People's Democratic Republic of Algeria

Ministry of Higher Education and Scientific Research
Mohamed El Bachir El Ibrahimi University of Bordj Bou Arréridj
Faculty of Mathematics and Computer Science
Department of Computer Science

THESIS
In order to obtain the Doctorate degree in LMD (3rd cycle)
Branch : Computer Science
Option : Information and Communication Sciences and Technologies.

THEME

On the efficiency of the transformation-based template protection algorithms

By : Zineb Maaref

Publicly defended on (07/07/2025)
In front of the jury composed of:

Pr. Farid Nouioua	University of B.B.A	**President**
Pr. Abdelouahab Attia	University of B.B.A	**Supervisor**
Dr. Foudil Belhadj	University of B.B.A	**Co-Supervisor**
Pr. Samir Akhrouf	University of M'sila	**Examiner**
Dr. Moussa Semchedine	University of Setif 1	**Examiner**
Dr. Mohamed Amine Beghoura	University of B.B.A	**Examiner**

2024/2025


بسم الله الرحمن الرحيم

Dedication

To the cherished memory of my beloved father, whose lessons in patience remain with me always.

To my dear and caring mother, for her unwavering love and support.

To my husband, whose steadfast encouragement carried me through every challenge of this journey.

To my brothers and sisters, whose kindness and help were invaluable along the way.

To my professors and colleagues, whose belief and guidance inspired me, especially in the final stretch.

To everyone who encouraged and supported me along the way.

Acknowledgements

Praise be to God alone.

I would like to express my sincere gratitude to my supervisor, ***Dr. Abdelouahab Attia****, for his unwavering encouragement, invaluable advice, and tireless efforts throughout this journey. His guidance and dedication have been a profound source of inspiration and an exemplary model for me to follow.*

I am equally grateful to my co-supervisor, ***Dr. Foudil Belhadj****, for his steadfast support, commitment, and for imparting to me the essence of being a researcher. His guidance and encouragement have not only made my journey significantly smoother but also deeply enriched my experience.*

I would like to thank the jury members for taking the time to read and evaluate this thesis. Your proposals and comments will undoubtedly contribute to its enrichment.

I would like to extend my heartfelt gratitude to my family, whose unwavering support, encouragement, and love have been a constant source of patience and strength throughout my journey to complete this thesis from its very beginning.

Zineb Maaref

Abstract

With the intense proliferation of biometric identification systems (BIS), several security concerns about the vulnerability of the user templates have emerged. Indeed, unlike the conventional security systems that are based on passwords or tokens which are renewable, a biometric template is not renewable once compromised. In addition, a compromised template can reveal the original biometric data, which constitutes a clear threat, as it can be used to track the user from one application to another. In fact, new algorithms have been proposed in the literature to reconstitute the original biometric trait by using the extracted features, attacking the stored features makes it possible to reconstruct the user's fingerprint, face, or other biometric trait in order to usurp the identity of another person or entity. For these reasons, cancelable biometric template protection methods have been proposed to overcome these problems. Their basic idea is to transform the biometric data and achieve the matching in the transformed domain. The transform function must simultaneously fulfill the following four properties: non-invertibility, cancelability, accuracy and diversity. The non-invertibility property guarantees that the original biometric data can't, or it is hard to, be recovered even if some parameters of the transform function are known. This is generally ensured by the non-existence of the inverse transform function (one-to-many inverse-transformation) or by, simply, making the search-space size very large to escape to a brute-force attack.

This thesis aims to investigate the robustness of cancelable biometric systems by analyzing and classifying various attacks targeting these systems based on well-defined criteria to enhance their security level. Additionally, it proposes a comprehensive evaluation framework grounded in stringent standards to assess the effectiveness of protection schemes against such attacks. Furthermore, a protection system for palmprint templates is implemented using irreversible transformation, ensuring a high level of security while ensuring the practical characteristics of these systems.

On the other hand, we are interested in transformation-based techniques that establish a mapping between the original biometric template points and the transformed template. An attack against a cancelable fingerprint scheme is conducted to demonstrate the possibility of inverting the transformation function and to analyze the impact of correlation between multiple instances of protected templates generated from the same biometric trait on the efficiency of such algorithms.

Keys words : image registration, cancelable biometrics, privacy, Biometric Template Protection, Security Analysis, Performance Evaluation.

Résumé

Avec la prolifération intense des systèmes d'identification biométrique (BIS), plusieurs préoccupations liées à la sécurité des modèles utilisateurs ont émergé. En effet, contrairement aux systèmes de sécurité classiques basés sur des mots de passe ou des jetons, qui sont renouvelables, un modèle biométrique n'est pas renouvelable une fois compromis. De plus, un modèle compromis peut révéler les données biométriques originales, ce qui constitue une menace claire pour suivre l'utilisateur d'une application à une autre. En fait, de nouveaux algorithmes ont été proposés dans la littérature pour reconstituer les données biométriques originales d'un sujet à partir des caractéristiques extraites , ce qui rend une attaque contre les caractéristiques stockées plus facile pour reconstruire l'empreinte digitale, le visage ou tout autre trait biométrique d'un utilisateur, afin d'usurper l'identité d'une autre personne ou entité. Pour ces raisons, des méthodes de protection des modèles biométriques annulables ont été proposées pour résoudre ces problèmes. Leur idée de base est de transformer les données biométriques et d'effectuer la correspondance dans le domaine transformé. La fonction de transformation doit simultanément remplir les quatre propriétés suivantes : non-inversibilité, annulabilité, précision et diversité. La propriété de non-inversibilité garantit que les données biométriques originales ne peuvent pas, ou il est très difficile, d'être récupérées, même si certains paramètres de la fonction de transformation sont connus. Cela est généralement assuré par l'absence de fonction de transformation inverse (transformation un-à-plusieurs) ou, tout simplement, en rendant la taille de l'espace de recherche très grande pour éviter une attaque par force brute.

Cette thèse vise à examiner la robustesse des systèmes biométriques annulables en analysant et en classifiant les attaques qui les ciblent, sur la base de critères bien définis, dans le but de renforcer leur niveau de sécurité. En outre, elle propose un cadre d'évaluation complet reposant sur des normes strictes pour évaluer l'efficacité des mécanismes de protection face à ces attaques. De plus, un système de protection des empreintes palmaires a été mis en œuvre à l'aide de transformations irréversibles, garantissant un haut niveau de sécurité tout en préservant les caractéristiques pratiques de ces systèmes.

D'autre part, nous nous intéressons aux techniques de transformation qui établissent une correspondance entre les points du modèle biométrique d'origine et le modèle transformé. Une attaque contre un schéma d'empreintes digitales annulable est menée afin de démontrer la possibilité d'inverser la fonction de transformation et d'analyser l'impact de la corrélation entre plusieurs instances de modèles protégés générés à partir du même sujet biométrique sur l'efficacité de ces algorithmes.

Mots clés : Enregistrement d'images, Biométries annulables, Confidentialité, Protection des modèles biométriques, Analyse de sécurité, Évaluation des performances.

ملخص

مع الانتشار الواسع لأنظمة التعرف البيومتري، ظهرت العديد من المخاوف الأمنية بشأن ضعف قوالب المستخدمين. في الواقع، على عكس أنظمة الأمان التقليدية المعتمدة على كلمات المرور أو الرموز، التي يمكن تجديدها، فإن القالب البيومتري لا يمكن تجديده بمجرد اختراقه. بالإضافة إلى ذلك، قد يكشف القالب المخترق عن البيانات البيومترية الأصلية، مما يشكل تهديدًا واضحًا لتتبع المستخدم من تطبيق إلى آخر. في الواقع، تم اقتراح خوارزميات جديدة في الأدبيات العلمية لإعادة تكوين بيانات المستخدم البيومترية الأصلية اعتمادًا على الميزات المستخرجة؛ مما يجعل الهجوم على الميزات المخزنة سهلًا لإعادة بناء بصمة الإصبع أو الوجه أو أي سمة بيومترية أخرى، بهدف انتحال هوية شخص أو كيان آخر. لهذه الأسباب، تم اقتراح طرق حماية للقوالب البيومترية القابلة للإلغاء للتغلب على هذه المشكلات. الفكرة الأساسية لهذه الطرق هي تحويل البيانات البيومترية وإجراء المطابقة في المجال المحول. يجب أن تحقق وظيفة التحويل أربع خصائص أساسية في آن واحد: عدم القابلية للعكس، القابلية للإلغاء، الدقة، والتنوع. تضمن خاصية عدم القابلية للعكس أن البيانات البيومترية الأصلية لا يمكن استردادها، أو يصعب استردادها، حتى إذا كانت بعض معلمات وظيفة التحويل معروفة. يتم تحقيق ذلك عادةً من خلال عدم وجود دالة تحويل عكسية (تحويل من واحد إلى متعدد) أو ببساطة من خلال جعل مساحة البحث كبيرة جدًا بحيث يصعب تنفيذ هجوم باستخدام القوة الغاشمة.

تهدف هذه الأطروحة إلى دراسة مدى قوة أنظمة القياسات البيومترية القابلة للإلغاء من خلال تحليل وتصنيف الهجمات التي تستهدفها بناءً على معايير محددة تهدف إلى تعزيز مستوى الأمان في هذه الأنظمة. كما نقدم إطارًا تقييمياً شاملاً يعتمد على معايير صارمة لتقييم فعالية أنظمة الحماية في مواجهة هذه الهجمات. بالإضافة إلى ذلك، قمنا بتطبيق نظام حماية لبصمة اليد باستخدام تحويل غير قابل للعكس، بما يضمن تحقيق مستوى عالٍ من الأمان مع ضمان الخصائص العملية لهذه الأنظمة.

من ناحية أخرى، نهتم بالتقنيات القائمة على التحويل التي تُنشئ تطابقًا بين نقاط القالب البيومتري الأصلي والقالب المُحوّل. نُجري هجومًا على مخطط بصمة قابل للإلغاء لإثبات إمكانية عكس دالة التحويل، ولتحليل تأثير الارتباط بين نسخ متعددة من القوالب المحمية المُولّدة من نفس الكائن البيومتري| على كفاءة هذه الخوارزميات.

الكلمات المفتاحية: تسجيل الصور، القياسات البيومترية القابلة للإلغاء، الخصوصية، حماية نماذج القياسات الحيوية، تحليل الأمان، تقييم الأداء.

Contents

List of Tables

List of Figures

List of acronyms

- **ANPDP** : National Authority for the Protection of Personal Data.
- **FTC** : Federal Trade Commission.
- **FAR** : False Acceptance Rate.
- **FRR** : False Rejection Rate.
- **EER** : Equal Error Rate.
- **FMR** : False Match Rate.
- **FNMR** : False No Match Rate
- **FTA** : Failure to Acquire Rate.
- **FTER** : Failure To Enroll Rate.
- **ZFRR** : Zero False Rejection Rate.
- **ZFAR** : Zero False Acceptance Rate.
- **ROC** : Receiver operating characteristic curve.
- **CMC** : Cumulative match characteristic curve.
- **BTP** : Biometric Template Protection.
- **CB** : Cancelable Biometric.
- **ARM** : Attack via record multiplicity.
- **AMRS** : Attack via missed record synchronization.
- **CT** : Cartesian Transformation.

Chapter 1

Introduction

"The quest for security is eternal, and it is in the vigilance, not the walls, where true security lies."

Henry Kissinger - 1985

Recently, computer networks (such as the Internet and mobile networks, ect...) have significantly influenced the world of communications and the exchange of information and services between individuals. As a result, communications, commercial services, and other interactions are now possible through these networks. Many of these services include e-commerce, healthcare, online banking, social networking, entertainment, and remote work. In this particular context, it is crucial to authenticate the identities of users to ensure the proper conduct of transactions among individuals. With the continuing increase in identity theft and related crimes, identification has become critical for governments, corporations, and federal crime units. Furthermore, a large number of personal identifying details contribute to the formation of what is called an identity. Identity is defined as a set of acquired or hereditary characteristics that distinguish individuals from one another. These characteristics can include biometric data, personal history, and behavioral patterns. Given the rise in identity-related crimes, the importance of accurate and secure identification processes has become increasingly crucial to effectively protect individuals and organizations.

For example, the U.S. Federal Trade Commission (FTC) reported that identity theft accounted for approximately 19% of all complaints in 2023, with a total of 5.4 million reports across various types of fraud. This increase is partly attributed to opportunities for fraudsters arising from heightened digitization and government assistance programs which inadvertently facilitated data theft. The cost of such theft was estimated at $52 billion, with over 40 million potential victims in the United States affected. This phenomenon is not limited to the United States; similar increases have been observed globally as online activities expand and criminals exploit new avenues for identity theft.

1.1 Limitations of Traditional Identification Systems

Traditional identification systems typically rely on two main methods: knowledge-based and object-based authentication. Knowledge-based authentication methods are defined as a set of information known exclusively to the user, such as passwords, IDs, and PIN codes...,ect. Object-based authentication relies on physical personal property of the individual, such as identity cards, passports, or secure memory cards...,ect.

In the evolving landscape of digital security, securely authenticating users remains paramount. Many research works [1] have argued that despite the security provided by authentication methods, unauthorized access still poses a clear threat due to the use of knowledge-based authentication methods, object-based authentication.

Moreover, with the pervasive threat of identity theft, traditional methods like passwords, despite their ubiquity, often fail to provide robust protection [1]. Unfortunately, these systems do not offer adequate security as credentials may be forgotten, stolen, or replicated, and other risks such as database leaks and keylogging.

The vulnerabilities inherent in passwords, such as susceptibility to brute-force attacks, underscore the need for more sophisticated authentication solutions. Additionally, passwords can often be easily guessed or cracked if users choose weak or common passwords. A notable example of password security failure is the Morris Worm incident of 1988 [2], where weak passwords were exploited to propagate one of the first widespread internet worms. Object-based authentication methods are not immune to vulnerabilities either, as physical items like identity cards or secure memory cards can be lost, stolen, or forged. These limitations highlight the critical need for advancing beyond traditional methods to ensure robust and reliable security measures.

1.2 Biometrics

Biometrics are used as an alternative to traditional authentication methods, as they cannot be lost or forgotten and offer a high degree of reliability due to their unique connection to the individual. It were first employed for security by law enforcement for criminal identification, initially with Alphonse Bertillon's **'anthropometry'** or **'human measurements'** system [3]. Fingerprints were among the earliest biometrics utilized in this domain, serving as a reliable identifier due to their uniqueness and permanence. Biometrics refers to a pattern recognition system that utilizes biometric data obtained from an individual, such as fingerprints, iris patterns, facial features, voice , or behavioral characteristics like , gait, typing rhythm,ect . It involves capturing a biometric signal, processing it to extract a set of distinctive features known as a **"biometric template"**, and subsequently comparing this template to stored models in a database. Essentially, biometrics operates as a signal processing system integrated with a pattern recognition architecture to authenticate or identify individuals based on their unique physiological or behavioral characteristics.

The biometric security system primarily relies on verifying an individual's identity based on what they know or possess, which can be a significant source of weakness and subsequent security problems. For instance, in financial institutions, biometrics are increasingly used for secure access to accounts and transactions, yet concerns about identity theft and fraudulent activities persist. In border control and immigration, biometric technologies such as facial recognition and fingerprint scanning aid in identity verification, but issues related to accuracy, privacy infringement, and algorithmic bias remain contentious. Moreover, in workplace environments, biometrics are employed for time and attendance tracking, raising issues of employee privacy and data protection.

1.3 Vulnerabilities of Biometric Systems

While biometric systems provide enhanced security and privacy for individuals' data, offering reliable and effective authentication across numerous applications, they still face significant

challenges, particularly concerning security and protection. Evaluating the security vulnerabilities of biometric systems is essential due to their susceptibility to specific weaknesses and the potential exposure to various risks, including spoofing, data breaches, and unauthorized access.These vulnerabilities may stem from either deliberate attacks or inherent weaknesses within the biometric system itself. For example, an attacker could reconstruct an artificial sample that closely mimics the original, enabling impersonation of a specific individual. Additionally, unlike passwords, biometric data is inherently public and accessible; for instance, a user's voice can easily be recorded, or fingerprints left on surfaces can be lifted, making biometric traits vulnerable to unauthorized capture and misuse. A notable example of this occurred in 2014 when hacker Jan Krissler successfully recreated the fingerprint of the German Defense Minister. Additionally, a well-known disadvantage of biometrics is their permanence; they cannot be replaced or changed. Consequently, misuse or theft can result in their irrevocable loss. Given these risks, it is crucial to exercise caution and implement comprehensive security measures to protect biometric data. This involves thoroughly studying the various types of vulnerabilities present in biometric authentication systems and establishing stringent protocols to evaluate and safeguard them.

1.4 Canacelable Biometrics

Cancelable biometrics was proposed as a prominent solution to the problems faced by classical biometric systems, aiming to enhance security and privacy [4][5][6]. It also provides a radical solution to scenarios where an attacker might use a stored template to obtain the original biometric data of a legitimate user or potentially usurp their identity. By securely transforming and storing an altered version of the original template, cancelable biometrics ensures that the original biometric information remains safeguarded even if the stored template is compromised.

A cancelable biometrics-based system typically comprises several stages: a data extraction phase, a transformation stage with a parameterized transformation function that alters the original features, and a matcher module. In the transformation stage, parameters such as passwords, random arrays, or pseudo-random numbers are used to create unique transformations, securing the biometric data. Finally, the matcher compares templates within the transformed domain, ensuring that biometric data remains protected while allowing for re-issuance of templates if needed.

Cancelable biometrics is characterized by several properties as determined by ISO24757 [7], among them the irreversibility property, which means that even if a fraudster gains access to the transformed template or the transformation function itself, they cannot reconstruct the original biometric data. Additionally, if the transformed template is compromised, it can simply be canceled and replaced with a new one by applying a different secret key. This flexibility allows cancelable biometrics to generate an unlimited number of unique transformed templates, each tailored to a specific application, ensuring that the compromise of one template does not affect others and maintains overall security.

1.5 Motivation and objectives of research

With the rise in security issues today, data protection authorities are working diligently to ensure privacy is maintained in biometric systems. As a result, specialized committees dedicated to protecting personal data have emerged. As an example, in Algeria the authority responsible

for data protection, ensuring compliance with data protection regulations, and addressing issues related to the processing of such data is the National Authority for the Protection of Personal Data(ANPDP) (Autorité nationale de protection des données à caractère personnel, ANPDP).

Current research in this field necessitates technical solutions to integrate privacy as a functional aspect of biometric systems, ensuring robust protection of users' personal data and restricting biometric data access to authorized individuals only. One promising approach is the development of transformation-based biometric systems, where transformed templates are used for authentication instead of the users' original templates.

Although Cancelable biometrics protect individuals' biometric data and enhance security and privacy, they still require further study due to their inherent limitations. This thesis aims to safeguard cancelable biometric systems by identifying and analyzing their various vulnerabilities. By thoroughly examining these weak points, the goal is to raise awareness and develop solutions that ensure the protection and privacy of individuals. The following paragraph details the objectives of our research.

1. **Developing a comprehensive survey of vulnerabilities and attacks against revocable biometrics** In the existing literature, there is a lack of research addressing the security effectiveness of protection methods for cancelable biometric schemes. Existing surveys have reviewed some of them, but they have not sufficiently covered the security and privacy aspects. Therefore, it was necessary to conduct a recent comprehensive survey of these various security aspects and clarify the weak points in their schemes to strengthen their security. Additionally, emphasizing these weaknesses encourages the development of more advanced and secure cancelable biometric techniques, thereby enhancing overall user privacy and trust in biometric technologies. In another side, evaluating the effectiveness and identifying weaknesses of transformation-based algorithms is very necessary. There are several transformation algorithms designed to protect biometric data by creating a transformation function that uses secret parameters specific to each user. In this way, the transformed biometric template is stored instead of the original, and authentication occurs within the transformed domain. One key property of this transformation function is irreversibility, meaning it is not possible to reverse-engineer the original data from the transformed template. Consequently, if an attacker obtains the transformed biometric data, they cannot retrieve the original data or the transformation parameters. However, in this thesis, we demonstrate that these protection techniques still require further study.This field currently lacks comparative analyses between various attack types, which are essential for understanding the severity and effectiveness of these threats. To address this gap, we conducted a series of classifications and comparisons using established criteria, shedding light on the vulnerabilities within protection systems. Additionally, we proposed a rigorous evaluation framework for protection systems that relies on transformation methods and adheres to strict security benchmarks.

2. **Developing transformation-based protection system for safeguarding palmprint data:** Apart from the weaknesses found in the protection algorithms, a Cartesian transformation-based algorithm has been proposed for palmprint protection, providing security and privacy for individuals' biometric data. This innovative methodology involves extracting features from the palmprint, creating the biometric template, and then generating a transformed template using a cartesian transformation function. The process also includes a matching stage within the transformed domain. A key advantage of this approach is that it stores the transformed palmprint templates in databases instead of the original ones. As a result, if the transformed templates are stolen, it will not be

possible to revert to the original palmprint templates. Additionally, the system allows for the cancellation and renewal of templates by updating the user's secret code, further enhancing security in case of theft.

3. **Developing an attack on an irreversible fingerprint transformation scheme :** In cancelable biometrics, the core concept involves applying a transformation function, parametrized with a secret key, to distort the original biometric template. The generated template is intended to be non-invertible, ensuring that an attacker cannot reconstruct the original biometric data even if the key is compromised. However, despite their advantages, many of these systems remain vulnerable to attacks. In this study, we analyze the security aspects of a well-known transformation-based CB algorithm introduced by [8] in its cartesian version. Our findings indicate that the algorithm's security heavily relies on the management of the user key. If this key is compromised, the entire biometric template becomes vulnerable. The attack is carried out in two key phases: first, the user key is extracted by leveraging inconsistencies in information sharing across multiple transformed templates of the same individual; second, the original template is reconstructed by formulating and solving a system of constraints. Experimental results demonstrate the effectiveness of the proposed attack.

1.6 Research contributions

The main contributions associated with this work are :

1. Z. Maaref, A. Attia, F. Belhadj
   Generating cancelable multispectral palmprint templates based on cartesian transformation, in: 2023 5th International Conference on Pattern Analysis and Intelligent Systems (PAIS), IEEE, 2023, pp. 1–7. https://doi.org/10.1109/PAIS60821.2023.10322061 (IEEE Publisher).

2. Zineb Maaref, Foudil Belhadj, Abdelouahab Attia, Zahid Akhtar, Muhammed Basheer Jasser, Athirah Mohd Ramly, Ali Wagdy Mohamed.
   A comprehensive review of vul- nerabilities and attack strategies in cancelable biometric systems. Egyptian Informatics Journal, 27:100511, 2024 https://doi.org/10.1016/j.eij.2024.100511

3. Zineb Maaref, Foudil Belhadj, Abdelouahab Attia, Zahid Akhtar.
   Attack against key-dependent transformation-based fingerprint template protection Algorithms : which is under review in the Journal of Ambient Intelligence and Humanized Computing (Springer, Electronic ISSN : 1868-5145).

1.7 Thesis outline

This dissertation is structured as follows:

Chapter 2 : This chapter provides an in-depth exploration of biometrics and authentication systems. It provides a detailed description of the biometric identification process, various biometric modalities, their characteristics, modes, and system architectures. Furthermore, it describes the points of vulnerability within biometric systems.

Chapter 3 : This chapter delves into the significance of cancelable biometrics in protecting individuals' data and privacy. We outline the architectural principles behind cancelable biometric systems and provide a comprehensive overview of their various types, with a particular focus on transformation-based approaches.

Chapter 4 : This chapter focuses on the various attacks targeting cancelable biometrics. We categorize these attacks based on their methodologies and provide a detailed analysis of each type. Additionally, we conduct a comprehensive survey of the existing attacks within each category, highlighting the specific vulnerabilities that adversaries exploit. Furthermore, the chapter includes comparisons of these attack types and introduces a framework for evaluating protection systems, facilitating a deeper understanding of the challenges and potential solutions in this field.

Chapter 5 : In this chapter, we present a method for safeguarding palmprint templates using a Cartesian transformation. This approach generates robustly protected templates through a non-invertible transformation function, effectively preventing reverse engineering of the original data. Our method not only enhances the security of palmprint templates but also achieves high performance in terms of accuracy and reliability.

Chapter 6 : In this chapter, we analyze the security of the well-known Cartesian transformation [8], with a particular focus on its non-invertibility. We propose an attack algorithm that successfully reverses the transformation function, demonstrating that the cartesian transformation scheme fails to ensure the required level of security. Our findings highlight the need for further evaluation and refinement to enhance its robustness against potential attacks.

Finally, we conclude this thesis with a general summary of the research, outlining the main conclusions and various future directions.

Chapter 2

Biometric Systems

2.1 Introduction

Biometrics aims to identify or confirm identity across various services and applications used in daily life, such as computers, mobile phones, banks, and buildings, ensuring access only for legitimate users. Biometric identification leverages physiological or behavioral characteristics for this purpose.

The concept of identifying individuals using physiological characteristics dates back thousands of years. In the mid-19th century, Alphonse Bertillon, head of the criminal identification department in the Paris police force, pioneered the use of body measurements along with eye, hair, and skin color to verify the identity of criminals. This idea has since evolved, where many identity verification agencies now store fingerprints in databases, a practice that remains relevant today.

However, biometrics extend beyond fingerprints to include various other modalities/traits such as iris recognition, facial recognition, handwriting analysis, and even gait analysis. This diversity in authentication techniques enhances the speed and efficiency of human identification processes.

In this chapter, we introduce the fundamental concepts of biometrics, providing a detailed explanation of how biometric systems operate. We discuss the most commonly used biometric modalities and highlight their effectiveness in replacing traditional identification systems. Additionally, we present the architecture of biometric systems and examine the key performance evaluation metrics.Finaly, we discuss the main vulnerabilities of biometric systems.

2.2 Biometric Modalities

Biometrics has been defined as the science dedicated to identifying individuals through unique physiological and behavioral traits. Its core objective is to achieve accurate identification based on distinct physical or behavioral characteristics [9]. Broadly, biometrics encompasses all processes designed to recognize individuals by measuring one or more of their physical, behavioral, or biological attributes [10].

Moreover, these characteristics are intrinsically linked to the individual, providing a level of permanence and reliability that traditional methods of identification lack.

The biometric traits can be categorized as follows :

1. **The physiological traits:** are the unique and permanent physical characteristics that exist for every individual. These traits include fingerprints, iris , facial features, palm prints, and hand geometry, DNA; ect.,. Each of these characteristics is distinct and remains stable over time, making them highly reliable for identification and verification purposes. Here are explanations of some commonly used physiological traits:

    a. **Fingerprints** :Fingerprint-based identification is one of the most common and historically utilized methods of identification. It is based on the unique ridges and patterns on the fingertips, which are formed during the first seven months of fetal development. These distinct patterns remain unchanged throughout a person's life, making them highly reliable for identification purposes. Fingerprint-based systems are widely employed in law enforcement and security systems due to their accuracy and efficiency.

    b. **Iris** : The complex and unique patterns in the colored part of the eye, known as the iris, are used for identification. The intricate tissue of the iris contains detailed information sufficient for distinguishing individuals. These patterns are formed during fetal development and stabilize within the first two years of life. Iris-based identification systems are highly accurate and reliable, making them a valuable tool for security and identification purposes.

    c. **Face** : Facial recognition is a widely used method of identification that relies on the location, shape, and spatial relations of distinct facial features such as the nose, eyebrows, eyes, and mouth. Advanced algorithms analyze these features to create a unique facial map for each individual. This technology has become increasingly sophisticated, enabling high accuracy in both identification and verification processes. Facial recognition is commonly used in various applications, from unlocking smartphones to enhancing security in airports and public spaces. Additionally, it can operate in real-time, making it a valuable tool for surveillance and monitoring. The non-invasive nature of facial recognition further contributes to its popularity and broad adoption.

    d. **Palmprint** : The palmprint shares similar patterns of ridges and valleys found in fingerprints but differs in terms of area, as the palm is larger than the fingerprint. Additionally, the palm print includes other distinctive features, such as wrinkles and major lines, which provide further unique characteristics for identification. The larger surface area of the palm allows for the capture of more detailed and varied information, enhancing the accuracy and reliability of palm print-based identification systems.

    e. **Hand geometry** : Recognition systems based on hand geometry utilize the size, width, and length of the palm, as well as the length of the fingers, to identify individuals. While these geometric characteristics can provide useful identification information, they are currently not as well-established or unique as other biometric traits. This limitation affects the scalability of hand geometry-based recognition systems, making them less effective for applications that require distinguishing individuals within a large population. Consequently, hand geometry is often used in combination with other biometric methods to enhance accuracy and reliability.

    f. **DNA** : Deoxyribonucleic acid (DNA) serves as the unique genetic code for each individual, except identical twins who share identical DNA sequences. DNA-based identification is extensively used in forensic and identification applications, offering the highest level of accuracy. However, this method requires more complex and time-consuming analysis compared to other biometric systems. Despite the complexity,

DNA's unparalleled precision makes it invaluable for legal and investigative purposes, ensuring definitive identification.

g. **Ear** : Ear features are generally considered insufficiently distinctive for reliable identification on their own. As a result, existing ear recognition systems focus on measuring and matching the distances between prominent points on the pinna and other distinctive locations on the ear. This method enhances the accuracy of identification by leveraging the unique geometric relations between these key points.

h. **Finger knuckle print(FKP):** This trait leverages the unique patterns on the dorsal (back) surface of the finger, which contains distinctive features, including prominent main lines, secondary lines, and characteristic peaks. This modality is robust even in suboptimal imaging conditions, as these characteristics are often still detectable in low-quality images. This biometric feature has a less abrasive surface than fingerprints and can be captured non-invasively without physical contact, making it ideal for hygiene-sensitive applications [11].

2. **The behavioral traits:** Behavioral characteristics are unique patterns in the way individuals perform specific activities. These traits are derived from actions or behaviors that are measurable and distinct for each person. For example, the way one types on a keyboard, including hand movement, speed, and arm movement, can be analyzed. These characteristics are influenced by the individual's physical and emotional state, such as mood, health, and environment.

   Behavioral biometrics provide valuable insights and an additional layer of security when used alongside physiological traits for identification and authentication purposes.

   a. **Signature** : The signature is considered one of the behavioral biometric features recognized by identification systems, as each individual has a unique way of signing. Despite the possibility of forgery and the risk of deceiving the system, many governmental and private institutions continue to use signatures as a tool for identification. The distinctive patterns in a person's handwriting, such as stroke order, pressure, and speed, add layers of complexity that can help differentiate genuine signatures from imitations. While not infallible, signatures remain a widely accepted method of authentication in various legal and financial contexts.

   b. **Keystrocke** : Typing patterns serve as a unique behavioral biometric, allowing individuals to verify their identity. Each person has a distinct typing method, characterized by factors such as keystroke pressure, typing speed, and rhythm. These unique patterns enable the differentiation of one individual from another, providing an additional layer of security for identity verification. By analyzing these specific typing behaviors, systems can accurately distinguish between users, making typing biometrics a valuable tool in both security and authentication processes.

   c. **Voice** : Voice recognition relies on the unique and distinctive physiological characteristics of an individual's voice. While these traits are generally stable, they can be influenced by factors such as age, medical conditions, and emotional states. Voice recognition systems typically require users to pronounce a fixed, predefined text or phrase for accurate identification. Despite potential variations, the distinctiveness of each person's voice makes it a valuable tool for secure and reliable authentication.

Figure 2.1 illustrates the majority of biometric traits.

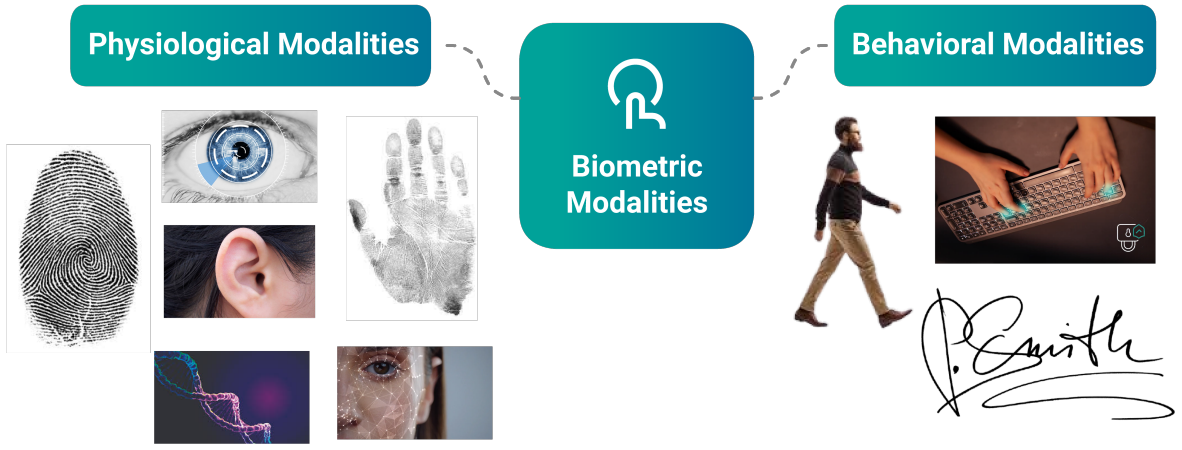


Figure 2.1: Various types of biometric modalities.

2.3 Utilization of Biometrics

In 2018, *"Findbiometrics.com"* conducted a survey revealing the biometric technology trends across various industries. As illustrated in Figure .2.2, face recognition technology dominated the market with a significant 37% share. This marked a shift from previous years, where fingerprint recognition had been the leading modality. Although fingerprint recognition still held a substantial share, it was surpassed by face recognition as the most prevalent biometric technology in the corporate sector during that year.[12]

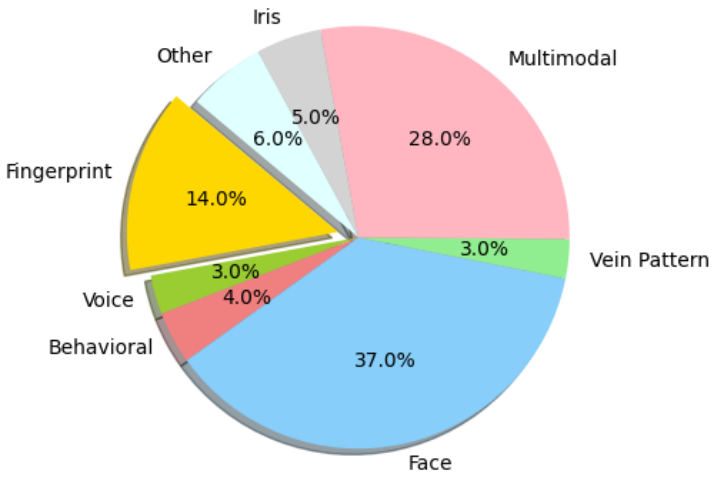


Figure 2.2: Biometric Modality Trends in 2018.-The figure highlights the market share distribution of biometric technologies, showing the rise of face recognition as the most adopted modality.

