hash function alone is not strong enough in this case due to the quantization of the input. MPT can enhance the system's security.

All the ζ values obtained by evaluating all four polynomials are then translated into a binary string and concatenated altogether position-wisely. In addition, each ζ value will be given one extra bit to indicate its sign following the simple rule: If $\zeta \geq 0$, its sign bit is '1'. Otherwise, it is '0'. Note that all the sign bits are appended at the end of the string. The whole binary string is then translated back into a decimal number. This means that each cluster is now represented by:

$$F_T = \{f_T\}_1^k \tag{3.13}$$

where each f_T is now a decimal number.

At this stage, F_T is used to represent each minutia and will be stored in the database functioning as the template to be compared against.

3.4.2 KNN Minutia Descriptor Similarity

The normalized similarity between two descriptors: template υ_T and υ_Q KNN Minutia Descriptors is calculated as follows:

$$S(\upsilon_{Tp}, \upsilon_{Qr}) = 1 - \frac{|\mathrm{P}(\upsilon_{Tp}) \backslash \mathrm{P}(\upsilon_{Qr})| + |\mathrm{P}(\upsilon_{Qr}) \backslash \mathrm{P}(\upsilon_{Tp})|}{|\upsilon_{Tp}| + |\upsilon_{Qr}|} \tag{3.14}$$

where:

- $P(t)$ is a set function that converts KNN minutia descriptor data t into a set, meaning that no duplication is allowed.
- $\backslash$ is the set difference operation.

After the similarity between all pairs has been calculated, the process first ranks them in a descending order. Scores with higher ranks are given higher weights. The hypothesis underpinning this is that if the query comes from the same finger as the template, more high scores are present. On the other hand, in case of a false-accept attack, a very low number of high scores are present. The formula to generate the KNN score S_{knn} is as follows:

$$S_{knn} = \sum_{1}^{k_p} S_i w_i \tag{3.15}$$

where:

- k_p is the number of considered pairs
- S_i is the score at rank ith

- w_i is the corresponding weight given for score at rank ith. Kindly note that all the weights sum to 1.0.

3.4.3 Experimental Performance

The scheme is evaluated with the four publicly available databases previously discussed; FVC2002-DB1, FVC2002-DB2, FVC2002-DB3, and FVC2004-DB2. Each database has 100 fingerprints with 8 samples each. There are a total of 800 fingerprint images in the database. The quality of the fingerprint images in these database ranges from very good to very poor, respectively.

In order to evaluate the performance of the module, the traditional FVC protocol is used: to generate the FRR, each sample is matched against all other fingerprint samples of the same finger, yielding 2800 genuine tests. On the other hand, FAR is generated by matching each fingerprint's first sample with one another, yielding 4950 impostor tests in total.

3.4.3.1 Lost-Key Scenario

To simulate the Lost-Key scenario, the same set of parameters are applied to generate the Multivariate Polynomial systems of Equations to transform the whole database. The EER is recorded and presented in the Table 3.3.

Table 3.3: KNN-MPT's performance in EER (%)

	FVC2002 DB1	**FVC2002 DB2**	**FVC2002 DB3**	**FVC2004 DB2**
KNN-MPT	4.02	3.64	11.62	18.95

The ROC curve for the four databases is shown in Fig. 3.3

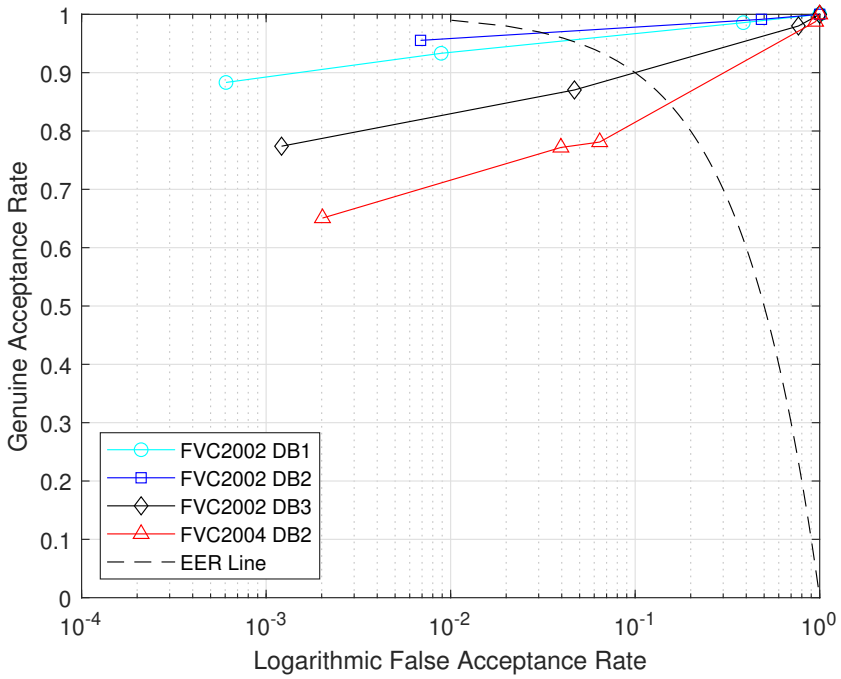


Figure 3.3: KNN-MPT's performance over four publicly available databases.

3.5 Conclusion

This chapter presented a robust local-structure-based set of fingerprint features along with an ARM-resistant transformation to protect the biometric templates. Two transformations: the pDFT and the newly proposed Multivariate Polynomial Transformation have been evaluated with the feature set. While the former mitigates the ARM, the latter enables the feature set with ARM-resistance capability. However, in comparison with the current state-of-the-art methods, this system's performance is inferiror. This means that the requirement from the Research Question stated in Chapter 1 to retain good performance is not satisfied. Hence, the proposed method only gives a partial solution to the Research Question stated in Chapter 1 by resolving the problem of the ARM. In the next chapter, a cancellable template framework is constructed by incorporating the KNN-MPT module proposed in this chapter with another cancellable fingerprint template module. The latter also provides resistance to the ARM while the framework achieves the best performance among the current state-of-the-art cancellable fingerprint template methods.

Chapter 4

An Enhanced Minutia Cylinder Code Design and a Multi-filter Fingerprint Cancellable Template Framework

The work reported in this chapter (mostly from Section 4.2 and Section 4.3), has been partially published in the following article:

Tran QN, Hu J. A Multi-Filter Fingerprint Matching Framework for Cancelable Template Design. IEEE Transactions on Information Forensics and Security. 2021 Mar 26;16:2926-40.

4.1 Introduction

As outlined in Chapter 1, there is a significant need for privacy preservation when biometric authentication is used. This chapter seeks to answer the research question that this thesis raised in chapter 1 by incorporating the KNN-MPT module with the newly proposed EMCC module into a complete framework that provides high level of accuracy and security. In detail, this chapter proposes a novel framework for cancellable fingerprint template and validates it by comparing it with the current state-of-the-art algorithms. The framework improves the performance by combining

two cancellable fingerprint modules: the KNN-MPT and the EMCC. Each of them is able to defend the fingerprint features from the current notorious attacks in the field, such as: ARM, hill-climbing, and pre-image attack as shown later in this section.

The remainder of this chapter is structured as follows: In Section 4.2, the concept of MCC is briefly reviewed and followed by the methodology of how MCC is applied in order to generate new features. It also presents the standalone performance of this module. The design of the framework along with the experiments and security analysis is presented in Section 4.3.

4.2 Enhanced Minutiae Cylinder Code (EMCC)

In this section, after revisiting the main concept of the MCC, the newly proposed Enhanced MCC is explained. Afterward, the process of applying the so-called Irreversible Order-based Binary Encoding is explained.

4.2.1 MCC Concepts

Minutia Cylinder Code (MCC), introduced by Cappelli et al. [24] in 2010 represents each minutia based on a 3D structure that contains information of relative minutiae's Euclidean distance and angle. This section briefly reviews the concept of creating the MCC for each minutia. More details on MCC can be found in the original publication [24].

The cylinder of a minutia $m = \{x_m, y_m, \theta_m\}$ in the set M is constructed by setting m as the center associated with a radius R and the height 2π. The cylinder is wrapped around by a cuboid with the base being aligned with the minutia's orientation. The cuboid is divided equally into L_D layers. The total number of cells of each cylinder is: $L_S \times L_D = L_C$. Then, each layer is equally partitioned into L_S number of small cuboid cells. The value of the cell at the position (i, j, k) is determined by the directional and spatial contributions of the minutiae within its

neighborhood.

Each of which is formed by a $\Delta_S \times \Delta_S$ base and Δ_D height, where $\Delta_S = \frac{2\times R}{L_S}$ and $\Delta_D = \frac{2\times\pi}{L_D}$. At this point, each cell is given three indices (i, j, k) to define its position in the cuboid.

The angle associated to all cells at height k in the cylinder is defined as: $d_{\varphi k} = -\pi + (k - \frac{1}{2}) \times \Delta_D$. The coordinates of the center of each cell with indices (i, j) when projected onto the cylinder's base is given as:

$$p_{i,j}^m = \begin{bmatrix} x_m \\ y_m \end{bmatrix} + \Delta_S \cdot \begin{bmatrix} \cos(\theta_m) & \sin(\theta_m) \\ -\sin(\theta_m) & \cos(\theta_m) \end{bmatrix} \cdot \begin{bmatrix} i - \frac{N_S+1}{2} \\ j - \frac{N_S+1}{2} \end{bmatrix} \tag{4.1}$$

Note that this is the position expressed in the spatial coordinates of the minutiae template.

Each cell possesses a numerical value $C_m(i, j, k)$ to which the contributions from the minutiae in the neighboring region $N_{p_{i,j}^m} = \{m_t \in T; m_t \neq m, d_S(m_t, p_{i,j}^m) \leq 3\sigma\}$ around p_{ij}^m add up. 3σ is the radius of the region whereas $d_S(m_t, p_{i,j}^m)$ is the Euclidean distance between the minutia m and p. The cell value of each cell is calculated as follows:

$$C_m(i, j, k) = \left\{ \Psi(\textstyle\sum_{m_t \in N_{p_{i,j}^m}} (C_m^S(m_t, p_{i,j}^m) \cdot C_m^D(m_t, d_{\varphi k}))) \right\} \tag{4.2}$$

if $\xi_m(p_{i,j}^m) = valid$

In case $\xi_m(p_{i,j}^m) = invalid$, $C_m(i, j, k)$ is *invalid*, too.

In equation 4.2:

- $C_m^S(m_t, p_{i,j}^m)$ and $C_m^D(m_t, d_{\varphi k})$ refer to the spatial and directional contribution to cell (i, j, k), respectively, of minutia m_t. They are defined as follows:

$$C_m^S(m_t, p_{i,j}^m) = G_S(d_S(m_t, p_{i,j}^m)) \tag{4.3}$$

  where:

$$G_S(t) = \frac{1}{\sigma_S\sqrt{2\pi}} e^{(-\frac{t^2}{2\sigma_S^2})} \tag{4.4}$$

and

$$C_m^D(m_t, d_{\varphi k}) = G_D(d_\phi(d_{\varphi k}, d_\theta(m, m_t)))$$

where:

$$d_\phi(\theta_1, \theta_2) = \left\{ \begin{array}{l} (\theta_1 - \theta_2) \text{if} -\pi \leq \theta_1 - \theta_2 \leq \pi \\ (2\pi + \theta_1 - \theta_2) \text{if} \theta_1 - \theta_2 < -\pi \\ (-2\pi + \theta_1 - \theta_2) \text{if} \theta_1 - \theta_2 \geq \pi \end{array} \right\} \quad (4.5)$$

in which:

$$G_D(\alpha) = \frac{1}{\sigma_D \sqrt{2\pi}} \int_{\alpha - \frac{\Delta_D}{2}}^{\alpha + \frac{\Delta_D}{2}} e^{-\frac{t^2}{2\sigma_D^2}} dt \quad (4.6)$$

- $\Psi(v) = \frac{1}{1+e^{-\tau(v-\mu)}}$ is a sigmoid function that is used to not only limit the contribution of dense minutiae region but also map the value in the range $[0, 1]$. It is controlled by two parameters τ and μ.

- $\xi_m(p_{i,j}^m)$ determines if a point $p_{i,j}^m$ is invalid or not by assessing the region around it with the following rule: if $d_S(m, p_{i,j}^m) \leq R$ and $[p_{i,j}^m \in Conv(T, \Omega)$, then $\xi_m(p_{i,k}^m)$ is *valid*. Otherwise, it is *invalid*. $Conv(T, \Omega)$ is the convex hull [121] of the minutiae in set T. This function is used to filter out the parts of the cylinder that are outside of the considering fingerprint area which might not contain discriminative information.

In the end, the cylinder set generated from an ISO/IEC 19794-2 minutiae template is: $CS = \{C_m | C_m \text{ is valid}, m \in M\}$. Each C_m is the cylinder of the minutia m that contains values $C_m(i, j, k)$. In order for a cylinder C_m to be valid, it has to satisfy certain conditions. These conditions are presented in the original paper [24].

To summarize, an MCC vector contains the cell values in the range $[0, 1]$, which are the spatial and directional contributions of the neighboring minutiae. The next section uses the MCC cell values to derive new features for better matching.

4.2.2 EMCC

This section introduces a new method based on the concept of natural language processing. The main idea is to transform each cylinder C_m in the Cylinder Set CS into a bag of words Γ_m. Within each word, an encoding process will be applied as an irreversible transformation. Therefore, the Cylinder Set CS becomes the Bag Set $BS = \{\Gamma_m | m \in T\}$, which will be stored in the database for matching. Pseudo-code of this process is presented in Algorithm 1.

Algorithm 1: Generate Encoded Bag of Words

```
Data: Set of Cylinder CS, Number of Words Λ, Projection Matrix R_P
Result: Set of Bag of Words BS
foreach Vector C_m in CS do
    multiply R_P with C_m to get C_mP;
    generate Λ words from C_mP to get Bag of Words Γ_m;
    foreach word w in Γ_m do
        Binarize w orderly;
```

4.2.2.1 Random Projection of C_m:

In order to generate the cancellable template, a random projection will be applied on the vector of MCC values. In more detail, a random *Projection Matrix* R_P with dimension $d_R \times L_C$ is generated to project the C_m. Each R_P's value lies in the range of (0, 100].

$$C_{mP} = R_P * C_m \tag{4.7}$$

4.2.2.2 The Generation of Bag of Words

After projecting the MCC value vector, a bag of words is generated from the C_{mP}. Each bag contains individual unit of words. Each word comprises of two adjacent cell values that are chosen from the cylinder. Such word construction can help retain the relationship among the cells, making the words more discriminative. Λ words for each bag are generated. Λ is randomly chosen. After this

process, each bag of word can be represented as: $\Gamma_m = \{w_1, w_2, ..., w_\Lambda\}$ in which $w = (C_{mP}(i,j,k), C_{mP}(i',j',k'))$.

4.2.2.3 Irreversible Order-based Binary Encoding

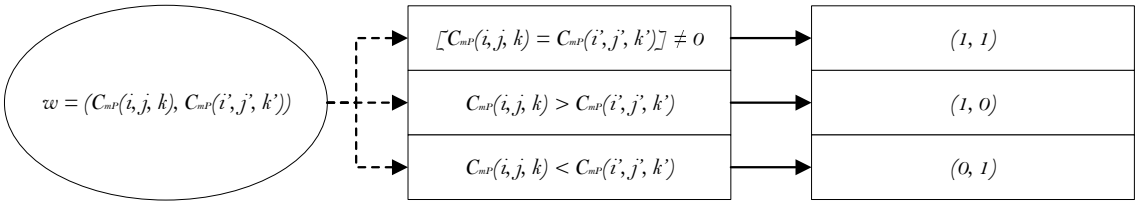


Figure 4.1: Irreversible Order-based Encoding Process: A word consisting of two real-valued parts is encoded into a binary code based on their relative values.

A random projection-based cancellable template design is subject to the ARM. Each word (i.e. cell values) is protected by applying an Irreversible Order-Based Encoding function as indicated in Fig. 4.1. Specifically, the two parts $C_{mP}(i,j,k)$ and $C_{mP}(i',j',k')$ of each word, which are MCC neighboring cells in real-valued form, will be compared against each other. The greater value yields bit '1' while the smaller yields bit '0'. If they are equal, then both yield '1'. Both values cannot be zero due to the fact that based on Eq. 4.7, C_m is non-negative and R_P is generated in a non-negative manner. The order-based encoding provides an irreversible transformation on the fingerprint features. If an adversary is able to retrieve the transformed template, which is in the binary form, he can only determine which part of a word yields a greater real number. There is no way to find out the original value. For instance, assume that $C_{mP}(i,j,k) = 0.95$ and $C_{mP}(i',j',k') = 0.62$. After the irreversible Order-based Encoding, this word is encoded as $[1,0]$. There is an infinite number of words that can be encoded as $[1,0]$.

Therefore, the Order-based Binary Encoding will be applied to the C_{mP} as the irreversible transformation. On the other hand, the projection matrix is a parameterized transformation with random elements. Hence, in order to generate a new cancellable template, a different projection matrix R yields a different C_{mP}. In the end, the C_{mP} can be used as the cancellable fingerprint template to be stored in the

database.

Next, each bag will be separated into small chunks with length of Φ words. The purpose of this separation is to enhance the tolerance of the bag of words by the localization of error tolerance at the chunk level, thus improving the overall performance. Therefore, each Bag of Word contains $\lceil \frac{\Lambda}{\Phi} \rceil$ words and eventually becomes: $\Gamma_m = \{\gamma_1, \gamma_2, ..., \gamma_{\lceil \frac{\Lambda}{\Phi} \rceil}\}$ in which each $\gamma = \{w_{b1}, w_{b2}, ..., w_{b\Phi}\}$ and w_b is the two-bit encoded word. This is the transformed data which is stored in the database as the templates.

4.2.2.4 Similarity between Two Bags of Words

To evaluate the similarity between two Bags of Words, the similarity between two chunks is generated. The similarity between two chunks is the Jaccard similarity calculated position-wisely, meaning that the chunk at *i-th* position in the template will be compared against its counterpart at the same position. Specifically, it is given in the following formula:

$$\delta_{\gamma_{ti},\gamma_{qi}} = \frac{H(\gamma_{ti}, \gamma_{qi})}{2\Phi - H(\gamma_{ti}, \gamma_{qi})} \tag{4.8}$$

where $H(\gamma_{ti}, \gamma_{qi})$ is the Hamming distance between two chunks γ_{ti} and γ_{qi}, respectively. A word from template and a word from query are considered a match to each other if and only if each of their bits is the same to its counterpart position-wisely.

The similarity between two chunks is filtered by a parameter ϵ: Those pairs possessing passed similarity are considered as matched chunks. Counting the number of matched chunks (η) between two Bags of Words and using the Jaccard similarity, it is possible to evaluate the similarity between two Bags of Words. Hence, Eq. 4.8 becomes:

$$\Delta_{\Gamma_m,\Gamma_n} = \frac{\eta}{2\lceil \frac{\Lambda}{\Phi} \rceil - \eta} \tag{4.9}$$

After the similarity between all pairs of Bag of Words has been calculated, the next step is to determine the matching score S_{emcc} for this layer. The Dynamic

Local Similarity Sort (DLSS) is proposed, a modified version of the Local Similarity Sort (LSS) from [24] to do this.

DLSS: In the original version, LSS sorts all the similarity scores in a descending order and calculates the average score based on the n_P pairs chosen, which is partially dependent on the number of minutiae of the template and the query. In our scheme, this parameter is chosen based on the behavior of the scores. First, a threshold ω_{bag} is set to filter the low similarity scores between two Bags of Words. Sorting is performed after this. The score values lower than ω_{bag} will be set to 0 after sorting. When matching with a genuine fingerprint, a low matching score is not desired. On the other hand, an impostor sample should not generate a high score. Therefore, it is necessary to control the number of considered pairs so that the genuine matching yields a high score while the impostor matching generates a low score. An *upper bound* and a *lower bound* are set to overcome this challenge with the hypothesis that a genuine sample possesses a high number of highly correlated Bag of Words meanwhile an impostor sample has a low number of similar Bag of Words. In short, these parameters are used to ensure that the number of considered pairs falls in the specified range.