Biometrics has a broad range of applications across multiple fields, enhancing both security and convenience. For example, biometrics is used to produce more secure identity documents, such as national ID cards and biometric passports, which bolster personal and national security. Beyond security, biometrics also improves everyday convenience; for instance, at select airports, biometric systems streamline boarding for frequent travelers, significantly reducing wait times.

2.4 Objectives of Biometrics

The adoption of biometrics is driven by multiple objectives [13], including:

1. Enhanced Security: Biometrics provides robust security through unique individual characteristics, often coupled with biometric template encryption and other anti-fraud techniques to prevent unauthorized access and identity fraud.
2. User Convenience: Biometrics offers a high level of convenience, simplifying authentication processes compared to traditional methods like passwords, making identity verification faster and more user-friendly.
3. Data Integrity and Accountability: To ensure that interactions are securely linked to individuals, creating a record of access or actions associated with them, thus aiding in audits and accountability.

2.5 Characteristics of the Biometric System

Identifying and authenticating individuals is crucial, requiring biometric traits to fulfill several key requirements [3]. To ensure secure and accurate verification of identities and maintain high levels of security and reliability, these biometric features must adhere to the following criteria:

1. **Universality** : Every individual must be able to present this trait to the biometric system. This ensures that the biometric method can be applied across the entire population without exclusion.
2. **Distinctiveness** : Each feature used by the biometric system must be able to sufficiently distinguish one individual from another. This ensures that the biometric trait is distinct enough to identify each person uniquely.
3. **Permanence** : The trait used must be permanent and remain consistent over time to be considered a reliable biometric characteristic.
4. **Collectability** : The trait should be quantitatively measurable to ensure it can be effectively analyzed during the feature extraction phase, thereby providing accurate and valuable information for identification and verification purposes.
5. **Performance** : The performance and speed of a biometric system are directly linked to the quality of the traits it uses. High-quality biometric information ensures efficient and accurate system performance, while poor-quality data can significantly degrade both speed and reliability. Therefore, the effectiveness of the system is highly dependent on the precision and clarity of the biometric traits being analyzed.

6. **Acceptability** : The chosen biometric trait must be acceptable to individuals, ensuring their willingness to cooperate with the system during data capture. This consideration includes accommodating the conditions and constraints of the capture method.

7. **Circumvention** : This criterion assesses how easily the biometric system can be deceived into making an incorrect decision.

2.6 Architecture of Biometric System

The biometric system is a pattern recognition system that compares visual images of individuals. These images are pre-processed to ensure they are suitable for computer analysis and storage. This preprocessing step enhances the quality and consistency of the images, making them reliable for use in biometric identification and verification processes. During the registration process, biometric features are captured and stored in the database as reference templates for use during authentication or verification. The biometric system comprises several sections, detailed as follows:

1. **Capturing Phase** : During the capturing phase, the biometric identity is converted into a digital image using a sensor device, transforming a real-world phenomenon into a digital form. Sensor devices vary in quality, cost, and method of use, which can impact the effectiveness of the biometric system. The quality of the captured data significantly affects the authentication process and can be influenced by various factors, including the quality of the sensor, environmental noise, sweat, humidity, and physical conditions such as injuries. Ensuring optimal conditions and high-quality sensors is crucial for obtaining accurate and reliable biometric data.

2. **Feature Extraction Phase** :Firstly, the captured digital biometric data undergoes enhancement to ensure that the features can be accurately extracted. This improvement process involves using advanced extraction algorithms, such as those that identify minutiae points in fingerprint images, to derive a **template**. This template contains all the necessary information to identify the individual. By refining the data and focusing on critical features, the system enhances the accuracy and reliability of subsequent identification and verification processes. Additionally, this enhanced template minimizes storage requirements and speeds up the matching process, improving overall system efficiency.

3. **Storage Phase** : At this stage, the created biometric template is stored either as a simple file on a smart card or within a large database. In addition to the biometric template, personal data such as the user's first name, last name, and other relevant details can also be stored. This additional information helps in associating the biometric template with the correct individual, facilitating accurate identification and authentication processes.

4. **Matching Phase** : The individual who wants to authenticate or verify their identity inputs their biometric data into the system. This data undergoes the same extraction stage, producing what is known as a query template. The biometric system's matcher then compares the query template with the stored templates in the database. The result will be either acceptance or rejection, depending on whether the degree of matching meets the pre-determined decision threshold.

Figure 2.3 illustrates the architecture of the biometric system.

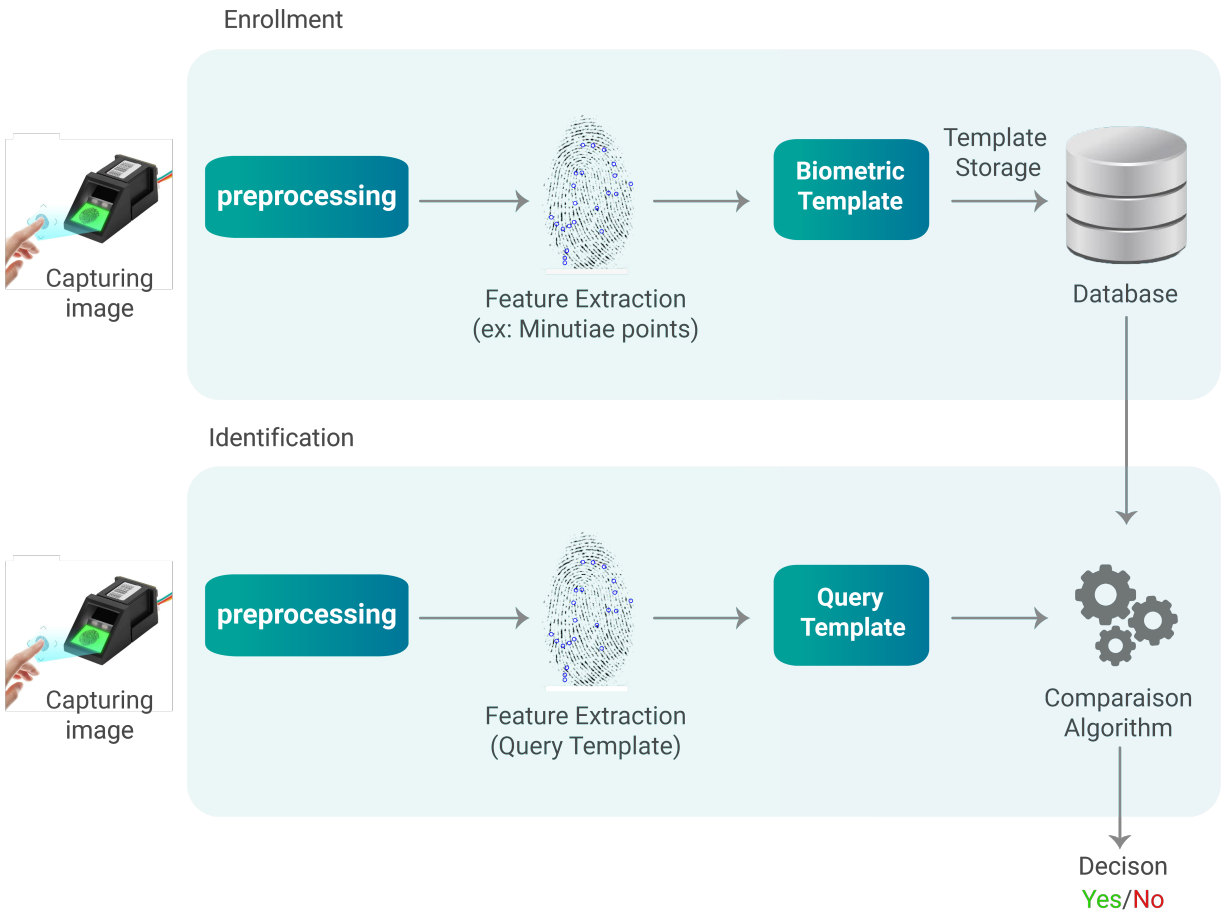


Figure 2.3: Architecture of a Biometric System

2.7 Operating Modes of the Biometric System

Biometric systems identify individuals by using their unique biometric traits and comparing them with templates stored in databases for authentication [3]. These systems operate in two modes:

1. **Enrollment Phase** : This initial stage serves as the entry point into the biometric system, where the user is registered. During this process, the individual's biometric data is presented to a sensor, which captures an image and extracts the relevant information. The captured data is then converted into a digital format and processed to create what is known as a biometric template using specific algorithms. Depending on the application and security requirements, the generated template is stored either in a centralized database or on a personal device unique to each user. This stage is common to both the verification and identification phases in biometric systems. Figure 2.4 illustrates the enrollment phase.

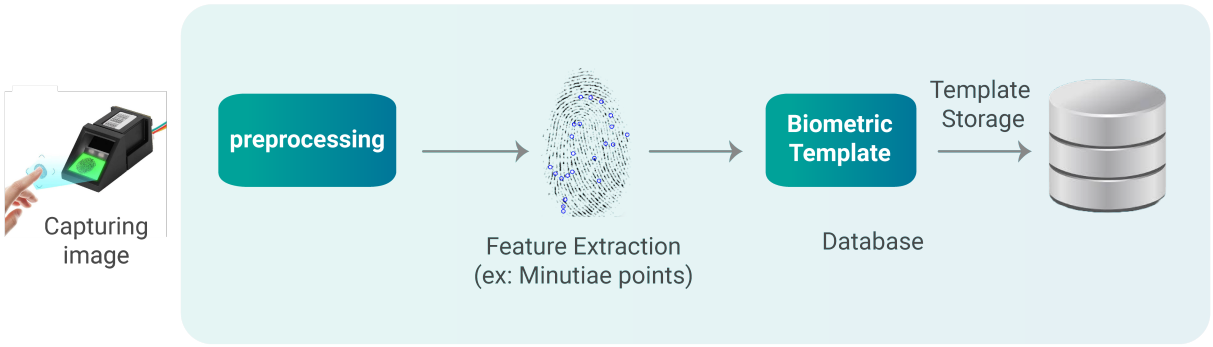


Figure 2.4: Biometric System Enrollment: Capturing and Storing Identity Templates.

2. **Verification Process**: In verification mode, the system confirms a person's claimed identity by comparing their biometric data with a specific template. It is 1:1 comparaision. The user first provides their identity, allowing the verification system to locate the corresponding registration template. The system then performs a comparison between the provided biometric data and the stored template. If the comparison result is positive, the user gains the privileges associated with their identity. If the result is negative, these privileges are denied. This process ensures that only authenticated individuals can access the associated benefits and services. Figure 2.5 illustrates the verification phase.

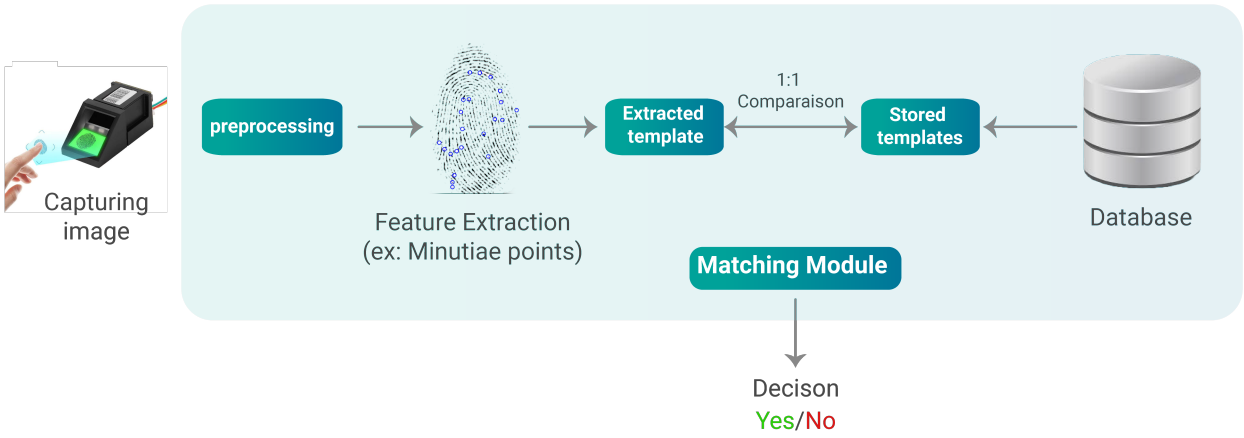


Figure 2.5: Verification Module: Matching captured biometric data against a stored template to confirm an individual's claimed identity

3. **Identificationn Process** : In identification mode, the system determines an individual's identity by comparing their biometric data against multiple templates within the database. This process is also known as a 1:N comparison, where N represents the number of stored identities that the system compares against the identity to be determined. The result is positive if the query biometric data sufficiently matches the stored template, indicating that the system's performance exceeds the decision threshold. In this case, the user gains the privileges associated with the identity linked to the registration template. Conversely, the user will be rejected if the result falls below the decision threshold or if the person is not registered in the system database. The biometric system ensures that each individual is not already registered by comparing the new biometric data with all

existing templates in the database. This prevents users from registering multiple times under different names. The registration process is carefully monitored to prevent the submission of incorrect data by users. Additionally, robust security measures are in place to detect and mitigate any attempts at fraud or identity manipulation, ensuring the integrity of the system. This comprehensive approach helps maintain accurate and reliable user identification, enhancing overall system security. Figure 2.6 illustrates the identification phase.

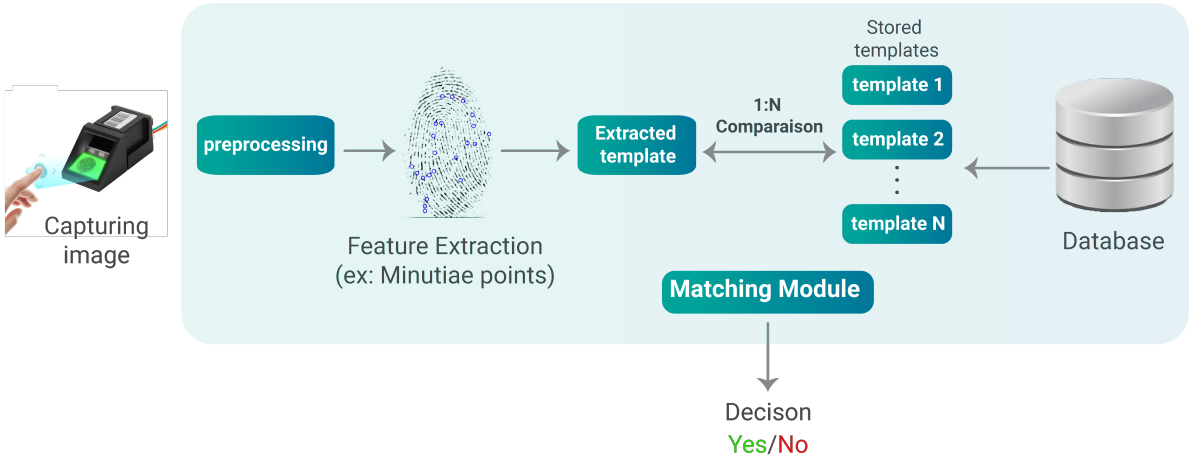


Figure 2.6: Identification Module: Comparing captured biometric data across multiple stored templates to determine an individual's identity.

2.8 Evaluation of a Biometric System

Assessing biometric systems is crucial because it equips researchers with the means to thoroughly test and refine their systems while considering user behavior during evaluation. This approach not only enhances our understanding of user needs but also facilitates the effective integration of biometric technology into everyday life. Moreover, it enables the identification of suitable industrial applications for each system based on various factors, including performance, usability, security, and the cost of technology deployment. Several factors can influence the outcome of biometric system evaluations, including:

1. Environmental Conditions: Variations in lighting, temperature, and background noise that can impact data capture.
2. Sensor-Related Imperfections: Such as noise, quality and resolution, directly affect the quality of the captured data.
3. Quality of Input Data: The clarity and accuracy of the biometric data (e.g., fingerprint, facial image) captured during enrollment and authentication.
4. User Variability : Physical variations, such as changes in appearance, alterations in fingerprint patterns, aging, and other similar factors.
5. User Cooperation: The level of cooperation and proper use of the system by individuals during biometric data capture and authentication.
6. Database Size and Quality: The size and comprehensiveness of the biometric database, as well as the quality of stored data.

2.8.1 Performance evaluation

With the growing reliance on biometric systems, it has become increasingly essential to rigorously evaluate their performance. The primary goal of these systems is to accurately identify individuals as either legitimate users or impostors. Legitimate users are those whose information has been previously registered in the system's database, while impostors are individuals attempting to gain authentication without prior registration, and therefore, the system treats them as unknown entities. However, biometric systems are not infallible and can sometimes mistakenly identify an impostor as a legitimate user (false acceptance) or reject a legitimate user and consider them an impostor (false rejection). Moreover, there remains a lack of universally reliable methods to ensure the absolute accuracy and dependability of biometric identification systems.

On the other hand, *intra-class variation* refers to the subtle differences observed in the biometric features of the same individual. These variations can arise from factors such as the pressure applied to the fingerprint sensor,changes in pose during face capturing, or other environmental influences. Typically, these differences are minimal, enabling the biometric authentication system to accurately verify the legitimate user. However, significant intra-class variation can lead to misidentification, where the system may erroneously flag a genuine user as an impostor. Figures 2.7 and 2.8 illustrate the extent of intra-class variation among biometric traits.

Figure 2.7: Snapshots of the same individual in different poses, illustrating the intra-class variation associated with an individual's face image and the resulting challenges for biometric systems in achieving accurate recognition.

(a) (b) (c) (d)

Figure 2.8: The following figure illustrates a low intra-class variation between four fingerprints of the same finger.

2.8.1.1 Error rate measurements

1. **Flase acceptance rate (FAR)**: which refers to the percentage of unauthorized or fraudulent users who are mistakenly recognized as legitimate by a biometric system. This error

occurs when the system inaccurately matches a fraudster's biometric data to that of an authorized user. The FAR can be calculated using the following equation:

$$\text{FAR}(\%) = \frac{\text{Number of false accepts}}{\text{Number of impostors tested}} \times 100$$

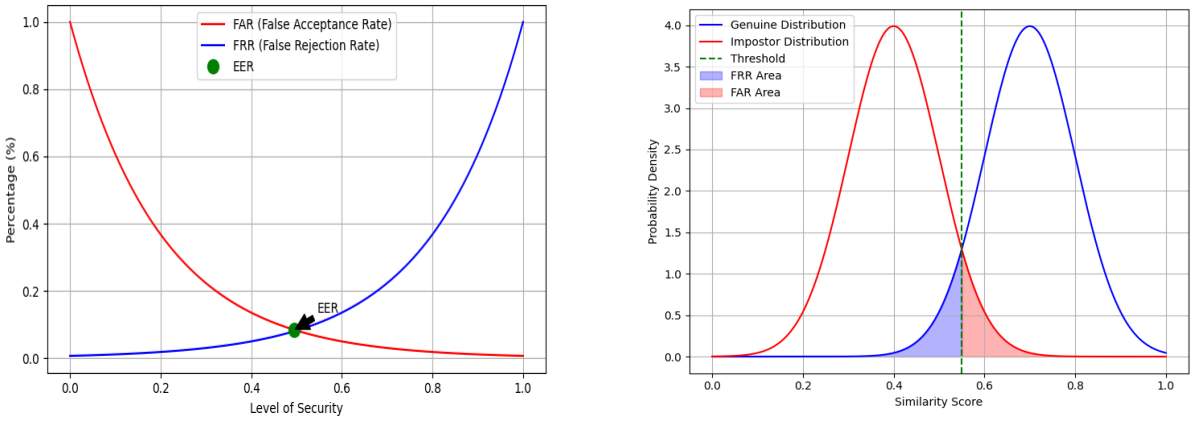
2. **Flase rejection rate (FRR)**: refers to the percentage of legitimate users who are incorrectly rejected by a biometric system. These rejections occur either because t-he matching algorithm fails to correctly match the biometric data or due to failures in the data acquisition process. As a result, legitimate transactions are mistakenly denied, highlighting a key challenge in biometric system accuracy. The FRR can be calculated using the following equation:

$$\text{FRR}(\%) = \frac{\text{Number of false rejects}}{\text{Number of clients}} \times 100$$

3. **Equal error rate (ERR)**: represents the point at which the False Acceptance Rate (FAR) and the False Rejection Rate (FRR) are equal, as shown in Fig.2.9- (a). A lower EER value indicates better system performance, as it reflects a more balanced trade-off between false acceptances and false rejections. In other words, as we attempt to lower the FRR (False Rejection Rate), the FAR (False Acceptance Rate) tends to increase. While a higher FAR can make the system more secure by reducing the likelihood of unauthorized access, it also makes the system less user-friendly, as legitimate users are more likely to be incorrectly rejected by the system. The EER is also referred to as the intersection rate or intersection error rate, the following equation illustrates the Equal Error Rate (EER) :

$$\text{EER} = \text{FAR} \quad \text{where} \quad \text{FAR} = \text{FRR}$$

Other terms, such as False Match Rate (FMR) and False Non-Match Rate (FNMR), are often used interchangeably with FAR and FRR [3] [4], particularly in identification systems where biometric query data is compared against a database of stored templates. FMR and FNMR are key metrics in evaluating system performance in this context. Figure 2.9-(b) illustrates an example of the distributions of true and false match scores, along with the corresponding FAR and FRR at a specific decision threshold.



(a) (b)

Figure 2.9: (a) FRR and FAR in Relation to the Security Level of a Biometric Authentication System. (b) Distributions of Genuine and Impostor Variations with FAR and FRR Areas

In addition, several other important metrics play a crucial role in providing a comprehensive assessment of biometric system performance.[14] These metrics offer further insights into the system's effectiveness and reliability in various operational contexts, including metrics such as:

- **Failure to Acquire Rate (FTA)** : measures the rate at which a biometric system fails to capture a specific user's biometric sample. This failure can occur for several reasons, such as poor image quality, unfavorable environmental conditions, or issues with the biometric sensor. A high FTA indicates that the system frequently fails to recognize or capture user data, which can significantly impact the usability and overall efficiency of the biometric authentication process.

- **Failure To Enroll Rate (FTER)** : measures the rate at which a biometric system fails to register an individual's biometric data. This failure can occur for several reasons, including poor quality of biometric samples, insufficient data, or issues with the enrollment process. A high FTER indicates that a significant number of users are unable to successfully enroll in the system, which can limit the system's accessibility and overall effectiveness.

- **Zero False Rejection Rate (ZFRR)** : It means the minimum False Acceptance Rate (FAR) achievable when the system correctly identifies all genuine users without any false rejections. In other words, it represents the FAR value at which the system perfectly recognizes all legitimate users, resulting in a False Rejection Rate (FRR) of zero.

- **Zero False Acceptance Rate (ZFAR)** : is defined as the lowest False Rejection Rate (FRR) that can be achieved when there are no false acceptances. In other words, it represents the FRR value at which the system completely avoids accepting any unauthorized users.

2.8.2 Performance Curves

- **ROC curve(Receiver operating characteristic curve)**: The ROC curve is used to evaluate the overall performance of a biometric authentication system. This curve illustrates the relationship between the False Acceptance Rate (FAR) and the False Rejection Rate (FRR) across different decision threshold values. The ROC curve provides a visual representation of the trade-off between FAR and FRR, helping to assess the system's ability to distinguish between legitimate and unauthorized users. Figure 2.10 displays an example of an ROC curve.

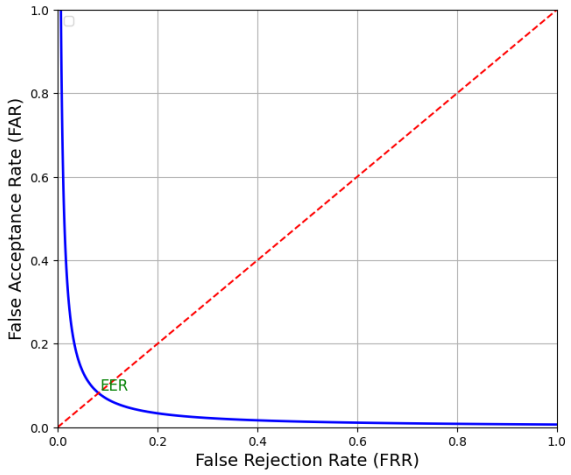


Figure 2.10: Example of the ROC Curve: Variation of FRR as a Function of FAR with Changing Decision Threshold.

- **CMC curve (Cumulative match characteristic curve)** : This curve represents the probability that a correct match for a given identity appears within the top N matches returned by the system. It shows how often the correct identity is ranked among the top candidates by the biometric system. The curve typically starts with the recognition rate at rank 1 and increases as the rank increases. A steeper CMC curve indicates better performance, as it shows that the system is more likely to correctly identify individuals at lower ranks. Figure 2.11 displays an example of an CMC curve.

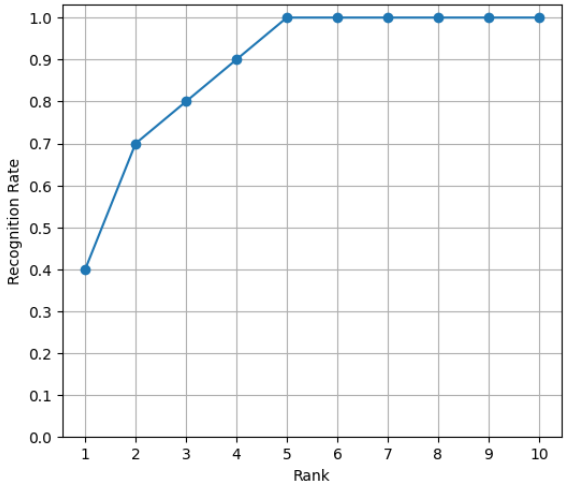


Figure 2.11: CMC curve showing the probability of correctly identifying an individual within the top N matches.

2.9 Benefits and Limitations of Biometric Technologies

2.9.1 Benifits of a biometric system

Biometrics significantly enhance security and protect individual privacy, offering distinct advantages over traditional authentication systems. Unlike passwords or access cards, which can be lost or forgotten, biometric traits are inherently linked to the individual and are always available. Instead of remembering multiple complex passwords, users can conveniently authenticate themselves by simply placing a finger on a sensor or capturing a facial image. The uniqueness and permanence of biometric identifiers provide a highly effective and reliable means of verifying a person's identity, making them a superior choice for secure authentication.

In certain scenarios, the transmission of biometric data poses significant concerns, particularly in token-based attendance systems where users transmit their IDs for authentication. In these systems, accountability is tied to the possession of the token rather than the identity of the person presenting it. Biometrics can address this issue by ensuring that accountability is directly linked to the individual, not just the token. This is especially valuable in applications where precise identification is crucial.

In traditional recognition systems, a user can exploit the system by enrolling multiple times under different identities, enabling them to fraudulently gain additional benefits, such as applying for multiple visas or social welfare claims. This loophole allows users to deny one of their enrolled identities after receiving the service, making it difficult for classical systems to detect such fraud. The challenge lies in confirming whether an individual is already enrolled in the system, even if they deny it, a problem known as the "negative recognition" issue. Biometrics offers a solution to this problem by ensuring that each individual can only be enrolled once, effectively preventing such fraudulent activities.

2.9.2 Limitations of the biometric system

While biometrics offer significant advantages over traditional authentication methods and are widely regarded as the solution to many of the issues inherent in conventional systems, they are not without their disadvantages and limitations. The weaknesses in a biometric system can arise either from inherent flaws within the system itself or from deliberate attacks targeting its vulnerabilities [5][15]. Traditional authentication methods, such as passwords or PINs, can be easily canceled or changed if compromised. However, biometrics present a unique challenge in this regard because biometric traits are inherently public and can be exposed, they are more vulnerable to theft. If biometric data is stolen, it is permanently compromised. Unlike passwords, biometric traits cannot be changed or recovered, making them vulnerable to lifelong misuse if breached.

Additionally, biometric-based authentication can be less accurate than traditional methods. Unlike passwords, where a correct input is either right or wrong, biometric systems operate on a similarity scale between 0% and 100%, with 100% accuracy rarely achieved. This variation in accuracy is influenced by several factors, including noise during data capture, lighting conditions, and sensor quality... For example, voice recognition becomes impractical in very noisy environments, and facial recognition may fail in the dark when using a visible light camera. These elements can introduce inconsistencies, making biometric systems more susceptible to errors compared to traditional authentication methods. These inconsistencies are reflected in two key types of variances: intraclass variance and interclass variance. Intraclass variance refers

to the variability observed within biometric samples from the same individual, highlighting inconsistencies in how the system recognizes the same person across different instances. Interclass variance, on the other hand, pertains to the differences observed between biometric samples from different individuals, indicating how distinct the system perceives the biometric traits of various people. These variances can impact the accuracy and reliability of biometric systems.

Furthermore, the use of an individual's biometric data across multiple applications can enable tracking due to the unique and unchangeable nature of biometric identifiers. For example, the India's Aadhaar system [16], where personal biometric information such as fingerprints and iris scans are collected for identification and government services. Despite its intended use for convenience and security, there have been reports of data breaches and unauthorized access to Aadhaar information. This raises significant privacy concerns, as leaked biometric data could allow individuals to be tracked across various services without their consent, with no way to revoke or change their biometric identifiers once compromised.

There are also cultural and usage-related restrictions associated with biometric systems. For example, fingerprints are often associated with criminal identification, investigations, and surveillance, which can create a negative perception of their use in everyday contexts. Additionally, fingerprints can sometimes be lifted from surfaces, replicated, and used without the owner's consent, raising concerns about security [17]. The physical contact required for fingerprint scanning also poses hygiene and personal privacy issues for some users, further limiting the acceptance and widespread adoption of this biometric modality.

On the other hand, identity theft has been demonstrated in many studies, not only through stealing biometric sample images or lifting them from surfaces, but also by exploiting compromised biometric templates. Attackers can use these compromised templates to reconstruct the original biometric image, allowing them to impersonate the legitimate user. For instance, the work in [18] demonstrated a successful approach to reconstruct a fingerprint image from the standard ISO/IEC 19794-2 template [7]. This format serves as the foundational standard for structuring, storing, and comparing fingerprint characteristics. It specifies a template that represents key fingerprint features, including minutiae location, orientation, and type (e.g., ridge ending or bifurcation). By adhering to this standardized template, fingerprint recognition systems ensure compatibility and interoperability. Reconstructing fingerprints through these types of attacks can expose individuals' privacy, potentially revealing sensitive information such as their financial background or personal lifestyle habits.

2.9.2.1 Biometric system vulnerabilities

Biometric systems are vulnerable to various security risks, including hacking, illegal trespass, damage and inherent weaknesses. Ratha et al.(2001) [5][19] identified eight specific points of vulnerability within these systems. Figure 2.12 illustrates their proposed model of these vulnerabilities. We will examine the vulnerabilities depicted in figure 2.12 and provide a detailed explanation of each one as follows:

1. **Fake biometric**: In this vulnerability, the fraudster presents a counterfeit biometric trait to the sensor, such as a forged fingerprint, face mask, or other fake biometric . Claude et al. [20] introduced a novel material called glycerin, which, due to its durability and optimal softness, is highly suitable for reconstructing fingerprints, offering a superior alternative to gelatin. Matsumoto et al.[21] also developed an attack targeting 11 biometric systems using counterfeit fingers crafted from gelatin. In 2018 Maro et al.[22] developed a method to unlock mobile phones using synthetic gelatin fingerprints, achieving approximately a

70% success rate on both the iPhone 6 and the Meizu M5s.

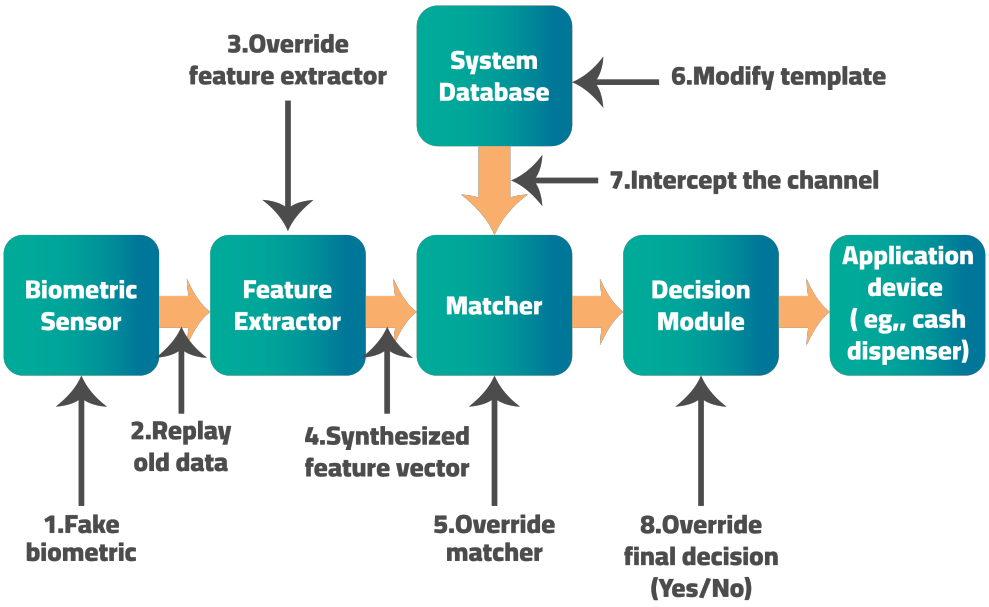


Figure 2.12: points of vulnerabilities of biometric system

2. **Replay old biometric data** : The vulnerability arises when old or previously captured biometric data, such as an old fingerprint or face image, is presented to the system instead of the new one. This allows attackers to bypass the direct sensor capture requirements, effectively spoofing the system and undermining its authentication process.

3. **Override feature extractor** : At this stage, the attack targets the feature extractor by introducing false data or deploying a Trojan horse, enabling the attacker to manipulate the system to generate specific feature sets aligned with their malicious intent. Additionally, user data can be compromised through various attacks, such as hill climbing, dictionary, and brute-force methods, which bypass legitimate inputs and exploit the system's vulnerabilities.

4. **Synthesized feature vector**: This vulnerability refers to an attack where the attacker intercepts and replaces the genuine biometric data extracted by the system (such as a fingerprint or facial features) with fraudulent data.

5. **Override matcher** : The matching module is responsible for calculating the similarity score between two biometric templates to verify an individual's identity. This score is then compared to a predefined decision threshold. Based on this threshold, the module provides a final decision, determining whether the template is genuine or fake. The attacker manipulates the matching score, artificially inflating or deflating it. This allows them to deceive the system into either falsely accepting an unauthorized individual (by raising the score) or wrongly rejecting a legitimate user (by lowering the score).

6. **Modify the stored biometric template** :The data storage stage is a fundamental component of the biometric system, responsible for storing biometric templates. However, biometric templates may be vulnerable at this stage. In such cases, a fraudster could alter the stored biometric template to either grant unauthorized access to a fraudulent individual or deny service to the legitimate user associated with the compromised template.

7. **Intercept the channel** : The stored template is transmitted to the matcher for comparison with the query template. In this instance, the attacker intercepts and alters the template during transmission, in the channel between the database and the matcher, compromising the integrity of the matching process.

8. **Override final decision** : In this scenario, the fraudster manipulates the matching result, either by falsely accepting and authenticating themselves or by rejecting the legitimate user, thereby compromising the system's accuracy and security.

Table 2.1 illustrates examples of the causes of attacks at each point in the biometric system.

Attack Point	Attack
1	- The attacker deliberately provides their biometric data to impersonate the legitimate user, typically targeting a weak biometric pattern of the legitimate user. - Provide biometric data similar to that of the legitimate user (an identical twin). - Stealing biometric data and submitting it to the sensor (such as fingerprints from surfaces).
2,4,7	-Intercepts the channel and replaces the legitimate biometric data with fake data. -The attacker continuously inputs data to render the system inaccessible to legitimate users. - Modify the original biometric data.
3,5	- Introducing false data or deploying a Trojan horse. - Hill climbing, dictionary, and brute-force methods
6	- The attacker modifies or deletes the stored biometric template.
8	- Manipulating the matching score by artificially inflating or deflating it.

Table 2.1: Vulnerabilities to Attacks in Biometric Systems

2.10 conclusion

In this chapter, we explored the concept of biometric systems, highlighting their advantages over traditional identification methods. Unlike classical systems that rely on codes and passwords, which can be easily hacked, lost, or forgotten, biometrics offers a more secure and reliable alternative by utilizing the unique biological and physiological traits of individuals to authenticate their identity.

The biometric authentication process consists of two key stages: registration and verification. During the registration stage, an individual's biometric data is captured via a sensor or camera and then processed to create a biometric template, which is stored in the system's database. In the verification stage, new biometric data provided by the individual is compared with the stored template to determine a match, resulting in either acceptance or rejection.

However, due to inherent variations between individuals and even within an individual's biometric samples, errors can occur. The system's performance is traditionally measured by two key metrics: the False Rejection Rate (FRR) and the False Acceptance Rate (FAR). FRR refers

to the system incorrectly rejecting a legitimate identity, while FAR measures the system's failure to reject an unauthorized identity. The balance between these two errors is known as the Equal Error Rate (EER), where both FAR and FRR are equal, indicating the system's overall accuracy.

While biometrics offers significant advantages, such as increased security and convenience, it is not without its limitations. No single biometric feature can achieve perfect accuracy, which is why combining multiple biometric modalities can improve recognition accuracy. Despite these benefits, biometric systems remain vulnerable to certain types of attacks and continue to be a subject of ongoing research. One promising development in this area is cancellable biometrics, a technique designed to enhance security by allowing biometric templates to be securely revoked and replaced if compromised. In the next chapter, we will delve deeper into cancellable biometric systems and their potential to address the challenges faced by traditional biometric systems.

Chapter 3

Biometric Template Protection Techniques

3.1 Introduction

Biometrics have gained widespread adoption across various fields due to their ease of use and enhanced data protection compared to traditional authentication methods, such as passwords, tokens, and ID cards..., which are prone to being lost, forgotten, or easily hacked [3]. However, biometric systems are not without flaws, as they are vulnerable to some serious weaknesses.For example, Cappelli et al. [18] show that a subject's original biometric sample can be reproduced from the stored template. This includes various types of attacks on biometric systems, which can lead to the exposure of personal and sensitive information, as well as identity theft [23] [24][25]. This poses a significant threat, as it enables the tracking of a user across different applications through the cross-matching of their biometric data. In addition, if a biometric template is stolen or compromised, it cannot be revoked, as it is permanently tied to the user's identity.

In recent years, many researchers have proposed ***Biometric Template Protection Techniques (PTP)*** [26][6][27] as a notable solution to address issues related to biometric template problems and mitigate scenarios where an attacker could exploit a stored template to reconstruct a legitimate user's original biometric data, potentially leading to identity theft [18]. BTP techniques aim to mitigate these risks by providing robust protection mechanisms, safeguarding user privacy, and preventing identity theft. Furthermore, it aims to distort an individual's original biometric template and modify the auxiliary information that defines the processing parameters or conditions. This approach safeguards privacy and ensures robust protection of personal data, making it resilient against unauthorized access and misuse.[28] However, several studies have observed that the performance of biometric systems tends to deteriorate somewhat when using cancelable biometrics compared to classical biometric systems [27] [6].

BTP is divided into two categories : ***Biomtric Cryptosystems (BC)*** and ***Cancelable Biometric (CB)*** [29]. In some studies, these two approaches have been integrated to form a hybrid system that enhances security measures and provides robust protection for personal biometric data against potential breaches and misuse [30].

In this chapter, we present an in-depth analysis of the two main categories of BTP algorithms, detailing their underlying architectures and operational mechanisms. Particular emphasis is placed on our research focus **cancelable biometrics** where we explore its fundamental categories and examine the most prominent schemes within each. This discussion provides a

comprehensive overview of existing approaches, highlighting their design principles, security properties, and practical applications.

3.1.1 Biomtric Cryptosystems

Cryptosystem-based methods rely on combining an encryption key, with the extracted biometric data to create the protected template. Cryptographic systems are further classified into key-binding systems and key-generation systems, depending on how the auxiliary data is used. In key-generation systems, both the auxiliary data and the key are generated directly from the biometric template. In key-binding systems, the auxiliary data is created by combining the key with the biometric template. One of the key difficulties in applying biometric cryptosystems is that they often require the biometric data to be transformed into a vectorized and discretized format, which can be challenging to achieve accurately for certain biometric representations, leading to a loss of precision and security [31]. The cryptographic methods, like fuzzy vaults [32] or fuzzy commitment [33], ensure that even if an attacker gains access to the transformed biometric template, it would be computationally infeasible to reverse-engineer the original biometric data.

The main disadvantages of biometric cryptosystems stem from the variability of biometric samples with each presentation. In key generation or key binding schemes, this variability may result in the generation of different keys, thereby reducing matching accuracy. Furthermore, storing biometric data locally for authentication and key release introduces significant security risks. For example, bit injection attacks can override the authentication process and force the release of cryptographic keys, making the system vulnerable to exploitation [24]. Figure 3.1 illustrates the biometric cryptosystems procedure.

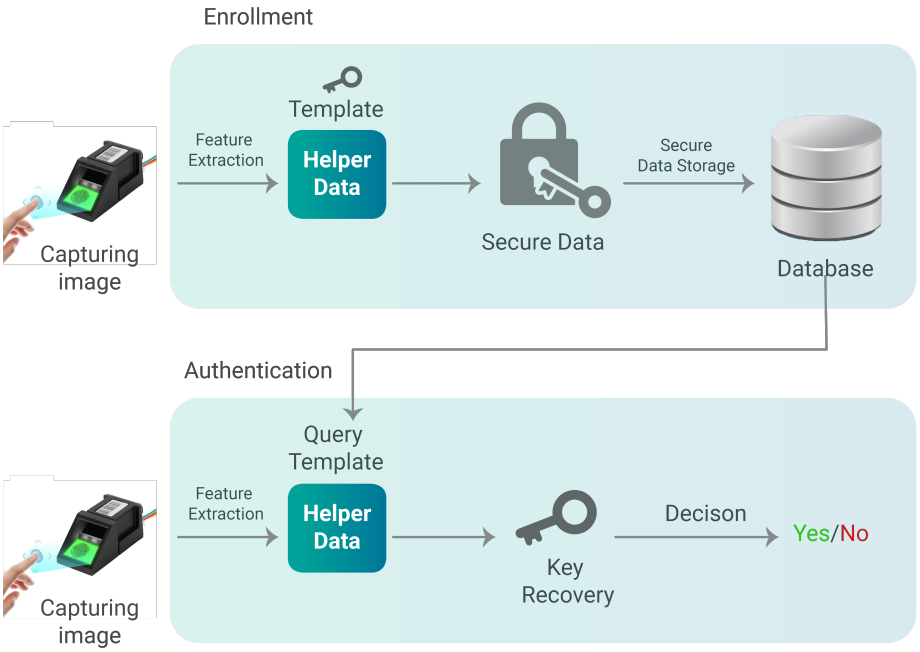


Figure 3.1: Overview of the biometric cryptosystems procedure, illustrating the enrollment and authentication processes.

3.1.2 Cancelable Biomtric

In 2002, Bolle et al. [15] described two transformation classes: the signal-domain transformation and the feature-domain transformation. In the first, the biometric signal is transformed directly after image acquisition. In the signal-domain approach, distortion is applied to the raw signal, which is then processed by a traditional biometric system that may not be aware of the distortions. Furthermore, the system only matches this distorted signal to a database if it is distorted in the same consistent manner. The distortion applied to the signal must be substantial enough to effectively alter the original signal for privacy purposes, yet controlled to reliably allow feature extraction and accurate identification.

For the feature domain transformation, the distortion is applied after the feature extraction phase. This means that the original features must be altered to generate entirely new ones that do not match with the original features. In this chapter, we are interested in feature-domain transformation approaches.

Cancelable biometrics involve deliberate and irreversible distortions of the original biometric data, achieved through a transformation function that utilizes unique parameters for each individual. Instead of storing the original biometric data, the transformed version is securely stored in the database, allowing the matching to occur in the transformed domain as long as the same transformation is consistently applied. This approach ensures that the template remains distinctive while incorporating a unidirectional transformation, preserving both security and matching performance. This allows for the generation of an unlimited number of cancelable templates from the same set of biometric attributes. Each time a transformed template is compromised, it can be canceled and replaced with a new transformed template, which explains the concept of revocation. This approach enhances flexibility and security by enabling the easy replacement of compromised templates without impacting the original biometric data. For example, a user could have an unlimited number of virtual fingerprints, each assigned to a specific application. This makes it extremely difficult to track an individual based on a compromised template. Cancelable biometrics utilize computationally simpler transformations compared to biometric encryption, eliminating the need for encryption and decryption phases during authentication.[34]

The international standard ISO/IEC24745 outlines the key requirements that a cancelable biometrics (CB) scheme must fulfill. Let z represent the biometric user, and $f(\cdot)$ denote the transformation function. Let K_z be the transformation parameters, where $f(b_z, K_z)$ represents the transformed template for user z. The original biometric template and query data are denoted by b_z and b'_z, respectively. Define D_O and D_T as the distance functions that measure the similarity between biometric features in the original and transformed domains, respectively. The cancelable biometric system determines a positive match if the distance between the template and the query data, as measured by D_O and D_T, is below a predefined threshold t. Following the approach outlined in [35] [36], we mathematically express these requirements on the transformation function f as follows:

1. **Diversity** : Multiple transformed templates derived from the same biometric attributes cannot be matched. In other words, distinct transformed templates should not be linked to one another or to the original template (cross-matching), as each transformed template uses different transformation parameters. This prevents cross-attacks between different biometric databases created using the same transformation function to secure different applications, i.e.,

$$D_T(f(b_z, K_z), b_z) > t \tag{3.1}$$

$$D_T(f(b_z, K_z^1), f(b_z, K_z^2)) > t \tag{3.2}$$

Figure 3.2 illustrates the diversity property:

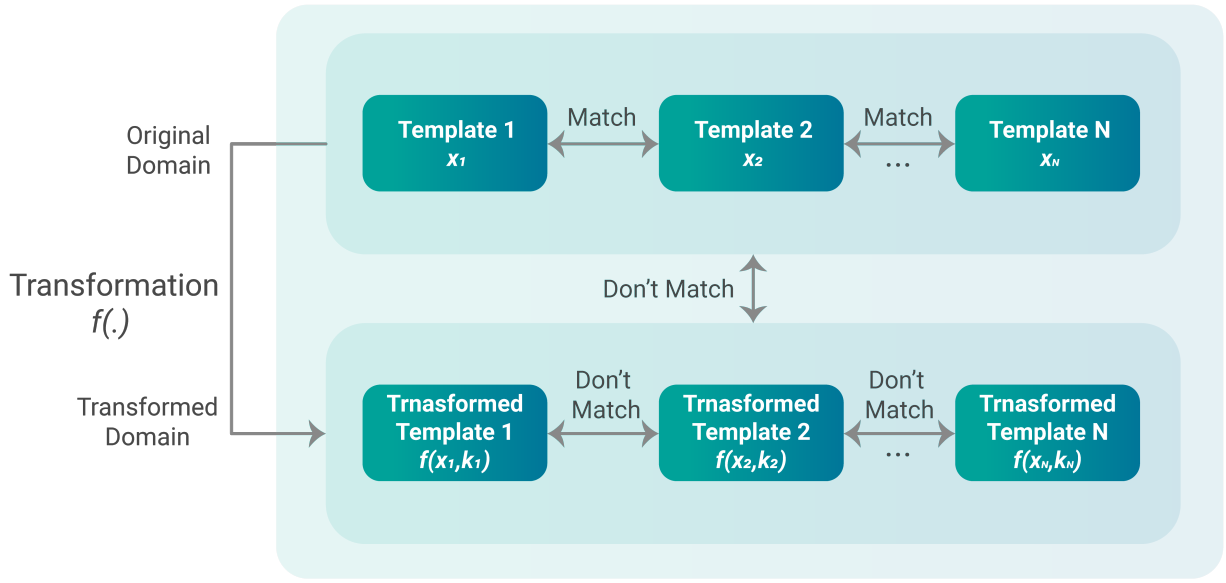


Figure 3.2: Multiple transformed templates derived from the same biometric data, each using different transformation parameters, are unmatchable and unlinkable. This ensures cross-matching prevention and enhances security across applications.

2. **Revocability (cancelability)** : If the stored transformed biometric template $f(b_z, K_z^1)$ is compromised or hacked, that template can be canceled, and a new template $f(b_z, K_z^2)$ can be generated using different user-specific transformation parameters. This feature enables the creation of a new pseudo-identity whenever needed, preventing the user from being traced, particularly in cases where a compromised template is detected. Figure 3.3 illustrates the revocability property.

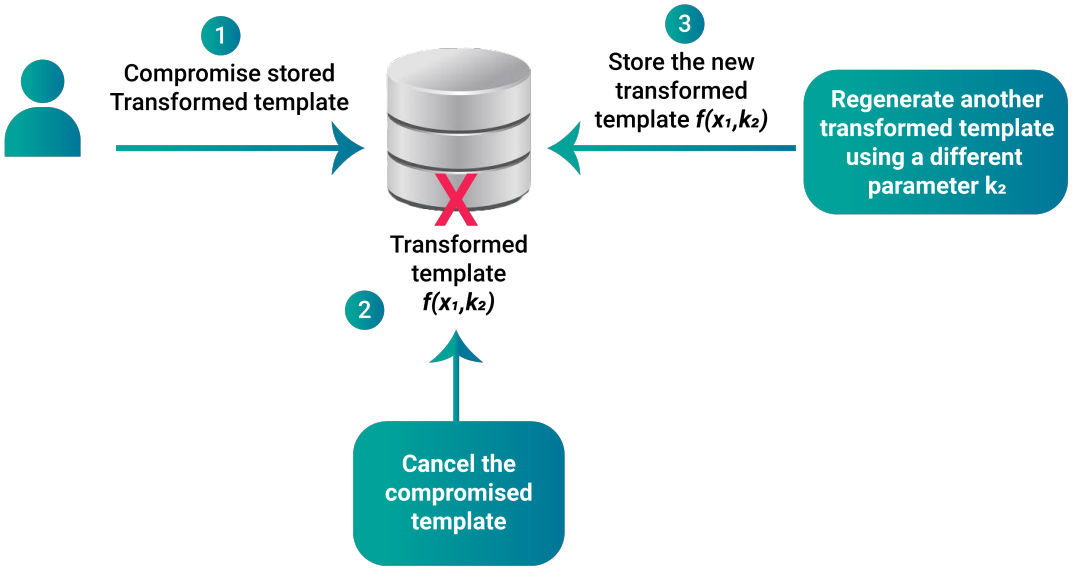


Figure 3.3: A compromised transformed template can be replaced with a new one using different transformation parameters, creating a fresh pseudo-identity and preventing traceability.

3. **Irreversibility** : This property ensures that even if an attacker obtains the transformed template $f(b_z, K_z)$, some transformation parameters K_i, or even the transformation function f, it remains impossible to recover the original biometric data b_z. This is because the transformation function is designed to be irreversible and the recovery process is too difficult to implement. This feature is crucial for preserving the privacy of the user's biometric data.

4. **Performance** : The implementation of a security system should not degrade identification accuracy. In other words, intra-user variability must be preserved in the transformed domain to prevent an increase in the False Reject Rate (FRR) when applying the transformation function.

$$D_O(b_z, b'_z) < t \Longrightarrow D_T(f(b_z, K_z), f(b'_z, K'_z)) < t \tag{3.3}$$

Additionally, inter-user variability must result in a negative match to prevent an increase in the False Accept Rate (FAR) within the transformed domain.

$$D_O(b_{z1}, b_{z2}) > t \Longrightarrow D_T(f(b_{z1}, K_{z1}), f(b_{z2}, K_{z2})) > t \tag{3.4}$$

3.2 Cancelable Biometric System Architecture

Additionally, inter-user variability must result in a negative match to prevent an increase in the False Accept Rate (FAR) within the transformed domain.

1. **Registration Stage** : In this stage, the user provides their biometric data (such as a fingerprint, face, or iris scan) through a sensor, camera, or other device. The raw biometric data is then processed through a feature extraction step, where the relevant biometric features are identified. Afterward, the extracted biometric data undergoes transformation using a conversion function, along with user-specific transformation parameters. This results in a transformed biometric template, which is securely stored in the system's database.

2. **Authentication Stage** : During authentication, the user provides their biometric data again through the sensor. The system extracts the biometric features from this query data, just as in the registration stage. The extracted query data is then transformed using the same conversion function and user-specific parameters. The transformed query data is compared with the stored template in the database. If the comparison falls within an acceptable threshold, the result is a positive match (authentication succeeds); if not, it results in a negative match (authentication fails).

Figure 3.4 shows the architecture of cancelable biometric system.

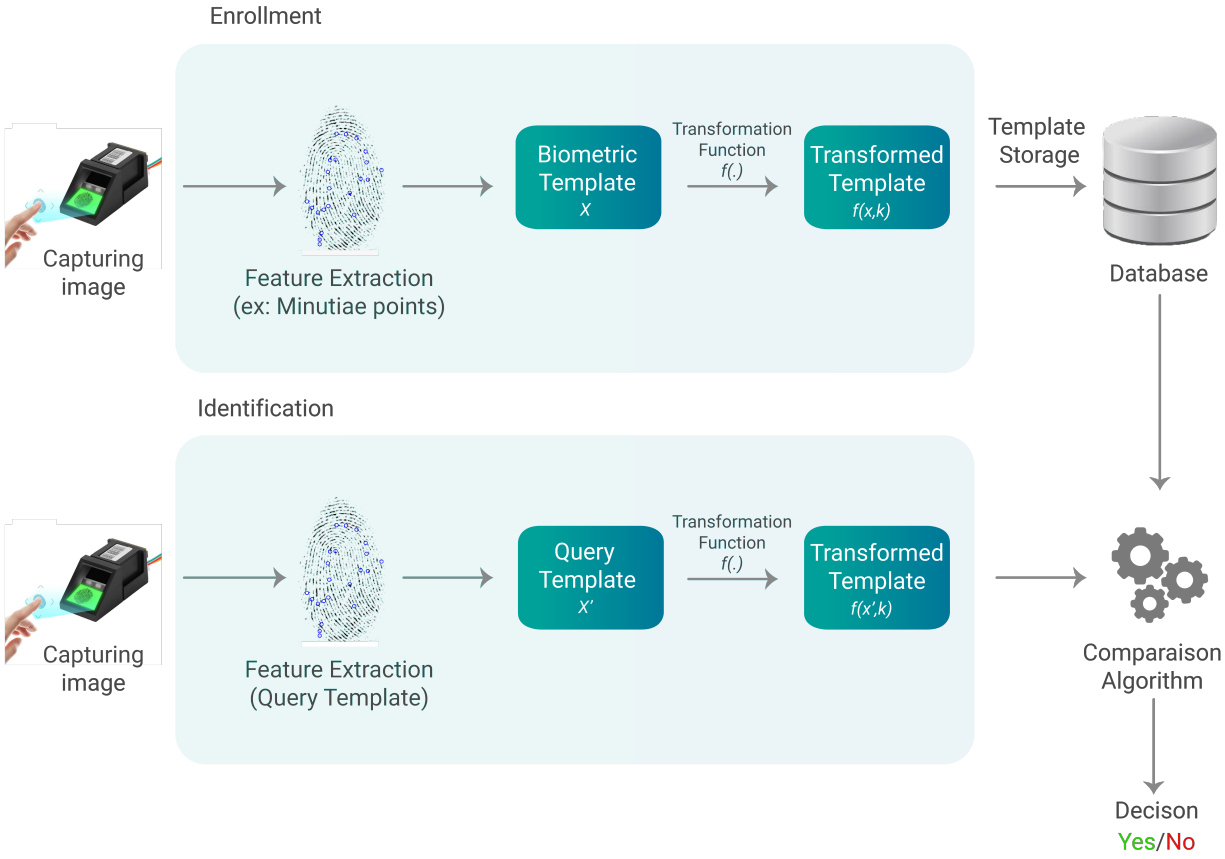


Figure 3.4: Architecture of a Cancelable Biometric System

3.3 Biometric Template Protection Methods

Biometric template protection (BTP) can be classified into various types[27] [6]. A detailed description of each type is provided below. Figure 3.5 illustrates a taxonomy of biometric template protection methods.

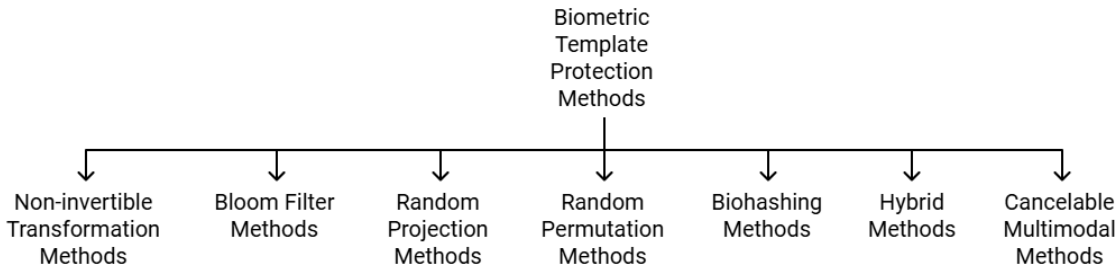


Figure 3.5: Taxonomy of biometric template protection (BTP) methods, illustrating the various classification types and approaches

3.3.1 Non-invertible transformation

Non-invertible transformation is one of the primary protection methods in cancelable biometrics [5] [27] [8] . A transformation function $f(\cdot)$ is applied, using the user's secret key K_z, to convert the original biometric template b_z into a transformed template $f(b_z, K_z)$, which is then stored in the database instead of the original template. The transformation function is mathematically irreversible (i.e., no inverse function f^{-1} exists) and should exhibit significant computational complexity to reinforce this irreversibility, ensuring that even if the transformed biometric template is compromised, the original template cannot be recovered. Since the transformation function operates independently of the raw biometric data, it does not need to be kept confidential. Instead, security is maintained through the non-invertibility of the function and the use of unique, user-specific keys, allowing the function itself to be publicly known without compromising the system's privacy and integrity [37].

The challenge lies in designing effective transformation functions that have significant computational complexity, making it difficult for a fraudster to reverse-engineer the original biometric templates. Numerous protection methods in cancelable biometrics are based on transformation functions, each employing its own unique approach to creating these functions. The complexity and security of the system depend heavily on how the transformation function is constructed. In this section, we will explain some non-invertible transformation approaches.

The key differences between transformation functions in arise from several factors:

1. **Input Data:** Different biometric modalities (e.g., fingerprints, face, iris) require varying types of biometric templates. For fingerprints, some transformations may operate on binary templates (like fingerprint images), while others specifically require minutiae-based templates.

2. **Transformation Method:** Each transformation function has its algorithm and design, determining how the biometric data is altered. Some methods apply geometric transformations, while others employ different approaches. A well designed transformation ensures that even if the transformed data is compromised, the original biometric cannot be recovered.

3. **Output Data:** The variation in output format is critical for ensuring interoperability and secure matching of biometric templates.

4. **Performance:** The effectiveness of a transformation function varies depending on factors like computational complexity, speed, and security. High-performance transformations minimize errors such as false matches or rejections while providing strong resistance against attacks, such as replay or template reconstruction.

Ratha et al. [8] suggested three methods of transformations : cartesian, polar and folding transformations. The Cartesian transformation divides the fingerprint area into a defined number of cells(grid of cells), using a core point as a reference. Each cell contains one or more minutiae points. The transformation function then randomly maps these cells to other randomly selected cells, allowing multiple cells to share the same cell number after the transformation (one-to-many). Mathematically, the Cartesian transformation involves multiplying the grid of cells by a transformation matrix, which is derived from the user's secret key.

In polar transformation, the fingerprint area is divided into sectors using a core point as a reference. Each minutia point is assigned to a specific sector, with each sector being numbered uniquely. A sector can contain one or more minutiae points. The transformation process

involves randomly reassigning the sectors to new positions, while the angles of the minutiae points are adjusted based on the new sector positions.

In functional transformation, minutiae positions are altered using a transformation function, with its parameters defined by either mixed Gaussian distributions or randomly distributed electric charges. The direction of translation is governed by the phase ϕ, while the extent of translation is determined by the magnitude $|\vec{F}|$ or by another function $\phi(a, b)$ as follows:

$$|\vec{F}| = \left| \sum_{i=1}^{J} \frac{q_i(w - w_i)}{|w - w_i|^3} \right| \tag{3.5}$$

$$\phi(a, b) = \frac{1}{2} \arg \left(\sum_{i=1}^{J} \frac{q_i(w - w_i)}{|w - w_i|^3} \right) \tag{3.6}$$

Here, $w = a + ib$ represents the position vector, and $J = [q_1, q_2, \ldots, q_j, w_1, w_2, \ldots, w_j]$ comprises random keys that define both the magnitude and the position of the electric charge. The transformation is described as follows:

$$A' = a + J|\vec{G}(a, b)| + J\cos(\phi_F(a, b)) \tag{3.7}$$

$$B' = b + J|\vec{G}(a, b)| + J\sin(\phi_F(a, b)) \tag{3.8}$$

$$\theta' = \mathrm{mod}(\theta + \phi_G(a, b) + \phi_{\mathrm{rand}}, 2\pi) \tag{3.9}$$

Ratha et al. [8] argued that the folding transformation outperforms the other two methods in terms of effectiveness. Furthermore, the authors of [8] claimed that recovering the original template from the transformed one is highly challenging.

Ahmad et al. [38] suggested a non-invertible transformation based on pair polar coordinates of fingerprint templates. The first step operates by selecting a subset of minutiae points from the initial set in a fingerprint that are sufficiently spaced apart. These points are then randomly mapped to different sectors, following the same principle as the polar transformation method developed by Ratha et al. [8] The main difference between these methods lies in the additional stage of selecting points. To further process the spatial relationship between these minutiae, the distance between minutiae points can be calculated as follows: suppose m_i and m_j are two minutiae points, and we want to determine the distance between them. The information extracted from the relationship between these minutiae is represented as a vector $V_ij = (D, \alpha_1, \alpha_2)$, where D is the distance between the two points, α_1 is the angle between minutia m_i and the link connecting m_i and m_j, and α_2 is the angle between minutia m_j and the link between two the two minutiae. Figure 3.6 illustrates the distance between two points.The polar space is divided into sectors based on the reference point, where each sector may contain one or more minutiae points. The transformation consists of two basic steps: sector transformation, where each sector is mapped to a new sector, and radial distance transformation, where each vector in the polar coordinate space is transformed into a new vector $V_ij' = (D', \alpha_1', \alpha_2')$.

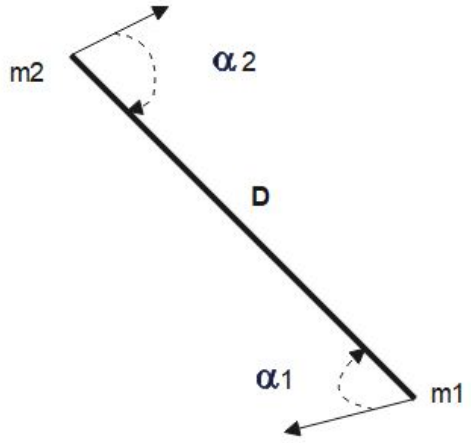


Figure 3.6: The distance calculation between minutiae points.

Wang et al. [39] proposed a densely infinite to one mapping (DITOM), This approach relies on a transformation function that applies quantization to minutiae points, generating an infinite number of possible transformed minutiae configurations. This ensures the function's irreversibility by concealing the original fingerprint template among countless potential solutions, thereby preventing its recovery. According to the same distance calculation method as Ahmad's approach [38], Wang et al.'s method is based on a similar principle, where the distance between each pair of minutiae m_i and m_j in the fingerprint is represented as $V_ij = (D, \alpha_1, \alpha_2)$. To avoid repetition, the symmetric pair V_{ji} will not be considered. The vector V_{ji} is quantized, where $N = N_D + N_{\alpha_1} + N_{\alpha_2}$, and then converted into a binary vector representation B. The binary vector B is then transformed using a discrete Fourier transform.

Lee et al. [40] developed a non-invertible transformation that is free of alignment. This approach involves altering both the direction and position of each minutia point in the fingerprint template. It employs two distinct transformation functions: the first modifies the positions of the minutiae, while the second adjusts their orientations. As a result, the transformed template consists of minutiae points with randomized positions and directions.

Yang et al. [41] proposed a non-invertible transformation that projects each pair of minutiae onto a circle along a direction perpendicular to the line connecting the minutiae. Their transformation approach is based on using local and global features, where the local features include distances and angles between minutiae points, and the global features incorporate ridge frequency and orientations. The irreversibility of this approach is ensured by the fact that multiple pairs of minutiae can be mapped to the same point on the circle, thereby obscuring the original minutiae configuration.

Ferrara et al. [42] proposed a two-factor protected minutia cylinder-code to secure the original fingerprint, utilizing the Minutia Cylinder Code (MCC) proposed by Cappelli et al [43] and the Protected Minutiae Cylinder Code (PMCC) [42]. This method integrates a two-factor security mechanism to enhance protection by transforming the minutiae data. The PMCC approach was claimed to preserve cylinder distance in the transformed domain, even though the original information is not present in the protected template. However, despite this advantage, the PMCC approach is not revocable, meaning that the biometric data cannot be reset or updated if compromised. This limitation led to the suggestion of an alternative two-factor protection method.

Ouda et al [44] proposed a cancelable biometric scheme known as bio-encoding. In this method, a vector of consistent bits is extracted from the original iris code. The protected biocode is then generated by randomly mapping these consistent bits to various bit sets within a pseudorandom sequence S. Specifically, each bit in the consistent bit vector is mapped to a single bit value in the pseudorandom sequence, with the position of each bit corresponding to the value of that bit in the vector. This BioEncoding approach is based on a single-factor design, where biometric encoding is individually based on the iris code.

Zhao et al. [45] developed a cancelable biometric (CB) scheme that utilizes local ranking to secure iris data, producing a template consisting of local rank values. The binary iris values are converted to decimal values by application-specific random strings. The protection process begins by XORing the iris data with an application-specific string. The resulting data is then divided into blocks, each represented by its corresponding decimal value. These blocks are further grouped and ranked based on their decimal values. Ultimately, the transformed template is composed of the rank values obtained through this process.

Ragendhu et al. [46] proposed a novel cancelable biometric scheme designed to address the shortcomings of existing methods. This approach employs patch-level distortion using Voronoi patches, where images are divided into these patches based on a rotation- and scale-invariant seed point generation solution. The feature vectors from each patch are then concatenated to distort the log-Gabor feature vector, enhancing security by eliminating the need for a user-specific key—a critical vulnerability in other techniques. The method also ensures irreversibility through randomization and distortion mechanisms.

Siddhad et al. [47] applied convolutional autoencoders and random noise to extract key features from palm vein, palmprint and wrist images and compress them into a latent space representation.To create cancelable templates from these features, they introduced random noise and utilized random convolution techniques. The features are extracted using CAEs, then subsequently salted and convolved with a random 7×7 kernel generated from a uniform distribution [48].

3.3.2 Bloom filter methods

A Cancelable Biometric Filter is a method uses convolution techniques to irreversibly transform biometric data, ensuring privacy and security. One such method involves the use of Bloom Filters, which are space-efficient, probabilistic data structures designed to represent sets and efficiently support membership queries (i.e., determining whether an element is part of a set). When applied to biometric data, such as a binary feature vector, the Bloom filter transforms it into a format that is irreversible, meaning that the original data cannot be reconstructed from the transformed output. A Bloom filter consists of a set of n bits, initially set to zero. Hash values h is then calculated, producing a set of positions in the bit array where 1 are placed instead of 0. The bit value 1 may be set in the same position multiple times by different hash functions. To verify the presence of an element A in the Bloom filter, all bit positions produced by the hash functions $h(A)$must be set to 1. Figure 3.7 illustrates the Bloom filter method.