The EMCC matching score between two fingerprint images is generated as follows:

$$S_{emcc} = W(n_p) * \Delta_{\text{mod}} \tag{4.10}$$

where:

$$\Delta_{\text{mod}} = \frac{\sum_{1}^{n_p} \Delta_i^2}{n_p} \tag{4.11}$$

On the other hand, $W(n_p)$ is a dynamic weight function of the number of chosen pairs n_p controlled by the parameter ρ. It is defined as:

$$W(n_p) = e^{-\rho * \left(\frac{1}{n_p} - 0.1\right)} \tag{4.12}$$

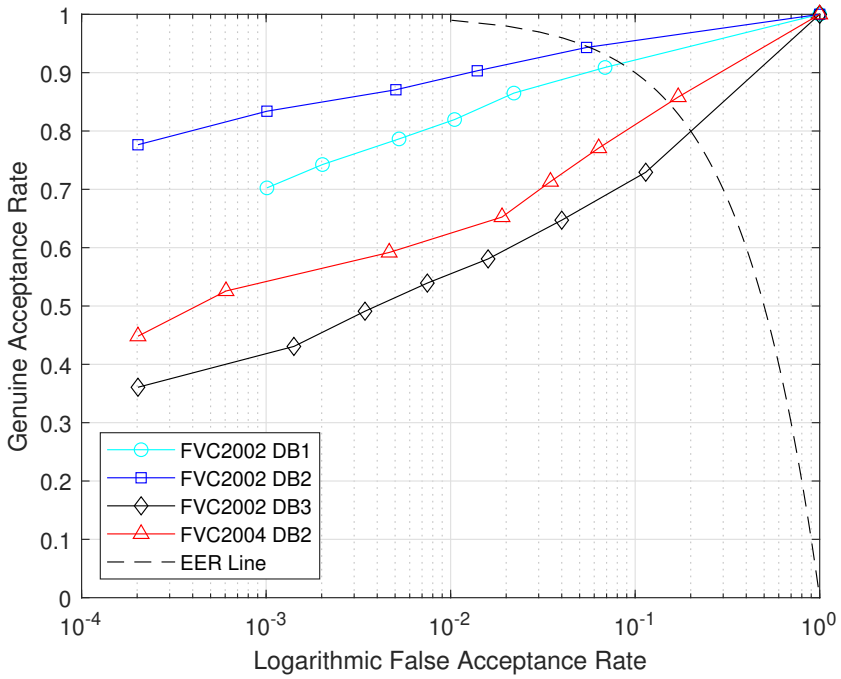


Figure 4.2: EMCC's performance over four publicly available databases.

4.2.3 Experimental Results

In order to evaluate the performance of the EMCC, it was implemented with four publicly available databases FVC2002-DB1, FVC2002-DB2, FVC2002-DB3, and FVC2004-DB2. As mentioned from the previous chapters, the quality of these databases range from very good to very noisy, respectively. In addition, the FVC protocol is chosen for the evaluation: To calculate the FRR, each sample is matched against the other samples of the same fingerprint. With FAR, The first sample of each fingerprint is matched against its counterpart of other fingerprints. Finally, the EER is employed to provide the most accurate evaluation of the proposed method's performance.

Lost Key Scenario To simulate the "Lost-Key" Scenario, the same projection matrix is applied as the parameter key to transform the features before the Irreversible Order-based Encoding is applied. The performance is presented in Table. 4.1 while the ROC curves are illustrated in Fig. 4.2.

As shown in Figure 4.2, these results are comparable but still inferior to the

Table 4.1: EMCC's performance in EER (%)

	FVC2002 DB1	**FVC2002 DB2**	**FVC2002 DB3**	**FVC2004 DB2**
EMCC	8.9	5.67	23.40	15.49

state-of-art methods. However, the Irreversible Order-based Encoding has a strong security, especially against the ARM attack. Therefore, combining the current approach with the KNN-MPT to create a framework that provides not only stable performance but also increased template security.

4.3 Multi-filter Fingerprint Cancellable Template Design

In order to improve the performance of fingerprint matching, yet retain the template security, EMCC and KNN-MPT are both incorporated into a multi-filter framework in which the decision is given based on multiple measures. Firstly, a fingerprint's minutiae are fed to both the EMCC and KNN-MPT module. These two modules will extract the features and apply the transformation on the corresponding templates, respectively. Finally, the two transformed templates are stored in the database. When a query fingerprint comes, it goes through the same process to have its transformed template generated. Three measures are used to assess the similarity of the two fingerprints: EMCC measure, KNN measure, and the fused measure from which, a decision is made. The overall structure of this framework is illustrated in Fig. 4.3.

As shown in Fig. 4.3, as a fingerprint is enrolled in the system, two modules will simultaneously extract the features and generate their corresponding cancellable template using their own user keys. The templates are stored in the database. In the verification stage, the same user keys are used to transform the query fingerprint for the appropriate modules to produce the cancellable templates. Matching is performed feeding the three measures: KNN measure, EMCC measure, and fused

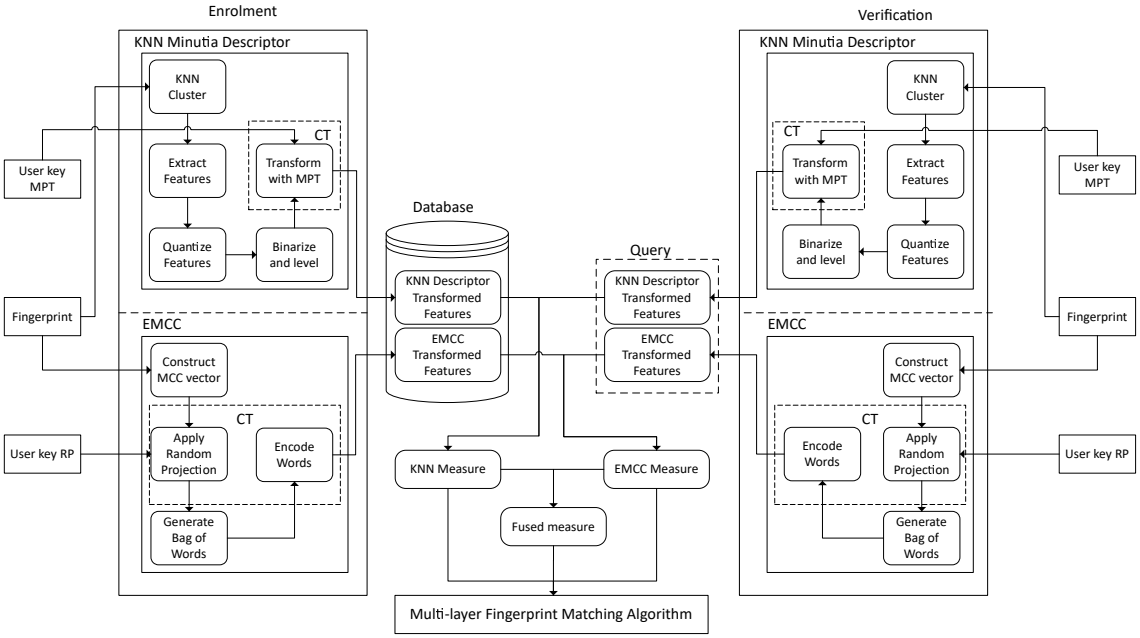


Figure 4.3: Multi-filter Fingerprint Matching Framework

measure into a Multi-layer Fingerprint Matching Algorithm.

4.3.1 Multi-filter Fingerprint Matching Algorithm

As the features have already been extracted, and the similarity calculated from both layers, the next stage is to generate a fused matching score and make a decision: whether the query B is from the same fingerprint as the template A or it is only an impostor trying to gain unauthorized access.

Eq. 4.12 is expanded to generate a fused score as follows:

$$S_{fused} = e^{-\lambda\left(\frac{1}{w_{emcc}S_{emcc}+w_{knn}S_{knn}}\right)} \tag{4.13}$$

This score will be fed to the decision-making module for the consideration along with other measures.

Traditionally, a single fused score has been used for matching decision. Although a fused score can take into account multiple different characteristics, the end result tends to be a trade-off score which can filter out some subtle discriminative char-

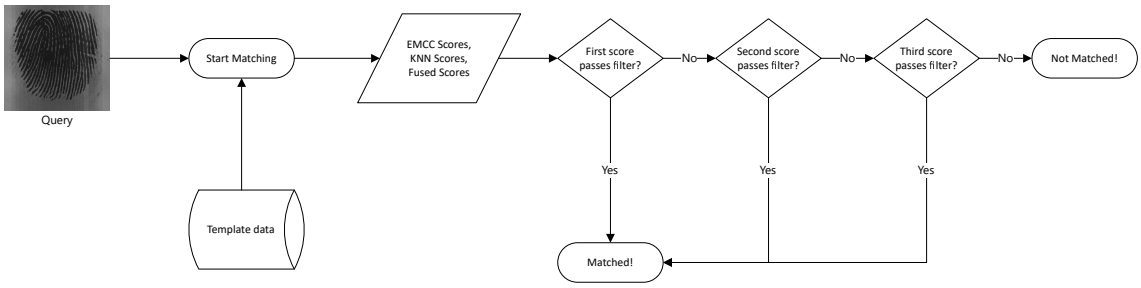


Figure 4.4: Multi-layer Fingerprint Matching Algorithm: After all three measures have been generated and fed to the Matching module in the framework, the stored template data is retrieved from the database. A predefined measure is chosen to be compared first. If the similarity satisfies the threshold in the current filter, a "matched" decision is given. Otherwise, another measure is compared for the similarity in the next filter. This process repeats until either a measure satisfies its corresponding threshold or there are no more measures to compare with, leading the decision to be "non-matched."

acteristics of some instances. In order to address this issue, a multilayer-filtering algorithm is proposed as shown in Fig. 4.4. A multi-staged matching decision scheme that takes the EMCC similarity score, the KNN similarity score, and the fused score into consideration is designed in this framework to determine if two fingerprints come from the same finger. In details, after the three measures have been generated, a predefined measure will be compared against the threshold $T1$. If it does not pass this threshold, the next measure is checked against the threshold $T2$; If unsuccessful, the last measure is checked against the threshold $T3$. If none of the measures is successful, the decision will be "non-matched".

4.3.2 Experimental Results

Table 4.2: Computation time in seconds

	KNN Descriptor		EMCC	
	Generate	Match	Generate	Match
FVC2002 DB1	2.82	0.34	0.33	1.47
FVC2002 DB2	3.94	0.63	0.47	3.18
FVC2002 DB3	1.12	0.09	0.27	1.05
FVC2004 DB2	1.24	0.13	0.30	1.33

Table 4.2 shows the average computational cost for the EMCC and the KNN

Descriptors. Two methods were implemented in Python 3.6 and run on the 6th generation Intel Core i7-6700 3.4Ghz with 16GB of RAM. As shown, the total time to generate a cancellable template for both measures with this system is approximately 4 seconds, which is practically acceptable in real-world applications. With the KNN Descriptor, the maximum base and power of the operation are 6 and 28, respectively, which correspond to approximately 3 and 5 bits. Therefore, the calculations performed in an MPT are not exponential, which means that not much computational power is required. In addition, the program was not written in its most optimal manner. Hence, it can be tuned to use much less computational power. Importantly, the framework can be implemented in C with optimization techniques to achieve its best efficiency.

In order to evaluate the accuracy of the framework, the four publicly available datasets FVC2002-DB1, FVC2002-DB2, FVC2002-DB3, and FVC2004-DB2 are chosen to be implemented. The parameters used in the experiments are presented in Table 4.3. Note that the parameters introduced in this scheme are shown. The parameters from other papers are detailed in the original papers.

Both the traditional FVC and One versus One protocol were employed. In One versus One protocol, the FRR is generated by matching the first and the second instance of each fingerprint against each other while FAR is calculated the same as FVC's.

Lost Key Scenario:

In order to simulate this scenario, the same parameter key is used to generate the polynomials for all users in the KNN-MPT module. For the EMCC module, the same random projection matrix is used to evaluate the impostor performance in the lost key scenario. Since two methods are fused, the separate performances of the EMCC module and the KNN-MPT module are evaluated, then compare them with the proposed fused method to show the effect in improving the performance. All variations of the matching algorithms are assessed and shown in Table 4.5. Bold text indicates the lowest EER. In addition, the Receiver Operating Characteristic

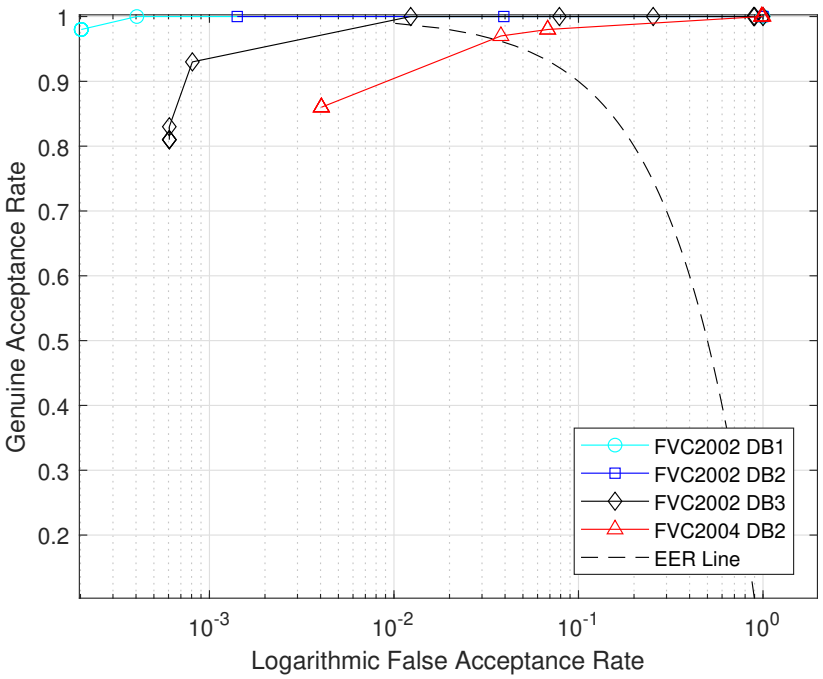


Figure 4.5: ROC for One versus One protocol

(ROC) curves for all the datasets in One versus One protocol and the FVC protocol are shown in Fig.4.5 and Fig.4.6. The thresholds T1, T2, T3 varied based on the databases. In order to generate the ROC curves, two of the three thresholds will be fixed while the other is changing. The best EER is recorded and chosen to generate the ROC curves.

The resultant EER's of the proposed framework are presented and compared in Table 4.4 and Table 4.6. As shown in these tables, the proposed framework shows the best performance in comparison with the other state-of-art methods in the field. On the other hand, with the traditional FVC protocol, except the work proposed in [132], the proposed framework shows a superior performance when compared with the rest, even when dealing with the FVC2004 DB2, which has been considered to be a tough dataset due to the noise and distortion present in the fingerprint images. The reason for the slightly worse performance than the work in [132] is because Sadhya et al. [132] only conducted 1000 genuine tests in their experiments while the FVC protocol with 2800 tests is followed strictly. Hence, it is not comparable.

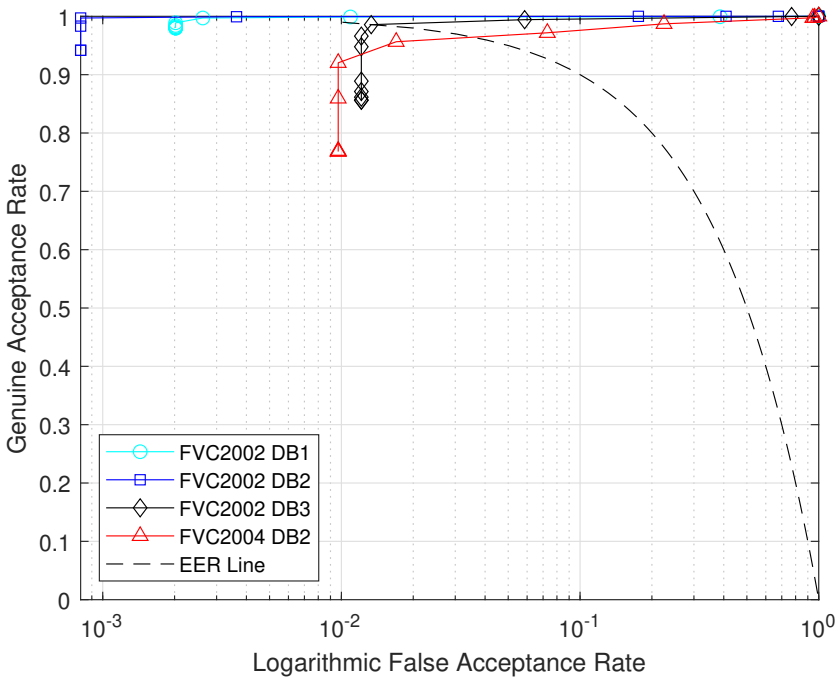


Figure 4.6: ROC for FVC protocol

Table 4.7 shows the decidability index *d'* for each database using the standalone measure EMCC, KNN, or Fused. However, since the proposed framework applies multiple thresholds to make a decision, these indices do not reflect fairly how separate the genuine and impostor distributions are in terms of matching decision. Thus, a more sophisticated decidability analysis is conducted.

Decidability Analysis: According to the original definition in [167], decidability index is used to evaluate the gap between the same samples' matching score distribution and impostor samples' matching score distribution. Therefore the whole database's d' has lost its interpretation. For illustration purpose, a fingerprint is chosen to calculate the decidability index *d'* as follows: Each of the fingerprint's impressions is matched against the other impressions of the same fingerprint to build the genuine matching score distribution; the first impression of the fingerprint is matched against the first impression of other fingerprints to build the impostor matching score distribution. This protocol yields 28 genuine scores and 99 impostor scores for each measure: EMCC, KNN-MPT, and Fused measure. The match-

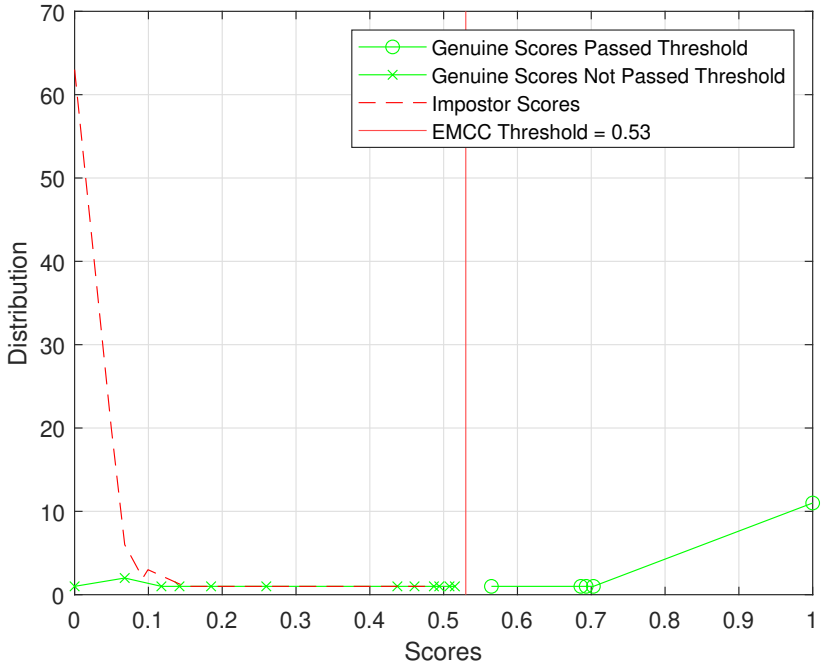


Figure 4.7: EMCC's d' = 2.2547

ing algorithm being used in this experiment follows the order EMCC-KNN-Fused, meaning that the EMCC score will be compared against EMCC threshold first. If it passes this threshold, decision is made. If not, the KNN score is checked against a KNN threshold and the same process applies. If the pair comparison cannot pass any of the three layers, the query is considered as an impostor. Fingerprint 1 from FVC2002-DB1 is chosen as the subject for this experiment. The whole process is illustrated in Fig. 4.7, Fig. 4.8, and Fig. 4.9. Kindly note that there exist discontinuities in these graphs because no database can generate continuous scores.

As shown in Fig. 4.7, Fig. 4.8, and Fig. 4.9, after the first filter EMCC with threshold being set to 0.53, from the 28 genuine tests, 15 tests passed this filter while 13 failed. All of which were carried on to the second filter of KNN where 10 tests were correctly identified as genuine and three still failed. In the end, the last filter of the fused measure accepted these last three tests. On the other hand, all 99 impostor tests have been filtered out correctly with no single impostor has been falsely accepted by any of the three filters. The *d'* index progressively increases from 1.147

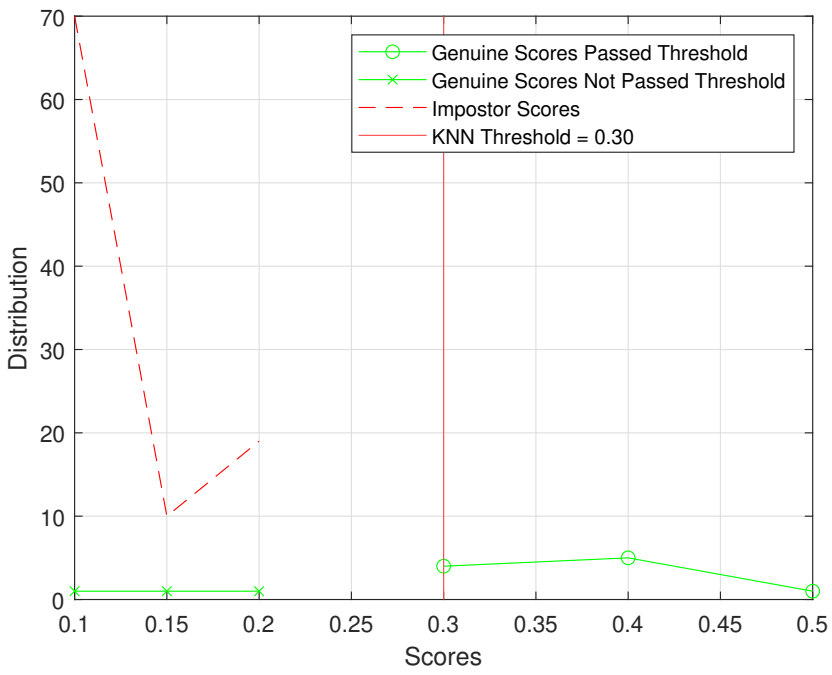


Figure 4.8: KNN's d' = 2.2712 (before entering EMCC filtering, original KNN's d' = 2.5418)

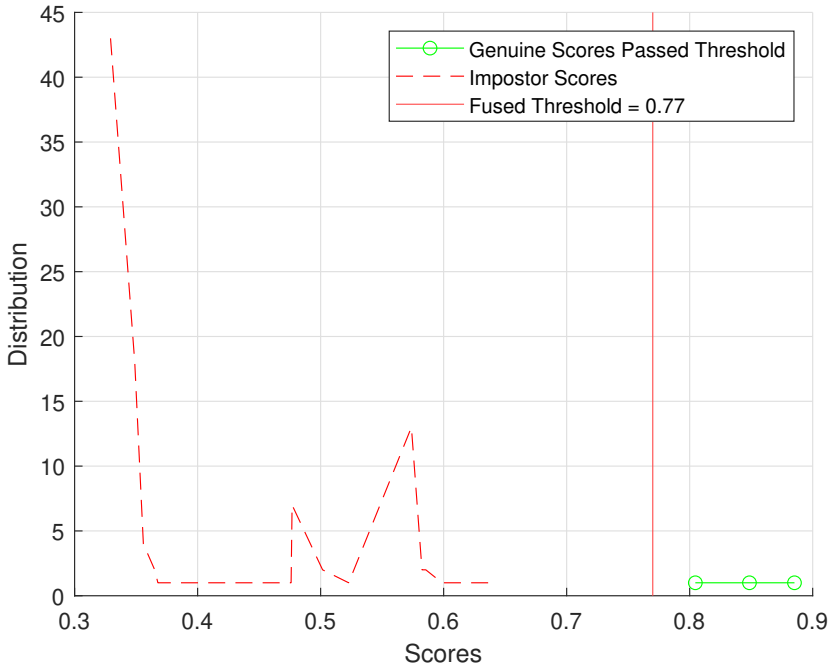


Figure 4.9: Fused's d' = 5.8250

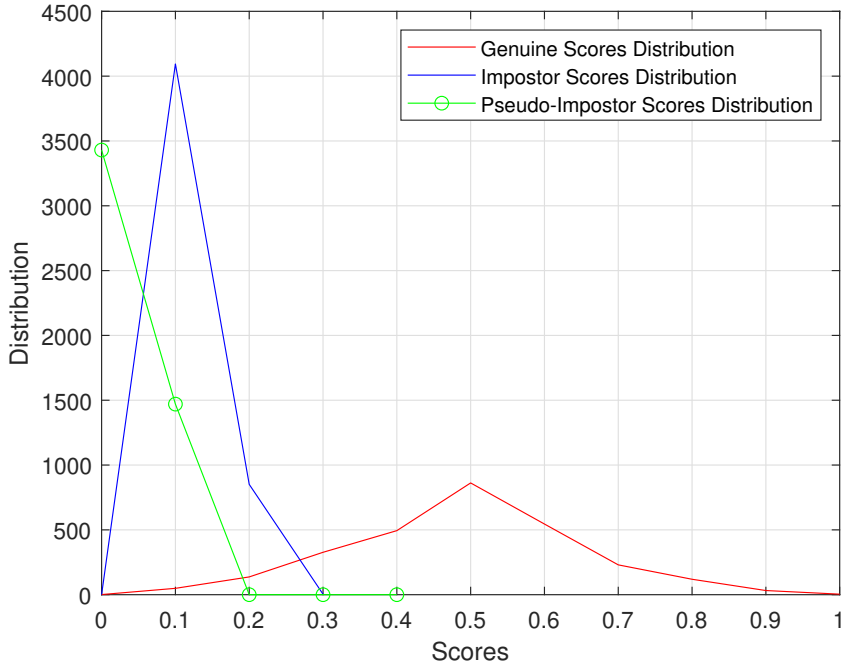


Figure 4.10: Revocability Test with KNN Minutia Descriptor Measure

in the EMCC filter to 2.2712 in the KNN-MPT filter, and finally reached 5.8250 with the Fused filter. The very last *d'* index is of crucially important as it is the point where the framework decides to reject or not. In addition, as shown from the graphs, the overlapped region between the genuine and impostor score distribution shrinks from the beginning to the end of the matching process. This analysis not only shows the uniqueness but also the accuracy of this proposed framework. A unique advantage of our multi-layer matching decision framework is: a high threshold sufficiently far away from the overlapped region of the genuine and imposter score distributions could be used to make a "yes" decision in the first two stages. Therefore, a "yes" result tends to be highly reliable. For the instances that could not pass the high threshold will be passed to the next layer with different feature distributions where an additional information is introduced to aid the matching decision. Note that statistics in this one example is not reliable due to small population. However, it well illustrates the workings of the proposed framework.

Revocability and Diversity are what makes a cancellable template strong or not.

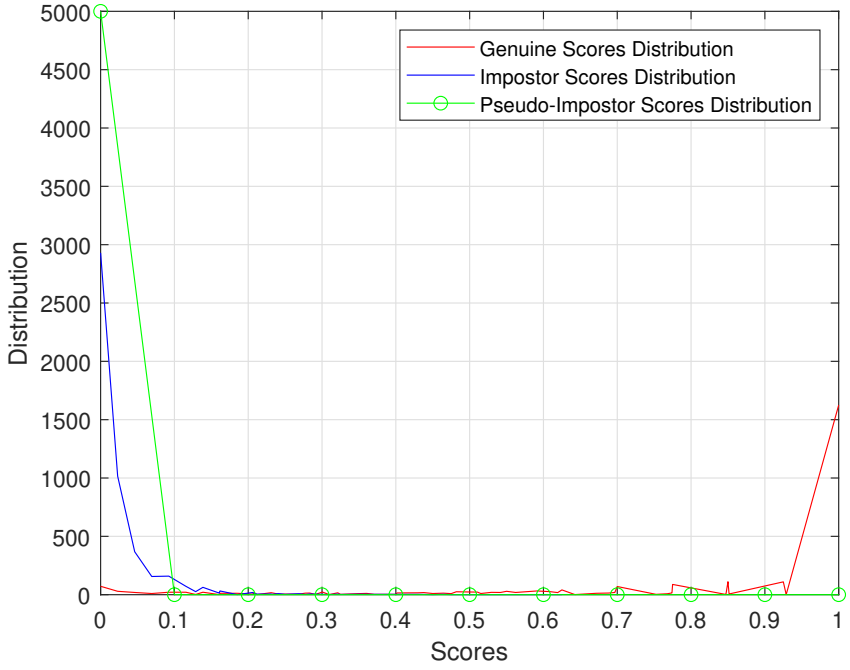


Figure 4.11: Revocability Test with EMCC Measure

Specifically, these characteristics of a cancellable template authentication system proves that templates generated by different parameter keys even from the same fingerprint should have no correlation. In order to evaluate this framework's ability to satisfy the revocability and the diversity, the same practice is followed as in [164], which is to use FVC2002 DB2 and the following evaluation protocol. For each fingerprint, the first impression is chosen to generate 50 different transformed templates with 50 disparate parameters to compare with the original templates. This experiment was conducted for all measures: EMCC scores, KNN-MPT scores, and Fused scores. These are called *pseudo-impostor* test scores. The pseudo-impostor scores are then plotted together with genuine scores and impostor scores to compare the distribution as illustrated in Fig.4.11, Fig.4.10, and Fig.4.12 for the EMCC, the KNN-MPT, and the Fused measures, respectively. The pseudo-impostor score distribution should not have a significant overlapped region with the genuine score distribution.

Looking at the figures, it can be seen that the genuine score distribution from all

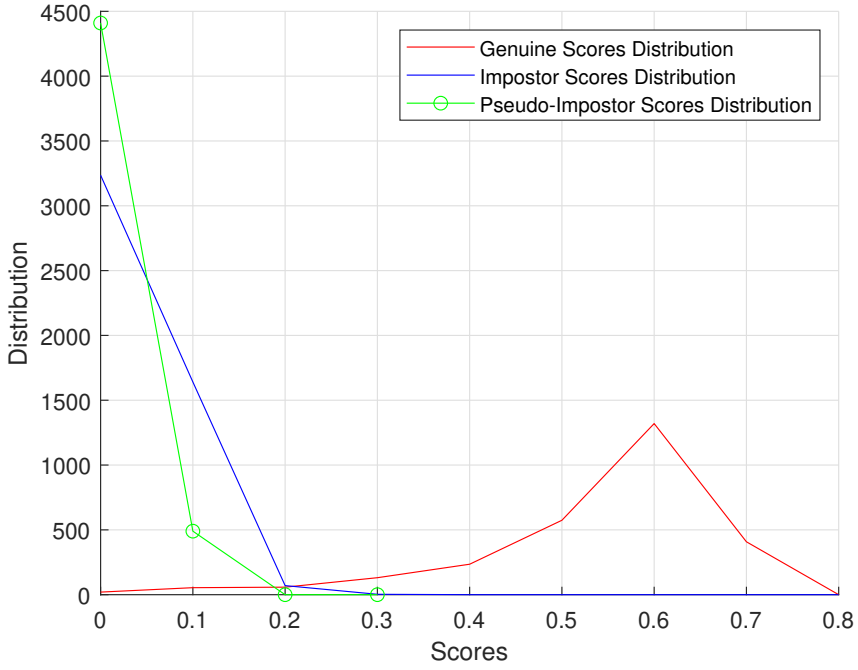


Figure 4.12: Revocability Test with Fused Measure

three measures is different from the pseudo-impostor score and the real impostor score distributions. The detailed statistics data is presented in Table 4.8.

The Standard Deviation and Mean of each type of scores are presented. There is a big difference in terms of both Standard Deviation and Mean of genuine and impostor scores. On the contrary, the EMCC Pseudo-impostor score distribution's standard deviation and mean (0 and 0, respectively) are very close to the EMCC Impostor score distribution's counterpart (0.0538 and 0.0255, respectively). The same situation happens to KNN-MPT's and Fused's Pseudo Impostor and Impostor scores.

It can be concluded that in the proposed framework, different keys generate different cancellable templates and that the attacker cannot perform a cross-template attack even if he or she is able to retrieve a cancellable template of the same finger with a different key. Therefore, the framework does satisfy the Revocability and Diversity condition.

Unlinkability Analysis: Unlinkability of a cancellable biometric template de-

sign measures the difference among transformed templates that originate from the same fingerprint. The framework in [63] proposed two linkability measures: Local Measure $D_{\leftrightarrow}(s)$ - System Score-Wise Linkability and Global Measure $D_{\leftrightarrow}^{sys}$ – System Overall Linkability. These two measures depend on the distributions of the probability $p(H_m|s)$ and $p(H_{nm}|s)$ of two templates belonging to mated or non-mated pair given a linkage score. In this test, the protocol described in [63] is followed to evaluate the $D_{\leftrightarrow}(s)$ and the $D_{\leftrightarrow}^{sys}$ for both the KNN-MPT module and the EMCC module. In details, for each module, six transformed databases are generated using six different keys. Mated score distribution is recorded by cross matching the images from the same biometric object. Non-mated score distribution is generated by collecting the scores from cross-matching different biometric object. The results for the KNN measure are plotted in Fig.4.13.

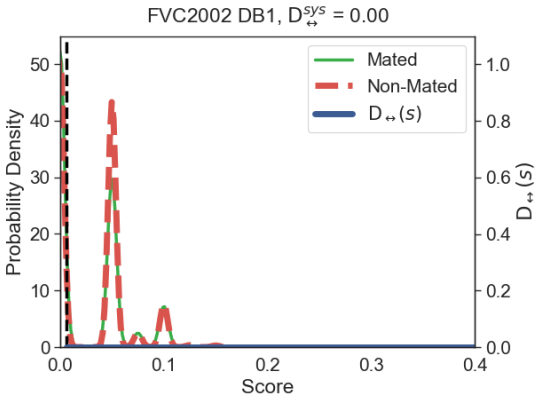
The mated and non-mated distributions in all four databases overlap the whole region. Besides, $D(s)$ is consistently 0 through the whole score distribution.

With the EMCC module, as the mated and non-mated cross-matching are evaluated, the score distribution consists of all 0's for both distributions without any variance. This means:

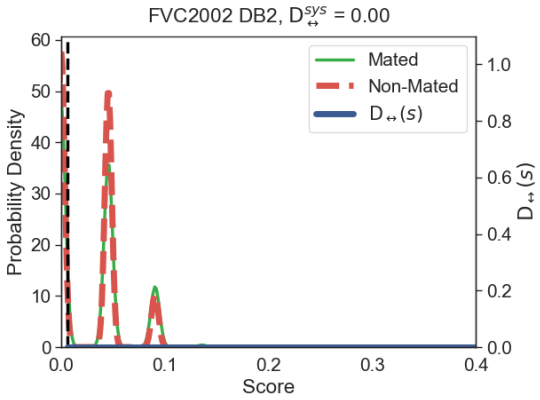
- The mated and non-mated score distribution both contain only score of 0, leading to the full unlinkability: $D_{\leftrightarrow}(s) = 0$.
- For scores other than 0, $p(H_m|s)$ and $p(H_{nm}|s)$ are undefined. Hence, $D_{\leftrightarrow}(s)$ does not exist when $s \neq 0$.
- For scores other than 0, $p(s|H_m)$ and $p(s|H_{nm})$ are undefined. Consequently, based on the mathematical definition in [63], $D_{\leftrightarrow}^{sys} = 0$.

It can be concluded that the two measures KNN-MPT and EMCC both satisfy the unlinkability condition in this protocol.

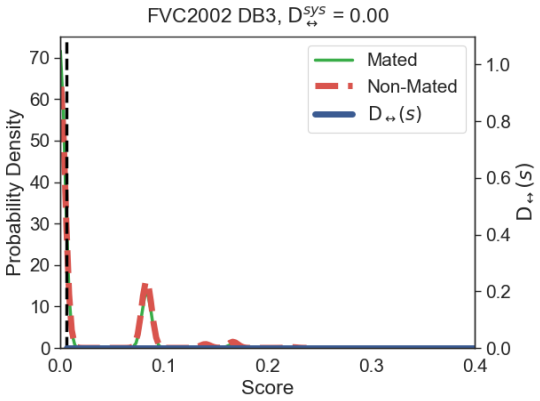
False Cross Match Rate (FCMR) and False Non-Cross Match Rate (FNCMR) Analysis: According to [139], FCMR is defined as the probability of fingerprints generated from different fingers but are considered successful match



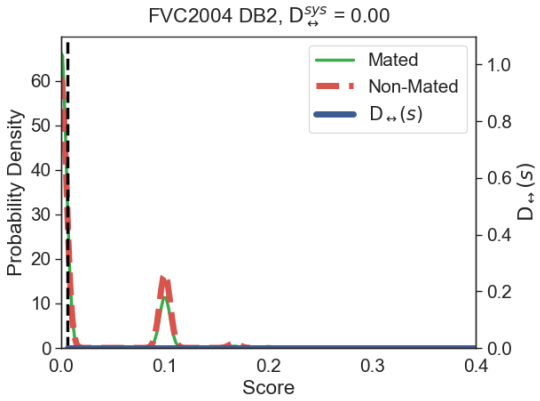
(a) KNN-MPT with FVC2002-DB1: $D_{\leftrightarrow}^{sys} = 0.0$



(b) KNN-MPT with FVC2002-DB2: $D_{\leftrightarrow}^{sys} = 0.0$



(c) KNN-MPT with FVC2002-DB3: $D_{\leftrightarrow}^{sys} = 0.0$



(d) KNN-MPT with FVC2004-DB2: $D_{\leftrightarrow}^{sys} = 0.0$

Figure 4.13: KNN-MPT's unlinkability analysis with all four databases

while FNCMR refers to the probability of unsuccessfully matched pairs of fingerprints that come from a finger using different keys. These two measures are expected to sum approximately to 1 at all points (i.e.: $FCMR + FNCMR \approx 1$).

In order to measure the FCMR, in FVC2002 DB1, the transformed template of each of the fingerprints' first impression is matched against the first impression of other fingerprints in the database. With FNCMR, the transformed templates with different keys of the first and second impression of each fingerprint are matched. The result of this test is plotted and visualized in Fig. 4.14. It can be observed from this graph that at all points, the framework satisfies the condition $FCMR+FNCMR \approx 1$.

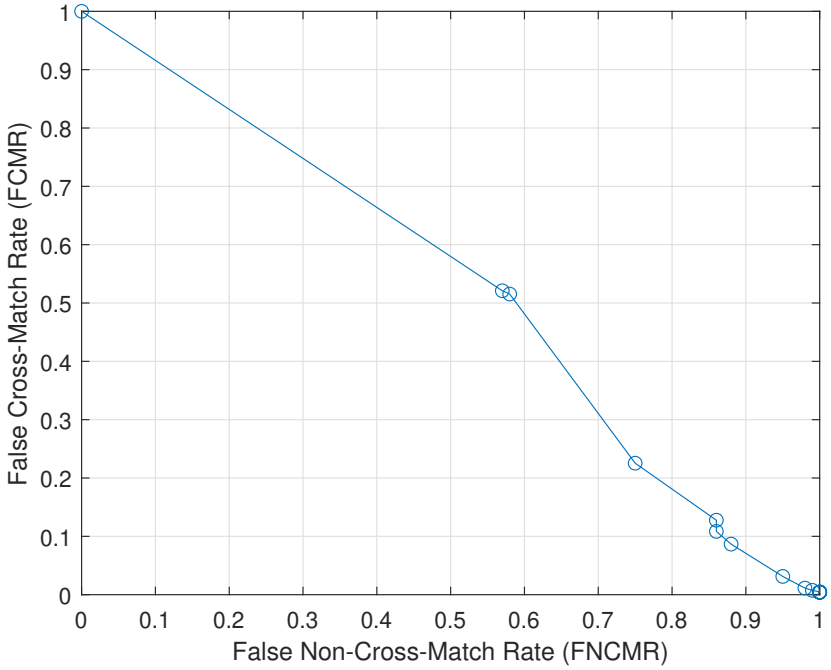


Figure 4.14: FCMR and FNCMR when $\epsilon = 0.35$, KNN Descriptor Threshold and EMCC Threshold are set at 0.7 and 0.45, respectively.