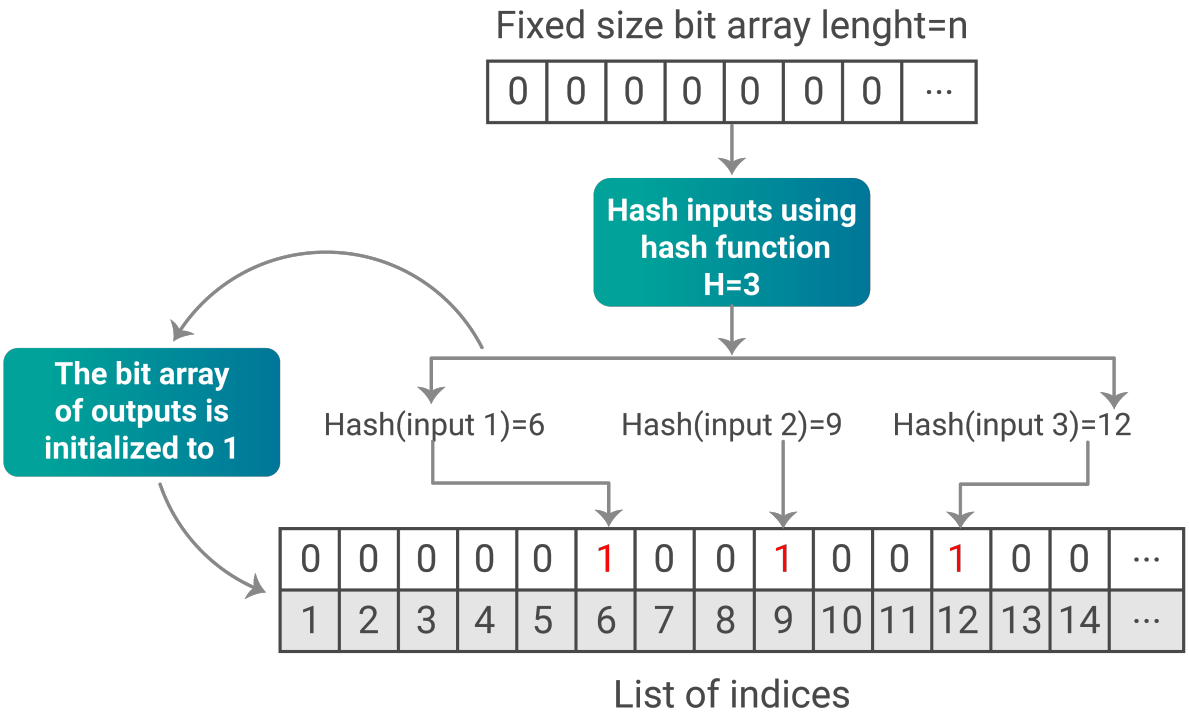


Figure 3.7: Overview of bloom filter approach.

Rathgeb et al. [49] developed a method to secure iris templates using a Bloom filter. The binary iris code is partitioned into K equally sized blocks, where each block generates a "codeword" consisting of W bits. A Bloom filter b of length 2^W is initially set to all zeros. The transformation is then applied by performing an XOR operation with a user-specific key, which alters certain bits in the Bloom filter, setting them to 1. In this approach, the Bloom filter aims to compress biometric data and reduce computational time while maintaining recognition performance.

3.3.3 Random Projections

Random projections are a commonly used technique in cancelable biometrics. In this approach, the biometric data $\mathbf{x}$, which belongs to $\mathbb{R}^N$, is projected onto a randomly generated subspace $\mathbf{K}$, where $\mathbf{K}$ belongs to $\mathbb{R}^{N\times n}$ with $n < N$. Each entry a_{ij} of $\mathbf{K}$ is an independent realization of a random variable. This process transforms the biometric data into a new space, making it difficult to reconstruct the original biometric information, thereby ensuring privacy and security. The process can be outlined as follows:

$$Y = xK \tag{3.10}$$

where Y represents the random projection vector in n dimensions. ***Ngo et al.*** [50] proposed a bio-hashing scheme based on random projections. In this approach, the extracted feature vector $\mathbf{x}$ is projected onto a pseudo-random matrix $\mathbf{M}$ to generate a bio-hash vector $\mathbf{z} = \mathbf{xM}$. This random projection is then followed by a quantization process, which converts the resulting vector into a binary feature vector $\mathbf{b} \in \{0, 1\}$. This random projection is then followed by a quantization process, which converts the resulting vector z into a binary feature vector $\mathbf{b} \in$

$\{0, 1\}$ according to a predefined threshold τ, where $b_i = 0$ if $z < d$ and $b_i = 1$ if $z > d$, for $i = 1, 2, \ldots, n$. Then, the binary vector $\mathbf{b}$ is stored in the database as a protected template.

Jin et al. [51] suggested a cancelable biometric (CB) scheme to secure facial biometric templates using a ranking-based locality-sensitive hashing method called Index of Max Hashing (IoM). A biometric feature vector $\mathbf{x} \in \mathbb{R}^N$ is multiplied by a set of Gaussian random matrices $\mathbf{R}_l \in \mathbb{R}^{N \times K}$ to produce the random projected vector $\mathbf{z}_l = \mathbf{R}_l \mathbf{x}$, where $l = 1, \ldots, L$, K represents the subspace dimension. The entries of the matrix $\mathbf{R}_l$ are drawn from a standard Gaussian distribution $N(0, 1)$. The hash code h_l is then derived from the index of the maximum value in the projected vector.

In [52], a random projection-based method for cancelable iris recognition was introduced by ***pillai et al***. Direct application of random projections to entire iris images tends to degrade performance. This occurs because different regions of the iris have varying quality, and real iris images, even with accurate segmentation, often contain outliers from specular reflections, eyelashes, and eyelids. A linear transformation applied to the whole vector mixes high-quality regions with these outliers, corrupting the data. To mitigate this, [52] proposes sectored random projections, where each sector of the iris undergoes random projections separately. The resulting transformed vectors are then concatenated to create a cancelable template, ensuring that outliers only affect their respective sectors rather than the entire iris vector.

To protect the stored face template, ***Dong et al.*** [53] developed a Non-linear multi-dimensional spectral hashing (NMDSH) technique. First, the Eigen functions $\Theta_{ij}(x_i)$ and their corresponding Eigen values λ_{ij} are calculated and sorted in ascending order. The top K indices are selected to form the set $A = \{(i_1, j_1), (i_2, j_2), \ldots, (i_3, j_3)\}$. Each data point x is then encoded using $y_{ij}(x) = \sin(\Theta_{ij}(x))$ for all $(i, j) \in A$. The final output, y, is determined by applying the softmod function $q(\Theta_{ij}(x))$, defined as:

$$q(x) = \frac{2}{1 + e^{-8 \sin(\pi x)}} - 1 \tag{3.11}$$

and α is the nonlinear rate to be determined empirically. The technique maintains recognition performance while achieving other essential properties of cancelable biometrics.

3.3.4 Random Permutations

Random switching is a technique used in cancelable biometrics, where biometric features are randomly altered to generate the cancelable template. ***Lai et al.*** [54] proposed a cancelable biometric scheme based on iris permutation, where the biometric features (X) are permuted using P randomly generated permutation vectors to create a permuted iris code (X'). The Hadamard product code is then generated by multiplying all the permuted iris codes, as detailed below:

$$X^p = \prod_{i=1}^{P} (X'_l) \tag{3.12}$$

Next, the first k elements of each row of the Hadamard product code are selected, and the value corresponding to the first binary bit 1 is recorded as C_x. Lastly, for every $C_x > k - \tau$, the output is conducted $C'_x = C_x \mod (K - \tau)$, and this procedure is recurrent by using m different permutation sets to generate an $n \times m$ protected template as follows: $\{C'_{xi} \in \mathbb{Z}^n, i = 1, \ldots, m\}$.

In [55], ***Jinyuan et al.*** proposed a secure template generation scheme for face recognition employing a chaotic system. They begin by eliminating internal correlations within the face

feature vector through permutation. The vector is then transformed using an orthogonal matrix, ensuring that distances are preserved. Finally, templates are generated by calculating the cosine values between random vectors and the transformed feature vector.

3.3.5 Biohashing Methods

BioHashing is a technique used in cancelable biometrics to enhance the security and privacy of biometric data. ***Rathgeb et al***[49] proposed a biohashing method, where the biometric features are extracted from the input data vector $\mathbf{x}$, which resides in $\mathbb{R}^N$. The process involves generating a user-specific token along with orthogonal pseudo-random vectors $\mathbf{v}_i \in \mathbb{R}^N$ for $i = 1, \ldots, N$. The inner product between the biometric feature vector and the user-specific token is calculated, resulting in a transformed vector. This transformed vector, combined with the pseudo-random vectors, helps create a secure BioHash code. This approach ensures that the biometric data is obfuscated, making it difficult to reverse-engineer the original features. The BioHashing process can be mathematically expressed by the equation :

$$c = Sign(\Sigma x^T v_i - \tau) \tag{3.13}$$

Sign represents the signum function, and τ denotes a threshold determined through experimentation. The BioHashing framework offers a high degree of security by serving as a one-way transformation for biometric data and mitigating the impact of external factors. This robustness is achieved through a detailed statistical analysis of the framework, which evaluates the effectiveness of random multispace quantization operations. Such an analysis confirms that BioHashing effectively obscures biometric features, ensuring secure and resilient data protection. Figure 3.8 illustrates the bioHashing method

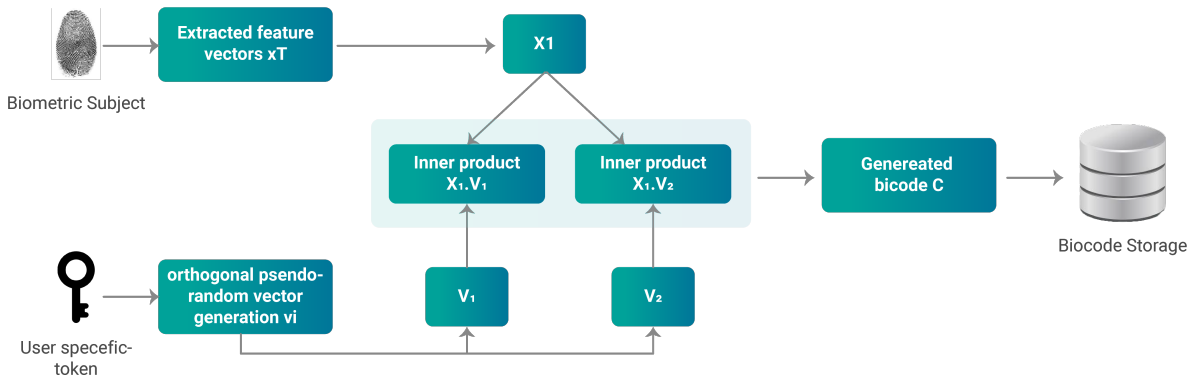


Figure 3.8: Overview of Biohashing method

3.3.6 Hybrid Methods

Hybrid methods combine two or more techniques to create cancelable biometric templates, often integrating cancelable biometrics with encryption. The use of such hybrid systems aims to enhance security levels compared to other protection methods, preserve system performance, and mitigate vulnerabilities associated with the stored template. For instance, ***Boult et al.*** [56] proposed a hybrid biometric system designed to protect facial data, introducing the concept

of the "biocode." This biocode is defined as "a revocable identity code generated by applying a revocable transformation to biometric data, such that identity matching is performed in the encrypted/revocable form" [56][57]. Additionally, ***Wong et al.*** [58] proposed another hybrid method, called Cancelable Secure Sketch (CaSS), which integrates Multi Line Code (MLC) with Secure Sketch (SS). The MLC process involves five stages: (i) extraction of fine details, (ii) generation of the Multi Line Code (MLC), (iii) random projection, (iv) Kernel Principal Component Analysis (KPCA), and (v) denoising. The SS method combines the bit string generated by MLC (obtained from the deduplication step) with a random code word selected from code books such as Reed-Solomon (RS) and BCH (Bose-Chaudhuri-Hocquenghem) codes. Figure 3.9 illustrates an example of a hybrid method:

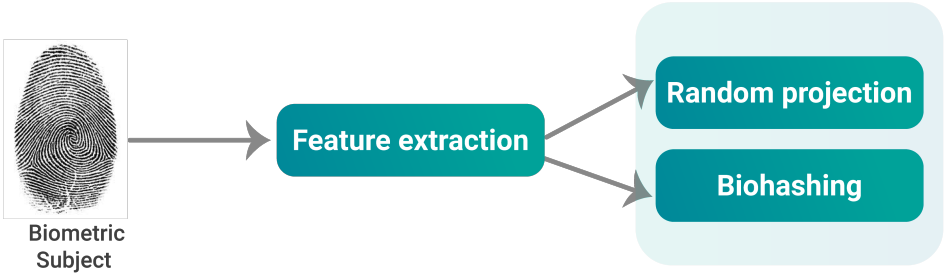


Figure 3.9: Overview of a hybrid methods in biometric template protection algorithms.

3.3.7 Cancelable Multimodal Methods

Unimodal biometric systems face several challenges, including intraclass variability, variations in data quality, and similarities between interclass samples. To address these issues, multimodal biometrics combine multiple biometric traits using various feature extraction approaches to create more secure templates. This approach enhances security and accuracy by integrating different types of biometric data, such as iris, face, and fingerprint information from the same individual, for identity recognition. By leveraging multiple biometric traits, multimodal systems overcome the limitations of unimodal systems and provide a more robust solution for identity verification. Numerous methods for multimodal biometrics have been proposed in the literature. These include techniques such as cross-fold random indexes [59], rank-level fusion [60], and real-time situational awareness [61]. Other notable methods are feature fusion [59], bit extraction [62], random distance [63], and biometric credential systems [64]. Each of these approaches addresses different aspects of multimodal biometrics to enhance accuracy and security.

In Table 3.1, we provide a summary of the reviewed CB schemes, highlighting the modality used, the adopted security approach, and the method employed for ensuring irreversibility.

CB protection scheme	Modality	Approach adopted	Irreversibility
Functional transformation [8]	Fingerprint	Non-invertible transformation	Many to one mapping
Transformation based perpendicularly projection [41]	Fingerprint	Non-invertible transformation	Many to one mapping
Polar transformation [38]	Fingerprint	Non-invertible transformation	Many to one mapping
Transformation based on local minutiae information [40]	Fingerprint	Non-invertible transformation	Unknown Invariant value based
DITOM [39]	Fingerprint	Non-invertible transformation	Infinite to one mapping
Bio-hashing [65] ,[66] ,[50]	Face, Fingerprint, Face	Random projection	Random projection
Bloom filter [49]	Iris	Projection on bloom filter	Many to one mapping
Index of Max Hashing (IoM) [66]	Face	Ranking based hashing	Many random projection
Indexing-First-One Hashing (IFO) [54]	Iris	Ranking based hashing	Many random projection
Non-linear multi-dimensional spectral hashing (NMDSH) [53]	Face	Random projection	Non-invertible randomized graph based hamming embedding
Two-factor protected minutia cylinder-code [67]	Fingerprint	Permutation	User-unique permutation
Bioencoding [44]	Iris	Non-invertible transformation	Many to one mapping
Local ranking cancelable biometrics (LRCB) [45]	Iris	Local ranking based transform	Many to one transform
Alignment-free fingerprint hashing algorithm based on minimum distance graphs [68]	Fingerprint	Non-invertible transformation	Many to one transform
Irreversible and Revocable Template Generation Scheme Based on Chaotic System [55]	Face	Local sensitive hashing	Many to one transform
Cancelable biometric scheme based on dynamic salting of random patches [46]	Face	patch-level distortion with random noise derived from difference vectors	non-invertible randomized based on random noise from difference vectors
Cancelable Biometric Template Generation Using Convolutional Autoencoder[47]	palmprint, palmvein, wristvei	Non-invertible transformation	Random noise and random convolution

Table 3.1: Summary of multiple CB systems

3.4 Conclusion

Cancelable biometrics are regarded as a solution to address the challenges and vulnerabilities associated with traditional biometric systems, securing stored biometric templates against theft, fraud, and other risks that may violate an individual's privacy. In our discussion, we explored the various types of cancelable biometric methods presented in the literature. Despite the differences in their structure and the construction of protection schemes, all of these approaches share a common goal: to secure biometric data and safeguard individuals' privacy. This is achieved by storing a transformed version of the template, rather than the original, thereby

preventing breaches or theft of the original biometric data. One of the key features of this approach is that the original biometric template cannot be recovered from the transformed template, ensuring security and mitigating the risk of hacking the original data. Additionally, this method allows for the cancellation and regeneration of biometric templates, due to the use of an individual's secret key. By simply replacing the secret key with a new one, a new transformed template can be generated whenever needed, further enhancing security and flexibility.

In this chapter, we introduced the concept of cancelable biometrics, outlining its key characteristics, and explaining the Cancelable Biometric System Architecture. We then provided a detailed overview of the various types of cancelable biometrics, highlighting numerous schemes proposed by researchers for each category. Despite the numerous advantages of cancelable biometrics, are they truly sufficient to protect an individual's data? Can we confidently assert that cancelable biometrics are resistant to all types of attacks? Is it genuinely impossible for an attacker to compromise the original template or reverse the transformation function? Or could an attacker, armed with knowledge of certain transformation tools such as the transformed template, the transformation function, or even the secret key potentially reconstruct the original template? We will investigate this in the next chapter.

Chapter 4

Attacks Against Cancelable Biometrics

4.1 Introduction

Cancelable biometrics have emerged as a leading solution to address the limitations of traditional biometric systems, offering enhanced security and flexibility. By allowing biometric templates to be transformed and replaced without compromising the original data, cancelable biometrics significantly improve both security and accuracy. Numerous methods in the literature focus on cancelable biometrics, aiming to create templates that are revocable, irreversible, and untraceable, which are stored in databases instead of the individual's original biometric data. While these approaches offer significant advantages, further investigation is required, as several studies have highlighted vulnerabilities, proving that many CB schemes are susceptible to attacks. Consequently, it is crucial to identify and classify these attacks to strengthen security measures and enhance the overall protection of cancelable biometric systems.

Highlighting the various attacks and vulnerabilities identified in the literature is essential, as they pose significant security risks and provide attackers with opportunities to breach protection systems. This serves as a wake-up call for the research community focused on securing cancelable biometric templates, especially since some of these methods are proposed to secure sensitive applications, as noted in [69], drawing attention to these weaknesses and raising awareness to mitigate the impact of severe attacks. Classifying attacks and identifying their various vulnerabilities is crucial for several reasons:

- **Limited focus on attack types** : The number of documented attacks against cancelable biometrics in the literature is relatively small compared to protection methods. As a result, the research community often focuses on the most prominent attacks, such as ARM and spoofing attacks..., while potentially overlooking others. This underscores the importance of clearly defining different attack types, as understanding the full spectrum of attacks is essential for developing effective defense systems.

- **Difficulty in building protection systems:** Without a deep understanding of the attack details and how they are executed, it becomes challenging to design robust systems that can effectively prevent these attacks. A well-defined classification of attack methods is necessary to anticipate and mitigate security risks.

- **Misconception of cancelable biometrics as an ideal solution:** There is a misconception that cancelable biometrics provide an ideal solution for enhancing both security and privacy. This can lead to a degree of complacency, where protection systems are not subjected to rigorous evaluations, making them vulnerable to attacks.

- **Balance between security and accuracy:** One of the key challenges in biometric protection systems is the trade-off between security and accuracy. Many methods that have been compromised prioritize security accuracy at the expense of security, leading to inadequate defenses against attacks. Achieving a balance that ensures both high accuracy and robust security remains a complex challenge.

Addressing these details is crucial for enhancing security and privacy. Ignoring them exposes individuals and organizations to significant risks, including data breaches and cyberattacks. The loss of personal data can be irreversible, leaving individuals vulnerable, while organizations may face severe financial consequences, such as compensation costs, regulatory fines, and the need to invest in new security measures. Furthermore, they may be subject to legal action from affected individuals and suffer long-term damage to their reputation, which can be even more costly than the immediate financial impact.

In this chapter, we classify the various types of attacks targeting cancelable biometrics and examine the vulnerabilities within certain protection schemes that raise significant security concerns, allowing attackers to compromise the system. Additionally, we provide a comparative analysis of multiple attacks on cancelable biometric systems, considering several key factors. Building on this analysis, we propose a rigorous framework for evaluating protection schemes and mitigating these attacks. By identifying weaknesses and assessing their potential impacts, we aim to encourage further research and innovation to strengthen the security of cancelable biometric systems.

4.2 Proposed Classification of Attack Strategies on Cancelable Biometric Systems

Attacks on cancelable biometric systems can be broadly categorized into presentation and software-based attacks. Presentation attacks involve using counterfeit or fabricated materials to deceive the biometric authentication sensor, tricking the system into recognizing the fake input as genuine and granting unauthorized access to the attacker. In contrast, software-based attacks require more sophisticated tools and expertise, including hacking or penetration testing skills, to exploit vulnerabilities within the biometric authentication system. In this section, we will focus primarily on software-based attacks. We have further classified attacks on cancelable biometrics into three distinct categories, which will be discussed in the following subsections. A comprehensive review of each category will be provided, outlining the specific threats and vulnerabilities associated with these attacks. Figure 4.1 illustrates our developed taxonomy for the complete classification of these attack types.

4.2.1 Reversibility attacks

A reversibility attack against cancelable biometric methods aims to undo the transformation applied to a user's biometric template to recover the original data. Cancelable biometrics employ transformation functions to alter the original biometric data into a secure, non-reversible template to protect user privacy. However, in a reversibility attack, an attacker attempts to reverse-engineer or bypass this transformation, allowing them to reconstruct part or all of the original biometric template. The danger of such an attack is significant because if an attacker can recover the original biometric data, they could impersonate the legitimate user or compromise the integrity of the biometric system. This type of attack undermines the core

purpose of cancelable biometrics, which is to provide a revocable, secure template that cannot be easily traced back to the original biometric data. A reversibility attack is executed by leveraging the appropriate skills and insights to reverse the transformation function, targeting the specific vulnerabilities inherent in each protection algorithm. Based on this approach, we can classify the methods of reversibility attacks as follows:

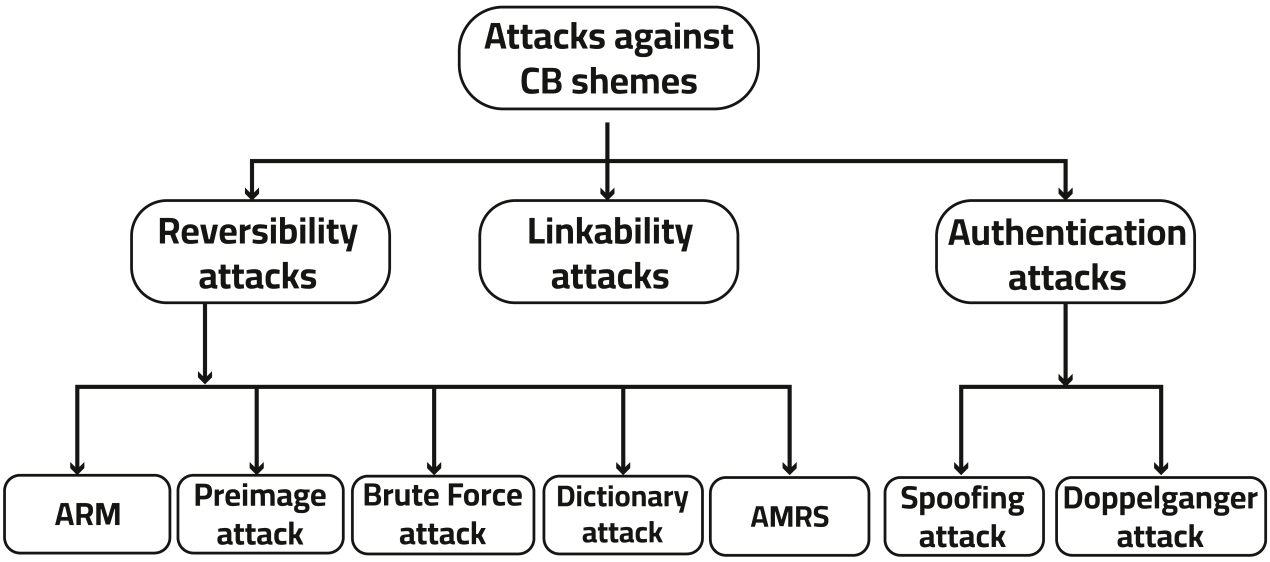


Figure 4.1: Proposed taxonomy of various attacks against CB.

4.2.1.1 Dictionary attack :

In this type of attack, the attacker compiles a set of biometric templates that are most likely to match the target's protected template. The attacker then submits these high-probability templates to the decision-making unit, hoping to achieve a successful match. This type of attack leverages pre-selected or generated templates to increase the chances of bypassing the authentication system.

While the folding transformation method proposed by Ratha et al. [8] is an effective approach to safeguard an individual's biometric data, a study by Shin et al. [70] highlights its vulnerability. Their research demonstrates that the original template can be reconstructed using two transformed templates derived from the same source. They showed that if an attacker gains access to a transformed template and its transformation key, T, they could launch a dictionary attack. By simulating the transformation, the attacker can generate a set of possible pre-images for each minutia, ultimately forming $A_1 ... A_n$ groups and compromising the security of the system. Each group includes all possible sources of pre-images for the original minutiae. The fewer pre-images an attacker has to deal with, the easier it becomes to identify the original minutiae. If the attacker can obtain two or more transformed templates from the same original template, along with their transformation keys, they can use the Cartesian product $(A_1 \times \cdots \times A_n)$ or the union $(A_1 \cup A_2 \cup \cdots \cup A_n)$ of the candidate pre-image sets. By selecting the intersections between these sets, the attacker can narrow down the possible pre-images.

4.2.1.2 Attacks via record multiplicity (ARM)

Many cancelable biometric (CB) schemes are vulnerable to the attack known as Attack via Record Multiplicity (ARM). In this attack, an adversary generates multiple transformed tem-

plates, $T(X_1, K_1), T(X_2, K_1), \ldots, T(X_n, K_1)$, from the same biometric data X using the same transformation parameter K_1. By analyzing the correlations between these transformed templates, the attacker can potentially reconstructs the original biometric template. Figure 4.2 illustrates the ARM attack.

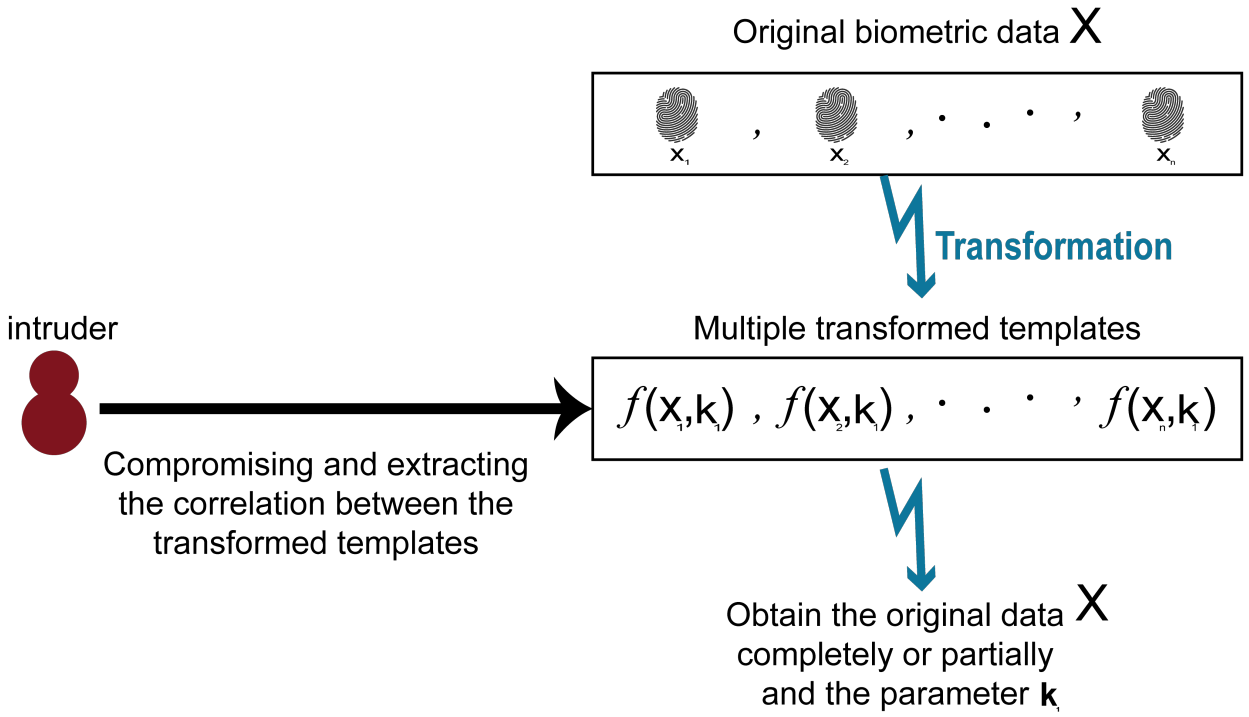


Figure 4.2: Attack via record multiplicity principle illustrated in fingerprint system. X_i are multiple real impressions related to a same user finger. $f(X_i)$ are their respective transformed templates. Once the intruder gain these last ones, he can launch the attack.

Although Yang's method [41] is considered an effective scheme for protecting biometric data, it was successfully attacked by Li et al. [71] using ARM. In this case, the attacker can retrieve the original template by obtaining two or more transformed versions (circles) with the same raduis r and identifying the correlations between them. By matching corresponding transformed minutiae (represented by circles) in both templates and finding the correct intersection points, the original minutiae can be recovered. Therefore, this CB scheme is not resistant to ARM.

The non-invertible approach proposed by Ahmad et al. [38] is vulnerable to Attack via Record Multiplicity (ARM) as demonstrated by Li et al. [71]. In this attack, if an adversary obtains multiple transformed templates and the transformation parameters, he can reconstruct the original template by recovering the sectors and coordinates (such as radial distances) of the original template. The primary weakness lies in the sector transformation process, where the angles remain unchanged before and after transformation. This consistency simplifies the recovery of sectors, allowing the attacker to retrieve the minutiae in the original sectors by comparing the angles across the transformed templates. Once the sectors are identified, the attacker can further reconstruct the original distances between the center point and the minutiae by using the distance-related parameters and recalculating the new radial distances.

The cancelable scheme proposed by Wang et al. [39] was compromised by Li et al. [71] through the ARM attack. Despite the real solution being obscured among an infinite set of possibilities, their attack successfully recovered the original template. Their attack relies on

collecting numerous transformed matrices and templates to construct a linear equation system, the solution of which facilitates the recovery of the original template.

Lee et al.'s protection scheme [40] claims that it is challenging for an attacker to recover the original user's template even if a single transformed version is obtained, as the recovery of the original data relies on an invariant feature of the user's fingerprint image. However, this protection approach is vulnerable to the ARM attack [71]. If an attacker can acquire multiple transformed templates along with the user's PINs, they can potentially reconstruct the original template. By analyzing the correlations between the transformed templates, the attacker can narrow down the invariant value to a very small range or even isolate a single invariant value if a sufficient number of transformed templates are available.

In 2008, Quan et al. [72] launched an ARM attack on the folding transformation proposed by Ratha et al. [8], drawing parallels to the ARM attack previously introduced by Scheirer and Boult [73]. Scheirer and Boult demonstrated that by analyzing multiple encodings of the same biometric template, an attacker could exploit correlations between them to retrieve the original template and the associated secret. This method had been effectively used to compromise fuzzy vault systems, where the original minutiae set is mixed with chaff points. By matching two vaults, they could isolate the original minutiae points projected onto the polynomial, while chaff points are discarded. Similarly, Quan et al. proposed that using a single transformed template allows an attacker to extract multiple solutions, some of which are the original minutiae and others chaff points. With an additional transformed template, they could refine these solutions, ultimately reconstructing the correct minutiae points by filtering out chaff points. Ratha's protection scheme [8] is similarly vulnerable, as the original minutiae can be inverted and recovered. This scheme's many-to-one property enables an attacker to match the correct minutiae points across multiple transformed templates, thereby reconstructing the original template from among the chaff points.

Ouda et al.[74] evaluated the non-invertibility of the bioencoding algorithm [44] by launching three attacks: brute force, optimization, and ARM. Their analysis demonstrated that while the biometric encryption scheme is resilient against brute force and optimization attacks, it remains vulnerable to ARM attacks. They argued that each bit in the biocode could originate from 2^{m-1} possibilities; thus, if an attacker can access K biocodes, the number of possibilities can be reduced from 2^{m-1} to 2^{m-K}. The optimal case for retrieving the original template occurs when $m = K$. To strengthen the bioencoding algorithm against ARM attacks, this study proposes multiple enhancements. Additionally, Ouda et al. [74] demonstrated that negative iris recognition [75] is susceptible to ARM attacks, showing that a substantial portion of the original iris code can be reconstructed if an attacker gains access to several negative databases.

4.2.1.3 Solving equations

This type of attack works by constructing a system of equations, the solution of which enables the recovery of the original template. One prominent example is the attack on the folding transformation proposed by Ratha et al. [8], in which a flaw was identified by Quan et al. in [72]. The issue is that the transformation of minutiae points is limited to small, reversible areas. Specifically, while the folding process occurs in a localized region, most areas only experience distortion rather than true transformation. Consequently, by solving nonlinear equations, an attacker can recover the original minutiae points for most transformed points, even with access to just a single transformed template.

4.2.1.4 Brute force attack

A brute force attack systematically sifts through all possibilities to determine the original biometric data. In this context, the attacker attempts to reverse-engineer the transformation by exhaustively searching through the transformed template space until they identify a template that matches the original biometric attributes. This attack is computationally intensive and relies on the ability to generate or test multiple transformed versions, aiming to bypass the irreversibility and security measures designed to protect the original biometric information in cancelable biometric systems.

Quan et al. [72] demonstrated that a brute force attack can be launched on a limited range of transformations using only a single transformed template. In this approach, the attacker does not need to precisely recover the exact positions of the original minutiae points; an approximate restoration is sufficient to produce a matchable result. This approximation increases the feasibility of a brute force attack, as even a rough alignment can compromise the security of the transformation.