4.3.3 Security Analysis

4.3.3.1 Attack via Record Multiplicity

With only the projection matrix R_P and the compromised transformed templates, an attacker can easily reverse the random projection matrix to get the original cell values C_m as this is an invertible operation in the context of an ARM. However, before getting to the C_{mP}, the attacker must compromise the encoding transformation. Unlike the binarization process introduced in the original MCC [24] which determines the bit value based on a fixed threshold, the encoding is based on the order of the two C_{mP} values in a word. Hence, even if the attacker collects massive amount of encoded data and uses statistics tools to get the distribution of the values, the attack will be unsuccessful since no information on the cell value is exposed after encoding. In detail, two real numbers A and B will be encoded as $[1, 0]$ if $A > B$. Given $[1, 0]$, as the domain of A and B is dense, such encoding satisfies infinity-to-one mapping. It is similar in the case of $[0, 1]$ being given as the encoded

word. Given $[1, 1]$ as the encoded word, the only leaked information is that $A = B$. It also satisfies infinite-to-one mapping. Hence, it is irreversible. Without further information about A and B, the probability of finding the true values of A and B is almost zero. Even when A and B are random but not uniformly distributed, the probability of finding the true values of A and B is still negligible due to their dense domain. Therefore, this method is ARM-free.

The KNN-MPT module has many possible solutions. In addition, since the system has as many equations as the number of variables, it is a well-behaved system. An attacker can use two tools to attack this system; the Groebner method or the Newton-Ralphson method.

When an attacker uses a Groebner basis-based solver to launch the attack onto the KNN-MPT module, the complexity could get to doubly exponential in the number of variables [14]. More details and analysis on the scenarios are presented in [112]. According to [13], given a well-defined Multivariate Polynomial System of Equations of n variables with degree of at most d, the arithmetic complexity to retrieve Groebner bases is $d^{O(n^2)}$. However, this is only the complexity to calculate Groebner bases of one system that associates with one feature vector f_b. The embedded hash function increases the number of variables for the MPT, leading to more complexity to solve the system of equations.

On the other hand, the Newton-Raphson method can also be used to estimate one of the solutions of the Multivariate Polynomial System of Equations. However, due to the nature of this method, several assumptions must be satisfied. One of the most important conditions is that the starting point must be chosen appropriately. Otherwise, the method might fail to converge or the solution returned is not the correct solution of the template. According to Bezout's theorem, given that d_1, d_2, d_3, and d_4 are the degrees of each polynomial equation in the system, respectively, the system has at most $d_1.d_2.d_3.d_4$ solutions. This makes Newton-Raphson method hardly suitable to solve the Multivariate Polynomial System of Equations in the system because the solutions space grows exponentially and there is no suitable

means to verify whether a guessed solution is the correct template solution.

The above analysis is the complexity upperbound without considering the hash function as well as the constraints of the variables. In practice, these variables are in limited range instead of the whole real field. It is unclear whether there exists a deterministic solution to the constrained Multivariate Polynomial Equations System.

4.3.3.2 Pre-image Attack

Pre-image attack refers to that: given an y, it is difficult to find an x such that $y = f(x)$ [95].

EMCC module: Given the transformed templates, it is hard to find a systematical way in conducting the pre-image attack, including its approximated version, against the EMCC module. This is because of the combination of the random projection and the irreversible order-based encoding. To the best of our knowledge, there is no known closed-form mathematical solution available. For the feedback score guided solution search, please refer to the discussion on the hill-climb attack. For the input solution search without feedback score guidance, please refer to the discussion in the entropy analysis.

KNN-MPT module: Each local structure comprises of k minutiae, corresponding to k quantized feature vectors f_b's. These quantized vectors are represented by a stream of b bits. After transformation (hash+MPT), the local structure similarity scores are ranked to construct a KNN-MPT score S_{knn} from the top ranked local structure similarity scores. Given the transformed templates, it is hard to find a systematical way in conducting the pre-image attack because the hash functionality embedded in the transformation has the pre-image resistant feature.

4.3.3.3 Hill-climbing Attack

Hill-climbing attack assumes that the similarity score is accessible by the adversary. As a result, modified templates of the biometric are iteratively fed into the

recognition module until it is successful [110]. Each time, the attacker adjusts the input based on the retrieved similarity score from the previous trial to gradually approach the correct input, hence successfully gains access to the system. In the proposed framework, both the the EMCC module and the KNN-MPT module show strong security against the hill-climbing attack. Similar to the pre-image attack discussed above, this section's focus is in finding the solution that can match the original biometric feature under protection.

EMCC module: the attacker may obtain the binary representation of the transformed template, which is the result of the Irreversible Order-based Encoding. Given that the original encoded word is $[0, 1]$, other possible combinations of $[1, 0]$ or $[1, 1]$ may give a lower similarity. As a result, the attacker is able to identify the correct direction for further exploits. However, any further trials toward this direction do not reveal more information on how close the modified template is to the template stored in the database. In other words, the feedback from the similarity score does not provide any further information that helps the attacker modify the input. For example, given the two MCC values $C_{mP}(i, j, k) = 83.4$ and $C_{mP}(i', j', k') = 35.7$, the 2-bit encoded word constructed by the Irreversible Order-based Encoding is $w = [1, 0]$. Assume that the attacker launches a hill-climbing attack by choosing $C'_{mP}(i, j, k) = 70$ and $C'_{mP}(i', j', k') = 90$. After some iterations, the attacker adjusts these values based on the retrieved similarity score and ends up with $C'_{mP}(i, j, k) = 80$ and $C'_{mP}(i', j', k') = 79$, which gives the correct encoded word $w' = [1, 0]$. However, once this point is reached, any further adjustments of $C'_{mP}(i, j, k)$ and $C'_{mP}(i', j', k')$ along this direction do not change the similarity score. Hence, the attacker is not able to exploit further from this direction. As far as these two elements are concerned, there is no way to identify better points if they have the same order relationship.

KNN-MPT module: the hash function not only helps increase the number of input variables to the MPT but also makes it harder for an adversary to launch a hill-climb attack. This is because the embedded hash function destroys the input/output relationship. Each pair of input/out is uncorrelated to one another. Hence, the previous trials do not help to find the better points.

Note that many optimization methods need information from previous trials in finding the next better points, which is similar to the principle of the hill-climbing attack approach. Therefore, the advantages of the proposed KNN-MPT module and EMCC module are still useful against such attacks.

4.3.3.4 Entropy Analysis

Strictly speaking, entropy measures the probability of guessing the secret successfully. For convenience, this work adopts the common practice with the uniform distribution assumption of the concerned variables. In this case, the analysis is about the brute-force search space.

EMCC module: There is no feature quantization in this module. Therefore, feature points are dense which implies the infinite entropy if the secret is about the exact original feature point. In this module, the error tolerance is achieved via an order encoding. In practical applications, approximated features can also break into the systems, especially when the matching threshold is small. It is very difficult to provide an accurate estimation of the system entropy in this situation if the secret includes the approximated feature. A coarse entropy estimation could be made by calculating the number of quantized feature points where the quantization takes the effect of the approximation into consideration. This is plausible but also challenging as it does not have quantization in this module. In order to simulate the effect of feature quantization, the following experiment is conducted. A random template X_0 is stored which is a bag of words. Then a matching experiment is performed against artificial templates, which are generated by perturbing X_0 by adding random values of δ to each of its elements. If the bound of δ is fixed and ten times of matching experiments do not change the matching score significantly for most of the artificial templates, the maximum magnitude of δ is used as the quantization step for all elements of the feature. Through this experiment, the bound of δ is determined as 0.2. This means that the quantization zone of each feature element is 0.4, leading to 2.5 disjoint quantization zones for each of the feature elements as the feature element

value is normalized in the range [0,1]. For convenience, two possible quantized values for each feature element are used. There are 1280 cells in a feature vector. Therefore, there are 2^{1280} distinct quantized feature points, leading to the entropy being 1280 bits.

KNN-MPT module: As mentioned above, each local structure in this module is represented by the k feature vectors. Each of them is quantized and represented by b bits. When the matching is performed, the number of involved local structure pairs LS is taken into consideration. Hence, the total number of entropy bits are given as: $E_b = b * k * LS$. In the experiment, each of the three features l, α, and β is represented by 5 bits. Adding the last bit that represents the minutia type, $b = 16$. In order to generate the KNN-MPT score S_{knn}, the local structure scores are ranked in descending order then choose the two pairs with the highest scores. Hence, LS is set at 2. The number of feature vectors k depends on the database.

The brute-force search space in terms of number of trials for each method is given in Table 4.9.

There is no doubt that any result from the theoretic security analysis tends to be conservative due to the simplified assumptions. In practice, the system's FAR is a more realistic indicator of the security strength. For example, the security strength against the pre-image attack, and a practical system's entropy will be bounded by the FAR performance. This is because the FAR represents the false acceptance rate produced from the imposter attacks. It has included the effects of the matching threshold and the real biometrics distribution which a theoretic analysis is infeasible to consider. It is easy to achieve a very low FAR by increasing the matching threshold. However, it will also decrease the FRR performance at the same time. Therefore, the EER performance would be a fair indicator for measuring the security strength of a practical system as it provides the FAR performance with the balance of the FRR. The proposed system provides the best EER performance which should also provide a superior security strength in terms of entropy and resistance to the pre-image attack.

4.4 Discussion and Conclusion

In this chapter, a framework that is constituted by two cancellable fingerprint template modules is proposed. Each of these modules have been shown to be resistant to some of the current attacks on the biometric template, especially the ARM. In addition, the overall performance of the framework is comparable with the current state-of-the-art systems at the time.

The framework proposed in this chapter is a complete solution to the Research Question stated in Chapter 1 due to the following reasons: (i) It is privacy-preserving due to the ability to defend from the current attacks on the biometric template, especially the ARM as shown in the previous sections; (ii) In order to achieve the template security, the framework does not have to sacrifice its performance. However, as the Research Question suggests, there are multiple solutions. In the next chapter, an alternate solution is sought using a different approach.

Table 4.3: Parameters used in the experiments

Parameters	**Descriptions**	**Value**	
		1v1	FVC
Λ	Number of words in each bag	1280	
Φ	Number of words in each chunk	100 - 350	100, 300
d_R	Number of rows in Projection Matrix	1280	
ϵ	Chunk filtering threshold parameter	0.7 - 0.75	
ω_{bag}	Low Bag of Words similarity score filter	0.3 - 0.6	
n_P	Number of considered pairs in Eq. 4.11	[4, 10]	
ρ	Parameter in (4.12)	6.6336	
k	Number of nearest neighbors used in KNN algorithm	5 - 11	
μ	Number of monomials in a polynomial equation	2 - 3	
ν	Number of variables in each monomial	1 - 112	
χ	Power of a variable	0 - 4	
k_p	The number of considered pairs in Eq. 3.15	2	
w_i	Weight of the score at ith rank in Eq. 3.15	0.55 - 0.7	
w_{emcc}	The weight of S_{emcc} in Eq. 4.13	0.1 - 0.3	
w_{knn}	The weight of S_{knn} in Eq. 4.13	0.9 - 0.7	
λ	The parameter of Eq. 4.13	0.1 - 0.3	

Table 4.4: EER (%) Comparison in One vs. One Protocol

	FVC2002 DB1	**FVC2002 DB2**	**FVC2002 DB3**	**FVC2004 DB2**
Ferrara et al. [50]	0	0.37	4.94	-
Jin et al. [82]	4.36	1.77	-	21.82
Wang and Hu [162]	3.5	5	7.5	-
Wang and Hu [164]	3	2	7	-
Wang et al. [161]	1	2	5.2	13.3
Wang et al. [165]	0.19	1	4.29	9.01
Tran et al. [149]	0.2	0.04	4.78	7.64
Kho et al [90]	0	0	2	4
Proposed Framework	**0**	**0**	**0.14**	**2.71**

Table 4.5: EERs (%) of different order in the matching algorithm

	FVC2002 DB1	**FVC2002 DB2**	**FVC2002 DB3**	**FVC2004 DB2**
EMCC - KNN - Fused	**0.28**	**0.08**	1.41	**3.38**
EMCC - Fused - KNN	**0.28**	**0.08**	**1.40**	3.45
KNN - EMCC - Fused	**0.28**	**0.08**	1.41	**3.38**
KNN - Fused - EMCC	0.38	0.23	1.43	3.83
Fused - EMCC - KNN	**0.28**	**0.08**	**1.40**	3.45
Fused - KNN - EMCC	0.42	0.23	1.43	3.83

Table 4.6: EER (%) Comparison in FVC Protocol

	FVC2002 DB1	**FVC2002 DB2**	**FVC2002 DB3**	**FVC2004 DB2**
Ferrara et al. [50]	3.33	1.76	7.78	-
Das et al. [34]	4	-	-	-
Wang and Hu [164]	4	3	8.5	-
Kho et al. [90]	2.28	1.25	6.4	7
Jin et al. [81]	0.43	2.10	6.60	8.02
Abdullahi et al. [4]	0.364	0.538	2.395	5.925
Proposed Framework	**0.23**	**0.08**	**1.46**	**3.25**

Table 4.7: Decidability index *d'*

	FVC2002 DB1	**FVC2002 DB2**	**FVC2002 DB3**	**FVC2004 DB2**
EMCC	2.8634	3.2811	1.6117	2.0391
KNN-MPT	3.03	3.1912	2.1816	1.7644
Fused	4.0002	4.9040	2.8152	2.7037

Table 4.8: Standard Deviation and Mean of each score type

	Std Dev	Mean
EMCC Genuine	0.4900	0.7995
KNN Genuine	0.1614	0.4740
Fused Genuine	0.0848	0.8017
EMCC Impostor	0.0538	0.0255
EMCC Pseudo Impostor	0	0
KNN Impostor	0.0933	0.3848
KNN Pseudo Impostor	0.0423	0.0232
Fused Impostor	0.0287	0.0391
Fused Pseudo Impostor	0.0024	0.0172

Table 4.9: Number of trials to attack each database with each method

	KNN Descriptor	EMCC
FVC2002 DB1	2^{320}	2^{1280}
FVC2002 DB2	2^{352}	2^{1280}
FVC2002 DB3	2^{192}	2^{1280}
FVC2004 DB2	2^{160}	2^{1280}

Chapter 5

A Privacy-preserving Biometric Authentication System with Binary Classification and Error Codes Corrections in a Zero Knowledge Proof Protocol

The work reported in this chapter (mostly from Section 5.2 and Section 5.3), has been partially published for publication in the following article:

Tran Q, Turnbull B, Wang M, Hu J. A Privacy-preserving Biometric Authentication System with Binary Classification in a Zero Knowledge Proof Protocol. IEEE Open Journal of the Computer Society. 2021 Dec 24.

.

5.1 Introduction

The previous chapters have proposed biometric template protection mechanisms based on cancellable biometric template with high accuracy. This chapter seeks to provide an alternative solution to the Research Question that was raised in Chapter

1 in the sense that it explores another approach using an SVN classifier and an MLP Neural classifier and cryptography-based protocol to provide privacy preservation. With this method, the biometric sample is represented by a binary stream. In the Enrollment phase, the hash value of this stream is stored along with the parity bits of a Reed-Solomon Error Codes Correction (ECC). Besides, the chosen classifier is trained to identify the genuine and impostor users. In the Verification phase, the query will first be examined by the classifier. If it passes, it will be fetched to the Reed-Solomon Error Codes Corrections to reconstruct the original binary stream such that an exact hash value can be produced. This process in integrated in a Zero-Knowledge Proof protocol to ensure that privacy is preserved. Finally, if the hash value is the same as the stored version, authentication is granted. To evaluate the potential of the proposed method, the FVC2002-DB1, FVC2002-DB2, FVC2002-DB3, and FVC2004-DB2 for fingerprint and UBIRISv1 for iris have been chosen to implement.

As the Research Question asks "How to develop biometric authentication frameworks that can address major security and privacy threats while retaining a good authentication performance", we need to explore the alternate methods. This approach is fundamentally different from the processes outlined in the previous chapters. Thus, it is expected to have different advantages and disadvantages. Exploring this will enable a more complete response to the Research Question. In detail, in privacy-preserving biometric authentication, templates are directly used for matching. This makes the templates a weak point that needs protection in order to ensure the privacy of the users. However, the work proposed in this chapter does not involve the direct use of the biometric template. Instead, the power of the classifiers combines with the ECC can deliver a stable performance while securing the biometric template features with the cryptographic hash function.

With this hypothesis, this work seeks a privacy-preserving biometric authentication system that is AI-enabled in which a cryptographic hash function can apply to protect the biometric template features while a stable performance is still retained. The intra-class difference caused by the distortion is resolved by an ECC, making

the reconstruction of the original template's hash value feasible.

This chapter is structured as follows: The detailed proposed method is presented in Section 5.2. Section 5.3 is dedicated to analyzing the experimental results. Some discussion is provided in Section 5.4. Finally, Section 5.5 concludes the chapter.

5.2 Proposed Method

In this work, beside the traditional strategy that uses the features from a single image illustrated in Fig. 5.2, a strategy that utilizes the composite features from double images is proposed as indicated in Fig. 5.3. This strategy combines the features from two images of the sample biometric subject to create the so-called composite feature, which is used for both training and testing the classifier.

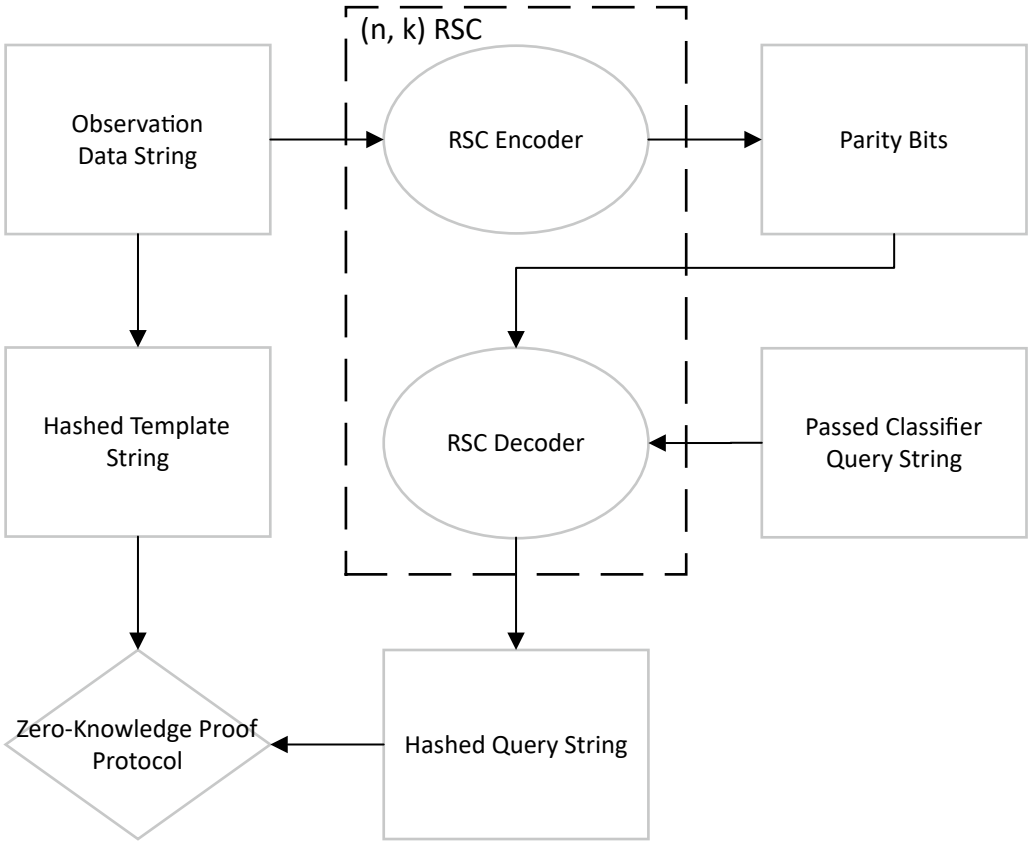


Figure 5.1: Overall Scheme

In the first stage, which is illustrated in the Fig. 5.1, the biometric data is

processed and filtered by a classifier before being corrected by the ECC. In more detail, first, biometric features are extracted and represented in the form of binary representation. Then, a model for each subject is trained using the binary data. When a query comes, after its features in the binary format have been retrieved, the model verifies the authenticity of the query. If it is authenticated by the model, the query is passed to the ECC to be prepared for hash string generation, which is described in later sections.

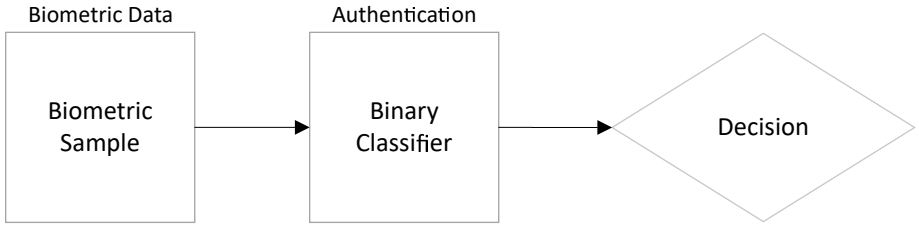


Figure 5.2: Traditional Authentication

Due to the flexibility of the scheme, any biometric features that can be represented in binary form is compatible with the proposed scheme, though a different composite biometric feature might be used. The proposed scheme is evaluated with fingerprint and iris, which are among the most widely used biometric modalities.

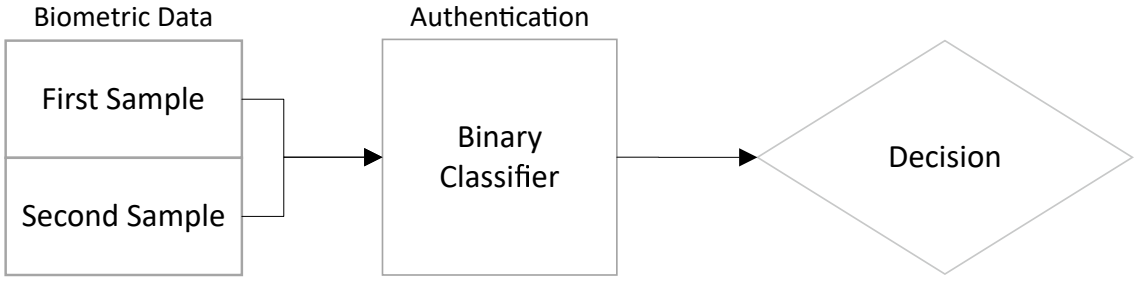


Figure 5.3: Composite Feature-based Authentication

5.2.1 Fingerprint with Bitstring Representation by Normalized Local Structures

The raw fingerprint bitstring representation proposed in [91] will be adopted. This single fingerprint image based feature presentation is constructed from the

normalized local structures. At first, the minutiae of a fingerprint are extracted. Then, for each minutia being set as the reference, two sets of local structure features are extracted: Minutiae-based Local Structure (MBLS) and Texture-Based Local Structure (TBLS). As two sets of features are extracted, a subspace projection is applied to reduce the dimensionality of both feature sets before fusion. The fused local structures from a set of fingerprints are fed into a K-means clustering to produce K clusters. As a query fingerprint is assessed, it goes through the same process. Its bitstring b_f is created by applying the K-means clustering based on the clusters created before. The i-th bit is set to 1 if the i-th cluster contains any minutia of the fingerprint. After this process, a fingerprint is represented by a 4,500 bit long binary string. A detailed description of this method can be found in [91].

5.2.2 Iris with Bitstring Representation by Perceptual Hash

Perceptual hash (pHash) of a multimedia file is its fingerprint that is derived from its content's features [93]. For this chapter, the Discrete Cosine Transformation (DCT) pHash from the pHash library implemented by Zauner [191] is used: At first, the input image is converted to greyscale using luminance. Afterward, the image is resized to the size of 32×32 to simplify the computation of the DCT by using a 7×7 kernel for convolution. The DCT matrix is generated based on this resized image. A 8×8 DCT coefficient matrix is then calculated. The pHash value is computed by normalizing the elements of the one dimensional array created from the DCT coefficient matrix with its median. The details of how pHash works and is implemented can be found in [191].

Following the method in [65], the pHash of an iris image is extracted as follows: First, a segmentation process is applied onto the image to identify the iris region. After that, the pHash of the segmented iris image is generated. This step results in an integer in the range of $[0, 2^{64} - 1]$. This number is then translated to its corresponding binary form, which is used to represent the iris image.

5.2.3 Composite Features Retrieval

Traditional biometric authentication uses the features extracted from a single biometric image. However, due to the noise, the features extracted from this single biometric image are not discriminative enough. Importantly, if these features are used for template construction, the error rates are hypothetically high. Therefore, it is crucial that stable features are selected to be used for matching. This process is referred to as: Composite Features Retrieval (CFR). With the sparse binary representation from [91], this process is as simple as follows:

Given two binary representations b_1 and b_2 that belong to the same subject, a new binary representation b_c with the same length is constructed by selecting only the common bit 1's positions between two binary strings. The newly generated binary string b_c is the input data to the model trainer.

Upon applying the CFR, the number of samples per subject increases: The FVC databases now, instead of having eight samples per subject as they did previously, contain $\binom{8}{2} = 28$ samples per subject. Similarly, the original UBIRISv1 database has 241 subjects with 5 samples each while the CFR-based strategy has $\binom{5}{2}$ samples per subject. The detailed comparison of before and after applying the CFR is shown in Table. 5.1

Table 5.1: Number of samples

	Fingerprint		Iris	
	Traditional	CFR	Traditional	CFR
Samples/subject	8	28	5	10
Total samples	800	2800	1205	2410

Prior to training a model, binary strings from the same subject are labeled as positive data while those that are from different subject as negative data. How these two types of data are used is presented in the next sections.

5.2.4 AI-based Classifiers

In this section, the details of the settings for each AI-based classifier employed are presented: the Support Vector Machine and the Multilayer Perceptron Neural Network.

First, a dataset for each of the subjects in a database is constructed. Afterward, this dataset is separated such that: 80% of the data is used for training while the rest 20% is used for testing. The specific amount of data used for training and testing is different for each strategy. This information is presented in the Table 5.2.

Table 5.2: Amount of data used for testing and training for each biometric subject in a database

		FVC Databases		UBIRIS	
		Traditional	CFR	Traditional	CFR
Training	Positive	6	22	4	8
	Negative	594	2178	960	1920
Testing	Positive	2	6	1	2
	Negative	198	594	240	480

For fingerprints, there will be $2 \times 100 = 200$ positive tests and 198×100 negative tests for the traditional strategy. On the other hand, the CFR-based strategy yields $6 \times 100 = 600$ positive tests and $594 \times 100 = 59,400$ negative tests. Similarly, traditional strategy for iris yields 241 positive and 57,840 negative tests while CFR-based strategy yields 482 positive and 115,680 negative tests.

5.2.4.1 Support Vector Machine Classifier

SVM is a widely applied classifier [17]. Given a set of classes Y and a set of attributes X with $|Y|$ and $|X|$ being the total number of classes and attributes, respectively, the Support Vector Machine (SVM) finds the hyper planes that assign each attribute x in the set X to a class y in the set Y. In this scheme, the SVM is chosen for subject identification due to the following reasons:

- The publicly available databases for fingerprints and iris posses limit number

of samples per subject. Hence, the model has to be trained in a data-restricted environment.

- The purpose of the scheme is to verify a user's authenticity. Therefore, it is a binary decision: Yes/No.

SVM does not require a significant amount of data to train a model. More importantly, SVM was traditionally designed to provide binary decisions. It is for these reasons that SVM is an appropriate choice for the verification role.

SVM uses some kernel functions to optimize the process of assigning training data x to its associated class y. Similar to [65]'s, this method uses Radial Basis Function (RBF) as the kernel function whose parameters C and γ are chosen from a 10-fold cross validation grid search. The proposed scheme differs in the sense that the SVM used outputs a binary decision, instead of the class label as in [65]. This is because the classifier is set up to give a yes/no decision without exposing any information about the subjects in the database.

5.2.4.2 Multi-layer Perceptron Neural Network

In addition to the SVM, a Multi-layer Perceptron (MLP) Neural Network is employed to evaluate and compare the performance. MLP belongs to the Feed-forward Neural Network. It has three kinds of layers: input layer, hidden layer, and output layer. The data flows from the input layer to the hidden layer where all the computational tasks occur before it gets transfered to the output layer. While SVM is a good classifier against linearly distributed data, MLP is a strong tool to classify non-linearly separable data.

In this work, a vanilla neural network is implemented, meaning that an MLP neural network that has a single hidden layer. The details of the parameters used are given in Table. 5.3.

Table 5.3: Parameters used for the MLP neural network training

Parameter	Value
Number of hidden layers	1
Number of neurons/hidden layers	100-500
Activation function	ReLU
Solver	Adam
Alpha	10^{-4}
Learning rate	0.001
Maximum number of iterations	200

5.2.5 Hashed ECC

As a model is being trained, ECC is applied with one of the positive observations in the training dataset. Specifically, an (n, k) RSC is used to encode the observation where n is the codeword length and k is the number of parity bits that determines how many errors can be corrected. After this step, the k parity bits retrieved are stored along with the hash value of the observation. These parity bits are used for error corrections on the query binary string. Fig. 5.1 visualizes this process. In this section, how the biometric binary representation is preprocessed to input into the (n, k) RSC is presented.

5.2.5.1 Hashed Fingerprint Bitstring

At first, the 4500-bit string b_f is chunked into groups of eight bits each. Since 8 does not divide 4500, four bits of '0' are padded to make the last byte complete. This yields a string of byte B_S of 563 bytes.

In this scheme, an RSC with a fixed codelength $n_f = 255$ is used. The number of parity bits k_f that determines how many errors can be corrected ($\frac{k}{2}$) is dynamically changed. Since $n_f < 563$, the string of bytes is chunked into the length of $n_f - k_f$ bytes each as input for the RSC. For instance, given that $k_f = 32$, B_f consists of three sub-strings. The first two substrings are $(255 - k)$ byte-long while the last substring is $563 - 2(255 - k) = 53 + 2k$ byte-long. Normally the last substring is not long enough to be the input of the RSC scheme. The RSC will pad with the

byte of '0' to make it long enough. In the encoding phase, the parity bits p_i for each substring are generated. After this phase, the set of parity bits $P = \{p_i\}_{i=1}^{3}$ for each substring are stored along with the hash of the input byte string. In the decoding phase, after the query is chunked and padded, the parity bits are appended to the end of each substring and inserted into the decoder. If there are maximum $\frac{k_f}{2}$ errors in a substring, it is correctable to the original byte string. The hash of the query is compared against the template hash stored in the system.

5.2.5.2 Hashed Iris Bitstring

The length l_i of the iris bitstring is 64-bit long. The number of parity bit k_i ranges are chosen such that: $l_i + k_i + p_i = n_i$ where p_i is the number of padded bits '0' due to the fact that the iris bitstring is not long enough to serve as the input of the RSC. After being corrected by the RSC, the hashed iris bitstring is stored with the parity bits.

5.2.6 Chaum-Pedersen Protocol

The Chaum-Pedersen is one of the interactive Zero Knowledge Proof protocols. It allows the verification of a secret without having to reveal it. In this case, it is used to authenticate the user if he can present the original hash string. Assume that **P** is the prover and **V** is the verifier. **P** needs to prove to **V** that he/she possesses the hash string S without revealing it.

Chaum-Pedersen Protocol [22]:

- Let G be a cyclic group of prime order q generated by some generator $g \in G$.
- Let C be a challenge space used by the verifier **V**, which is a subset of Z_q.
- **P** produces the triplet (u, v, w), $v = g^S$, $w = u^S$. The triplet is a public parameter which is accessible by both the prover and the verifier. S will become the commitment of the prover.

When **P** needs to prove to **V** that they own the private biometrics hash string S, they randomly pick a number S_t from Z_q and calculates v_t and a w_t where $v_t \leftarrow g^{S_t}$ and $w_t \leftarrow u^{S_t}$ and send them to the verifier **V**. Upon receiving v_t and a w_t, **V** generates a challenge $c \in C$ and sends it to **P**. With the challenge c, **P** calculates $S_z \leftarrow S_t + S * c$ and sends it back to **V** as the answer. Finally, **V** checks if $g^{S_z} = v_t * v^c$ and $u^{S_z} = w_t * w^c$. If the equality holds, **P** is authenticated as the holder of the biometrics hash string S. In the proposed privacy-preserving scheme, the biometrics hash string S is generated on the spot. It is not stored anywhere and there is no secret mapping anywhere. The security strength depends primarily on the cryptography strength of the Chaum-Pedersen Protocol.

5.3 Experimental Results

In this section, the experimental results that have been conducted for the fingerprint databases FVC2002-DB1, FVC2002-DB2, FVC2002-DB3 and FVC2004-DB2 and the iris database UBIRISv1 are presented.

In order to evaluate the performance of the classifiers used, the False Acceptance Rate (FAR), False Rejection Rate (FRR), and Accuracy are used. To calculate these measures, the following figures are recorded: True Positive (**TP**), False Positive (**FP**), True Negative (**TN**), and False Negative (**FN**).

- **FAR** is the probability that the model mistakenly accepts a sample that is not from the same subject with which the model was trained. It is given as the ratio of the number of falsely accepted samples (FP) to the total number of impostor tests: $FAR = \frac{FP}{n_I}$ where n_I is the total number of impostor tests.
- **FRR** is the probability that the model mistakenly rejects a sample that is from the same subject with which the model was trained. It is given as the ratio of the number of falsely rejected samples (FN) to the total number of genuine tests: $FRR = \frac{FN}{n_G}$ where n_G is the total number of genuine tests.

- **Accuracy** is the probability that the model correctly identifies the genuine as well as the impostors. It is given as the ratio of the sum of correctly identified genuine and impostor samples to the total number of tests conducted: $Acc = \frac{TP+TN}{n_I+n_G}$.

The biometric performance is also evaluated using the Equal Error Rate (EER). The details on how EER is generated will be presented in the next sections.

5.3.1 Classifiers' Performance

5.3.1.1 Fingerprint

The classification performances of the SVM classifier and the MLP classifier for the fingerprint's FVC databases are presented in the Table. 5.4 and Table. 5.5, respectively.

Table 5.4: Fingerprint's SVM performance (%)

		Traditional	CFR
FVC2002-DB1	FAR	0.00	0.00
	FRR	11.00	1.83
	Accuracy	99.99	99.99
FVC2002-DB2	FAR	0.69	0.00
	FRR	0.50	1.17
	Accuracy	99.99	99.99
FVC2002-DB3	FAR	0.00	0.00
	FRR	13.00	4.17
	Accuracy	99.89	99.96
FVC2004-DB2	FAR	0.56	0.00
	FRR	6.00	9.00
	Accuracy	99.39	99.91

As shown in the Table. 5.4, the binary classification models for fingerprint trained with both strategies yield a very low FAR. Also, using the same strategy, the lower the quality of the images in the database is, the higher the FRR becomes. On the other hand, as the CFR strategy is applied, the FAR is decreased to 0.00% for

FVC2002-DB2 and FVC2004-DB2 while the FVC2002-DB1's and FVC2002-DB3's FRR decrease sharply.

Gunasinghe and Bertino [65] employed the concept of using SVM for biometric authentication with ECC with a Zero-Knowledge Proof, which achieved 0.21% FAR along with 21% FRR when implemented with iris. However, in their work, the ECC was applied on the biometric data before it was classified by the SVM model. Moreover, in their work, a multi-class SVM was used. This means that the SVM model will output a class label based on the input data. As the class label is used as one of the secrets for key derivation, it is likely to be hard-coded in the protocol. This poses security issue that an attacker can perform a series of attacks to learn which label corresponds to a dummy label.

This work is different in the sense that: First, it only outputs a binary decision (either yes or no). Hence, there is no hard-coded label. Second, the scheme in this chapter explores the use of not only the SVM classifier but also the MLP classifier. Last but not least, this work proposes a novel strategy to extract features from biometric samples, contributing to the improvement of the scheme's performance.

The performance with MLP Neural Networks is presented in Table. 5.5.

Table 5.5: Fingerprint's MLP performance (%)

		Traditional	CFR
FVC2002-DB1	FAR	0.00	0.00
	FRR	1.00	1.50
	Accuracy	99.99	99.99
FVC2002-DB2	FAR	0.00	0.00
	FRR	3.00	0.83
	Accuracy	99.97	99.99
FVC2002-DB3	FAR	0.00	0.00
	FRR	10.00	4.30
	Accuracy	99.90	99.96
FVC2004-DB2	FAR	0.00	0.00
	FRR	29.00	7.83
	Accuracy	99.67	99.92

Comparing with the SVM's performance, MLP performs better in terms of recognizing the impostors when CFR is employed. Except with FVC2002-DB1 having

a slight increase in FRR from 1.00% to 1.50%, MLP shows a sharp improvement of FRR when CFR is applied in all other databases while the FAR is kept at 0%.

The better performance shown by the MLP can be explained by its better ability to deal with non-linear data than SVM's counterpart. Though possessing the kernel functions that can work with non-linear data, SVM's ability to classify non-linear data is limited. More importantly, the minutiae on a fingerprint are distributed naturally randomly. This results in the non-linear distribution of the bits generated by [91]. Hence, using the same method to generate fingerprint bit string, MLP with its flexibility in working with non-linearity shows a better performance.

5.3.1.2 Iris

The classification results of the SVM and MLP classifier are presented in Table. 5.6, respectively.

Table 5.6: Iris's performance (%)

	SVM			MLP		
	FAR	FRR	Accuracy	FAR	FRR	Accuracy
Traditional	0.41	0.00	99.59	0.00	6.22	99.97
CFR	0.39	0.00	99.61	0.00	0.21	99.99

As it can be seen from the Table. 5.6, UBIRISv1's SVM performance kept FRR at 0.00% in both strategies, contrasting to the MLP that maintained FAR at 0.00%. In this situation, it can be said that the CFR-based MLP performs the best by rejecting all impostors while keep the FRR as low as 0.21%.

5.3.2 Biometric Performance

The classifier's ability in classifying the fingerprints has been investigated. In this section, the biometric performance of these classifiers will be evaluated using the EER, which is the rate when the FAR equals the FRR. Kindly note that the FAR and FRR used to generate the EER are not the same as the ones mentioned in the previous section. Previously, the classifiers generate two probabilities: one for

the positive class and one for the negative class. To make a decision, the classifier chooses the class with the higher probability. Consequently, the FAR and the FRR are generated based on this decision. On the contrary, multiple thresholds will be set to determine the corresponding pair of FAR and FRR. By changing the thresholds, the EER can be generated.

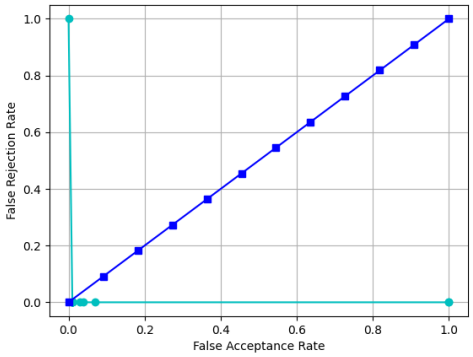
5.3.2.1 Fingerprint

The fingerprint recognition performance in terms of EER using different classifiers is presented in the Table. 5.7. In addition, some of the Detection Error Tradeoff (DET) curves are shown in Fig. 5.4.