4.2.1.5 Similarity based attack(pre-image attack/masquerade attack)

The pre-image attack is among the most prevalent and effective methods used against cancelable biometrics. In this attack, the adversary reconstructs an approximate version of the original biometric data, allowing them to perform matching within the transformed domain without needing the exact original biometric template. According to the definition by Dong et al.[76]. This type of attack is primarily motivated by the distance-preserving property of many transformations. In these cases, the distance between two biometric templates x_1 and x_2 of the same biometric data X remains largely unchanged after transformation. Consequently, the transformed features y_1 and y_2 in the resulting set $Y = f(X)$ retains the same distance. This property is attained as follows: $\|d - \bar{ds}\| < \epsilon, \exists \epsilon > 0$. Where $d = \|x_1 - x_2\|$ and $ds = \|y_1 - y_2\|$. Thus, the pre-image attack leverages this vulnerability and is defined as: $\hat{x} = argmin[d(f(\hat{x}), f(x)]$. Where, x is the original template, $\hat{x}$ is the pre-image of x, $f(.)$ the transformation function used to project $\hat{x}$ on the transformed space and $d(.)$ is the Euclidian or hamming distance between two feature Sets.

Dong et al.[53] performed a pre-image attack using genetic algorithm(GASAF) on Transformation Systems Bloom-filter [49] and Bio-hashing [65], leveraging the distance-preserving property between templates. In these models, it is assumed that the attacker has access to the transformation function, its parameters, and the transformed template. This knowledge enables the attacker to approximate the original template based on an initial estimation of the transformed template. The genetic algorithm enhances this approximation by iteratively creating new generations, guided by a fitness function that minimizes the distance between the approximated and transformed templates. Through this process, the genetic algorithm progressively reconstructs a close an approximation of the original biometric template.

Nanawat et al.[77] developed a Particle Swarm Optimization (PSO) algorithm, a metaheuristic approach designed for executing pre-image attacks. They applied this technique to both Transformation Systems Bloom-filter [49] and Bio-hashing [65]. The PSO algorithm effectively generated approximation of the transformed template, enabling good attack performance. In a comparative analysis with a genetic algorithm-based attack, they found that the genetic algorithm outperformed PSO in the case of Bio-hashing, whereas PSO demonstrated superior performance over the genetic algorithm for the Bloom-filter model.

Wang et al. [78] introduced a constrained optimization similarity-based attack (CSA) aimed at enhancing Dong's protection scheme [79] . By leveraging a genetic algorithm, CSA employs inequality constraints to optimize the generation of pre-images from a supervised perspective. This attack specifically targets IOM hashing [51] and Bio-hashing [65], exploiting the similarity-preserving property of cancelable biometrics. Additionally, the performance of CSA has been demonstrated to surpass that of dong's method (GASAF) [79], highlighting its effectiveness in compromising these biometric protection schemes.

The application of genetic algorithms in this domain has proven to be highly effective. This study therefore contributes to the ongoing analysis of vulnerabilities and security concerns within the scope of cancelable biometrics. In 2013, Lacharme et al. proposed an attack on the Bio-hash algorithm [66], which remains one of the most prominent protection schemes. This scheme transforms a finger code into a biocode using a random seed. Lacharme et al.[80] utilized a pre-image attack based on a genetic algorithm, demonstrating that if both the biocode and its associated random seed are accessible to an attacker, the Bio-hash algorithm can be reversed. This allows the attacker to reconstruct an approximate biometric template that closely resembles the original, exposing a significant risk in the security of this scheme.

Lee et al. [81] demonstrated in 2009 that the biohashing approach [66] is vulnerable to pre-image attacks. They proved that an attacker can reconstruct a pre-image of the original biocode by using only the lost biocode, without requiring access to the genuine private random vector. This is achieved through the use of a pseudo-inverse matrix, exposing a significant weakness in the biohashing method.

In another study, Dong et al [76] conducted a pre-image attack on six security algorithms: bloom-filter [49], Index of Max Hadhing (IoM)[51],Indexing-First-One hashing [54],spectral hashing [53], biohashing [65], two-factor protected minutiae cylinder code (2PMCC) [67] using a genetic algorithm. They highlighted the significant risks posed by pre-image attacks, particularly information leakage resulting from the distance-preserving property, which creates a challenging trade-off between accuracy and security. They also theoretically demonstrated that an attacker's ability to access multiple transformed templates increases the volume of leaked information that can be exploited in the attack. Furthermore, the study introduced the concept of a cross-transformation attack, a more complex variant of the pre-image attack. In this scenario, different systems may utilize varying transformation functions, significantly raising security risks compared to a single transformation attack. This underscores the heightened vulnerability of systems employing diverse transformations within cancelable biometric frameworks.

In 2020, two Index-of-Max (IoM) hashing protection schemes Gaussian Random Projection IoM (GRP-IoM) and Uniformly Random Permutation IoM (URP-IoM) [51] were subjected to pre-image attacks by Ghammam et al [82]. It was demonstrated that both schemes are vulnerable to authentication and reversal attacks. An optimization algorithm, incorporating inequality constraints, was employed to construct a pre-image of the IoM hash codes, thereby enabling unauthorized access to the biometric system. This approach underscores the security risks inherent in these CB schemes, revealing how easily an attacker can breach the system by exploiting its vulnerabilities.

Additionally, a pre-image attack was executed on the Biohashing system [65] by leveraging perceptron and neural network learning [83]. The researchers demonstrated that it is feasible to generate a synthetic face image from the binary template and stolen code, effectively compromising the user's identity. This attack unfolds in two scenarios. In the first scenario, where the attacker knows the binary algorithm, binary parameters are estimated using perceptron learning to create a synthetic template with real-valued features. Hill-climbing techniques are

then applied to reconstruct the face image. In the second scenario, where the attacker lacks knowledge of the binary algorithm, a Multilayer Perceptron (MLP) is utilized to model the binary matching process. Hill climbing is subsequently employed to recover the face image from the real-valued synthetic template.

In their study, Nagar et al. [36] revealed significant vulnerabilities within the Biohashing scheme [66], showing that it is susceptible to hacking. They conducted a thorough security assessment of the scheme, utilizing various metrics to evaluate its resilience. Moreover, they demonstrated that an attacker could feasibly approximate the original biometric template by inverting the transformed template a process framed as an optimization problem.

Researchers in [84] developed optimization-based attacks targeting Bio-hashing [50] and introduced four distinct approaches for predicting biometric data, including biometric feature vectors and images. These attacks operate under the assumption that both the user's secret key and the Bio-hash vector have been compromised. The first two attack scenarios utilize one-bit compressed sensing techniques, employing linear programming and binary iterative hard thresholding to address the reversibility of Bio-hashing. To further enhance the approximation of feature vectors, they incorporated minimum norm solutions. Additionally, Topcu et al. proposed a Rainbow attack, which differs from the previous methods in its objective. Instead of merely reconstructing feature vectors, the Rainbow attack aims to identify a biometric image that, when hashed with the compromised key, produces a Bio-hash vector matchable to the original. This innovative approach underscores the versatility of their optimization-based attacks and highlights potential vulnerabilities in Bio-hashing schemes.

Rozsa et al. [85] conducted a pre-image attack on three fingerprint authentication schemes using a genetic algorithm. This approach employs the genetic algorithm to generate fingerprint minutiae templates that achieve a high degree of matching. The study also analyzes the security and privacy of these protected schemes, revealing that the MCC scheme [43] exhibits significant weaknesses in both privacy and security. In contrast, while the PMCC [42] and basic Biotope schemes [86], [57] maintain privacy, they compromise security. Notably, the two-part Biotope scheme effectively preserves both security and privacy. The findings of this attack demonstrate that even if an attacker manages to achieve a high matching degree, they cannot recover the original details of the fingerprint template.

Ouda et al. [87] explored the irreversibility property of the LRCB scheme [45], revealing significant vulnerabilities. They demonstrated that an attacker could recover a close approximation of the original iris code, achieving 95% accuracy by reversing the rank values. Additionally, if an attacker knows the transformation function and its corresponding parameters, they can easily manipulate the distribution of rank statistics as discrete random variables. The close approximations obtained through this inversion attack are sufficient to facilitate authentication attacks, allowing unauthorized access to the biometric system. Furthermore, an attacker can employ an ARM if they acquire multiple transformed templates of the same biometric features. By reversing these templates, they can obtain close approximations, extracting repeated bits from identical positions across different reversed templates to reconstruct a code that closely matches the original biometric features. This process underscores the critical security risks associated with the scheme's irreversibility property.

Lacharme et al. [88] examined the irreversibility of the bio-encoding scheme developed by Ouda et al. [44]. They asserted that if the Boolean function used to generate the random sequences is compromised, it becomes possible to reconstruct pre-images of the bio-code, thus undermining the scheme's irreversibility property.

Ouda et al. [74] recently investigated the non-invertibility of negative iris recognition [75].

They demonstrated that an attacker could recover the original template by having access to just one protected template, which would then enable them to launch a pre-image attack using the retrieved code to perform authentication. This highlights the vulnerabilities associated with both the bio-encoding and negative iris recognition schemes.

4.2.1.6 Attack via missed record synchronization(AMRS)

This type of attack is regarded as a variation of ARM. In both cases, the attacker must extract information from multiple transformed templates of the same biometric feature. However, unlike the ARM attack, where the focus is on leveraging shared information across templates, this variation exploits the lack of shared information between the templates. This distinction allows the attacker to capitalize on discrepancies across transformed templates, making the system more susceptible to compromise.

Belhadj et al. [89], evaluated the effectiveness of transformation-based cancelable fingerprint algorithms and investigated their vulnerabilities [68]. They introduced an attack, known as AMRS, targeting the transformation algorithm by exploiting a key weakness: the improper synchronization of fingerprint points across multiple templates. Typically, fingerprint matching algorithms attempt to identify positive matches for points between templates of the same person. However, each incorrect match can lead to information leakage, ultimately enabling the recovery of the original minutiae. The AMRS attack involves classifying fingerprint points across multiple templates, then consolidating each class to a single representative minutiae point. By combining these elements, they formed a system of equations, the solution of which enables the reconstruction of the original fingerprint minutiae.

4.2.2 Authentication attacks(intrusion attacks)

An authentication attack occurs when an adversary submits falsified cancelable biometric data to deceive the biometric authentication system, causing it to incorrectly recognize an unauthorized individual as an authorized user. Broadly, these attacks can be classified into two types: spoofing and Doppelganger attacks, which will be discussed in the following subsections.

4.2.2.1 Spoofing attack

In this type of attack, the adversary leverages knowledge of the transformation algorithm, the user-specific key, or both to compromise an individual's biometric data. By exploiting these elements, he can create a falsified sample that the system authenticates as legitimate. This attack targets weaknesses within the transformation process or vulnerabilities in the biometric data capture, allowing the attacker to fabricate synthetic biometric samples that match the cancelable template associated with an authorized user. For instance, a spoofing attack [90] was launched against a transformation algorithm based on homomorphic encryption [91]. This attack specifically targets binary feature vectors, utilizing an unpredictable vector that maintains the same Euclidean distance with all binary vectors. This feature enables accurate matching between the input vector and the captured biometric information, thereby undermining the security of the system.

4.2.2.2 Doppelganger attack

The nature of transformation algorithms can sometimes result in transformed templates that share similar information across different users. This overlap occurs because the transformation function may lack unique differentiation for each individual. Consequently, an attacker may gain access to near-matches from multiple users. In large databases, the likelihood of encountering such doppelganger templates rises due to the sheer volume of data. Durbet et al. [92] recently introduced various authentication attacks targeting projection-based CB schemes, including the biohash algorithm [66]. Their approach allows an attacker to make slight modifications to their fingerprint to impersonate other individuals if they have access to protected fingerprint templates and corresponding passwords of legitimate users. They employed integer linear programming (ILP) and quadratically constrained quadratic programming (QCQP) to formulate this attack as a constrained optimization problem, highlighting the vulnerabilities in these systems.

4.2.3 Linkability attacks

One of the most crucial features of cancelable biometric transformation methods is non-linkability. This characteristic ensures that a person's biometric data cannot be used to track or identify them across multiple applications, thereby safeguarding their privacy. However, various attacks have been devised to undermine this feature. In these attacks, adversaries attempt to analyze and correlate biometric features to determine if they originate from the same individual. If successful, such attacks can establish links between applications, leading to the exposure of the original user's identity and potentially compromising their privacy.

A well-known attack targeting this property is the Ghammam attack [82], which demonstrated that both Gaussian Random Projection-IoM (GRP-IoM) and Uniformly Random Permutation-IoM (URP-IoM) based on Index-of Max Hashing [51] are vulnerable to correlation attacks. The attack showed that, despite using different transformation parameters, it is possible to detect when vectors x_1 and x_2 are derived from the same biometric features X. The attackers accomplished this by generating a pre-image for each biometric feature and then comparing the number of indices where the transformed vectors share the same sign. The experimental results revealed a significant susceptibility to these attacks, with a 97% success rate for GRP-IoM and an 83% success rate for URP-IoM in correctly linking features back to the same biometric source.

Recently, Ouda et al. [87] launched a correlation attack on the (LRCB) scheme [45]. Although the developers of this protection method assert that their scheme is resilient against correlation attacks, claiming that templates generated from the same biometric features are indistinguishable, Ouda et al.'s findings challenge this robustness. According to the LRCB developers, the transformation parameters are designed to make templates appear sufficiently distinct, thereby preventing an attacker from determining if two templates originate from the same individual. However, the attack involved generating two pre-images, X_1 and X_2 , from the transformed templates and calculating the Hamming distance between them. If the Hamming distance falls below a pre-defined threshold, it indicates that the two templates are indeed derived from the same user. This approach effectively bypassed the intended security of the LRCB scheme, suggesting that the transformation parameters may not fully prevent linkability as claimed.

Hermans et al. [93] introduced a linkability attack specifically targeting the Bloom filter-based cancelable biometric (CB) scheme [94],[49]. Their research revealed that the iris biometric template protection system developed by Rathgeb et al. does not adequately achieve unlinkability.

By exploiting the reuse of the same hash function within the Bloom filters, they demonstrated a 96% probability of accurately determining whether two Bloom filters were derived from the same biometric data. This finding highlights a critical vulnerability, indicating that the reliance on a consistent hash function can lead to the unintended linking of protected biometric templates, thus compromising user privacy.

Ouda et al. [74] argued that the negative iris recognition technique [75] is vulnerable to linkability attacks, where an attacker can identify that two protected templates originate from the same original biometric data. This vulnerability raises concerns about the privacy protection of the scheme, as it challenges the goal of untraceable biometrics a feature that BioEncoding aims to achieve by not requiring user-specific keys or tokens while maintaining robust security against such attacks.

Table 4.1 summarizes several attacks against CB schemes that enable an attacker to crack the original template easily.

The primary objective of any attack, as previously discussed, is to obtain a biometric template that allows the attacker to perform matching and compromise the original biometric data. However, it is important to note that attackers do not necessarily need to acquire the complete true template. In particular, in attacks such as ARM, brute force attacks, dictionary attacks, and equation-solving techniques, the attacker can derive a biometric model X that facilitates the cracking of the original template. In contrast, a pre-image attack enables the retrieval of an approximation of the original template X' , allowing the attacker to perform matching within the transformed domain.

These attacks exploit vulnerabilities in biometric systems by focusing on the transformation process that generates the biometric template, rather than the template itself. As a result, even an approximate or derived model can provide sufficient information for an attacker to bypass security measures and gain unauthorized access to sensitive information. The procedure of the attack is depicted in Figure 4.3.

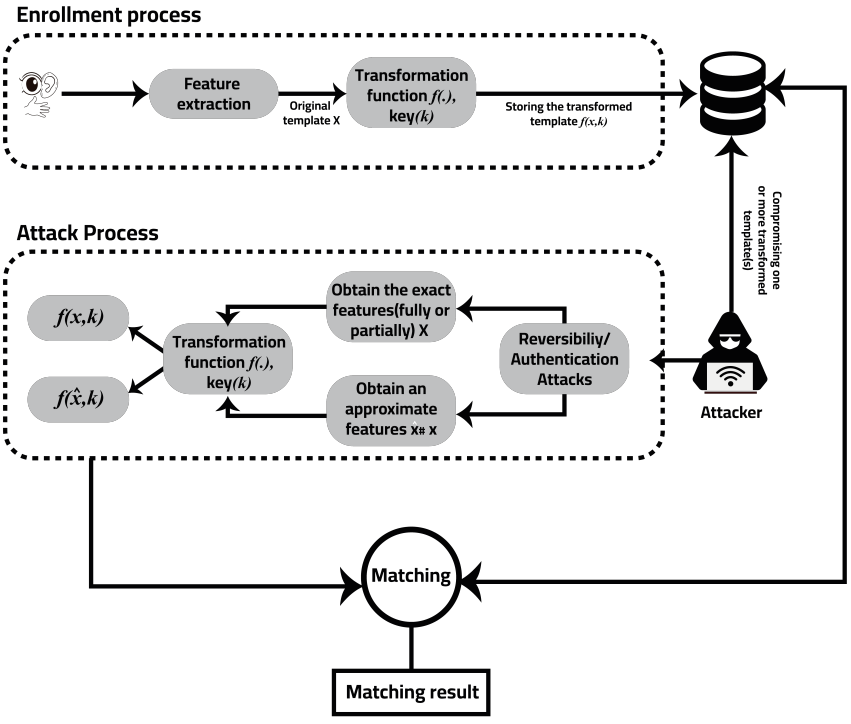


Figure 4.3: Illustration of attack procedure in CB system.

Furthermore, we can classify the attacks based on the number of transformed templates required to successfully execute the attack. In certain types of attacks, the attacker only needs a single transformed template to compromise the cancelable biometric system and gain access to the original biometric features. This indicates a vulnerability in the system that can be exploited with minimal effort. Conversely, other attacks may necessitate the acquisition of multiple protected templates to effectively breach the security measures in place. Figure 4.4 illustrates the classification of various attacks, providing a visual representation of the varying complexities involved in different attack strategies.

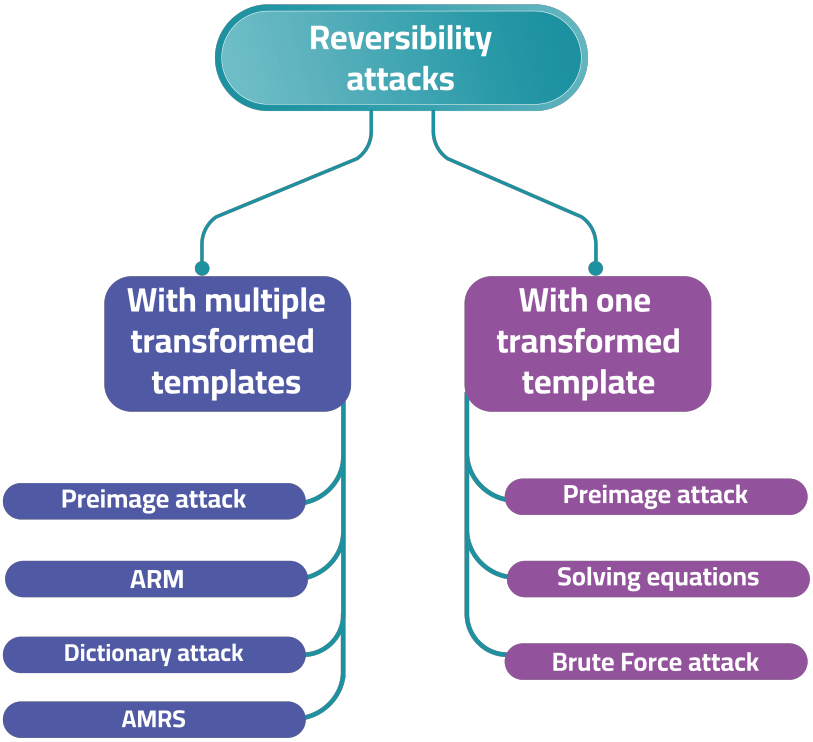


Figure 4.4: A block diagram explains the number of transform templates needed to lunch the reversibility attack.

4.3 Comparative study of various attacks

In this section, we present a thorough comparison of various biometric attacks found in the literature, aiming to assess their effectiveness and underscore the necessity for robust mitigation strategies to safeguard biometric data and uphold individual privacy. This analysis provides deeper insight into the vulnerabilities inherent in protection systems, facilitating the development of more secure biometric solutions. By systematically examining the weaknesses exploited by these attacks, researchers can better understand the critical steps required to reinforce biometric systems against emerging threats. Furthermore, we identify high-performing attacks that have successfully breached biometric defenses with minimal effort, exposing sensitive data and compromising user privacy. To ensure a rigorous evaluation, we adopted several key criteria: the type of attack, the targeted attack scheme, the success rate (SR) which is a crucial metric indicating an attack's efficacy in bypassing security, the Equal Error Rate (EER), time cost, and the attack method. These metrics serve as the foundation for the comparative analysis.

In addition to evaluating the effectiveness of these attacks, we assess them in terms of their advantages and disadvantages, offering a clearer introduction to the research community. This

Attack's type	Attack	References	Database	Target scheme	Vulnerability
Reversibility attacks	ARM	Attack on folding transformation [72]	–	Folding transformation of Ratha et al. [8]	The original minutiae can be easily retrieved by matching two transformed templates.
Reversibility attacks	Solving equations	Attack on folding transformation[72]	FVC2002 DB1	Folding transformation of Ratha et al. [8]	Due to the small ranges of non-linear properties, it is possible to solve the non-linear equations and recover the original minutiae solutions.
Reversibility attacks	Brute Force Attack	Attack on folding transformation [72]	–	Folding transformation of Ratha et al. [8]	Due to the small range of possible values, an attacker can try all possibilities to find the original minutiae.
Reversibility attacks	ARM	ARM against four CB schemes	–	Transformation based on local minutiae information [40]	Ease of retrieving the invariant value by solving a set of non-linear equations, which result from combining multiple transformed templates.
Reversibility attacks	ARM	ARM against four CB schemes	–	DITOM [39]	The possibility of extracting linear equations from the combination of the transformed templates and their corresponding transformation matrices.
Reversibility attacks	ARM	ARM against four CB schemes	–	Polar transformation of Ahmed [38]	Preservation of angles' measures after transformation. Ease of retrieval of the original distances by combining the new distances and distance-related parameters.
Reversibility attacks	ARM	ARM against four CB schemes	–	Transformation based on perpendicular projection [41]	The presence of original minutiae on the same side as the transformed ones within different circles, or their alignment on the same line as the original minutiae, facilitates finding points of intersection.

Reversibility attacks	ARM	Analysis of the security of the bio-encoding protection scheme [74]	CASIA-IrisV3-Interval	Bio-encoding protection scheme [44]	Bits in different bio-codes are addressed by the same value.
Reversibility, authentication, and linkability attacks	Similarity Attack	Attacks on Local Ranking-Based Cancelable Iris Recognition [87]	CASIA-IrisV3-Interval	LRCB protection scheme [45]	Vulnerability to similarity preservation property.
Reversibility, authentication, and linkability attacks	ARM	Attacks on Local Ranking-Based Cancelable Iris Recognition [87]	CASIA-IrisV3-Interval	LRCB protection scheme [45]	Repetition of K bits across multiple pre-images of the original template.
Reversibility, authentication, and linkability attacks	Correlation attack	Attacks on Local Ranking-Based Cancelable Iris Recognition [87]	CASIA-IrisV3-Interval	LRCB protection scheme[66]	Correlation among multiple protected iris codes can reveal that they originate from the same biometric data.
Reversibility attack	Dictionary attack	Dictionary attack on folding transformation [70]	FVC2002 DB1	Folding transformation of Ratha et al. [8]	An attacker can simulate all possible minutiae pre-images and attempt those that may succeed.
Reversibility and authentication attacks	Similarity Attack	Preimage attack using genetic algorithm [79]	CASIA-IrisV4-Interval	Bloomfilter [49]	Vulnerable to similarity preservation property.
Reversibility and authentication attacks	Similarity Attack	Preimage attack using genetic algorithm [79]	LFW	Biohashing [65]	Vulnerable to similarity preservation property.
Reversibility and authentication attacks	Similarity Attack	Preimage attack using PSO [77]	CASIA-IrisV4-Interval	Bloom filter [49]	Vulnerable to similarity preservation property.
Reversibility and authentication attacks	Similarity Attack	Preimage attack using PSO [77]	LFW	Biohashing [65]	Vulnerable to similarity preservation property.

Reversibility and authentication attacks	Similarity Attack	Analysis of the security of six CB schemes [76]	FVC2002 DB2	2PMCC [67]	Vulnerable to similarity preservation property.
Reversibility and authentication attacks	Similarity Attack	Analysis of the security of six CB schemes [76]	CASIA-IrisV4-Interval	IFO [54], Bloom filter [49]	Vulnerable to similarity preservation property.
Reversibility and authentication attacks	Similarity Attack	Analysis of the security of six CB schemes [76]	LFW	Biohashing [65], IoM, Biohashing [51], NMDSH [53]	Vulnerable to similarity preservation property.
Reversibility and authentication attacks	Similarity Attack	Pre-image attack on Bio-Hashing using GA [80]	FVC2002 DB3	Biohashing [65]	Vulnerable to similarity preservation property.
Authentication attacks	Similarity Attack	A constrained optimization similarity-based attack [78]	LFW	Biohashing algorithm [65], IoM hashing [51]	Vulnerable to similarity preservation property.
Reversibility, authentication, and linkability attacks	Similarity Attack	Cryptanalysis of URP-IoM and GRP-IoM [82]	FVC2002 DB1	IoM-hashing [51]	Vulnerable to similarity preservation property.
Reversibility, authentication, and linkability attacks	Similarity Attack	Intrusion and linkage attack [36]	FERET	Biohashing [66]	Vulnerable to similarity preservation property.
Authentication attack	Similarity Attack	Attack on protected template fingerprint systems using genetic algorithm [85]	FVC2006 DB2	MCC [43], BPMCC [42], Biotope [86], [73]	Vulnerable to similarity preservation property.
Reversibility, authentication, and linkability attacks	Similarity Attack	Attacks against biometric hashing using sparse recovery [82]	BioSecureds2 face database [95]	Biohashing [50]	Vulnerable to similarity preservation property.
Authentication attacks	Spoofing attack	Spoofing attack [90]		Homomorphic encryption algorithm [91]	Distance constancy of all binary vectors.

Reversibility and authentication attacks	Similarity Attack	Authentication attacks on projection-based CB schemes [92]		Biohashing [66]	Vulnerable to similarity preservation property.
Linkability attack	Correlation attack	Security analysis approach on Bloom filter [93]		Bloom filter [49]	Due to the use of the same hash function in multiple transformations.
Reversibility attack	Similarity Attack	Attack against bio-encoding scheme [88]		Bio-encoding protection scheme [44]	Due to the knowledge of the Boolean function, an attacker can construct an iris code that produces the same biocode.
Reversibility and Linkability attacks	Similarity Attack	Analysis of the security of negative iris recognition [74]	CASIA IrisV3 Interval	Negative iris recognition scheme [75]	Vulnerable to similarity preservation property.
Reversibility and Linkability attacks	ARM	Analysis of the security of negative iris recognition [74]	CASIA IrisV3 Interval	Negative iris recognition scheme [75]	A repetition code of K bits in multiple preimages of the original template.
Reversibility and Linkability attacks	Correlation attack	Analysis of the security of negative iris recognition [74]	CASIA IrisV3 Interval	Negative iris recognition scheme [75]	Multiple p-hidden-NDBs can be correlated jointly, resulting in the discovery that they are generated from the same biometric data.
Reversibility attack	AMRS	Attack via missed record synchronization on transformation-based fingerprint template protection algorithms [89]	FVC2002, FVC2004, FVC2006	DAS' algorithm [68]	Vulnerable to missed synchronization of information.

Table 4.1: Summary on several attacks on cancelable biometric systems

approach contributes to enhancing the security of biometric systems by highlighting areas that demand attention.

A concise summary of this comparison is presented in Table 4.2, while Table 4.3 delves into a detailed analysis of each attack's advantages and disadvantages. This comprehensive evaluation not only sheds light on the diverse range of attacks but also provides an in-depth understanding of the most prominent threats currently discussed in the literature. Moreover, it underscores the pressing need for continuous advancements in biometric security to stay ahead of evolving attack strategies.

4.3.1 Evaluation of the Comparative Analysis

The comparative study provides a structured and multi-dimensional assessment of the most prominent threats targeting cancelable biometric systems. By organizing the attacks based on vulnerability points, performance metrics (such as EER, SAR, and time cost), and their respective advantages and disadvantages, the study facilitates a comprehensive understanding of each attack's impact.

Notably, attacks such as ARM, AMRS and similarity-based attacks consistently demonstrate high success rates with minimal computational effort, revealing critical weaknesses in the design of many protection schemes. The evaluation shows that certain transformation-based systems are more susceptible due to weak irreversibility or reusability of transformation parameters. Moreover, the analysis highlights the lack of robustness in systems that rely on static or poorly diversified keys, which makes them prone to linkability and reversibility attacks. The use of detailed criteria in the evaluation tables enhances the comparability of different approaches and pinpoints the trade-off between security and performance. Overall, this multi-faceted evaluation not only guides the selection of resilient protection techniques but also emphasizes the urgent need for adaptive and strongly diversified transformation functions in future system designs.

4.4 Databases used in attacks against cancelable biometric schemes

A wide range of databases has been developed by researchers to facilitate experiments on cancelable biometrics and evaluate the effectiveness of various attack strategies. These databases play a critical role in validating experimental results and providing insights into the vulnerabilities that attackers may exploit. By using diverse datasets, researchers can simulate real-world scenarios, enabling them to test the robustness of cancelable biometric systems against different types of attacks. In this section, we review the primary databases employed in studies of cancelable biometrics, as summarized in Table 4.4. This review highlights the specific datasets that have proven useful for assessing attack methodologies and helps to identify patterns that could inform the development of more secure biometric systems.

4.5 Evaluation framework

Cancelable biometrics generally offer a promising approach to safeguarding individuals' data and privacy. However, their effectiveness cannot be fully assured due to numerous documented

Study	Attack	Target scheme	Success Rate	EER	Time cost	Modality
Dong et al.[79]	Similarity attack using genetic algorithm (GASAF)	Biohashing ($l = 500$), Bloom filter ($w = 8, l = 2^6$)	FAR@ET= 85.54% FAR@ET= 38.03%	14.07% 5.259%	30 min (1500 generations)	face iris
Nanwate et al.[77]	Similarity attack using Particle swarm optimization (PSO)	Biohashing($l = 500$)	FAR@ET= 97.025%	5.29%	100 generations	Face
		Bloom filer ($w = 8, l = 26$)	FAR@ET= 11.05 %	14.07%	2000 generations.	Iris
Wang et al.[78]	Similarity attack based constrained optimization (CSA)	IoM-Hashing($K = 16l = 512$)	SAR= 99.19%	0.60%	3661.63 s (5 generations)	Face
		Biohashing($l = 512$) ($K = 16, l = 512$)	SAR=34.43%	0.63%		Face
Wang et al.[78]	Similarity attack using genetic algorithm (GASA)	IoM-Hashing ($K = 16, l = 512$)	SAR= 64.12%	0.60%	97.84 s (94 generations)	Face
		Biohashing($l = 512$)	SAR= 34.43%	0.63%		Face
Ghammam et al.[82]	Authentication attack	GRP-IoM URP-IoM	100%			Fingerprint
	Linkability attack	GRP-IoM	97%			Fingerprint
		URP-IoM	83%			Fingerprint
	Reversibility attack	GRP-IoM				Fingerprint
Lee et al.[81]	Similarity attack using pseudo inverse-matrix	Biohashing				Fingerprint
Belhadj et al. [89]	AMRS	Das (FVC2002 DB1)	SAR=70.4		16.99s	Fingerprint

		Das(FVC2002 DB2)	SAR=69.8		19.694s	Fingerprint
		Das(FVC2002 DB3)	SAR=95		15.207s	Fingerprint
		Das(FVC2004 DB1)	SAR=87		15.841s	Fingerprint
		Das(FVC2002 DB3)	SAR=95		15.207s	Fingerprint
		Das(FVC2004 DB2)	SAR=80.08		16.216s	Fingerprint
		Das(FVC2004 DB3)	SAR=60.08		20.699s	Fingerprint
		Das(FVC2006 DB1)	SAR=37.8		30.467s	Fingerprint
		Das(FVC2006 DB2)	SAR=81.6		23.817s	Fingerprint
		Das(FVC2006 DB3)	SAR=81.4		16.963s	Fingerprint
Dong et al. [76]	Similarity attack	Biohashing ($l = 500$)	SAR= 85.54%	5.29%	17s (100 generations	Face
		IoM-Hashing($l = 500$)	SAR= 41.01%	5.57%	14s(100 generations)	Face
		NMDSH($\alpha = 0.1, l = 250$)	SAR= 69.11 %	5.43%	13 min (100 max generations)	Face
		2PMCC($k = c = 64$)	SAR= 28.37%	3.11%	21 min (100 generations)	Fingerprint
		IFO ($m = 800, \tau = 50$)	SAR= 81.45%	9.83%	9 min (300 generations)	Iris
		Bloom filer ($w = 10, l = 24$)	SAR= 8.6%	11.95%	33 min(1500 generations)	Iris
Nagar et al. [12]	Similarity attack	Biohashing				...
Rozsa et al.[85]	Similarity attack based on GA	MCC,PMCC,Biotope			Fingerprint	
Quan et al.[72]	ARM Brute force attack					
Ouda et al.[74]	ARM	Bioencoding algorithm	More than 75% of the true template can be recovered		100 iterations	Iris

Feng et al. [83]	Similarity attack	Biohashing Scenario1 (binarization algorithm is known)	100% rank one recognition rate for CMU PIE and 98.3% FRGC databases		≈ 8 (s) for CMU PIE DB, ≈ 33 (s) for FRGC DB	Face
		Biohashing Scenario2 (binarization algorithm is known)	Wihin the range of 20.59, 85.29% for CMU PIE database and 15.14, 46.57% for FRGC database		2541 (s) for CMU PIE DB ≈ 8551 (s) for FRGC DB	Face
Ouda et al. [87]	Similarity attack	LRCB	More than 95% of the true template can be recovered.	1.4Ö10⁻3 whene $b = 1$and $d = 2$ to 377(s) when $b = 8$ and $d = 6$	Iris	
	Authentication attack	LRCB				
	ARM	LRCB				
	Linkability attack	LRCB				
Shin et al.[70]	Dictionary attack	The surface folding transform	85.2% no difference between the stored template and the recovered one.		1 and 2 of the algorithms require 464.16s And Line 3 to 5 require 54.31ms	Fingerprint
	Solving equations	The surface folding transform	90.2% in the valid case have only one solution			Fingerprint
Izu et al. [90]	Spoofing attack	Homomorphic encryption algorithm				Iris
Durbet et al. [92]	Similarity attack	Bio-hashing				Fingerprint
Hermans et al. [93]	Linkability attack	Bloom filter				Iris
Lacharme et al. 2012 [80]	Preimage attack	Bioencoding algorithm				Iris

Li et al. ARM [71]	DITOM	Fingerprint
	Polar-transformation	Fingerprint
	Transformation Based perpen-dicularly projection.	Fingerprint
	Transformation based on local minu-tiae infor-mation	Fingerprint

Table 4.2: Comparison between several attacks against CB schemes.

attacks that have successfully targeted various protection schemes. These attacks often exploit vulnerabilities in transformation processes, potentially allowing attackers to reverse-engineer the transformation function and compromise individual privacy. As a result, there is a pressing need for ongoing research to enhance the security of cancelable biometric systems and to develop robust defenses against these evolving threats.