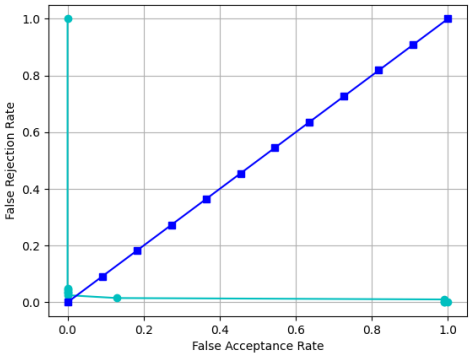
Table 5.7: Fingerprint's EER (%)

		SVM	MLP
FVC2002-DB1	Traditional	0.54	0.00
	CFR	0.33	0.00
FVC2002-DB2	Traditional	1.00	0.00
	CFR	0.00	0.00
FVC2002-DB3	Traditional	1.00	2.37
	CFR	2.17	2.34
FVC2004-DB2	Traditional	1.00	2.31
	CFR	2.47	2.50

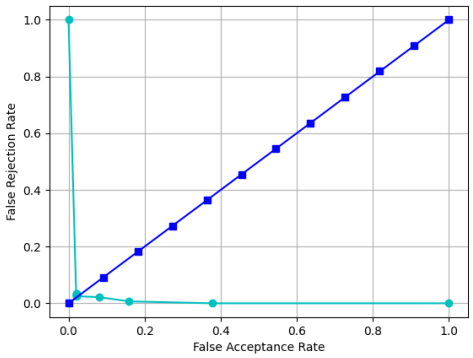
In terms of biometric performance, overall, both the classifiers perform well in all cases with very low EER. Within the same database, the MLP classifier even shows slightly higher EER than the SVM. On the other hand, it can be concluded that both the SVM and MLP classifier deliver good biometric performance. In general, the CFR performs better over good to moderate quality databases. It is observed that a very difficult database (DB2004) tends to produce much fewer bit 1's in the CFR binary template, leading to a noticeable performance degradation. This is closely related to the challenge in producing quality fingerprint features over the poor quality fingerprint images.



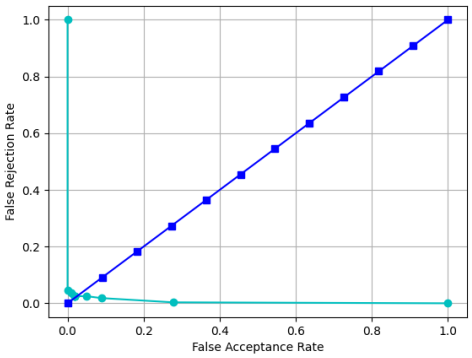
(a) SVM with Traditional Strategy implemented in FVC2004-DB2



(b) MLP with Traditional Strategy implemented in FVC2004-DB2

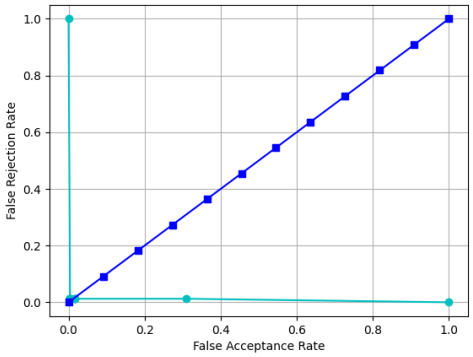


(c) SVM with CFR applied in FVC2004-DB2

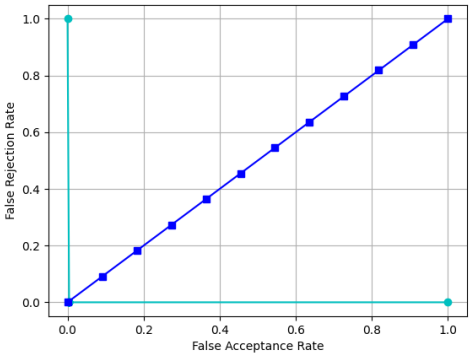


(d) MLP with CFR applied in FVC2004-DB2

Figure 5.4: Fingerprint's DET curves



(a) SVM with Traditional Strategy for Iris Recognition



(b) SVM with CFR Strategy for Iris Recognition

Figure 5.5: Iris's DET curves

5.3.2.2 Iris

Similar to the fingerprint's counterpart, iris's recognition performance with different classifiers is shown in Table. 5.8. The DET curves for different classifiers under different strategy are presented in Fig. 5.5.

Table 5.8: Iris's EER (%)

		SVM	MLP
UBIRISv1	Traditional	1.24	2.07
	CFR	0.41	0.0017

It can be seen that in this case, the CFR strategy performs better than the traditional strategy in both cases. This is related to the pHash feature that is used to represent each iris image: pHash is a 64-bit string that represents the features of the media file. This means that pHash was not originally devised for biometrics but instead for the generic recognition of the content in a file. Hence, pHash being the main features for iris recognition limits the discriminativeness of the iris's characteristics. Therefore, CFR contributes to lower the FRR while the FAR is kept at a lower level at the same threshold, leading to a decrease in the EER. Compared with fingerprint, iris tends to have more stable features where the CFR can play a bigger role.

The impact of ECC on the recognition accuracy of the system is discussed in the

next section.

5.3.3 ECC's Impact on the Overall Performance

The output of the classifier is the ECC's input. This means that the ECC plays an important role in making a decision. Even if the classifier identifies a biometric sample as genuine but ECC cannot correct it to the template's original binary string to produce an exact hash, the authentication still fails. This section investigates the influence of ECC on the whole biometric recognition system's performance. The length of the codeword used in the Reed-Solomon ECC scheme is 255 while the number of parity bits are dynamic.

5.3.3.1 Fingerprint

SVM: Since ECC's input is the classifier's passed samples, those that have already been rejected by the classifier will not be taken into consideration. Hence, the FRR will not change. On the other hand, whether a biometric sample is accepted depends on the performance of the ECC. As shown in Table 5.5 and 5.6 that MLP was able to identify all of the impostors, leading to $FAR = 0.00\%$ for both fingerprint and iris. Therefore, an ECC with a large enough number of parity bits can be used to recreate the template's bitstring. A low number of impostors can still bypass the SVM classifier in FVC2002-DB2 and FVC2004-DB2.

The impact of the ECC for Traditional and CFR Fingerprint using the SVM is presented in Table. 5.9 and Table 5.10, respectively. Table 5.9, ECC shows the impact on the performance of the scheme. With the number of parity bits $nsym$ increasing, the FRR rate decreases. For FVC2002-DB1, the FRR decreases and reaches the same rates with the SVM's performance when $nsym = 63$. Due to $FAR = 0.00\%$ for the SVM, this means that when $nsym = 63$, the ECC accepts all the samples that have been accepted by the SVM. The situation is slightly different with FVC2002-DB2 and FVC2004-DB2 datasets, as these have impostors that have

Table 5.9: ECC performance in percentage (%) with different number of parity bits for Traditional Fingerprint filtered by the SVM classifier

			FVC2002-DB1	FVC2002-DB2	FVC2002-DB3	FVC2004-DB2
nsym	32	FRR	44.00	77.00	42.00	98.50
		FAR	0.00	0.00	0.00	0.01
	40	FRR	26.50	42.50	18.50	95.50
		FAR	0.00	0.01	0.00	0.02
	60	FRR	11.50	0.50	13.00	18.00
		FAR	0.00	0.31	0.00	0.36
	63	FRR	11.00	0.50	13.00	11.50
		FAR	0.00	0.41	0.00	0.42
	80	FRR	11.00	0.50	13.00	0.50
		FAR	0.00	0.68	0.00	0.50
	100	FRR	11.00	0.00	13.00	0.50
		FAR	0.00	0.68	0.00	0.50

been accepted. The increase of $nsym$ lowers the FRR but increases the FAR. However, there is a jump when $nsym$ increases from 40 to 60: With FVC2002-DB2, the FRR decreases from 42.50% for $nsym = 40$ to 0.5% for $nsym = 60$. Its FAR remains at a fairly low level of 0.31% for $nsym = 60$. On the other hand, FVC2004-DB2's FRR drops from 95.50% when $nsym = 40$ to 18% when $nsym = 60$. Its FAR is also at a very low level: 0.36% when $nsym = 60$.

For the CFR-based strategy, Table 5.10 highlights the minimal impact ECC has on the performance. Specifically, in FVC2002-DB2, while the FAR remains 0.00% at all times, when the number of parity bits $nsym = 32$, the FRR of the whole scheme is 3% while $nsym = 40$, the FRR is 1.17%. This is also the original performance of the SVM classifier as indicated in Table. 5.4.

MLP: The impact of the ECC on the fingerprint-based authentication system's performance when using the MLP is presented in Table. 5.11 and Table. 5.12 for the traditional and CFR-based strategies, respectively. It is evident that for Traditional-based strategy, the increase in the number of parity bits $nsym$ creates a decrease in the FRR for all databases. On the other hand, as the use of the MLP with CFR-based strategy already has a good performance, the change in $nsym$ does

Table 5.10: ECC performance in percentage (%) with different number of parity bits for CFR-based Fingerprint filtered by the SVM classifier

			FVC2002-DB1	FVC2002-DB2	FVC2002-DB3	FVC2004-DB2
nsym	32	FRR	1.83	3.00	4.17	9.00
		FAR	0.00	0.00	0.00	0.00
	40	FRR	1.83	1.17	4.17	9.00
		FAR	0.00	0.00	0.00	0.00
	60	FRR	1.83	1.17	4.17	9.00
		FAR	0.00	0.00	0.00	0.00
	63	FRR	1.83	1.17	4.17	9.00
		FAR	0.00	0.00	0.00	0.00
	80	FRR	1.83	1.17	4.17	9.00
		FAR	0.00	0.00	0.00	0.00
	100	FRR	1.83	1.17	4.17	9.00
		FAR	0.00	0.00	0.00	0.00

not lead to any further decrease of the FRR, except for FVC2002-DB2 when *nsym* increases from 32 to 40.

Table 5.11: ECC performance in percentage (%) with different number of parity bits for Traditional Fingerprint filtered by the MLP classifier

			FVC2002-DB1	FVC2002-DB2	FVC2002-DB3	FVC2004-DB2
nsym	32	FRR	39.50	77.50	39.00	100.00
		FAR	0.00	0.00	0.00	0.00
	40	FRR	18.00	43.00	15.00	97.50
		FAR	0.00	0.00	0.00	0.00
	60	FRR	1.50	3.50	9.50	44.50
		FAR	0.00	0.00	0.00	0.00
	63	FRR	1.00	3.00	9.50	39.50
		FAR	0.00	0.00	0.00	0.00
	80	FRR	1.00	3.00	9.50	30.00
		FAR	0.00	0.00	0.00	0.00
	100	FRR	1.00	3.00	9.50	29.50
		FAR	0.00	0.00	0.00	0.00

5.3.3.2 Iris

SVM: The FRR and FAR when ECC is used with different number of parity bits for UBIRISv1 are reported in Table. 5.13. In this table, it can be seen that when

Table 5.12: ECC performance in percentage (%) with different number of parity bits for CFR-based Fingerprint filtered by the MLP classifier

			FVC2002-DB1	FVC2002-DB2	FVC2002-DB3	FVC2004-DB2
nsym	32	FRR	1.50	2.70	4.17	7.83
		FAR	0.00	0.00	0.00	0.00
	40	FRR	1.50	0.83	4.17	7.83
		FAR	0.00	0.00	0.00	0.00
	60	FRR	1.50	0.83	4.17	7.83
		FAR	0.00	0.00	0.00	0.00
	63	FRR	1.50	0.83	4.17	7.83
		FAR	0.00	0.00	0.00	0.00
	80	FRR	1.50	0.83	4.17	7.83
		FAR	0.00	0.00	0.00	0.00
	100	FRR	1.50	0.83	4.17	7.83
		FAR	0.00	0.00	0.00	0.00

the number of parity bits $nsym$ is low, the MLP classifier with CFR-based strategy tends to deliver less errors than it with the traditional strategy. Although when $nsym = 100$, the FRR reached 0.00% for both, while the FAR is equivalent (0.41% for Traditional and 0.39% for CFR), it is not recommended as a high number of parity bits would allow more impostors.

Table 5.13: ECC performance in percentage (%) with different number of parity bits for Traditional and CFR-based Iris filtered by the SVM classifier

			Traditional	CFR
nsym	32	FRR	31.54	17.63
		FAR	0.13	0.10
	40	FRR	18.26	8.09
		FAR	0.22	0.21
	60	FRR	7.05	1.04
		FAR	0.35	0.36
	63	FRR	7.05	0.21
		FAR	0.35	0.37
	80	FRR	0.41	0.00
		FAR	0.40	0.39
	100	FRR	0.00	0.00
		FAR	0.41	0.39

MLP: Table. 5.14 presents the performances when the MLP classifier is used. Unlike when the SVM classifier is used, the MLP classifier is able to detect all the

impostors in both Traditional and CFR-based strategy. On the other hand, with the same number of parity bits, CFR-based strategy delivers a much better FRR. The ECC accepts all samples that are identified as genuine by the classifier when the number of parity bits $nsym = 100$ and $nsym = 80$ with Traditional and CFR-based strategy, respectively.

Table 5.14: ECC performance in percentage (%) with different number of parity bits for Traditional and CFR-based Iris filtered by the MLP classifier

			Traditional	CFR
nsym	32	FRR	32.37	17.63
		FAR	0.00	0.00
	40	FRR	19.92	8.30
		FAR	0.00	0.00
	60	FRR	10.79	1.24
		FAR	0.00	0.00
	63	FRR	10.79	0.43
		FAR	0.00	0.00
	80	FRR	6.64	0.21
		FAR	0.00	0.00
	100	FRR	6.22	0.21
		FAR	0.00	0.00

5.3.3.3 Results Analysis

In summary, the results have shown the method's performance with fingerprint and iris using different strategies and different classifiers along with the help of ECC. Although the ECC does not help improve the FAR, it plays an important role in this scheme as without it, the hash value of the template cannot be reconstructed.

For fingerprint, when the SVM classifier is used, the traditional strategy shows that the ECC can make a big impact on the overall performance across all the databases: when the number of parity bits $nsym$ is low, the scheme has an extremely high FRR, especially the low-quality database FVC2004-DB2 with 98.50%. As $nsym$ increases, the FRR starts to improve until it accepts. On the other hand, the CFR-based strategy shows little influence of ECC in the scheme's overall performance as the change in $nsym$ does not lead to the change in the FRR and FAR. When the

MLP classifier is used, the situations for traditional and CFR-based strategy are the same as the SVM classifier's counterpart. We can conclude that for fingerprint, CFR-based strategy limits the scheme's reliance on the ECC.

For iris, with the same classifier being used, the CFR-based strategy shows better performance. However, the MLP classifier is more favorable as it is able to identify all the impostors for both strategies. Both Table 5.13 and 5.13 show that when $nsym$ is changed, ECC does influence the overall system's performance.

Although it is seen that with a high number of parity bits being used, the ECC can accept all the genuine samples that have been marked as passed by the classifier. However, it is not recommended to set $nsym$ high as this creates more chances for impostors to be authenticated.

5.4 Discussion

In this chapter, a light-weight privacy-preserving biometric authentication system using AI-based classifier has been proposed. Beside the traditional strategy that only uses one biometric sample to construct template and conduct matching, a Composite Feature Retrieval strategy has also been proposed. This strategy shows certain improvements in comparison with the traditional strategy. Last but not least, using the ECC and the hash function, this system is integrated with a Zero-Knowledge-Proof Protocol such that it can be used in subsequent applications that utilize biometric authentication.

Under different scenarios, a malicious adversary may choose to launch an attack on different points: Firstly, contrary to the work in [65], the proposed system only outputs the decision of the matching. The adversary will cope with difficulties if he wants to gain unauthorized access. Secondly,the system does not directly use any biometric template. Instead, the hashed value of the binary representation of the biometric is used in the last layer of authentication. In order to compromise a template, the adversary must first successfully compromise the hash function. This

attack is similar to the pre-image attack that was analyzed in Chapter 4. Therefore, in terms of privacy, the proposed system exposes minimal amount of information.

5.5 Conclusion

As discussed in Section 5.4, this chapter has provided an alternate solution for the research question stated in Chapter 1. The system proposed in this chapter is capable of providing biometric authentication with high accuracy yet retaining the users' privacy since it only uses the hashed value of the biometric template's binary stream. Therefore, it can be used in subsequent applications that utilize biometric authentication.

Chapter 6

Conclusion

In this chapter, an answer to the Research Question is given in Section 6.1. The novelties of this thesis as well as how each of them contributes to giving a solution to the Research Question are presented in Section 6.2. Finally, some potential future work directions are suggested in Section 6.3.

6.1 Answering the Research Question

As per Chapter one of this work, this thesis has sought to explore and understand the following research question:

> *How can we develop biometric authentication frameworks that can address major security and privacy threats while retaining a good authentication performance?*

To completely answer this research question, this work has explored several ways of preserving the privacy of the biometric authentication system users against the current attacks (especially the ARM) while retaining high recognition accuracy. This is a non-trivial research proposition, and has necessitated the development of multiple processes to accommodate.

Before answering this question, more information was required. Chapter 2 has two main goals from this perspective. First, it elucidates the current and emerging classes of attacks and threats to provide clarity on the subset of the research question that is asking about *...major security and privacy threats....* The second aspect of this chapter is to provide a high-level structure and taxonomy of the current state of the field. Neither of these answers the question, but provides more information that is then used in subsequent chapters.

In the first stage of responding to this question, Chapter 3 presents a robust local-structure-based set of fingerprint features along with an ARM-resistant transformation to protect the biometric templates. Although the processes implemented are effective at mitigating ARM, the resultant performance is not comparable with current state-of-the-art methods. Although this result can be expected, as the current processes compared do no protect against the ARM, this only partially answers the fundamental research question driving this thesis. Chapter 3 highlights that it is possible to develop an authentication framework that can address emerging security and privacy threats. However, it has not adequately shown that is possible to do this whilst retaining good or comparable performance.

Chapter 4 extends on the work of Chapter 3 to improve the performance of the fingerprint recognition by utilizing the KNN-MPT module from Chapter 4 with a newly proposed module EMCC. The outcome of this chapter is a multi-filter cancellable fingerprint framework, which has been proved to be resistant to certain types of attacks, including the ARM. In regards to the research question, this chapter has provided a solution that not only addresses the current major security and privacy threats but also delivers high performance. In effect, this provides a partial response to the overarching research question, highlighting that it is possible to avoid ARM and similar potential future attacks without significant degradation to the performance of such a system.

Chapter 5 takes a different approach to answering the thesis's research question. It develops and presents a light-weight biometric authentication system utilizing

the power of Artificial Intelligence and a cryptographic environment. Being another approach apart from the cancellable biometrics, this work seeks to mitigate the ARM and similar classes of attack but not using the biometric template directly. Instead, the hash value of the binary representation is stored along with the parity bits of a Reed-Solomon Error Codes Correction scheme. The first authentication filter is conducted by the AI classifier. If the query passes, it is sent to the ECC before passing through a hash function to retrieve its hash value. The hash value is compared with the template stored in the database via a Zero Knowledge Proof protocol, making information leakage as minimal as possible. This system is an alternate solution to the Research Question for the following reasons:

- it achieves high accuracy due to the power of the AI-based classifier;
- it does not directly use a template. Thus, in order to compromise a template, a malicious adversary needs to launch various attacks on the Zero Knowledge Proof to retrieve the hash value, on the hash function to reverse engineer the hash value to its input. Because of the nature of the hash function, this is not an easy task to accomplish.

As such, this work provides a suitable response to the research question guiding this thesis. Both of the solutions are able to address the privacy concerns targeting the biometric template. On the other hand, these systems still retain a high level of performance.

Previously, the research question that sets the theme for this thesis has sought the solutions to design biometric authentication framework that can address the major biometric template attacks while still possessing reliable performance. This thesis has provided two solutions to the question:

- The multi-filter biometric authentication framework that contains two cancellable fingerprint template modules can address the major attacks on the biometric template, including the ARM. It also achieves a reliable performance when compared with the current state-of-the-art systems [148].

- The light-weight privacy-preserving AI-based system proposed only uses the hash value of the biometric template. Authentication is performed in a Zero-Knowledge-Proof Protocol. This makes it difficult for a malicious actor to launch an attack to retrieve the original biometric template as the Zero-Knowledge-Proof Protocol and the hash function need to be compromised. On the other hand, with the power of the AI-based classifier, the system delivers a highly reliable performance in terms of accuracy [147].

Therefore, this research has shown that there is no single methodology that can be used, but several. This thesis has extended the knowledge of the field regarding the development of biometric authentication processes and systems resistant to the emerging attacks.

6.2 Novel Research Outcomes Originating From This Thesis

In the exploration of this research question, this thesis has achieved several novel outcomes for the biometric research community: (i) a taxonomy for the biometric authentication systems and the privacy mechanisms used in the field; (ii) a multi-filter cancellable fingerprint framework containing two modules that are resistant to the biometric-template attacks such as the ARM; and (iii) a light-weight privacy-preserving fingerprint authentication using AI-based classifier with a Zero-Knowledge-Proof protocol. Each of these is discussed separately.