Many protection methods have been subjected to limited or no comprehensive evaluations, which leaves them vulnerable to sophisticated attacks and undermines their reliability. Consequently, it is crucial to establish a rigorous evaluation framework that can thoroughly test cancelable biometric systems under diverse threat scenarios. This methodology is comprehensive for all protection systems in cancelable biometrics, ensuring a thorough assessment that enhances their resilience against potential attacks. By implementing such a framework, researchers can better assess the resilience of these systems and ensure their long-term viability as secure biometric solutions. The evaluation framework is explained in detail in the following subsections.

4.5.1 Evaluation for intrusion risks

4.5.1.1 Performance degradation

The effectiveness of the biometric system should be assessed while implementing the biometric protection scheme, which can be achieved using the following measures:

$$A = 1 - \frac{AUC(FAR_T, FRR_T)}{AUC(FAR_O, FRR_O)} \tag{4.1}$$

The AUC, or area under the ROC curve, represents the performance of the two systems. An AUC value of 1 indicates that the cancelable biometric scheme achieves perfect accuracy, with no errors. Conversely, a negative AUC value suggests that the biometric system's effectiveness deteriorates when using the protection scheme. Intrusion risks can further be evaluated by analyzing various attack scenarios, where the success probability of these attacks is measured by the False Accept Rate (FAR).

Study	Advantages	Disadvantages
Dong et al.[79]	This research proved that both of biohashing and Bloom-filter are vulnerable to similarity based attack using GA.	Requires the knowledge of the transformation function, a transformed template and the corresponding parameter
Nanwate et al.[77]	This research proved the vulnerability of both of biohashing and Bloom-filter to the similarity based-attack using PSO.	Requires the knowledge of the transformation function, a transformed template and the corresponding parameters.
Wang et al.[78]	This research proved that both of biohashing and IoM-hashing are vulnerable to similarity basedattack.	Requires the knowledge of the transformation function, a transformed template and the corresponding parameter. - The constraints imposed by the algorithm pose a difficulty in its application to some cancelable biometric schemes. -The absence of the produced pre-image.
Dong et al.[76]	This research proved the vulnerability of six cancelable biometric schemes to the similarity based-attack using GA.	Relies on less-realistic assumptions
Ghammam et al.[82]	This research proved that of both of GRP-IoM and URP-IoM are vulnerable to linkability and authentication attacks.	The contraints imposed by the algorithmpose a difficulty in its application to some cancelable biometric schemes. -Requires the knowledge of the transformation function, a transformed template and the corresponding parameter. -The linkabilty attack is not practical
Lee et al.[81]	This research proved the vulnerability of biohashing scheme to a preimage attack.	- Not practical. Requires the Knowledge of the protected template (biocode).
Nagar et al.[81]	This research proved the vulnerability of biohashing to preimage attack.	Requires the knowledge of the transformed template and the corresponding parameter.
Rozsa et al.[85]	This research proved the vulnerability of MCC, PMCC and Biotope to a similarity attack	

Ouda et al.[87]	More than 95% of the original template can be recovered. -Proved the vulnerability of LRCB to authentication ARM and linkability attacks.	Relies on lessrealistic assumptions
Shin et al.[70]	The attack is simple. More than 85% of the original features can be recovered.	Requires the knowledge of the transformation function, one or multiple transformed template(s) with their corresponding parameters
Quan et al.[72](ARM)	This research proved the vulnerability of the solving transformation to ARM.	Not practical.
Quan et al. [72](Solving equations)	Most of the exact minutiae can be recovered.	Requires the knowledge of the transformation function, the parameters and one transformed template.
Ouda et al.[74]	More than 75% of the original template can be recovered.	Requires the knowledge of the random sequence, the bio-encoding algorithm, and multiple bio-codes
Li et al.[71]	The attacks are simple. - The study shows theoretically the vulnerability point of each analyzed cancelable biometric scheme against ARM	Not practical.Requires the knowledge of the transformation function, multiple transformed templates, and their corresponding parameter
Izu et al.[90]	This research proved the vulnerability of Homomorphic encryption algorithm	The attack can be implemented only on binary features
Durbet et al.[92]	This research proved the vulnerability of biohashing to similarity attack	Requires the knowledge of the transformed template and the corresponding parameter. The attack is implemented only on small images size
Hermans et al.[93]	The linkability attack is successful with a probability of 96%.	Not practical
Lacharm e et al. 2012[88]	This research proved the vulnerability of bioencoding to a preimage attack.	Require the knowledge of the Boolean function.
Ouda et al. 2020[74]	More than 75% of the original template can be recovered.	Requires the knowledge of the transformation function and the corresponding parameters.

8 Lacharm et al. 2013[80]	This research proved the vulnerability of biohashing scheme to the similarity based-attack using GA.	Requires the knowledge of the transformed template and the corresponding parameter.
Topcu et al. 2016[84]	This research proved the vulnerability of biohashing to preimage attack.	Requires the knowledge of the transformation parameter.
Feng et al.[83]	The attack corresponds to two different scenarios based on the knowledge of the transformation algorithm. Achieve high rank one recognition for two different databases.	Complex realization.

Table 4.3: Advantages and disadvantages of attacks against cancelable biometric schemes

4.5.1.2 Zero force attack scenario

The attacker lacks knowledge of both the original biometric features and the transformation parameters specific to the user and attempts to impersonate the user's identity by using their own biometric data, b'_A, and parameters, K_A.

$$FAR_T(\varepsilon) = P(D_T(f(b_A, K_A), f(b'_A, K_A)) \leq \varepsilon) \tag{4.2}$$

4.5.1.3 Stolen biometric data scenario

The attacker is aware only of the biometric features of a legitimate user, b'_z, and proceeds to attempt various values of the transformation parameters K.

$$FAR_T(\varepsilon) = P(D_T(f(b_z, K_z), f(b'_A, K)) \leq \varepsilon) \tag{4.3}$$

4.5.1.4 Stolen token scenario

The attacker knows only the transformation parameter of a legitimate user, K_z, and tries various random values for the biometric features, $b\prime$.

$$FAR_T(\varepsilon) = P(D_T(f(b_z, K_z), f(b', K_z)) \leq \varepsilon) \tag{4.4}$$

4.5.1.5 Brute force attack scenario

The attacker attempts authentication by using various values of A_z (biometric data and parameters):

$$FAR_T(\varepsilon) = P(D_T(f(b_z, K_z), A_z) \leq \varepsilon) \tag{4.5}$$

Database	Modality	Number of images	Number of subjects	Image resolution	Image format
FVC2002(DB1)	Fingerprint	800	110	500 dpi	.tif
FVC2002(DB2)	Fingerprint	800	110	569 dpi	.tif
FVC2002(DB3)	Fingerprint	800	110	500 dpi	.tif
FVC2006(DB2)	Fingerprint	800	110	569 dpi	.bmp
CASIA-v3-IrisInterval	Iris	2639	249	320×280	.jpeg
CASIA-v4-IrisInterval	Iris	2639	249	320×280	.jpeg
LFW	Face	13233	5749	250×250	.jpg
CMU PIE	Face	41368	68	640×486	.jpg and .png
FRGC	Face	4007	465	1200×1600	.jpeg
FERET	Face	14126	1199	181×241	RGB
BioSecure-ds2 database	Face	1680	210	3504×2336	.JPG

Table 4.4: Databases used in various attacks against CB

4.5.2 Evaluation for reversibility risks

4.5.2.1 Inverse estimation from one or multiple protected template(s)

This approach aims to evaluate the likelihood of obtaining a partial or complete biometric template from one or multiple transformed templates to achieve authentication. Suppose an attacker knows a single transformed template $f(b_z, K_z)$ along with its corresponding parameter K_z, or multiple protected templates $f(b_z, k_z^1), ..., f(b_z, k_z^n)$ with the parameter set $K_z^1, ..., K_z^n$, and attempts to find the inverse function f^{-1} of f to estimate b_z.

$$FAR_O(\varepsilon) = P(D_O(b_z, f^{-1}(f(b_z, K_z), K_z)) \leq \varepsilon) \tag{4.6}$$

4.5.2.2 Estimation of pre-image from one or multiple protected template(s)

This objective is to assess the likelihood of obtaining an approximation $b_z^{\sim}$ of the original template. Assume an attacker has access to either a single transformed template $f(b_z, K_z)$ or multiple transformed templates $f(b_z, K_z^1), f(b_z, K_z^2), ..., f(b_z, K_z^n)$. In this context, $b_z^{\sim}$ is distinct from b_z, and $f(b_z^{\sim}, K_z)$ corresponds to the transformation $f(b_z, K_z)$. The aim is to enhance the inversion process when estimating f^{-1} is not obvious.

$$FAR_T(\varepsilon) = P\left(D_T\left(f(b_z, K_z), f\left((b_z^{\sim}, K_z)\right)\right) \leq \varepsilon\right) \tag{4.7}$$

4.5.2.3 Inversion in different biometric systems

In this scenario, an attacker possesses a transformed template $f(b_z, K_z^1)$ along with the corresponding parameter K_z^1 from System A, as well as the parameter K_z^2 associated with the same

user z in another System B. The attacker attempts to recover either a complete or partial version of the original template to impersonate the user z in system B.

$$FAR_T(\varepsilon) = f\left(f^{-1}\left(f(b_z, K_z^1), K_z^1\right), K_z^2\right), f\left(b'_z, K_z^2\right) \leq \varepsilon \tag{4.8}$$

4.5.3 Evaluation for linkability risks

Various scenarios are examined to assess the unlinkability of the protected templates belonging to the same user. In this context, an attacker attempts to establish a correlation among multiple templates associated with the same user.

4.5.3.1 Cross matching

To establish a correlation between two protected templates of the same user z with different parameters, an attacker can first invert the protected templates and then match them in the original domain. The cross match rate (CMR) is represented by:

$$CMR_O(\varepsilon) = P\left(D_O\left(f^{-1}\left(f(b_z, K_z^1), K_z^1\right), f^{-1}\left(f(b'_z, K_z^2), K_z^2\right)\right) \leq \varepsilon\right) \tag{4.9}$$

Alternatively, the attacker can directly match the templates in the transformed domain as follows:

$$CMR_T(\varepsilon) = P\left(D_T\left(f(b_z, K_z^1), f(b_z, K_z^2)\right) \leq \varepsilon\right) \tag{4.10}$$

Moreover, the unlinkability property can also be assessed from an information theory perspective by using mutual information.

4.5.3.2 Mutual information

It is a metric that quantifies the amount of shared information among several transformed templates. If Eq. (4.8) equals zero, it indicates that the transformed versions are independent.

$$I(x, y) = \sum_x \sum_y P(x, y) \log\left(\frac{P(x, y)}{P(x)P(y)}\right) \tag{4.11}$$

Where x and y represent two random variables, and P denotes the estimated probability. The maximum value of mutual information between multiple protected templates is quantified to assess unlinkability by calculating the average for all users in the database, as expressed in the following equation:

$$\frac{1}{N}\sum_{i=1}^{N}\sum_{j=1}^{M} \max\left(I\left(f(b_z, K_z), f\left((b_z, K_z^j)\right)\right)\right) \tag{4.12}$$

Where N represents the number of individuals in the database, M denotes the number of protected templates for each individual, and K_z^j signifies the jth parameter of individual z.

4.6 Discussion

Many cancelable biometric security algorithms are designed to protect individuals' original biometric data and prevent unauthorized access. However, significant vulnerabilities persist

within these systems and insufficient evaluation frameworks hinder the development of robust, attack-resistant algorithms. As a result, these systems remain exposed to various attack vectors, undermining their intended security.

Enhancing the security of protection systems is crucial from multiple perspectives. A primary focus should be on conducting comprehensive evaluations based on strict criteria (as outlined in Section 4.5) to minimize the risk of hacking biometric systems. This approach strengthens defenses against various attack vectors, particularly prevalent threats like ARM. Additionally, some research initiatives, such as those referenced in studies [96][97], have explored the integration of multiple biometric features with distinct characteristics to improve recognition performance. Furthermore, researchers in [98] introduced a dynamic multi-filtering approach, featuring two layers of reversible template designs and a sophisticated multi-layer fingerprint matching system. Their findings demonstrate competitive resilience against a range of attacks, including ARM, pre-image, and hill climbing attacks, while effectively reducing the risk of impostor acceptance.

In [99], researchers employed feature-adaptive random projection to enhance biometric template protection, effectively mitigating record multiplicity attacks and improving recognition accuracy by emphasizing local features. They tackled vulnerabilities associated with ARM by dynamically generating projection matrices from a base matrix, which is paired with local feature slots. This innovative approach not only strengthens the overall security of the biometric system but also optimizes performance by tailoring the projections to the unique characteristics of the data. Similarly, [100] proposed an innovative security system designed for identifying finger veins, utilizing the Rivest-Shamir-Adleman (RSA) encryption algorithm. This advanced system focuses on verification processes that leverage four distinct public databases, significantly enhancing security while ensuring high recognition accuracy. By integrating robust encryption methods with multiple data sources, the researchers aim to provide a more reliable and secure biometric identification solution.

Although many researchers have contributed to developing secure biometric systems, there is still considerable work needed to defend against a wide array of malicious threats. One of the critical gaps in cancelable biometric protection systems that researchers must address is the delicate trade-off between security and accuracy. While efforts to enhance security are paramount, they often result in a corresponding decline in accuracy. Conversely, striving for higher accuracy can inadvertently expose the system to significant security vulnerabilities. Researchers need to find a balanced approach that safeguards both aspects effectively.

Security in revocable biometric systems is closely tied to the revocation property, while accuracy depends on preserving the distances between biometric features in the original domain, which must be maintained in the transformed domain by the transformation function. Unfortunately, systems that prioritize accuracy without ensuring robust security are vulnerable to attacks exploiting the very property of distance preservation.

On the other hand, Another critical aspect to consider is the attacker's potential reliance on knowledge of the transformation function, the secret key, or both, as well as access to one or more transformed templates. While this scenario is common in biometric attacks, it introduces significant challenges when testing the effectiveness of the protection system, as it can impose constraints that complicate the evaluation of security measures.

In another aspect, , it is noticeable that most successful attacks have predominantly targeted specific biometric traits, such as fingerprints, eyes, and facial features, due to their widespread use and accessibility in security systems. In contrast, other biometric modalities, such as fingervein, palmprints..., have received far less attention from attackers, often because they are

less commonly integrated into high-security applications or present greater technical challenges for exploitation.

It is essential to investigate a broader range of attack types and conduct thorough, comprehensive analyses to strengthen security in the field of cancelable biometrics. Additionally, exploring other potential vulnerabilities in various protection schemes will be critical in enhancing the resilience of these systems against emerging threats.

4.7 Conclusion

Over recent years, numerous algorithms have been developed to protect stored biometric templates, with a primary focus on transformation functions that secure biometric data through their irreversibility. However, despite these advancements, significant vulnerabilities in revocable biometric systems continue to hinder their effectiveness. In this chapter, we have examined various attacks on revocable biometrics, providing a detailed analysis of the weaknesses in protection mechanisms that have allowed such breaches. Additionally, we explored studies that evaluated the irreversibility and unlinkability properties of transformation functions, which are critical to securing biometric systems.

Furthermore, we reviewed a range of databases commonly used in cancelable biometrics research and highlighted several revocable schemes that remain vulnerable to attacks due to inherent security flaws. A comparative analysis of these attacks was presented to demonstrate their varying degrees of success in compromising protection systems. In addition, we proposed an evaluation framework based on stringent criteria to assess the robustness of revocable protection schemes. We hope that the insights provided in this chapter will guide scientists and researchers in developing stronger defenses for revocable biometric data, making these systems more resilient to emerging attack strategies.

Chapter 5

Efficient Cancelable Multispectral Palmprint templates based on Cartesian Transformation

5.1 Introduction

One of the most widely adopted methods for securing biometric data is through biometric template protection schemes, particularly those leveraging the concept of "cancellable biometrics" (CB). This approach relies on applying a transformation function to distort the individual's original biometric template into a fully transformed version that bears no resemblance to the original. A key feature of cancellable biometrics is that the transformation is irreversible, meaning that the original template cannot be reconstructed from the transformed one. Even if an attacker gains access to the transformed template, part of it, or the transformation function itself, it remains impossible to reverse-engineer the original biometric data. Furthermore, this method provides flexibility, allowing individuals to generate an infinite number of transformed templates. If one transformed template is compromised, a new one can be easily created by altering the secret key used in the transformation. These attributes significantly strengthen the security and reliability of cancellable biometric systems, offering enhanced protection against potential breaches.

In this chapter, we introduce a robust transformation approach to safeguard cancelable multispectral palmprints [101] using the Cartesian transformation (CT) applied to minutiae points, as proposed in [8]. We also demonstrate that palmprint templates can be effectively protected using CT, making it applicable in various real-life scenarios. This method involves the design of a transformation function that distorts the original palmprint template by altering the positions of its minutiae points. The approach strengthens security by enforcing the irreversibility property, ensuring that the original template cannot be reconstructed under any circumstances. Even if an attacker gains access to the transformed template, the original minutiae points remain completely confidential. Additionally, the approach supports the revocability feature, allowing for the creation of a new transformed template if a security breach occurs. Figure 5.1 illustrates the core functioning model of a Cartesian transformation of palmprint templates.

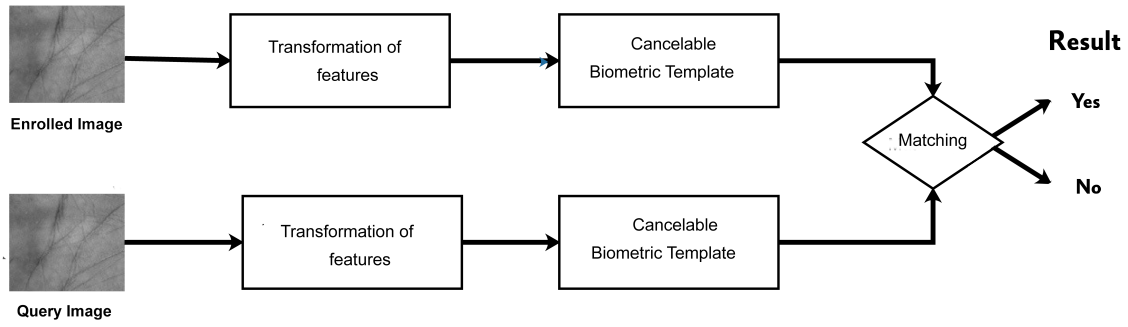


Figure 5.1: Cancelable Biometric Recognition Process

5.2 Related works

Fingerprints are among the most widely used biometrics in security applications, due to the rich set of distinctive features they contain. A key characteristic of fingerprints is the presence of minutiae points, which are defined by four attributes: (x, y, θ, t). Here, x and y represent the Cartesian coordinates, θ denotes the orientation of the minutiae, and t indicates the type of minutia. The two primary types of minutiae used in fingerprint matching are ridge endings and bifurcations. These features play a critical role in the matching process, helping to ensure accurate identification.

Ratha et al. [8] introduced a method for safeguarding fingerprint templates by applying a distortion function that repositions the fingerprint points to entirely new locations, ensuring that the original positions cannot be reconstructed from the transformed ones. Their approach works by dividing the fingerprint area relative to a reference point, typically the core, using orthogonal x and y axes, with the x-axis aligned with the core point. The coordinates of the fingerprint minutiae are then mapped based on this core point as the reference, effectively transforming the original layout while maintaining the protection of the original fingerprint data.

The fingerprint area is then partitioned into uniformly sized cells, each containing one or more original minutiae points. These cells are sequentially numbered in ascending order . The transformation process involves multiplying the original grid of numbered cells by a binary matrix that serves as the secret key for the transformation function. This operation alters the arrangement of the original cells, effectively relocating the minutiae points to new positions within different cells while preserving their original orientation. By doing so, the minutiae points' spatial arrangement is changed, while maintaining the integrity of their direction.

Equation Number 5.1 illustrates the transformation process through an example where the fingerprint is divided into a (2x2) grid, resulting in 4 cells. This grid is then multiplied by a transformation matrix K of size (4x4). The transformation matrix is a randomly generated binary matrix, where the value 1 specifies the new positions of the cells, guiding the rearrangement of the minutiae cells to their transformed locations. This operation effectively alters the spatial arrangement of the original cells while ensuring the integrity of the transformation.

$$\begin{bmatrix} 1 & 2 & 3 & 4 \end{bmatrix} \quad \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix} = \quad \begin{bmatrix} 2 & 1 & 2 & 3 \end{bmatrix} \tag{5.1}$$

The cancelability property lies in its ability to replace the transformation matrix if compromised. In such cases, a new, randomly generated binary matrix is created, entirely different from the original. This difference extends to the newly distorted template, which uses the same transformation function, results in completely different cell arrangements and minutiae point locations compared to the compromised template. This feature provides flexibility, enabling the cancellation of a breached template and the creation of a new, secure transformed template.

The irreversibility of this transformation lies in the fact that an attacker cannot trace the original minutiae points, even with access to the transformed template. This is due to the many-to-one mapping, where multiple original cells can be mapped to the same transformed cell. For instance, in equation 5.1, cells 1 and 3 are both mapped to cell 2. As a result, even if the attacker has knowledge of the transformation function, the transformed template, or both, it remains impossible to determine the original minutiae positions associated with cell 2, ensuring the security of the template.

Palmprints are a significant biometric modality in recognition systems due to their unique characteristics, including large surface areas rich in distinctive features, high user acceptance, and the convenience of image acquisition. These attributes make them particularly effective for secure and accurate identification. Yang et al. [102] proposed a new cancelable scheme for protecting palmprint templates, known as the dual-Level Cancelable Palmprint Verification Framework. Their approach begins by extracting palmprint data and encrypting it using a proprietary technology referred to as a competitive hash network token. This token acts as a key to safeguard the data. Subsequently, the encrypted data undergoes a second layer of encryption, further enhancing the security and robustness of the biometric data. This dual-layer approach ensures that even if an attacker compromises the data at the first level, accessing the second level remains significantly challenging.

Ali et al. [103] developed a cancelable approach for storing and protecting palmprint data using two hash tables. Before storing the palmprint data, each segment is combined with a random array to introduce variability. Next, random hashing is applied, incorporating different gray encoding methods to obscure the data. An additional layer of protection, known as MinHash, is then employed. This technique enhances efficiency while safeguarding the data against linkage attacks, which attempt to correlate different parts of the data to compromise security.

Despite the advantages of palmprints, their application in cancelable biometrics remains relatively limited especially due to feature extraction. Palmprints contain a dense array of minutiae points and intricate texture patterns, which introduce significant computational complexity. This complexity can make the transformation process not only computationally intensive but also challenging to optimize for security and efficiency [104]. In our approach, we addressed the computational complexities typically associated with processing palmprints by leveraging the PolyU multispectral palmprint database. By applying accurate and effective image enhancement, we significantly reduced the number of redundant minutiae [105]. This optimization improved the feature extraction process, minimizing computational demands while preserving the integrity and security of the cancelable biometric transformation.

5.3 Cartesian Transformation On Palmprint Templates

As previously discussed with fingerprints, we demonstrate that this approach can also be effectively applied to palmprints, offering a comparable level of protection. Palmprints are recognized as one of the most important biometrics in the security field due to their reliability in identifying individuals and the abundance of distinctive features they contain [104]. Similar to

fingerprints, palmprints possess minutiae points, including ridge terminations and bifurcations. Each minutiae point is characterized by four attributes: (x, y, θ, t), where x and y represent the Cartesian coordinates, θ indicates the orientation of the minutiae, and t denotes the minutiae type.

In this Cartesian transformation approach, the palmprint's minutiae coordinate space is first divided into a grid of uniformly sized cells, with the grid size determined by the dimensions of the palmprint image and a reference point. These cells are then arranged in a spiral pattern following a fixed sequence, with each cell containing one or more minutiae points. The transformation process begins by generating a secret key in the form of a randomly created binary matrix, whose size corresponds to the palmprint's cell grid, as described in Section 5.2 The transformation itself involves multiplying two matrices: one representing the cell grid and the other, the binary matrix acting as the secret key. This multiplication results in new minutiae coordinates, effectively changing the minutiae positions while maintaining their original orientation. This method ensures a secure transformation of the minutiae positions without altering their orientations.

As with typical cancelable biometric systems, this approach involves two stages. The first is the registration stage, where the palmprint template is transformed using the Cartesian transformation and securely stored in the database along with the corresponding secret key. In the matching stage, the same transformation key is used to apply the Cartesian transformation to the newly acquired palmprint template, which is then compared against the stored template in the database for matching and verification. The following steps outline the complete procedure.

- **Step 1**: Generation of a rectangular coordinate system. We partition the coordinate space into grid cells of size $(W * H)$, using the core point as the origin. Each original minutia point is assigned a corresponding cell number based on its position within the grid.
- **Step 2**: Generation of a transformation matrix.

  In this step, we generate a random binary matrix.
- **Step 3**: Obtain the transformed square. Multiply the original cell square by the transformation matrix.

$$M' = M * K \tag{5.2}$$
- **Step 4**: Obtain the transformed minutiae templates.

  Each original minutiae point is assigned new coordinates based on its updated position.

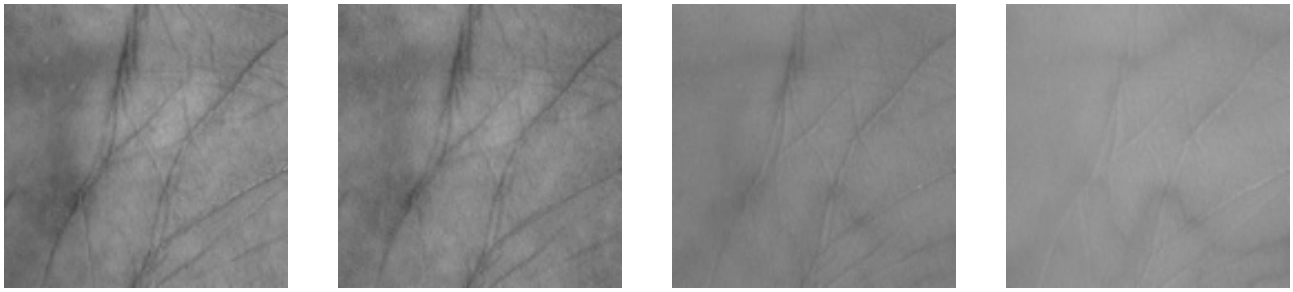
5.4 Experimental results and analysis

In this section, we conduct an experimental evaluation of the proposed Cartesian transformation applied to the palmprint template, following the method outlined in this study step by step. We then analyze and interpret the results by comparing the performance and accuracy of the system in both the original and transformed domains, providing insights into the effectiveness of the transformation. The implementation is performed on a machine running Python 3 with Jupyter notebook, powered by an Intel(R) Core(TM) i7-6700 CPU @ 3.40 GHz with 16GB of RAM.

5.4.1 The PolyU palmprint database description

To demonstrate the effectiveness of the proposed method, we conducted an experimental study using the PolyU multispectral palmprint database [106], developed by Hong Kong Polytechnic University, to perform a comprehensive transformation analysis.

The PolyU multispectral palmprint database includes captures from both near-infrared (NIR) and visible light spectrums, covering red, green, and blue channels. It contains a total of 6,000 palmprint images collected from 500 individuals, with 12 samples per person. For ease of use, the Hong Kong Polytechnic University (HKPU) has provided region of interest (ROI) images, which are available in 128 $\times$ 128 pixels and stored in JPG format (*.jpg). The database is designed to support a wide range of research in palmprint recognition and biometric analysis. Its multispectral nature offers enhanced feature extraction capabilities, making it ideal for evaluating transformation methods like the one proposed in this study. Figure 5.2 shows some multispectral palmprint samples in the PolyU database.



(a) (b) (c) (d)

Figure 5.2: Multispectral Palmprint samples: (a) Blue .(b) Green.(c)Red.(d)Nir databases

5.4.2 Results

The experimental results clearly demonstrate the success and effectiveness of the Cartesian transformation in safeguarding palmprint templates. Table 5.1(a) presents the experimental results of the authentication process in the original domain, while Table 5.1(b) displays the results in the transformed domain. The outcomes of the experiments are presented in Tables 5.1(a) and 5.1(b), respectively. To provide a thorough validation of our findings, we further present the results using Equal Error Rate (EER) plots and Receiver Operating Characteristic (ROC) curves, as illustrated in Figures 5.3,5.4,5.5 and 5.6. These visualizations offer deeper insights into the system's performance, confirming the robustness of the proposed transformation method.

5.4.3 Exploring the Performance Implications

From Tables 5.1a and 5.1b , and the EER and ROC curves 5.3,5.4,5.5 and 5.5, we can observe the effectiveness of the Cartesian transformation in securing palmprint templates by analyzing its impact on the FRR at a FAR of 1%. For instance, in the Blue database, the FRR in the original domain is 1.02%, while in the transformed domain, it increases to 3.49%. Similarly, the EER rises from 2.06% in the original domain to 4.60% in the transformed domain. This slight trade-off in recognition performance, reflected in the higher FRR and EER, is acceptable in exchange for the added layer of security. Although there is a slight performance decline

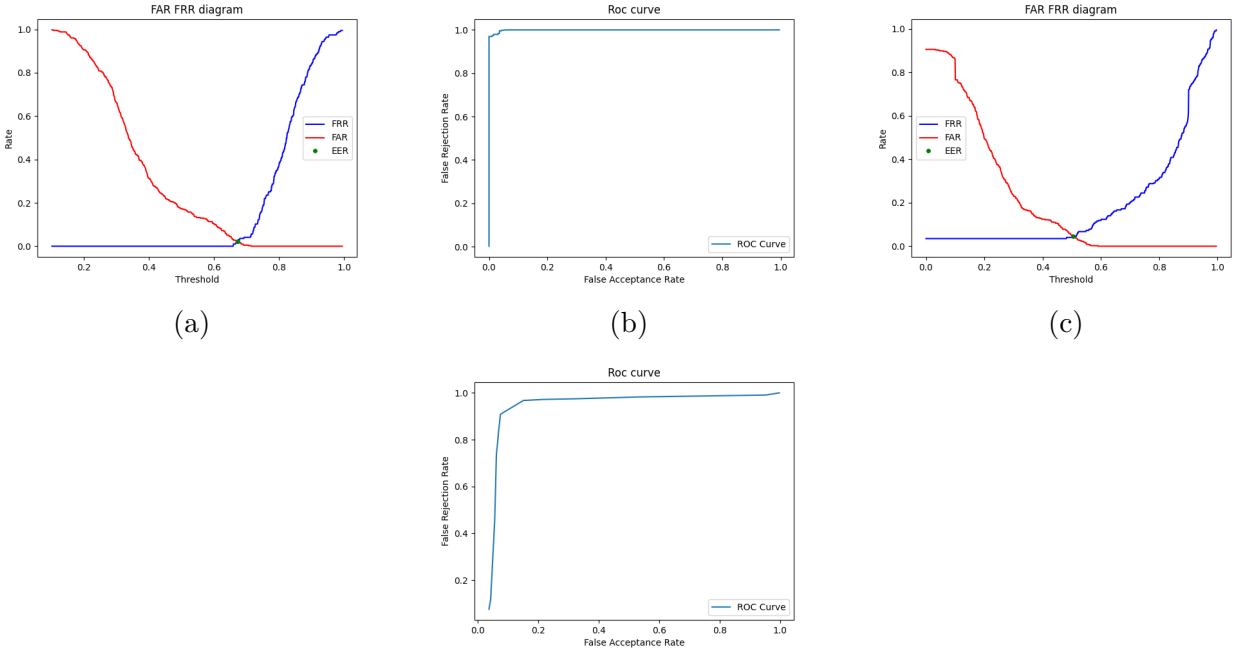
DB	EER	FRR FAR=1%	FRR FAR=0.1%
Blue	2.06%	1.02%	99.94%
Green	2.29%	0.76%	99.49%
Red	2.61%	1.02%	99.98%
Nir	3.28%	1.01%	99.49%

(a) Performance values in original domain

DB	EER	FRR FAR=1%	FRR FAR=0.1%
Blue	4.60%	3.49%	99.46%
Green	10.55%	4.60%	98.31%
Red	5.50%	1.01%	99.49%
Nir	8.33%	1.03%	99.49%

(b) Performance values in transformed domain

Table 5.1: Comparison of performance values in original and transformed domains



(a) (b) (c)

(d)

Figure 5.3: Graphics of System Performance of Blue dataset: (a) EER diagram in original domain,(b) Roc curve in original domain, (c) EER diagram in Transformed domain (d) Roc curve in Transformed domain

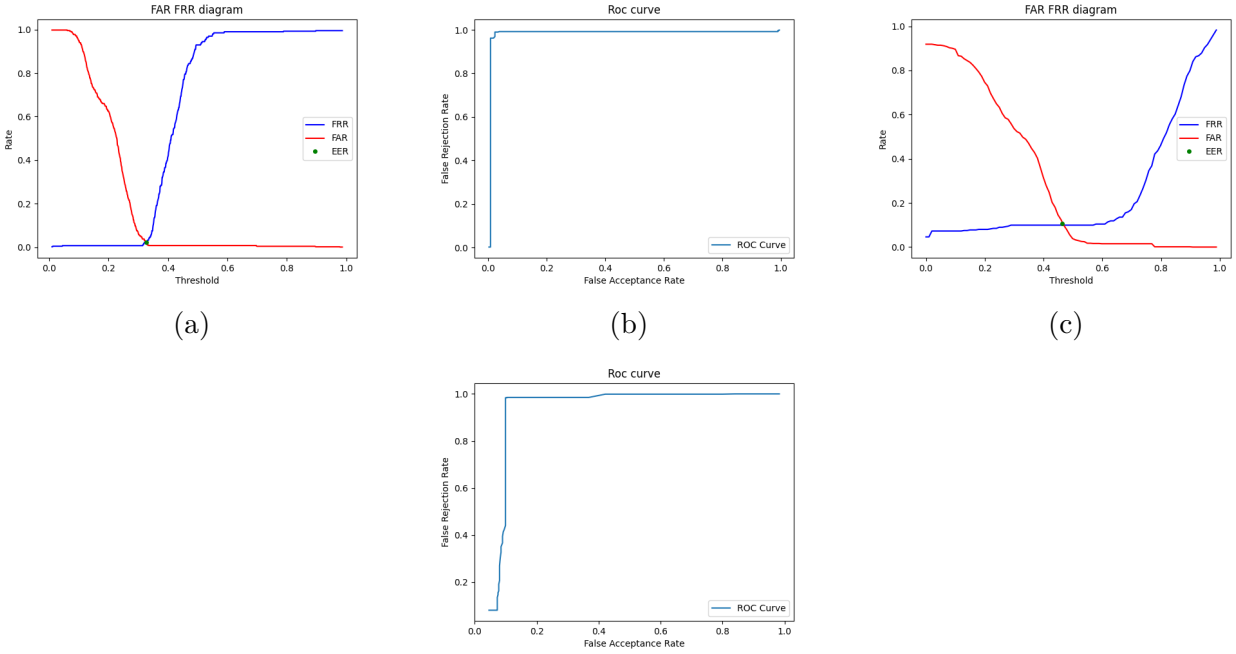


Figure 5.4: Graphics of System Performance of Green dataset: (a) EER diagram in original domain,(b) Roc curve in original domain, (c) EER diagram in Transformed domain (d) Roc curve in Transformed domain

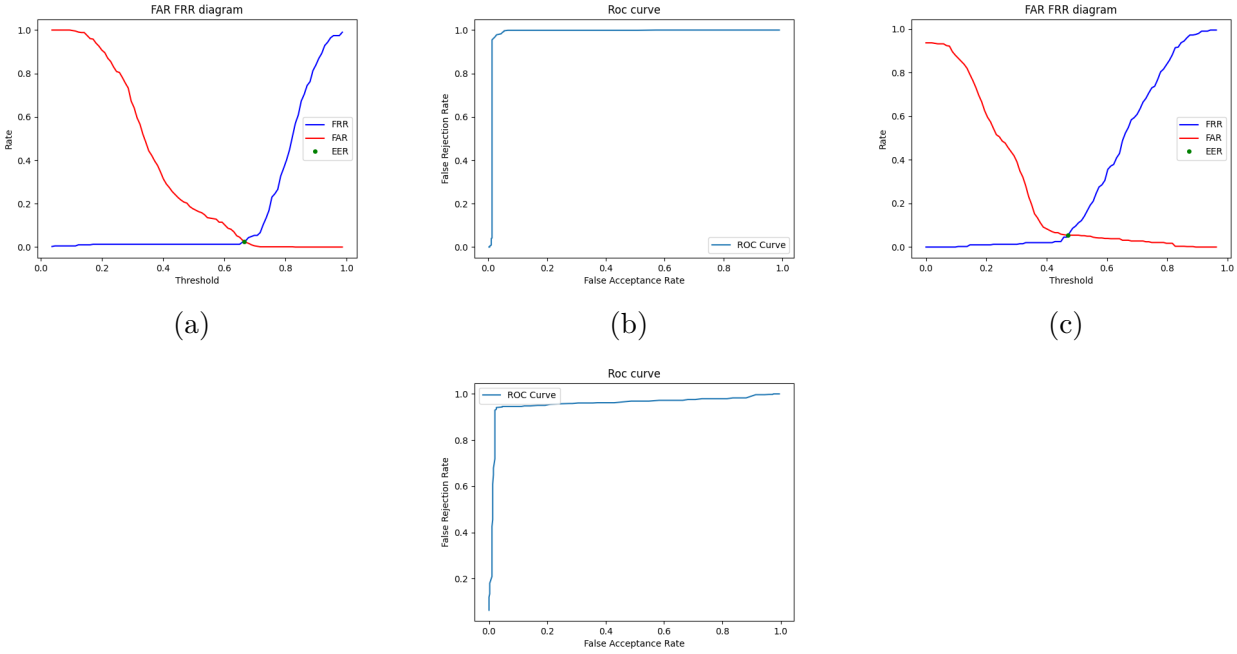


Figure 5.5: Graphics of System Performance of Red dataset: (a) EER diagram in original domain,(b) Roc curve in original domain, (c) EER diagram in Transformed domain (d) Roc curve in Transformed domain

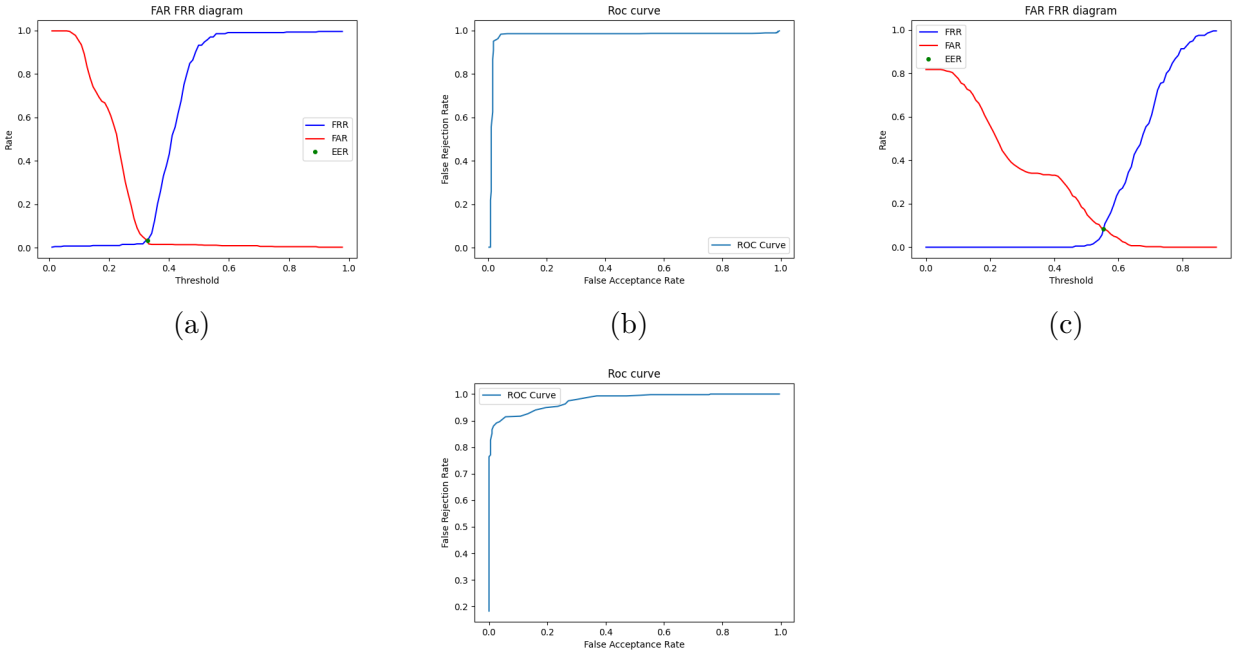


Figure 5.6: Graphics of System Performance of Nir dataset: (a) EER diagram in original domain,(b) Roc curve in original domain, (c) EER diagram in Transformed domain (d) Roc curve in Transformed domain

post-transformation, it remains within acceptable limits. This minor reduction is primarily due to the introduction of increased intra-user variability, which affects the consistency of minutiae point positioning. As a result, some minutiae points, which were initially located in specific cells, may shift to completely different cells after the transformation. This variability can cause overlaps in minutiae points that were previously well-separated, leading to a redistribution of points within the Cartesian grid. Despite this, the transformation still provides strong security, and the performance impact is outweighed by the protection it offers.

5.5 Conclusion

Despite the numerous protection methods proposed in the field of cancelable biometrics, some approaches fail to adhere to established protection standards and fall short of providing the required level of security [5] [27]. This vulnerability arises from the variety of threats and attacks they face, compounded by inherent weaknesses within these methods, which pose significant risks to individuals' data and privacy.

For these reasons, it is essential to develop robust and rigorously evaluated protection schemes capable of defending biometric data against a wide range of attacks. Such schemes must ensure that attackers are unable to compromise the data through any means, whether by retrieval attacks, linkage attacks, or other forms of malicious activity [107]. In this chapter, we discussed the significance of cancelable biometrics and the need to safeguard stored biometric templates against retrieval attacks, particularly for biometric traits that are less commonly used in this field. We also proposed a robust system, known as the Cartesian transformation, to protect palmprint templates from various attacks. We applied the Cartesian transformation approach to various databases, which are represented by the multispectral palmprint database (blue, green, red, and NIR). Initially, data was extracted from the palmprint images, represented as

a set of minutiae points, which were then mapped onto a grid of numbers. A secret key, represented as a binary matrix, was generated for the transformation process. The transformation function involved repositioning the minutiae points to new locations based on the transformation key. This Cartesian transformation satisfies the critical requirements for establishing a robust protection scheme. It is an irreversible process, ensuring that attackers cannot reverse the transformation function or recover the original minutiae positions from the transformed ones. Furthermore, this approach allows for the creation of a new transformed template if the stored template is compromised, simply by generating a new secret key. Experimental results demonstrate the effectiveness of this method in protecting palmprint data.

Chapter 6

Attack against key-dependent transformation-based fingerprint template protection Algorithms

6.1 Introduction

Cancelable biometrics has been introduced to address the security and privacy concerns associated with traditional biometric systems, particularly by protecting stored templates from misuse. This approach has gained significant traction, leading to the widespread adoption of revocable biometric protection schemes across various domains [69] . The transformation function must be irreversible, ensuring that the original biometric data cannot be reconstructed from the transformed template (one-way transformation). This irreversibility is achieved by constructing non-invertible mathematical operations or increasing the dimensionality and randomness of the transformed template, making the reversal process computationally infeasible. Additionally, the transformation expands the range of possible outputs for a given biometric input, mitigating the risk of brute-force attacks. To ensure revocability, the transformation function incorporates a user-specific parameter (user-specific key), which acts as a secret known only to the system and the legitimate user. This key allows for the generation of multiple distinct transformed templates from the same biometric data, enabling users to revoke and replace compromised templates without affecting the original biometric traits [27] [6]. Furthermore, by assigning different transformed templates for different applications, this approach prevents cross-application tracking, ensuring that a compromised template in one system does not expose the user's identity elsewhere, thereby significantly enhancing privacy.

Despite the advantages of cancelable biometrics in securing individuals' biometric templates and the numerous studies conducted to develop high-performing transformed templates, most of these approaches remain vulnerable to attacks [89] [76] and often rely on insufficient or impractical security analyses against various threats. Moreover, they often receive more attention than they truly merit. Attacks in the literature aim either to retrieve the original biometric data such as those exploiting the distance preservation property between templates in the transformed domain[53][79][77] or to identify computational weaknesses in the transformed system. Another type of attacks focuses on key-dependent transformation functions, where vulnerabilities in user key management [19] can lead to the direct reconstruction of the original biometric data if the key is compromised. In practice, the user's specific key is typically stored on a separate token to ensure its secrecy. In the event of a compromise, an intruder may attempt to either reverse-engineer the transformation function or guess the transformation

key, both of which are challenging tasks. However, if the design of the transformation function relies heavily on key management, a key compromise could lead to the complete recovery of the original template. In this chapter, we will describe the development of an attack against a key-dependent cancelable fingerprint algorithm proposed by [8]. We have demonstrated a security gap in the Cartesian transformation and shown that the use of a secret user-specific key, intended to ensure the revocability property, negatively impacts the security of fingerprint templates. This key introduces a vulnerability that allows the original fingerprint templates to be recovered.

This security algorithm has never been attacked before, making this the first analysis of its weakness. We exploited the lack of properly managed shared information across multiple templates of the same user to reconstruct the secret key, ultimately enabling the recovery of fingerprint templates.

6.2 Fingerprint Recognition

A fingerprint is a unique pattern of ridges and valleys found on the surface of a fingertip. These patterns are formed during fetal development and remain unchanged throughout a person's lifetime, making fingerprints a reliable biometric trait for identity verification. Fingerprints are characterized by various global and local features that contribute to their uniqueness. Ridges are the raised lines on a fingertip that come into direct contact with a surface when touched, while valleys are the recessed areas between these ridges. Each fingerprint is characterized by a distinct arrangement of ridges and valleys, with ridges containing unique features, such as **Minutiae points**, that define the fingerprint's individuality. Figure 6.1 illustrates an example of fingerprint features.

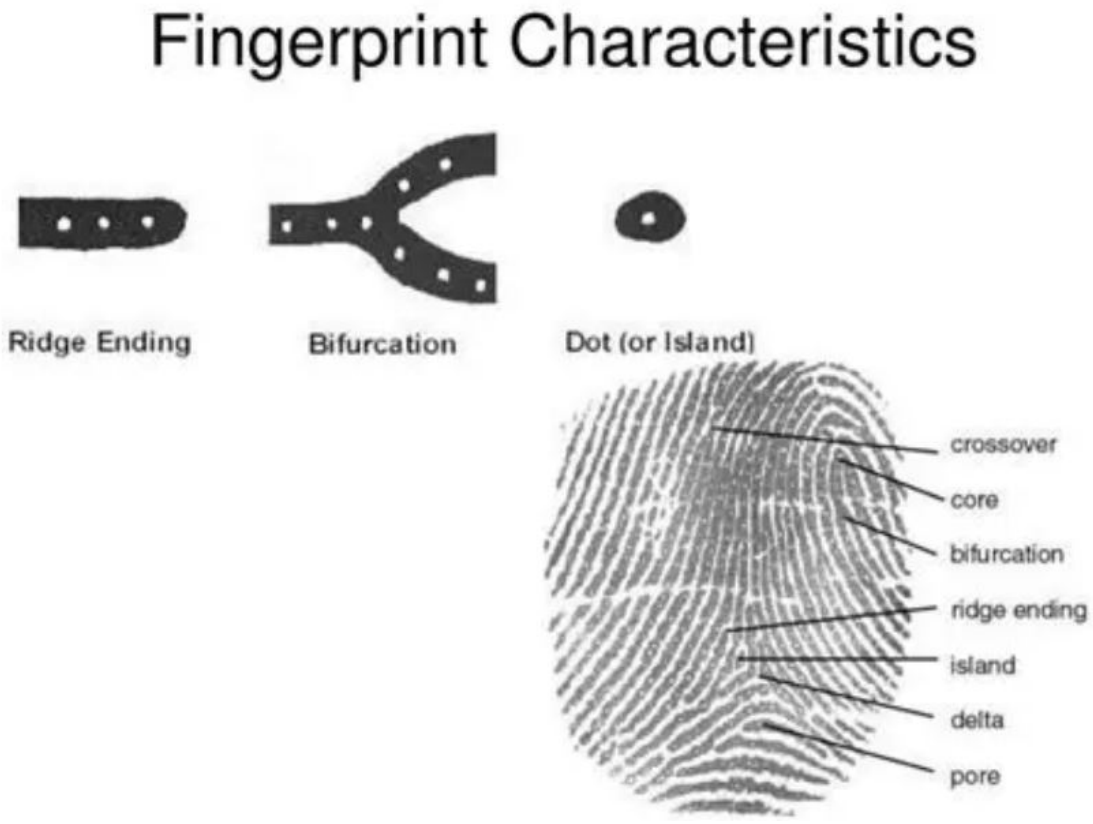


Figure 6.1: Fingerprint characteristics

Each minutia in a fingerprint image is defined by a triplet (x, y, θ), where (x, y) denotes its spatial coordinates, specifying its position within the image, and $\theta \in [0, 2\pi]$, represents its orientation.

6.2.1 Intra-Class Variability in Fingerprint Templates

In biometrics, intraclass variability is unavoidable across multiple instances of the same biometric trait, as the samples captured during authentication differ from those recorded during enrollment [3]. This variability can arise from various factors, such as the pressure applied to the fingerprint sensor, modifications to the sensor's parameters, or even changes in the sensor itself. Additionally, noise and other environmental influences contribute to these variations. Despite the biometric system's ability to authenticate a user's identity, there remains a risk of misidentification, where a genuine user may be mistakenly classified as an impostor. In our case, this variability can be exploited to launch an attack against the biometric system. Figue 6.9 illustrates the inta-class between two impressions of the same finger.

Figure 6.2: An illustrative representation of extracted minutiae points from two impressions of the same finger, highlighting intraclass variability. The variations in the set of minutiae points between the two images demonstrate the natural differences that occur across multiple acquisitions.

6.3 Cartesian Transformation Proposed by Ratha et al.

In the cartesian transformation (CT) the core point is utlized as a reference to divide the fingerprint coordinate system as illustrated in Figure 6.3.

In this approach, the minutiae point coordinates are transformed into new coordinates, where the fingerprint's core point serves as the center of the Cartesian system, and the x-axis is aligned with the core point's orientation. In this coordinate system, the space is divided into equal-sized cells ($h \times w$), with each cell potentially containing one or more minutiae points. The cells are sequentially numbered from 1 to N, where N=($H \times W$), with H representing the total number of rows (height) and W the number of columns (width). The numbering scheme is influenced by both the fingerprint structure and the chosen cell dimensions. During the transformation, minutiae points are relocated from their original cells to new ones, while their orientations remain unchanged, as illustrated in Fig. 6.4.

Figure 6.3: A sample fingerprint demonstrating a grid axis aligned with the core point's orientation.

Mathematically, this transformation is performed by applying a transformation matrix K to the minutiae-index vector. To illustrate this process, consider a coordinate system divided into four cells (2×2), where the transformation matrix K is a binary matrix that indicates the locations of the new cells. A value of 1 in the matrix specifies where the minutiae should be relocated. For example, the minutiae initially located in cell 1 are reassigned to cell 2, while those in cell 3 are also transferred to cell 2. This merging of minutiae from multiple cells into a single destination enhances the transformation's irreversibility.

$$\begin{bmatrix} 1 & 2 & 3 & 4 \end{bmatrix} \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 2 & 1 & 2 & 3 \end{bmatrix} \tag{6.1}$$

The revocability of this protection scheme is ensured by allowing the transformation matrix to be modified. This flexibility enables the cancellation of a compromised transformed template and the creation of a new one by updating the transformation matrix. The scheme's irreversibility is demonstrated in Equation 6.1, where multiple cells (e.g., cells 1 and 3) are mapped to the same cell (cell 2). As a result, even if an attacker obtains the transformation function or the transformed template, identifying the original minutiae locations within cell 2 remains infeasible without resorting to a brute-force attack. During registration, instead of storing the original minutiae positions, only their transformed coordinates and the secret transformation matrix are retained. The following steps detail the overall process :

- **Step 1: Generation of the Rectangular Coordinate System**

  The coordinate space is divided into a grid of cells ($H \times W$) based on a reference point, assigning each original minutia a corresponding cell number.

- **Step 2: Creation of the Transformation Matrix**

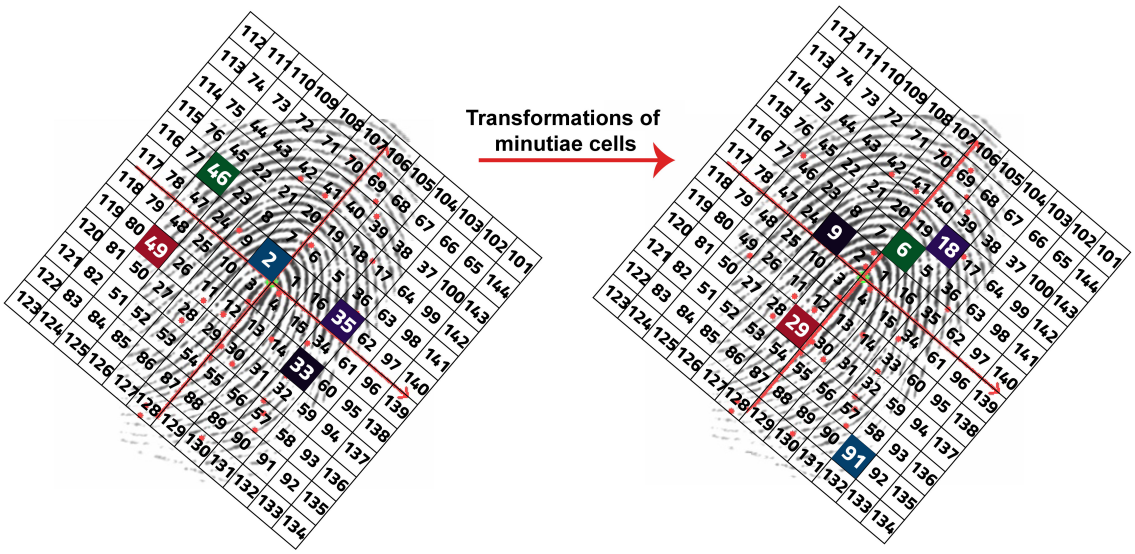


Figure 6.4: The Cartesian space is segmented into uniformly sized cells using the core point as a reference. In (a), the initial minutiae points are displayed, while in (b), the transformed minutiae illustrate how each point is assigned to a different cell. The figure also highlights examples of cell transformations using distinct colors.

A binary matrix is randomly generated, consisting of values 0 and 1, which will determine the new mapping of the minutiae locations.

- **Step 3: Transformation of the Grid**

  The original cell arrangement is modified by applying the transformation matrix, following the equation:

$$M' = M \times K \tag{6.2}$$

- **Step 4: Computation of Transformed Minutiae Templates**

  Each minutia point is reassigned new coordinates based on the updated cell positions resulting from the transformation.

Figure 6.5 illustrates the transformation process.

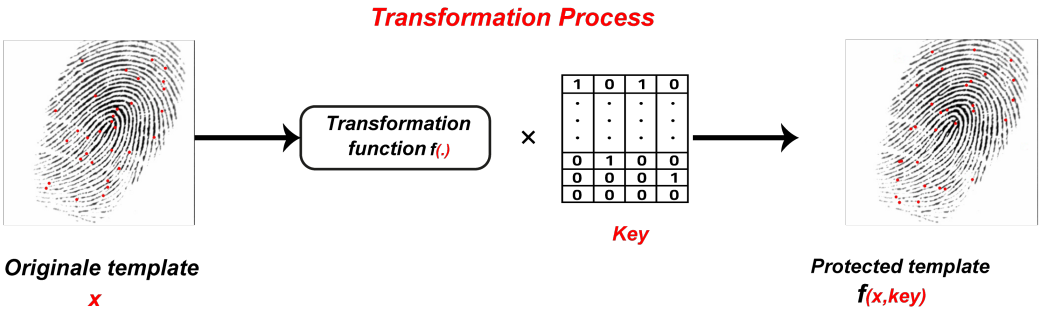


Figure 6.5: Cartesian transformation process.

When applying the Cartesian transformation approach, it is crucial to consider the impact of intra-user variations across different fingerprint instances. Minutiae points positioned near cell

boundaries may shift between instances, causing them to misalign with their corresponding points after transformation. This discrepancy arises due to the non-smooth nature of the transformation function, which can reduce matching accuracy. Additionally, some minutiae may be displaced to entirely different regions within the fingerprint image.

In the experiment, a predefined maximum width and height were chosen, set as $X = 32$, with a cell size of $X \times X$, following the approach used in [8]. This selection aimed to reduce the likelihood of cell exchanges during the transformation process. The coordinate system was segmented into a grid based on this parameter, and the key dimensions were determined accordingly. Each fingerprint was assigned a specific grid size tailored to its size.

For instance, Figure 6.4 illustrates an example using a fingerprint from the FVC2002 DB1 database [108], where a grid size of 12×12 was applied to match the fingerprint's dimensions. The transformation matrix is represented as a binary structure, where each column contains a single '1' to indicate the new cell number, while the remaining entries in that column are set to '0'.

6.4 Security and Performance Considerations

The non-invertibility of the Cartesian transformation in [8] depends primarily on the dimensions of the transformation matrix. The complexity further increases due to the mapping of multiple cells to a single cell, making it challenging to reconstruct the original fingerprint. The authors assert that: "We want to make it hard to invert the transformed version of the points back into the original point configuration. To be strictly non-invertible, it must be impossible to create a function that takes a transformed point and regenerates a unique input point".

The binary representation of the transformation matrix offers an initial estimate of the information contained in the key, with each matrix column encoding $\log_2(HW)$.

Given the robustness of the transformation, each resulting cell can potentially originate from $H.W$ possible source cells, forming a many-to-one mapping. Consequently, in a brute-force attack scenario, approximately HW^{HW} possibilities must be evaluated for a successful breach. Due to this vast search space, an attacker faces significant difficulty in tracing each transformed cell back to its original state and uncovering the key, as the sheer number of required attempts makes system penetration highly impractical.

6.5 Proposed Missing Template Information Attack

In most existing attacks, the primary vulnerability lies in information leakage during the transformation process. This leakage occurs due to the transformation's distance-preserving property, which adversaries can exploit to reconstruct the original biometric template [79] [76] [77].

The objective of Our attack is to reconstruct the original minutiae locations by exploiting the exposure of the transformation matrix. It is assumed that the attacker interacts directly with the identification system, allowing them to input multiple fingerprints and obtain the corresponding transformed templates. That is, the attack algorithm initiates with a real-world scenario where multiple original fingerprint templates are available alongside their corresponding transformed versions.

When discussing the exploitation of multiple templates to launch an attack on revocable biometrics, the concept of ARM [71] often comes to mind. However, our approach differs. Our attack can be considered a subvariant of ARM, yet it introduces a novel perspective. The key distinction lies in the point: traditional ARM-based attacks leverage multiple transformed templates derived from the same original biometric trait, exploiting shared information among them. In contrast, our attack begins with multiple templates and focuses on identifying and reconstructing the missing shared information, which represents leaked data. This ultimately enables the inference of critical details that can be used to approximate the original fingerprint template.

Most minutiae points in each pair of matched fingerprints correspond, however, due to intra-class variability, some points do not match. We refer to these **isolated minutiae points**. This matching relation is maintained in the transformed domain, where the isolated minutiae points remain preserved. In our approach, we leverage these isolated minutiae to uncover their transformations by tracking them across multiple fingerprints and their corresponding transformed versions using the matching relation.

To apply the attack, consider a scenario where we have N original fingerprint templates from the same user $\{OT\}_{i=1}^{N}$, along with their N corresponding protected templates $\{PT\}_{i=1}^{N}$. Each template comprises a set of minutiae points $\{m\}_{i=1}^{N}$ and a designated core points $\{CP\}_{i=1}^{N}$. To illustrate the idea, we take two original fingerprint templates, $Fp1$ and $Fp2$, along with their corresponding transformed ones, $Fp'1, Fp'2$, respectively.

In $Fp1$, the minutiae set consists of $\{m_0^1, m_1^1, m_2^1, m_3^1\}$, while in $Fp2$, it includes $\{m_0^2, m_1^2, m_2^2, m_3^2\}$. Their counterparts in the transformed domain $Fp'1, Fp'2$ contain the minutiae points $\{m_0'^1, m_1'^1, m_2'^1, m_3'^1\}$, and $\{m_0'^2, m_1'^2, m_2'^2, m_3'^2\}$ respectively.

We lunch the matcher between $Fp1$ and $Fp2$ to identify the corresponding minutiae pairs: $\{(m_0^1, m_0^2), (m_2^1, m_2^2), (m_3^1, m_1^2)\}$. Similarly, in the transformed domain, the matching is applied between $Fp'1$ and $Fp'2$ to determine the mapped minutiae: $\{(m_0'^1, m_0'^2), (m_2'^1, m_2'^2), (m_3'^1, m_1'^2)\}$. Although $Fp1$ and $Fp2$ are from the same finger, in each matching relation we discover an isolated minutiae points : m_1^1 in $Fp1$, $m_1'^1$ in $Fp'1$, m_3^2 in $Fp2$, and $m_3'^2$ in $Fp'2$. In this case, it is possible to determine the mapping of each isolated minutia from the original template to its counterpart in the transformed template. Specifically, m_1^1 in $Fp1$ corresponds to in $m_1'^1$ in $Fp'1$, while $m_2'^3$ in $Fp2$ is mapped to $m_2'^3$ in $Fp'2$.

For further illustration, we refer to Figure.6.6 to explain the exploitation of minutiae relation retrieval.

In our attack scenario, numerous minutiae points remain unmatched, making it impossible to determine the transformation of all original minutiae positions directly. However, increasing the number of templates to the maximum allows for better inference. Alternatively, expanding the set of constraints helps recover a greater part of the original minutiae mappings, effectively narrowing the search space and facilitating the reconstruction of their original coordinates. In other words, the search space decreases as the number of constraints increases.

As mentioned in the previous section, all fingerprint minutiae points are contained within cells that are repositioned using a secret binary matrix. Analyzing the relation between the original and transformed minutiae through the matching process enables the reconstruction of the transformation matrix. This is achieved by determining how the original cell indices correspond to their transformed counterparts.

In summary, the attack procedure is illustrated in Figure.6.7. It begins with multiple templates in both the original and transformed domains, followed by applying the matching relation to

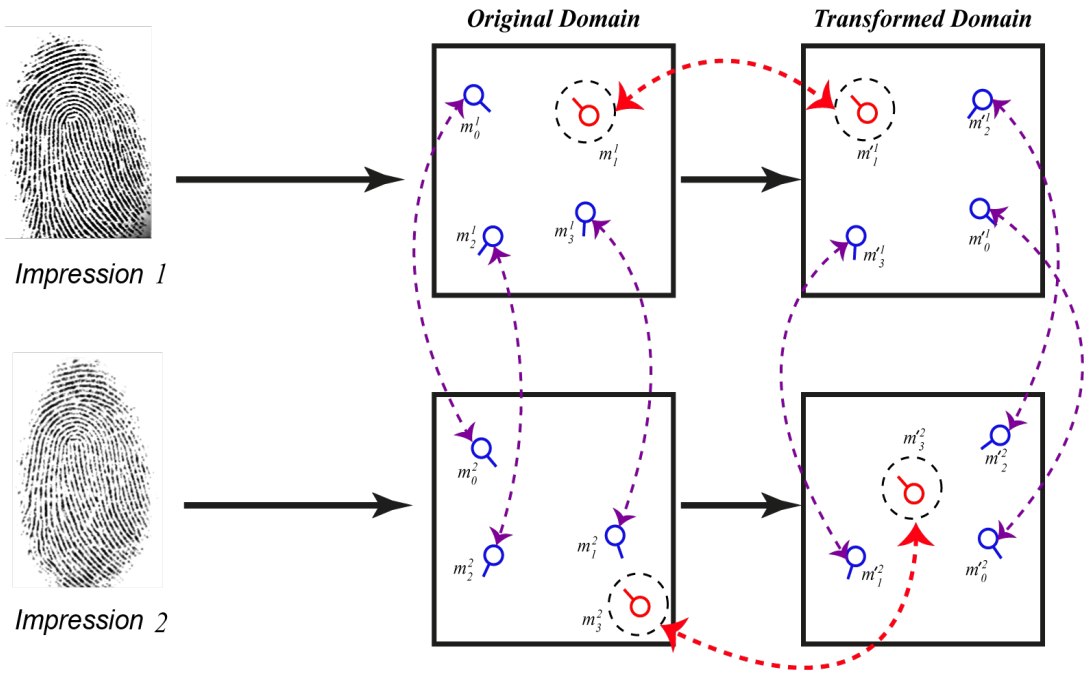


Figure 6.6: An illustrative example showcases two matched templates in both the original and transformed domains. The dotted blue arrows between impression 1 and impression 2, in both domains, represent the constraint imposed by paired minutiae based on a matching relation. The minutia m_1^1 (respectively m_3^2) is present in original template 1 (respectively template 2) but absent in original template 2 (respectively template 1). This lack of alignment between the templates facilitates the identification of the transformed minutiae $m_1'^1$ and $m_3'^2$ within transformed template 1.

.

establish exemplar minutiae sets across all templates. This process increases the number of constraints, effectively reducing the search space. A brute-force attack is then performed to determine the key for the transformation matrix.

6.5.1 Main Representative Minutiae Organization

The process of matching fingerprint templates is often affected by various factors such as the resolution of the sensor, the angle and pressure applied during finger placement, the naturally poor quality of certain fingerprints, and distortions introduced during acquisition. As a result, the set of minutiae points extracted from multiple impressions of the same finger may vary. By integrating the different minutiae sets during the matching phase, it becomes possible to infer information about specific minutiae. This approach enables most minutiae to be matched, albeit in a unique manner, with their counterparts in other templates, thereby facilitating the identification of new constraints among them.