Chapter 2 presented a novel and comprehensive taxonomy of the current state of privacy-preserving biometric authentication systems. This taxonomy not only contributes to the systematic categorization of the current and emerging works in the field but also helps visualize the trend of this field in a near future [150].

The second outcome that the thesis has achieved is the novel multilayer cancellable fingerprint framework, as outlined in Chapters 3 and 4. This framework

combines two cancellable modules that are resistant to the ARM. The first module employs a cluster-based local structure features and is transformed using the Multivariate Polynomial Transformation. The second module is an enhanced version of the widely used MCC [24]. It is transformed using an Irreversible Order-based Binary Encoding. The matching performed in this framework also contributes to the performance improvements in various ways using special weight functions and the dynamic Local Similarity Sort. In addition, the multi-filter that gives decision based on all three measurements is another point that helps stabilize the system's performance.

Another outcome from this thesis is the light-weight biometric authentication system that leverages the Artificial Intelligence classifier with the Error Codes Correction and the hash function. This system is implemented in Chapter 5. Without the direct use of a biometric template, the user's privacy in terms of biometric data is not exposed to as much stake. On the other hand, as demonstrated in this work, AI classifiers provide a reliable foundation for the ECC to correct the binary string such that if a genuine user is present, the original binary string can be retrieved. Last but not least, the Zero-Knowledge-Proof Protocol protects the generated secret, making it even harder for a malicious actor to acquire.

In combination, these outcomes have contributed to providing a comprehensive solution to the research question that underpins this thesis. At the same time, they open up opportunities for further discoveries in the field. In the next sections, some potential future work and research directions are suggested. These arise from different aspects of this thesis and may provide inspiration for future researchers in this field.

6.3 Potential Future Work and Research Directions

In the course of this research, several potential avenues for future research have become apparent. These are pathways that the researcher might explore, but are also opened to the wider research community.

The first aspect of future work is to more completely explore the ARM and similar classes of attacks to biometric systems. A greater understanding of the ARM and similar classes of attacks in more detail can provide a greater understanding of the threat. Biometric-specific attacks are an emerging research area, and understanding these in greater detail will provide greater safety and increase the strength of future biometric implementations. This may be in the form of testing harnesses and regimes, for example.

As outlined in Chapter 2, there are several potential areas of biometrics that are yet to be explored. For example, there are techniques that are being used in some biometrics that may be applicable to others, but the community has yet to test and evaluate. This includes the limited number of applications of privacy mechanisms on behavioral biometrics, or on new biometrics, especially the EEG. Beside these, the emergence of blockchain with its decentralized characteristic potentially provides new pathways for biometric authentication and biometric template security.

Although stated in Chapter 4 that there have not been any systematic way to launch the pre-image attack on the EMCC module, it is necessary to either formally prove that this module is resistant to such an attack or find the mathematical way to successfully launch this attack onto the module. This is a necessary research task to complete for the research community to ensure that a defense mechanism is to be found before a biometric template is compromised with this attack.

There are also potential improvements that can be made to the processes and algorithms used. In Chapter 4, the cell values of the original MCC vector play a crucial role in determining the recognition performance of EMCC. If the distribu-

tion of these cell values for each fingerprint can be modeled, it is very likely that the performance of EMCC would be improved. In addition, the proposed DLSS algorithm has shown that if as the similarity between a pair of local structures is chosen carefully and correctly, even the low-score pairs can contribute to the process of recognizing the corresponding local structures. A dynamic implementation of the Local Similarity Assignment (LSA) is expected to bring a competitive performance. These would lead to the overall improvement of the framework.

- The MPT is a powerful nonlinear transformation that is resistant against the ARM. However, there are some optimization issues that need addressing: the KNN-MPT module of the framework presented in Chapter 4 stores the transformed biometric template as a vector of big decimals. This could lead to the use of a great amount of computational resources, hindering the applicability of the framework in portable devices or constraint-restricted environment. Besides, if the degree of the multivariate polynomial is too high, the time to perform calculation and the amount of memory consumed are high as well. It is necessary to find an optimal degree that balances the security and the time and memory complexity.

- The two transformations are designed for the cancellable biometric template. However, biocryptosystem is also found to be vulnerable to the ARM. Therefore, a solution for the defense of biocryptosystem-based methods against this kind of attack needs to be devised.

- The use of block-based ECC (especially the Reed-Solomon Codes) in biometrics involves the storage of the parity bits, which are generated based on the original biometric data. To our knowledge, no research has been dedicated to evaluate the entropy of these parity bits and the feasibility of retrieving the original data from these parity bits.

The research in Chapter 4 has been successfully simulated. With tuning, the algorithms demonstrated here could be implemented and validated for deployment

into mobile phones, smart devices, and security implementations. There is future development work required to transition this from research to a robust implementation. However, this implementation would benefit the community as well as the commercial providers of the biometric authentication systems due to the secure and stable performance of the framework. This aspect of the future work is less about providing research outcomes, but instead about translating these outcomes into implementable libraries for wider dissemination. Software engineering skills will be required to achieve this.

6.4 Summary

This research thesis has successfully explored and answered the question *How can we develop biometric authentication frameworks that can address major security and privacy threats while retaining a good authentication performance?* From the above analysis, the research question has successfully been answered. It is possible for biometric frameworks to mitigate the current threats to security and privacy in this space. This has been evidenced by the development of two different approaches that are able to do this.

The first of these proposed two irreversible transformations in conjunction with a multi-filter cancellable template framework. This was found to be capable of defending against the current classes of biometric-specific attacks. The second of these is a novel, light-weight biometric authentication that utilizes the power of AI with high performance is embedded in a ZKP Protocol to be ready for use in a subsequent cryptography-based security system.

The field of biometric identification is currently moving rapidly, and will need to expand as new threats in this space occur. The proliferation of biometrics for authentication has seen an increase in global security due to their robust nature, but we must remain vigilant to the emerging threats in space.

Bibliography

[1] The face database of the university of bern, 2008.

[2] The face database of the university of stirling, 2013.

[3] B. Abd El-Rahiem, A. Sedik, G. M. El Banby, H. M. Ibrahem, M. Amin, O.-Y. Song, A. A. Khalaf, and F. E. Abd El-Samie. An efficient deep learning model for classification of thermal face images. *Journal of Enterprise Information Management*, 2020.

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

[5] Y. Aberni, L. Boubchir, and B. Daachi. Palm vein recognition based on competitive coding scheme using multi-scale local binary pattern with ant colony optimization. *Pattern Recognition Letters*, 2020.

[6] F. Ahmad, L.-M. Cheng, and A. Khan. Lightweight and privacy-preserving template generation for palm-vein-based human recognition. *IEEE Transactions on Information Forensics and Security*, 15:184–194, 2019.

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

[8] N. Ahmadi, M. Nilashi, S. Samad, T. A. Rashid, and H. Ahmadi. An intelligent method for iris recognition using supervised machine learning techniques. *Optics & Laser Technology*, 120:105701, 2019.

[9] D. Ahn, S. G. Kong, Y.-S. Chung, and K. Y. Moon. Matching with secure fingerprint templates using non-invertible transform. In *2008 Congress on Image and Signal Processing*, volume 2, pages 29–33. IEEE, 2008.

[10] W. N. I. Al-Obaydy and S. A. Suandi. Automatic pose normalization for open-set single-sample face recognition in video surveillance. *Multimedia Tools and Applications*, 79(3):2897–2915, 2020.

[11] A. Almansa and L. Cohen. Fingerprint image matching by minimization of a thin-plate energy using a two-step algorithm with auxiliary variables. In *Proceedings Fifth IEEE Workshop on Applications of Computer Vision*, pages 35–40. IEEE, 2000.

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

[13] M. Bardet and F. Chyzak. On the complexity of a gröbner basis algorithm. In *Algorithms Seminar*, pages 85–92, 2005.

[14] M. Bardet, J.-C. Faugère, and B. Salvy. On the complexity of the f5 gröbner basis algorithm. *Journal of Symbolic Computation*, 70:49–70, 2015.

[15] K. Bashir, T. Xiang, and S. Gong. Gait recognition without subject cooperation. *Pattern Recognition Letters*, 31(13):2052–2060, 2010.

[16] A. Beng, J. Teoh, and K.-A. Toh. Secure biometric-key generation with biometric helper. In *2008 3rd IEEE Conference on Industrial Electronics and Applications*, pages 2145–2150. IEEE, 2008.

[17] K. P. Bennett and E. J. Bredensteiner. Duality and geometry in svm classifiers. In *ICML*, volume 2000, pages 57–64. Citeseer, 2000.

[18] B. Bhanu and X. Zhou. Face recognition from face profile using dynamic time warping. In *Proceedings of the 17th International Conference on Pattern Recognition, 2004. ICPR 2004.*, volume 4, pages 499–502. IEEE, 2004.

[19] A. Bhargav-Spantzel, A. C. Squicciarini, S. Modi, M. Young, E. Bertino, and S. J. Elliott. Privacy preserving multi-factor authentication with biometrics. *Journal of Computer Security*, 15(5):529–560, 2007.

[20] A. Bhargav-Spantzel, A. C. Squicciarini, R. Xue, and E. Bertino. Multifactor identity verification using aggregated proof of knowledge. *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*, 40(4):372–383, 2010.

[21] K. Bobkowska, K. Nagaty, and M. Przyborski. Incorporating iris, fingerprint and face biometric for fraud prevention in e-passports using fuzzy vault. *IET Image Processing*, 13(13):2516–2528, 2019.

[22] D. Boneh and V. Shoup. A graduate course in applied cryptography, 2020.

[23] J. Bringer, H. Chabanne, and A. Patey. Privacy-preserving biometric identification using secure multiparty computation: An overview and recent trends. *IEEE Signal Processing Magazine*, 30(2):42–52, 2013.

[24] R. Cappelli, M. Ferrara, and D. Maltoni. Minutia cylinder-code: A new representation and matching technique for fingerprint recognition. *IEEE transactions on pattern analysis and machine intelligence*, 32(12):2128–2141, 2010.

[25] D. Chang, S. Garg, M. Hasan, and S. Mishra. Cancelable multi-biometric approach using fuzzy extractor and novel bit-wise encryption. *IEEE Transactions on Information Forensics and Security*, 15:3152–3167, 2020.

[26] H. Chao, Y. He, J. Zhang, and J. Feng. Gaitset: Regarding gait as a set for cross-view gait recognition. In *Proceedings of the AAAI Conference on Artificial Intelligence*, volume 33, pages 8126–8133, 2019.

[27] H. Choi, K. Choi, and J. Kim. Fingerprint matching incorporating ridge features with minutiae. *IEEE Transactions on information forensics and security*, 6(2):338–345, 2011.

[28] T. Chugh and A. K. Jain. Fingerprint spoof detector generalization. *IEEE Transactions on Information Forensics and Security*, 2020.

[29] H. Chun, Y. Elmehdwi, F. Li, P. Bhattacharya, and W. Jiang. Outsourceable two-party privacy-preserving biometric authentication. In *Proceedings of the 9th ACM symposium on Information, computer and communications security*, pages 401–412, 2014.

[30] T. Connie, A. Teoh, M. Goh, and D. Ngo. Palmhashing: a novel approach for cancelable biometrics. *Information processing letters*, 93(1):1–5, 2005.

[31] M. Coşkun, A. Uçar, Ö. Yildirim, and Y. Demir. Face recognition based on convolutional neural network. In *2017 International Conference on Modern Electrical and Energy Systems (MEES)*, pages 376–379. IEEE, 2017.

[32] N. Courtois, A. Klimov, J. Patarin, and A. Shamir. Efficient algorithms for solving overdefined systems of multivariate polynomial equations. In *International Conference on the Theory and Applications of Cryptographic Techniques*, pages 392–407. Springer, 2000.

[33] R. G. Cutler. *Face recognition using infrared images and eigenfaces*. University of Maryland, 1996.

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

[35] R. Das, E. Maiorana, D. La Rocca, and P. Campisi. Eeg biometrics for user recognition using visually evoked potentials. In *2015 International Conference of the Biometrics Special Interest Group (BIOSIG)*, pages 1–8. IEEE, 2015.

[36] J. Daugman. How iris recognition works. In *The essential guide to image processing*, pages 715–739. Elsevier, 2009.

[37] J. G. Daugman. High confidence visual recognition of persons by a test of statistical independence. *IEEE transactions on pattern analysis and machine intelligence*, 15(11):1148–1161, 1993.

[38] G. I. Davida, Y. Frankel, and B. J. Matt. On enabling secure applications through off-line biometric identification. In *Proceedings. 1998 IEEE Symposium on Security and Privacy (Cat. No. 98CB36186)*, pages 148–157. IEEE, 1998.

[39] J. Deng, G. Trigeorgis, Y. Zhou, and S. Zafeiriou. Joint multi-view face alignment in the wild. *IEEE Transactions on Image Processing*, 28(7):3636–3648, 2019.

[40] C. Ding and D. Tao. Trunk-branch ensemble convolutional neural networks for video-based face recognition. *IEEE transactions on pattern analysis and machine intelligence*, 40(4):1002–1014, 2017.

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

[42] M. Dua, R. Gupta, M. Khari, and R. G. Crespo. Biometric iris recognition using radial basis function neural network. *Soft Computing*, 23(22):11801–11815, 2019.

[43] Y. Duan, J. Lu, J. Feng, and J. Zhou. Context-aware local binary feature learning for face recognition. *IEEE transactions on pattern analysis and machine intelligence*, 40(5):1139–1153, 2018.

[44] Y. Duan, J. Lu, J. Feng, and J. Zhou. Topology preserving structural matching for automatic partial face recognition. *IEEE Transactions on Information Forensics and Security*, 13(7):1823–1837, 2018.

[45] B. Efraty, E. Bilgazyev, S. Shah, and I. A. Kakadiaris. Profile-based 3d-aided face recognition. *Pattern recognition*, 45(1):43–53, 2012.

[46] L. A. Elrefaei and A. M. Al-Mohammadi. Machine vision gait-based biometric cryptosystem using a fuzzy commitment scheme. *Journal of King Saud University-Computer and Information Sciences*, 2019.

[47] L. Fei, B. Zhang, W. Zhang, and S. Teng. Local apparent and latent direction extraction for palmprint recognition. *Information Sciences*, 473:59–72, 2019.

[48] J. Feng, Z. Ouyang, and A. Cai. Fingerprint matching using ridges. *Pattern Recognition*, 39(11):2131–2140, 2006.

[49] 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*, 5(1):103–117, 2010.

[50] M. Ferrara, D. Maltoni, and R. Cappelli. Noninvertible minutia cylinder-code representation. *IEEE Transactions on Information Forensics and Security*, 7(6):1727–1737, 2012.

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

[52] A. Fiat and A. Shamir. How to prove yourself: Practical solutions to identification and signature problems. In *Conference on the theory and application of cryptographic techniques*, pages 186–194. Springer, 1986.

[53] J. Fierrez, J. Galbally, J. Ortega-Garcia, M. R. Freire, F. Alonso-Fernandez, D. Ramos, D. T. Toledano, J. Gonzalez-Rodriguez, J. A. Siguenza, J. Garrido-

Salas, et al. Biosecurid: a multimodal biometric database. *Pattern Analysis and Applications*, 13(2):235–246, 2010.

[54] J. Fierrez, J. Ortega-Garcia, D. T. Toledano, and J. Gonzalez-Rodriguez. Biosec baseline corpus: A multimodal biometric database. *Pattern Recognition*, 40(4):1389–1392, 2007.

[55] I. O. for Standardization. Iso/iec 24745:2011 information technology — security techniques — biometric information protection, 2011.

[56] M. Frank, R. Biedert, E. Ma, I. Martinovic, and D. Song. Touchalytics: On the applicability of touchscreen input as a behavioral biometric for continuous authentication. *IEEE transactions on information forensics and security*, 8(1):136–148, 2012.

[57] M. Fraschini, A. Hillebrand, M. Demuru, L. Didaci, and G. L. Marcialis. An eeg-based biometric system using eigenvector centrality in resting state brain networks. *IEEE Signal Processing Letters*, 22(6):666–670, 2014.

[58] R. W. Frischholz and U. Dieckmann. Biold: a multimodal biometric identification system. *Computer*, 33(2):64–68, 2000.

[59] K. Fukunaga. Statistical pattern recognition. In *Handbook of pattern recognition and computer vision*, pages 33–60. World Scientific, 1993.

[60] I. I. Ganapathi, S. S. Ali, and S. Prakash. Geometric statistics-based descriptor for 3d ear recognition. *The Visual Computer*, 36(1):161–173, 2020.

[61] B. P. Gilkalaye, A. Rattani, and R. Derakhshani. Euclidean-distance based fuzzy commitment scheme for biometric template security. In *2019 7th International Workshop on Biometrics and Forensics (IWBF)*, pages 1–6. IEEE, 2019.

[62] I. Goel, N. B. Puhan, and B. Mandal. Deep convolutional neural network for double-identity fingerprint detection. *IEEE Sensors Letters*, 4(5):1–4, 2020.

[63] M. Gomez-Barrero, J. Galbally, C. Rathgeb, and C. Busch. General framework to evaluate unlinkability in biometric template protection systems. *IEEE Transactions on Information Forensics and Security*, 13(6):1406–1420, 2017.

[64] M. Gomez-Barrero, E. Maiorana, J. Galbally, P. Campisi, and J. Fierrez. Multi-biometric template protection based on homomorphic encryption. *Pattern Recognition*, 67:149–163, 2017.

[65] H. Gunasinghe and E. Bertino. Privacy preserving biometrics-based and user centric authentication protocol for mobile devices. *Proceedings of 2014 Network and System Security (NSS2014)*, pages 15–16, 2014.

[66] H. Gunasinghe and E. Bertino. Privbiomtauth: Privacy preserving biometrics-based and user centric protocol for user authentication from mobile phones. *IEEE Transactions on Information Forensics and Security*, 13(4):1042–1057, 2017.

[67] K. Gupta, G. S. Walia, and K. Sharma. Quality based adaptive score fusion approach for multimodal biometric system. *Applied Intelligence*, 50(4):1086–1099, 2020.

[68] A. Hadid and M. Pietikäinen. Manifold learning for video-to-video face recognition. In *European Workshop on Biometrics and Identity Management*, pages 9–16. Springer, 2009.

[69] M. Haghighat, M. Abdel-Mottaleb, and W. Alhalabi. Discriminant correlation analysis: Real-time feature level fusion for multimodal biometric recognition. *IEEE Transactions on Information Forensics and Security*, 11(9):1984–1996, 2016.

[70] D. He and D. Wang. Robust biometrics-based authentication scheme for multiserver environment. *IEEE Systems Journal*, 9(3):816–823, 2014.

[71] M. He, J. Zhang, S. Shan, M. Kan, and X. Chen. Deformable face net for pose invariant face recognition. *Pattern Recognition*, 100:107113, 2020.

[72] T. K. Ho, J. J. Hull, and S. N. Srihari. Decision combination in multiple classifier systems. *IEEE transactions on pattern analysis and machine intelligence*, 16(1):66–75, 1994.

[73] H. G. Hong, M. B. Lee, and K. R. Park. Convolutional neural network-based finger-vein recognition using nir image sensors. *Sensors*, 17(6):1297, 2017.

[74] J. Hu, D. Gingrich, and A. Sentosa. A k-nearest neighbor approach for user authentication through biometric keystroke dynamics. In *2008 IEEE International Conference on Communications*, pages 1556–1560. IEEE, 2008.

[75] Y. Imamverdiyev, A. B. J. Teoh, and J. Kim. Biometric cryptosystem based on discretized fingerprint texture descriptors. *Expert Systems with Applications*, 40(5):1888–1901, 2013.

[76] D. Isenor and S. G. Zaky. Fingerprint identification using graph matching. *Pattern recognition*, 19(2):113–122, 1986.

[77] K. Ito, A. Morita, T. Aoki, H. Nakajima, K. Kobayashi, and T. Higuchi. A fingerprint recognition algorithm combining phase-based image matching and feature-based matching. In *International Conference on Biometrics*, pages 316–325. Springer, 2006.

[78] A. K. Jain, L. Hong, S. Pankanti, and R. Bolle. An identity-authentication system using fingerprints. *Proceedings of the IEEE*, 85(9):1365–1388, 1997.

[79] Q. Jiang, N. Zhang, J. Ni, J. Ma, X. Ma, and K.-K. R. Choo. Unified biometric privacy preserving three-factor authentication and key agreement for cloud-assisted autonomous vehicles. *IEEE Transactions on Vehicular Technology*, 2020.

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

[81] Z. Jin, J. Y. Hwang, Y.-L. Lai, S. Kim, and A. B. J. Teoh. Ranking-based locality sensitive hashing-enabled cancelable biometrics: Index-of-max hashing. *IEEE Transactions on Information Forensics and Security*, 13(2):393–407, 2017.

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

[83] 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*, 39(6):6157–6167, 2012.

[84] T. Joseph, S. Kalaiselvan, S. Aswathy, R. Radhakrishnan, and A. Shamna. A multimodal biometric authentication scheme based on feature fusion for improving security in cloud environment. *Journal of Ambient Intelligence and Humanized Computing*, pages 1–9, 2020.

[85] V. Joshi and P. Sanghavi. Three tier data storage security in cloud using face fuzzy vault. In *2012 International Conference on Computing, Communication and Applications*, pages 1–6. IEEE, 2012.

[86] A. Juels and M. Sudan. A fuzzy vault scheme. *Designs, Codes and Cryptography*, 38(2):237–257, 2006.

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

[88] B. Kaur, S. Singh, and J. Kumar. Robust iris recognition using moment invariants. *Wireless Personal Communications*, 99(2):799–828, 2018.

[89] X. C. P. J. F. Kevin and W. Bowyer. Visible-light and infrared face recognition. In *Workshop on Multimodal User Authentication*, page 48. Citeseer, 2003.

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

[91] J. B. Kho, A. B. Teoh, W. Lee, and J. Kim. Bit-string representation of a fingerprint image by normalized local structures. *Pattern Recognition*, 103:107323, 2020.

[92] V. Kilian, N. Ally, J. Nombo, A. T. Abdalla, and B. Maiseli. Cost-effective and accurate palm vein recognition system based on multiframe super-resolution algorithms. *IET Biometrics*, 9(3):118–125, 2020.

[93] E. Klinger and D. Starkweather. The open source perceptual hash library, 2010.

[94] G. Kumar, S. Tulyakov, and V. Govindaraju. Combination of symmetric hash functions for secure fingerprint matching. In *Pattern Recognition (ICPR), 2010 20th International Conference on*, pages 890–893. IEEE, 2010.

[95] P. Lacharme, E. Cherrier, and C. Rosenberger. Preimage attack on biohashing. In *2013 International Conference on Security and Cryptography (SECRYPT)*, pages 1–8. IEEE, 2013.

[96] 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)*, 37(4):980–992, 2007.

[97] Y. Lee, Y. Chung, and K. Moon. Inverse operation and preimage attack on biohashing. In *2009 IEEE workshop on computational intelligence in biometrics: theory, algorithms, and applications*, pages 92–97. IEEE, 2009.

[98] Y. J. Lee, K. R. Park, S. J. Lee, K. Bae, and J. Kim. A new method for generating an invariant iris private key based on the fuzzy vault system. *IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics)*, 38(5):1302–1313, 2008.

[99] L. Leng and A. B. J. Teoh. Alignment-free row-co-occurrence cancelable palmprint fuzzy vault. *Pattern Recognition*, 48(7):2290–2303, 2015.

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

[101] J. Li, X. Yang, J. Tian, P. Shi, and P. Li. Topological structure-based alignment for fingerprint fuzzy vault. In *2008 19th International Conference on Pattern Recognition*, pages 1–4. IEEE, 2008.

[102] Y. Li, W. Zheng, Z. Cui, and T. Zhang. Face recognition based on recurrent regression neural network. *Neurocomputing*, 297:50–58, 2018.

[103] H. Liu, G. Yang, L. Yang, and Y. Yin. Learning personalized binary codes for finger vein recognition. *Neurocomputing*, 365:62–70, 2019.

[104] J. Lu, V. E. Liong, and J. Zhou. Simultaneous local binary feature learning and encoding for homogeneous and heterogeneous face recognition. *IEEE transactions on pattern analysis and machine intelligence*, 40(8):1979–1993, 2017.

[105] J. Lu, K. N. Plataniotis, and A. N. Venetsanopoulos. Boosting linear discriminant analysis for face recognition. In *Proceedings 2003 International Conference on Image Processing (Cat. No. 03CH37429)*, volume 1, pages I–657. IEEE, 2003.

[106] H. Maeng, H.-C. Choi, U. Park, S.-W. Lee, and A. K. Jain. Nfrad: Near-infrared face recognition at a distance. In *2011 International Joint Conference on Biometrics (IJCB)*, pages 1–7. IEEE, 2011.

[107] M. Maguire. The birth of biometric security. *Anthropology today*, 25(2):9–14, 2009.

[108] D. Maio, D. Maltoni, R. Cappelli, J. L. Wayman, and A. K. Jain. Fvc2002: Second fingerprint verification competition. In *Object recognition supported by user interaction for service robots*, volume 3, pages 811–814. IEEE, 2002.

[109] D. Maio, D. Maltoni, R. Cappelli, J. L. Wayman, and A. K. Jain. Fvc2004: Third fingerprint verification competition. In *International conference on biometric authentication*, pages 1–7. Springer, 2004.

[110] E. Maiorana, G. E. Hine, and P. Campisi. Hill-climbing attacks on multibiometrics recognition systems. *IEEE Transactions on Information Forensics and Security*, 10(5):900–915, 2014.

[111] A. N. Marana and A. K. Jain. Ridge-based fingerprint matching using hough transform. In *XVIII Brazilian Symposium on Computer Graphics and Image Processing (SIBGRAPI'05)*, pages 112–119. IEEE, 2005.

[112] E. W. Mayr. Some complexity results for polynomial ideals. *Journal of complexity*, 13(3):303–325, 1997.

[113] T. C. Meetei and S. A. Begum. A variant of cancelable iris biometric based on biohashing. In *2016 International Conference on Signal and Information Processing (IConSIP)*, pages 1–5. IEEE, 2016.

[114] M. K. Morampudi, M. V. Prasad, and U. Raju. Privacy-preserving iris authentication using fully homomorphic encryption. *Multimedia Tools and Applications*, pages 1–23, 2020.

[115] T. Nakamura, V. Goverdovsky, and D. P. Mandic. In-ear eeg biometrics for feasible and readily collectable real-world person authentication. *IEEE Transactions on Information Forensics and Security*, 13(3):648–661, 2017.

[116] S. Nazari, M.-S. Moin, and H. R. Kanan. Securing templates in a face recognition system using error-correcting output code and chaos theory. *Computers & Electrical Engineering*, 72:644–659, 2018.

[117] H. Nejati, L. Zhang, T. Sim, E. Martinez-Marroquin, and G. Dong. Wonder ears: Identification of identical twins from ear images. In *Proceedings of the 21st International Conference on Pattern Recognition (ICPR2012)*, pages 1201–1204. IEEE, 2012.

[118] B. Ngugi, B. K. Kahn, and M. Tremaine. Typing biometrics: impact of human learning on performance quality. *Journal of Data and Information Quality (JDIQ)*, 2(2):1–21, 2011.

[119] V. Odelu, A. K. Das, and A. Goswami. A secure biometrics-based multi-server authentication protocol using smart cards. *IEEE Transactions on Information Forensics and Security*, 10(9):1953–1966, 2015.

[120] Y. S. Pagar and G. Chowdhary. Strengthening elliptic curve cryptography—key generation via biometric fusion approach. In *Computing in Engineering and Technology*, pages 87–101. Springer, 2020.

[121] F. P. Preparata and M. I. Shamos. *Computational geometry: an introduction*. Springer Science & Business Media, 2012.

[122] H. Proença and J. C. Neves. Segmentation-less and non-holistic deep-learning frameworks for iris recognition. In *Proceedings of the IEEE conference on computer vision and pattern recognition workshops*, pages 0–0, 2019.

[123] J. Qiu, H. Li, and C. Zhao. Cancelable palmprint templates based on random measurement and noise data for security and privacy-preserving authentication. *Computers & Security*, 82:1–14, 2019.

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

[125] C. Rathge, A. Uhl, and P. Wild. Reliability-balanced feature level fusion for fuzzy commitment scheme. In *2011 International Joint Conference on Biometrics (IJCB)*, pages 1–7. IEEE, 2011.

[126] C. Rathgeb and A. Uhl. An iris-based interval-mapping scheme for biometric key generation. In *2009 Proceedings of 6th International Symposium on Image and Signal Processing and Analysis*, pages 511–516. IEEE, 2009.

[127] C. Rathgeb and A. Uhl. Context-based biometric key generation for iris. *IET computer vision*, 5(6):389–397, 2011.

[128] C. Rathgeb and A. Uhl. A survey on biometric cryptosystems and cancelable biometrics. *EURASIP Journal on Information Security*, 2011(1):3, 2011.

[129] R. N. Rodrigues, L. L. Ling, and V. Govindaraju. Robustness of multimodal biometric fusion methods against spoof attacks. *Journal of Visual Languages & Computing*, 20(3):169–179, 2009.

[130] C. G. Rodríguez-Pulecio, H. D. Benítez-Restrepo, and A. C. Bovik. Making long-wave infrared face recognition robust against image quality degradations. *Quantitative InfraRed Thermography Journal*, 16(3-4):218–242, 2019.

[131] N. D. Roy and A. Biswas. Fast and robust retinal biometric key generation using deep neural nets. *Multimedia Tools and Applications*, 79(9):6823–6843, 2020.

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

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

[134] M. Sandhya and M. V. Prasad. A bio-cryptosystem for fingerprints using delaunay neighbor structures (dns) and fuzzy commitment scheme. In *Advances in Signal Processing and Intelligent Recognition Systems*, pages 159–171. Springer, 2016.

[135] M. Sandhya and M. V. Prasad. Cancelable fingerprint cryptosystem using multiple spiral curves and fuzzy commitment scheme. *International Journal of Pattern Recognition and Artificial Intelligence*, 31(04):1756004, 2017.

[136] W. J. Scheirer and T. E. Boult. Cracking fuzzy vaults and biometric encryption. In *2007 Biometrics Symposium*, pages 1–6. IEEE, 2007.

[137] B. Schölkopf, A. Smola, and K.-R. Müller. Nonlinear component analysis as a kernel eigenvalue problem. *Neural computation*, 10(5):1299–1319, 1998.

[138] S. Sharma and V. Kumar. Voxel-based 3d face reconstruction and its application to face recognition using sequential deep learning. *Multimedia Tools and Applications*, pages 1–28, 2020.

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

[140] R. Snelick, U. Uludag, A. Mink, M. Indovina, and A. Jain. Large-scale evaluation of multimodal biometric authentication using state-of-the-art systems. *IEEE transactions on pattern analysis and machine intelligence*, 27(3):450–455, 2005.

[141] C.-W. Tan and A. Kumar. Accurate iris recognition at a distance using stabilized iris encoding and zernike moments phase features. *IEEE Transactions on Image Processing*, 23(9):3962–3974, 2014.

[142] X. Tan and B. Triggs. Enhanced local texture feature sets for face recognition under difficult lighting conditions. *IEEE transactions on image processing*, 19(6):1635–1650, 2010.

[143] D. Tao, X. Li, X. Wu, and S. J. Maybank. General tensor discriminant analysis and gabor features for gait recognition. *IEEE transactions on pattern analysis and machine intelligence*, 29(10):1700–1715, 2007.

[144] Y. Tian, Y. Li, X. Liu, R. H. Deng, and B. Sengupta. Pribioauth: Privacy-preserving biometric-based remote user authentication. In *2018 IEEE Conference on Dependable and Secure Computing (DSC)*, pages 1–8. IEEE, 2018.

[145] Ö. Toygar and A. Acan. Multiple classifier implementation of a divide-and-conquer approach using appearance-based statistical methods for face recognition. *Pattern Recognition Letters*, 25(12):1421–1430, 2004.

[146] Q. Tran. Cancellable template design and application to steganography, 2017.

[147] Q. Tran, B. Turnbull, M. Wang, and J. Hu. A privacy-preserving biometric authentication system with binary classification in a zero knowledge proof protocol. *IEEE Open Journal of the Computer Society*, 2021.

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

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

[150] Q. N. Tran, B. P. Turnbull, and J. Hu. Biometrics and privacy-preservation: How do they evolve? *IEEE Open Journal of the Computer Society*, 2:179–191, 2021.

[151] M. Trokielewicz, A. Czajka, and P. Maciejewicz. Post-mortem iris recognition with deep-learning-based image segmentation. *Image and Vision Computing*, 94:103866, 2020.

[152] K.-W. Tse and K. Hung. Behavioral biometrics scheme with keystroke and swipe dynamics for user authentication on mobile platform. In *2019 IEEE 9th Symposium on Computer Applications & Industrial Electronics (ISCAIE)*, pages 125–130. IEEE, 2019.

[153] S. Tulyakov, F. Farooq, P. Mansukhani, and V. Govindaraju. Symmetric hash functions for secure fingerprint biometric systems. *Pattern Recognition Letters*, 28(16):2427–2436, 2007.

[154] H. T. Van, C. M. Duong, G. Van Vu, and T. H. Le. Palm vein recognition using enhanced symmetry local binary pattern and sift features. In *2019 19th International Symposium on Communications and Information Technologies (ISCIT)*, pages 311–316. IEEE, 2019.

[155] F. Vogel. The genetic basis of the normal human electroencephalogram (eeg). *Humangenetik*, 10(2):91–114, 1970.

[156] G. S. Walia, T. Singh, K. Singh, and N. Verma. Robust multimodal biometric system based on optimal score level fusion model. *Expert Systems with Applications*, 116:364–376, 2019.

[157] M. Wang, H. A. Abbass, and J. Hu. Continuous authentication using eeg and face images for trusted autonomous systems. In *2016 14th Annual Conference on Privacy, Security and Trust (PST)*, pages 368–375. IEEE, 2016.

[158] M. Wang, S. Abdelfattah, N. Moustafa, and J. Hu. Deep gaussian mixture-hidden markov model for classification of eeg signals. *IEEE Transactions on Emerging Topics in Computational Intelligence*, 2(4):278–287, 2018.

[159] M. Wang, H. El-Fiqi, J. Hu, and H. A. Abbass. Convolutional neural networks using dynamic functional connectivity for eeg-based person identification in diverse human states. *IEEE Transactions on Information Forensics and Security*, 14(12):3259–3272, 2019.

[160] M. Wang, J. Hu, and H. A. Abbass. Brainprint: Eeg biometric identification based on analyzing brain connectivity graphs. *Pattern Recognition*, page 107381, 2020.

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

[162] S. Wang and J. Hu. Alignment-free cancelable fingerprint template design: A densely infinite-to-one mapping (ditom) approach. *Pattern Recognition*, 45(12):4129–4137, 2012.

[163] S. Wang and J. Hu. Design of alignment-free cancelable fingerprint templates via curtailed circular convolution. *Pattern Recognition*, 47(3):1321–1329, 2014.

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

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

[166] X. Wang and W. Q. Yan. Cross-view gait recognition through ensemble learning. *Neural Computing and Applications*, 32(11):7275–7287, 2020.

[167] G. O. Williams. The use of d'as a "decidability" index. In *1996 30th Annual International Carnahan Conference on Security Technology*, pages 65–71. IEEE, 1996.

[168] 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*, 34(11):1221–1229, 2013.

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

[170] K. Xi, T. Ahmad, F. Han, and J. Hu. A fingerprint based bio-cryptographic security protocol designed for client/server authentication in mobile computing environment. *Security and communication networks*, 4(5):487–499, 2011.

[171] K. Xi and J. Hu. Biometric mobile template protection: a composite feature based fingerprint fuzzy vault. In *2009 IEEE International Conference on Communications*, pages 1–5. Citeseer, 2009.

[172] K. Xi, J. Hu, and F. Han. An alignment free fingerprint fuzzy extractor using near-equivalent dual layer structure check (nedlsc) algorithm. In *2011 6th IEEE Conference on Industrial Electronics and Applications*, pages 1040–1045. IEEE, 2011.

[173] K. Xi, Y. Tang, and J. Hu. Correlation keystroke verification scheme for user access control in cloud computing environment. *The Computer Journal*, 54(10):1632–1644, 2011.

[174] X. Xi, L. Yang, and Y. Yin. Learning discriminative binary codes for finger vein recognition. *Pattern Recognition*, 66:26–33, 2017.

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

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

[177] J. Yang, P. Ren, D. Zhang, D. Chen, F. Wen, H. Li, and G. Hua. Neural aggregation network for video face recognition. In *Proceedings of the IEEE conference on computer vision and pattern recognition*, pages 4362–4371, 2017.

[178] L. Yang, G. Yang, Y. Yin, and X. Xi. Finger vein recognition with anatomy structure analysis. *IEEE Transactions on Circuits and Systems for Video Technology*, 28(8):1892–1905, 2017.

[179] W. Yang, J. Hu, and S. Wang. A delaunay triangle-based fuzzy extractor for fingerprint authentication. In *2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications*, pages 66–70. IEEE, 2012.

[180] W. Yang, J. Hu, and S. Wang. A finger-vein based cancellable bio-cryptosystem. In *International Conference on Network and System Security*, pages 784–790. Springer, 2013.

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

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

[183] W. Yang, S. Wang, J. Hu, A. Ibrahim, G. Zheng, M. J. Macedo, M. N. Johnstone, and C. Valli. A cancelable iris-and steganography-based user authentication system for the internet of things. *Sensors*, 19(13):2985, 2019.

[184] W. Yang, S. Wang, J. Hu, G. Zheng, J. Chaudhry, E. Adi, and C. Valli. Securing mobile healthcare data: a smart card based cancelable finger-vein bio-cryptosystem. *IEEE Access*, 6:36939–36947, 2018.

[185] 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*, 58:102704, 2021.

[186] Y. Yang, B. Guo, Z. Wang, M. Li, Z. Yu, and X. Zhou. Behavesense: Continuous authentication for security-sensitive mobile apps using behavioral biometrics. *Ad Hoc Networks*, 84:9–18, 2019.

[187] X. Yin and X. Liu. Multi-task convolutional neural network for pose-invariant face recognition. *IEEE Transactions on Image Processing*, 27(2):964–975, 2017.

[188] X. Yin, Y. Zhu, and J. Hu. Contactless fingerprint recognition based on global minutia topology and loose genetic algorithm. *IEEE Transactions on Information Forensics and Security*, 15:28–41, 2019.

[189] Y. Yin, L. Liu, and X. Sun. Sdumla-hmt: a multimodal biometric database. In *Chinese Conference on Biometric Recognition*, pages 260–268. Springer, 2011.

[190] A. L. Yuille, P. W. Hallinan, and D. S. Cohen. Feature extraction from faces using deformable templates. *International journal of computer vision*, 8(2):99–111, 1992.

[191] C. Zauner. Implementation and benchmarking of perceptual image hash functions. 2010.

[192] B. Zhang, L. Zhang, D. Zhang, and L. Shen. Directional binary code with application to polyu near-infrared face database. *Pattern Recognition Letters*, 31(14):2337–2344, 2010.

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

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

[195] X. Zhang, L. Yao, C. Huang, T. Gu, Z. Yang, and Y. Liu. Deepkey: A multimodal biometric authentication system via deep decoding gaits and brainwaves. *ACM Transactions on Intelligent Systems and Technology (TIST)*, 11(4):1–24, 2020.

[196] Y. Zhang and A. M. Martínez. A weighted probabilistic approach to face recognition from multiple images and video sequences. *Image and Vision Computing*, 24(6):626–638, 2006.

[197] Z. Zhang, L. Tran, X. Yin, Y. Atoum, X. Liu, J. Wan, and N. Wang. Gait recognition via disentangled representation learning. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, pages 4710–4719, 2019.

[198] S. Zhao and B. Zhang. Deep discriminative representation for generic palmprint recognition. *Pattern Recognition*, 98:107071, 2020.

[199] X. Zhu, X. Liu, Z. Lei, and S. Z. Li. Face alignment in full pose range: A 3d total solution. *IEEE transactions on pattern analysis and machine intelligence*, 41(1):78–92, 2017.

[200] Q. Zou, Y. Wang, Q. Wang, Y. Zhao, and Q. Li. Deep learning-based gait recognition using smartphones in the wild. *IEEE Transactions on Information Forensics and Security*, 15:3197–3212, 2020.