When working with information derived from multiple fingerprint templates of the same finger, a fundamental preliminary step involves organizing the primary exemplar minutiae of the model. Directly processing raw minutiae points from different impressions without prior structuring is impractical. Therefore, this phase is essential for classifying the minutiae types that appear across various templates of the same fingerprint. Since many templates may share overlapping data, it is important to consolidate redundant minutiae and exploit any new insights contributed

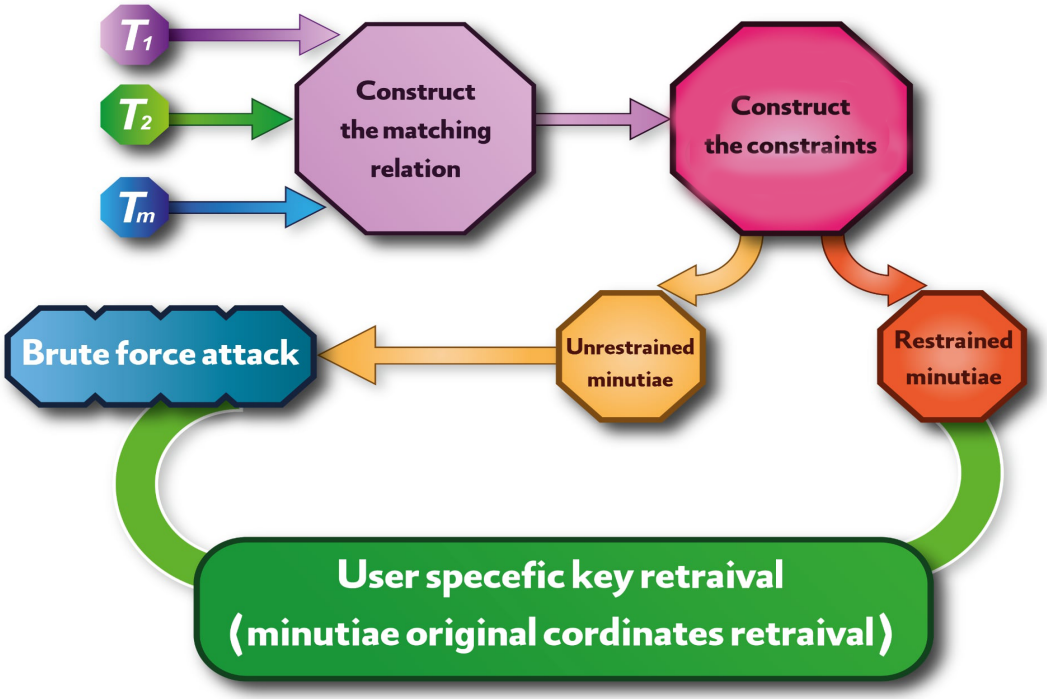


Figure 6.7: Attack Process Flow: The process begins with the construction of the matching relation, followed by the formulation of the equation system. It involves distinguishing between constrained and unconstrained minutiae points and applying a brute-force approach to reconstruct the fingerprint template

.

by each template. To ensure efficient processing and eliminate repetition, each unique piece of information should be handled once. This method employs a mathematical equivalence relation to group minutiae points, assigning a principal exemplar to each group. This strategy simplifies the retrieval process by focusing only on these representative minutiae rather than considering the entire set.

Let $S = \{p_k\}$ be a set of minutiae points, and define Δ as a matching relation over S, where each point $p_k \in S$ is associated with a corresponding point $p_l \in S$ through a fingerprint matching technique. The relation Δ can be regarded as an *equivalence relation* [89], as it satisfies the following criteria:

- **Reflexivity**: Every minutia point matches with itself.
- **Symmetry**: If a point p_k is matched with p_l, then p_l is also matched with p_k, for all $p_k, p_l \in S$.
- **Transitivity**: If p_k matches p_l, and p_l matches p_m, then p_k also matches p_m, for any $p_k, p_l, p_m \in S$.

These properties ensure that the relation Δ partitions the minutiae set S into equivalence classes, where each class contains minutiae corresponding to the same anatomical feature observed in different fingerprint impressions.

The initial phase of the retrieval process involves organizing all minutiae from the various fingerprint templates into distinct groups, referred to as the "matching class set." Within each

group, a single representative minutia termed the "exemplar minutia" is selected to stand for the entire class. Leveraging the transitivity property of the matching relation, each fingerprint template is compared with the others to identify sets of corresponding minutiae across templates, ultimately leading to the construction of these matching classes and the selection of their respective exemplars. Notably, an exemplar minutia encapsulates the common characteristics of matched minutiae appearing in multiple fingerprint samples.

Figure 6.8 depicts the established matching relation between fingerprint templates FP1 and FP2 shown in Figure 6.6. In this illustration, the minutiae points M_0^1, M_2^1, M_3^1, M_1^1, and M_3^2 serve as an exemplar minutiae in the original domain. These exemplars correspond to the equivalence classes $\{m_0^1, m_0^2\}$, $\{m_2^1, m_2^2\}$, $\{m_3^1, m_1^2\}$, $\{m_1^1\}$, and $\{m_3^2\}$, respectively.

In the transformed domain, the corresponding main exemplar minutiae are $M_0'^1$, $M_2'^1$, $M_3'^1$, $M_1'^1$, and $M_3'^2$, which represent the equivalence classes $\{m_0'^1, m_0'^2\}$, $\{m_2'^1, m_2'^2\}$, $\{m_3'^1, m_1'^2\}$, $\{m_1'^1\}$, and $\{m_3'^2\}$, respectively.

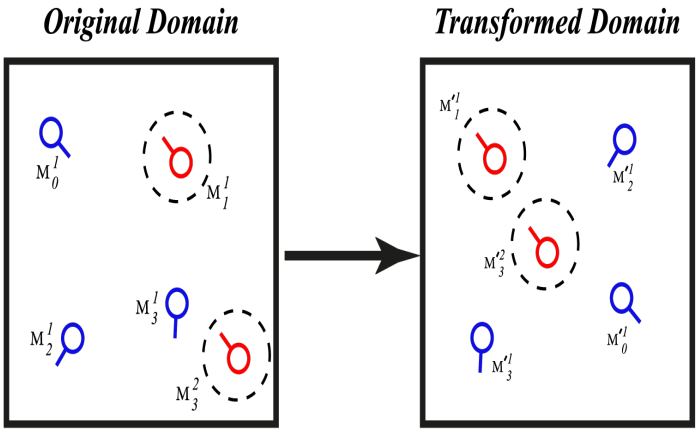


Figure 6.8: An illustrative example of a fingerprint template that demonstrates the use of the matching relation in both the original and transformed domains. In this case, each main exemplar minutia corresponds to a set of associated minutiae, defined as follows: $M_0^1 = \{m_0^1, m_0^2\}$, $M_1^1 = \{m_1^1\}$, $M_2^1 = \{m_2^1, m_2^2\}$, $M_3^1 = \{m_3^1, m_1^2\}$, and $M_3^2 = \{m_3^2\}$. A similar grouping is applied in the transformed domain, preserving the correspondence between matched minutiae across different fingerprint impressions.

6.5.2 Recovery Process

One key outcome of applying the matching relation in this context is the potential to uncover new insights regarding the correspondence between minutiae cells across different templates. As illustrated in Equation 6.1, consider an example where the original domain contains cells labeled [1, 2, 3, 4], and their respective transformed counterparts are [2, 1, 2, 3]. Each of these cells may hold one or more minutiae points, highlighting how transformations can result in reassignments that reflect underlying structural relation.

Additionally, as depicted in Figure 6.8, we consider M_0^1 to be a main exemplar minutia within the minutiae set of the original domain, associated with m_0^1 and m_0^2 at cell 1. Its transformed counterpart, $M_0'^1$, derived from the matching relation, serves as the exemplar minutia in a different cluster within the transformed domain, corresponding to $m_0'^1$ and $m_0'^2$ at cell 2. By

establishing the mapping of minutiae from cell 1 to cell 2, we can identify the complete set of correspondences from the equivalence class of M_0^1 to cell 2. equations 6.3 and 6.4 illustrate the cell's numbers of the representative minutiae and its equivalalence class.

$$CellNumber_O\{M_0^1\} = CellNumber_O\{m_0^1, m_0^2\} \tag{6.3}$$

$$CellNumber_T\{M_0'^1\} = CellNumber_T\{m_0'^1, m_0'^2\} \tag{6.4}$$

The key retrieval process leverages the matching relation and takes advantage of the lack of information sharing between different fingerprint templates. Each time the templates are compared, information is gathered about the transformation of minutiae cells that is, it constrains the mapping of certain sets of minutiae points, thereby narrowing down the possible transformations to a limited set or even a single cell (Reducing the search space of transformations.). As a result, this approach enables the exploration of cell mappings within the transformed domain, ultimately leading to the partial or full generation of the user key, depending on the number of templates available.

The complexity of the transformation matrix increases due to the inherent randomness, compounded by the fact that each cell may originate from one of approximately HW potential source cells, analyzing of cell transformations challenging. It is important to note that each column in the transformation matrix contains a 1, marking the cell's transformation, with all other entries being 0. By identifying the transformation of a given cell, we can pinpoint the location of the 1 in the matrix and generate the potential key by assuming the other entries are 0.

On the other hand, it is important to retrieve the original minutiae locations from the discovered constraints, which represent the mapping connections between the original and transformed minutiae points. As a result, a subset of minutiae points can be recovered using these constraints, while others remain confined within a limited set of transformed points. In such cases, a brute-force attack becomes the only viable approach, involving the substitution of potential values to explore possible solutions. Ultimately, this process yields a set of candidate solutions, among which the correct one is to be found.

6.6 Experimental Results and Discussion

This section provides an experimental assessment of the proposed attack on the Cartesian transformation.

6.6.1 Databases

The experimental evaluation is conducted using the Fingerprint Verification Competition (FVC) datasets from the years 2002, 2004, and 2006. Specifically, we utilize databases DB1_B, DB2 _B, DB3 _B, and DB4 _B from both FVC2002 and FVC2004, and databases DB2 _B, DB3 _B, and DB4 _B from FVC2006.

Each database in the FVC2002 and FVC2004 collections contains fingerprint images acquired from 100 distinct individuals, with 8 impressions per finger, totaling 800 images per dataset.

These datasets differ in sensor type and image quality, offering diverse acquisition conditions. In contrast, the FVC2006 dataset includes 12 images per subject and is designed to reflect more challenging scenarios, including higher variability in fingerprint impressions and the use of both real and synthetic data, thereby providing a more robust benchmark for performance evaluation.

6.6.2 Experiment results

The results presented in the table 6.1 demonstrate the effectiveness of the proposed attack algorithm. The implementation was carried out using MATLAB for extracting and matching minutiae points, following the method described in [105], while the remaining components of the algorithm were developed in Python (version 3) using the Jupyter environment.

The system used for testing features an Intel(R) Core(TM) i7-6700 processor running at 3.40 GHz, with 32 GB of RAM and operating on Windows 10.

Before running the experiments, each fingerprint undergoes a preprocessing phase, where minutiae and core points are extracted using the selected minutiae extraction technique. Afterward, a Cartesian transformation is applied to the extracted features using a randomly generated key unique to each subject. Both the original and transformed fingerprint templates are then utilized during the attack process.

6.6.2.1 Search Space Reduction via Multiple Template Utilization

The number of templates plays a crucial role in our attack strategy for narrowing the search space, as each additional template contributes new insights that help impose more constraints, thereby reducing the search space to a manageable size.

For example, the second subject in the FVC2002 DB1_B dataset has approximately 10^{31} potential combinations to impersonate the original fingerprint. This immense number makes it practically infeasible if not entirely impossible for an impostor to recover the genuine fingerprint. However, when eight different templates of the same fingerprint are utilized, the search space significantly narrows to around $10^7 \approx 8709120$ possibilities. This demonstrates a clear inverse correlation between the number of available templates and the resulting search space size.

Figure 6.9 illustrates how the search space decreases with the number of templates used for the second subject across the FVC2002, FVC2004, and FVC2006 databases.

Figure 6.10 demonstrates how the effectiveness of the proposed algorithm influences the reduction of the search space when applying multiple templates across the different databases. As shown, it is important to note that not all fingerprints are suitable for the recovery process, as some do not result in a sufficiently reduced search space. This limitation can be attributed to factors such as poor fingerprint quality or an insufficient number of extracted minutiae points. In such cases, a greater number of fingerprint templates beyond the eight initially used may be necessary to achieve a more manageable search space size.

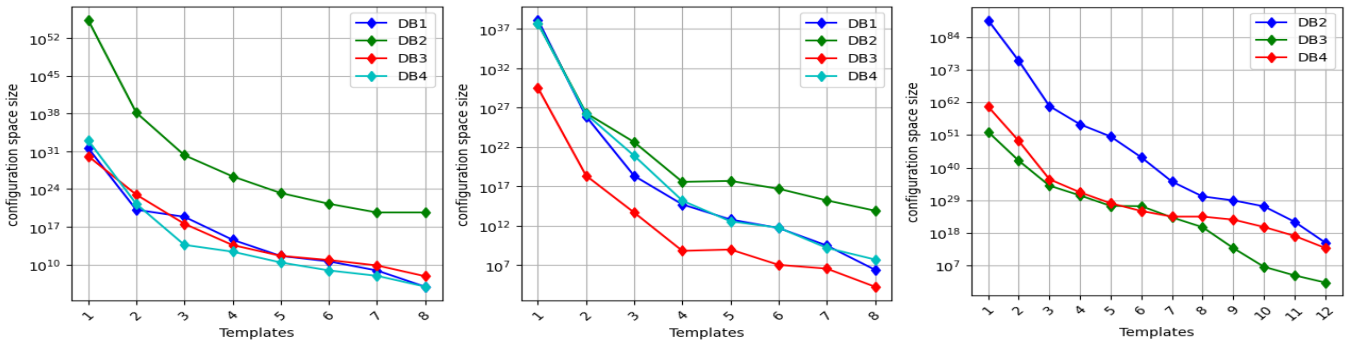


Figure 6.9: The Variation in Search Space Size for the Number of Transformed Templates Used to Impersonate Individuals in Different Datasets: (a) FVC2002(the second person) , (b) FVC2004(the first person) and (c) FVC2006 (the first person)

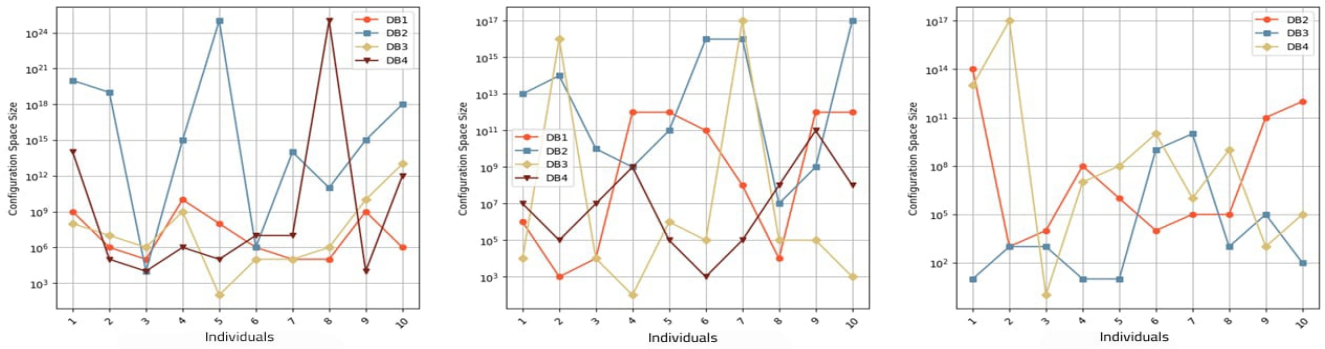


Figure 6.10: The count of potential configurations for each individual in every database, utilizing 8 transformed templates for FVC2002 and FVC2004, and 12 transformed templates for FVC2006.

6.6.2.2 Evaluating how the number of templates influences the number of constraints obtained

Defining the number of constraints is essential for the recovery process, as an increased number of constraints significantly enhances the likelihood of a successful reconstruction. Initially, when only a single template is available, the recovery process is nearly unconstrained, making it extremely difficult if not impossible to carry out a successful attack. Figure 6.11 presents how the number of inferred constraints progresses with the increasing number of templates for the first subject in each database of the FVC2002 dataset.

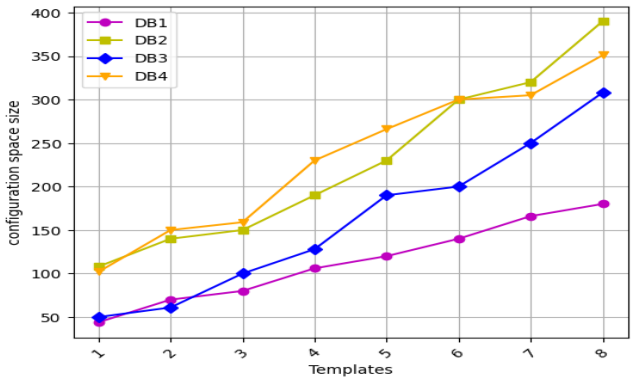


Figure 6.11: The progression of inferred constraints in relation to the number of transformed templates for the FVC2002 dataset.

6.6.2.3 Effectiveness of the Attack Algorithm

This section evaluates the performance of the proposed inversion attack using our minutiae-template reconstruction framework. To offer a qualitative perspective, example reconstructions are displayed in Figure 6.12. The attack's effectiveness is assessed using Spoof False Accept Rate (SFAR) and False Acceptance Increment (FAI), following evaluation approaches similar to those in [89],[79] and [109].

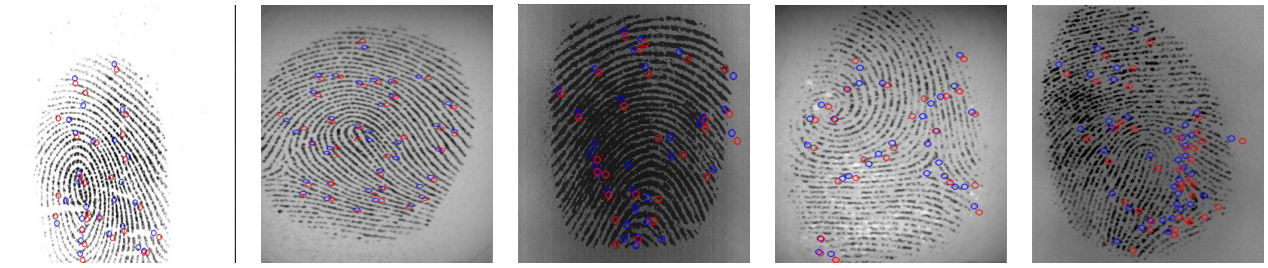


Figure 6.12: Reconstructed fingerprint images. Original minutiae in blue and the recovered minutiae in Red: (a) FVC2002 DB1, (b) FVC2002 DB2, (c) FVC2002 DB3, (d) FVC2002 DB4, (e) FVC2006 DB4

In our setup, the reconstructed template is matched against the original template of the corresponding subject. SFAR is defined as the proportion of impostor attempts that are wrongly accepted as genuine matches at the system's standard threshold derived from the Equal Error Rate (EER). This metric serves as an indicator of the system's vulnerability under attack conditions: a higher SFAR reflects greater susceptibility, while a lower value signifies stronger resilience.

Our experimental analysis spans multiple datasets, including FVC2002, FVC2004, and FVC2006. First, we compute the EER and the baseline False Acceptance Rate (FAR) under normal system operations. The decision threshold θ is then set based on the EER. Using this threshold, we conduct the attack and compare the reconstructed template with the original to calculate SFAR. The FAI is determined by the difference $FAI = SFAR - FAR$, as detailed in Table 6.1.

In a false accept scenario, an attacker with access to multiple transformed templates can attempt to breach the system by simulating authentication attempts. The likelihood of success in such attacks is influenced by the system's FAR, implying that one in approximately every $1/FAR$ attempt could result in unauthorized access.

In addition, we compare the performance of our algorithm with the attack methods described in [25] and [42], focusing specifically on the Spoof False Accept Rate (SFAR). A summary of the outcomes is presented in Table 6.2.

6.6.2.4 Performance Evaluation and Discussion

As outlined earlier, the instability and high intra-class variability of biometric templates along with the absence of several minutiae points due to poor sensor interaction can compromise the security of an individual's biometric data. This variability forms the core rationale behind our proposed targeted attack. The method proved effective on a wide range of fingerprint samples from the FVC2002, FVC2004, and FVC2006 databases. The key factor behind this success lies in the noticeable variations observed among different impressions of the same user's fingerprints, which were sufficient to enable data reconstruction through the attack.

Competition	**DB**	**Threshold** θ	**EER**	**FAR**	**SFAR**	**FAI**
FVC2002	DB1_B	0.64	3.68	1.25	60.00	58.75
	DB2_B	0.69	5.00	2.64	78.75	76.11
	DB3_B	0.66	8.75	7.22	80.14	72.92
	DB4_B	0.61	3.75	3.75	77.65	73.90
FVC2004	DB1_B	0.63	2.78	1.53	88.75	87.22
	DB2_B	0.68	7.89	9.56	65.69	56.13
	DB3_B	0.64	7.50	5.14	77.50	72.36
	DB4_B	0.61	1.32	1.39	80.00	78.61
FVC2006	DB2_B	0.68	2.31	2.78	68.33	65.55
	DB3_B	0.62	8.33	11.57	76.67	65.10
	DB4_B	0.65	6.67	9.17	84.17	75.00

Table 6.1: Attack evaluation on cartesian transformation(%)

	FVC2002			FVC2004			FVC2006		
	DB1	DB2	DB3	DB1	DB2	DB3	DB2	DB3	DB4
Quan et al[72]	44.2	45.0	83.6	62.4	59.4	44.6	16.2	69.4	76.2
Belhadj et al[89]	70.4	69.8	95.0	87.0	80.8	60.8	37.8	81.6	81.4
Proposed Attack	60.00	78.75	80.14	88.75	65.69	77.50	68.33	76.67	84.17

Table 6.2: A comparison of SFAR metric across different attack approaches

Nevertheless, we faced difficulties in reconstructing certain fingerprints from specific datasets. These issues stemmed from a lack of distinct features and limited variability between some samples belonging to the same individual. As a result, the evaluation of our attack limited to successfully reconstructed cases is illustrated through ROC curves presented in Figures 6.13, 6.14, and 6.15.

6.7 Conclusion

This chapter presents a security analysis of the cancelable biometrics scheme called cartesian transformation, originally introduced by Rtaha [8] Our study critically reexamines the irreversibility property of the CT scheme. Both theoretical and empirical findings demonstrate that CT is susceptible to reversibility attacks. The proposed attack exploits synchronization errors in minutiae alignment, which arise during the matching process in both the original and transformed domains across multiple fingerprint templates. The attack begins by identifying these errors and then categorizing the matched minutiae from different templates into key exemplar sets.By establishing links between templates in both domains, the transformation key is recovered, leading to the formulation of a set of constraints. These constraints enable the retrieval of certain original minutiae points. Moreover, the proposed attack is easy to implement and does not require extensive computational resources or processing time. This analysis

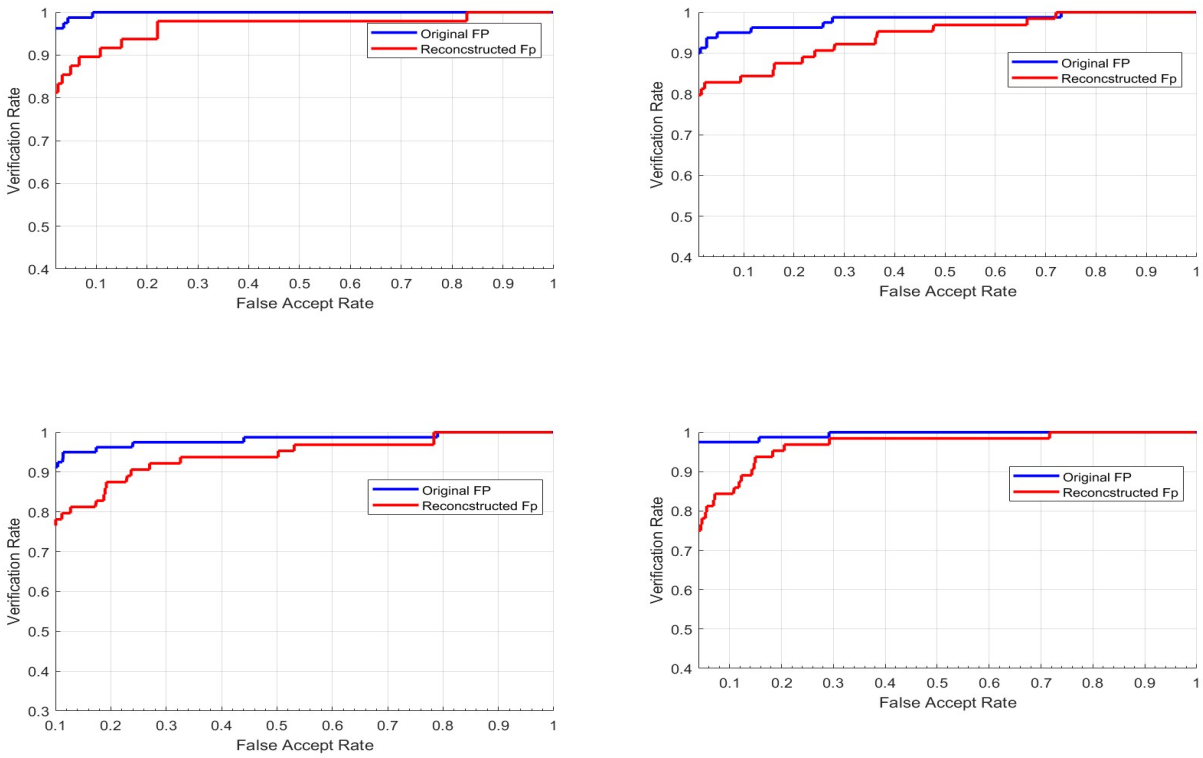


Figure 6.13: Comparison of ROC Curves for Original and Reconstructed Templates of the database FVC2002.

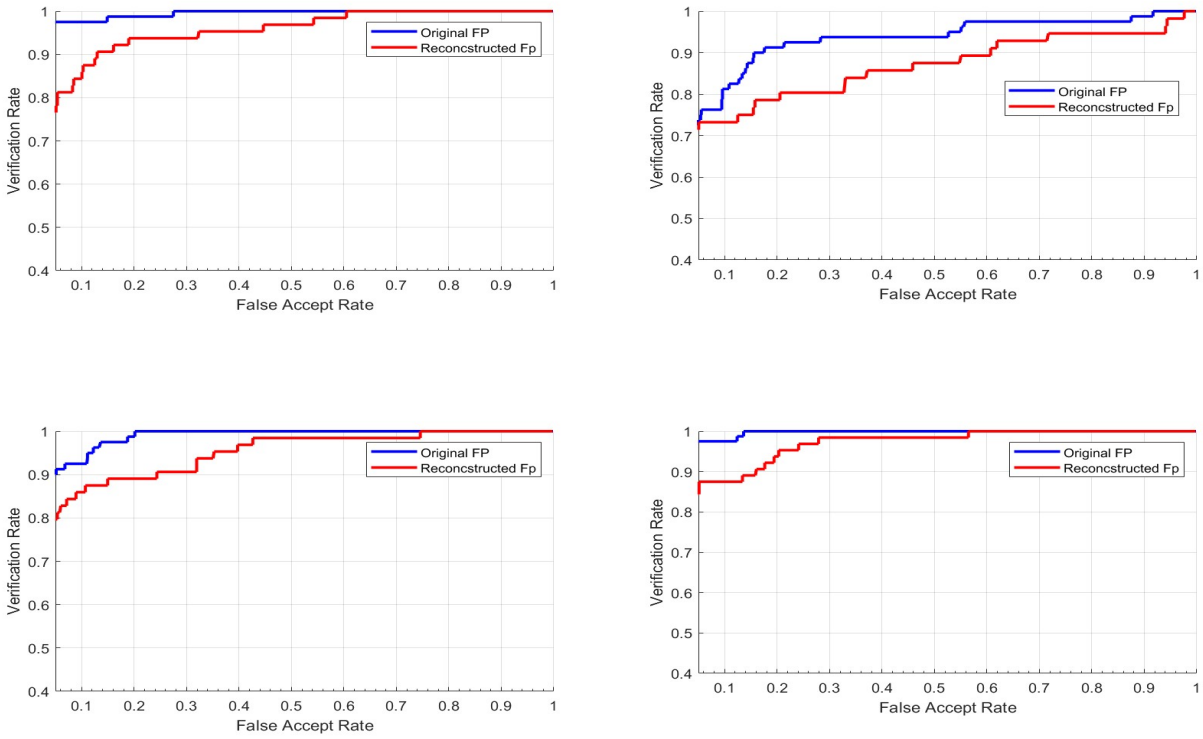


Figure 6.14: Comparison of ROC Curves for Original and Reconstructed Templates of the database FVC2004.

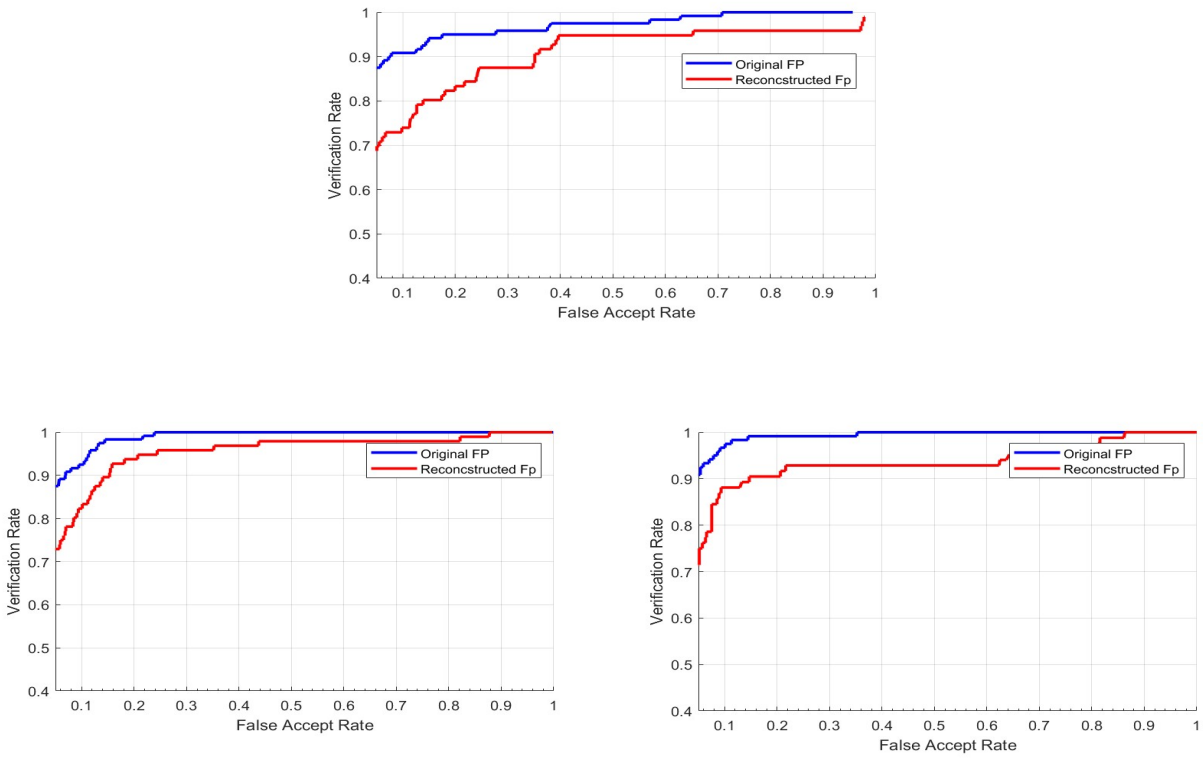


Figure 6.15: Comparison of ROC Curves for Original and Reconstructed Templates of the database FVC2006.

suggests that the CT scheme fails to ensure security and requires further evaluation. Specifically, the protection of the original template should be independent of key leakage to maintain privacy. In this regard, it is essential to ensure that the confidentiality of both the original template and the user's secret key remains unlinked. Additionally, evaluating the robustness of the transformed template demands thorough examination against established attack techniques and scenarios, necessitating careful assessment and in-depth study. Addressing these vulnerabilities is a critical direction for future research to enhance this CB scheme.

Chapter 7

General Conclusion

Biometrics play a crucial role in enhancing security and safeguarding individual privacy, with applications spanning various fields to authenticate personal data. They provide a reliable alternative to traditional authentication methods, such as passwords which are vulnerable to being lost or forgotten. However, the inherent weaknesses in biometric systems, such as susceptibility to spoofing or unauthorized access, highlight the urgent need for innovative methods to ensure robust protection of personal privacy. As such, efforts to develop advanced biometric protection mechanisms are increasingly critical to addressing these vulnerabilities and strengthening user security. For these reasons, cancelable biometric systems have been introduced as a secure and innovative alternative for protecting biometric data. However, despite their potential many cancelable biometric schemes have faced significant challenges in proving their effectiveness due to various vulnerabilities and the numerous attacks targeting these systems.

In this thesis, we focused on attacks targeting cancelable biometrics and the inherent vulnerabilities of these systems. While cancelable biometrics represent a promising approach, their effectiveness requires further investigation and study. In this thesis, our focus has been primarily directed toward addressing these main challenges :

- Examine the effectiveness of cancelable biometrics and investigate the various types of existing attacks along with their associated vulnerabilities : We conducted a comprehensive study of various attacks on cancelable biometric systems, analyzing in depth the biometric systems most vulnerable to such attacks and identifying the security weaknesses that make these protection methods susceptible. Highlighting these vulnerabilities aims to drive the development of more advanced and secure revoked biometric systems, ultimately strengthening user privacy and trust in biometric technologies. Additionally, we assessed the robustness of these systems against known attack methods and introduced a novel classification of attacks based on their methodologies. We also compared different types of attacks using established criteria to evaluate their severity and potential risks. Furthermore, we developed an evaluation framework based on strict criteria to assess the resilience of protection systems and mitigate various attacks.

- Cancelable palmprint protection scheme : Given the numerous vulnerabilities in existing protection systems, it is crucial to develop new methods that safeguard biometric data and resist attacks effectively. To address this, we have developed a protection system based on the Cartesian transformation of palmprints, offering enhanced security and privacy. This system transforms data extracted from palmprints, represented by minutiae points, into different locations using the Cartesian transformation function. This approach ensures the confidentiality of the original data by making it computationally infeasible to recover the original palmprint, even if the transformed template is compromised. Furthermore,

the system allows for the cancellation of a compromised template and the generation of a new one by simply updating the secret key used in the transformation function.

- Attack against cancelable biometric scheme: In this work, we presented an attack targeting a key-dependent cancelable fingerprint scheme initially introduced in [8]. Our analysis uncovered a significant vulnerability within the Cartesian transformation mechanism. Specifically, we demonstrated that although the user-specific secret key is intended to support the revocability of biometric templates, it inadvertently introduces a weakness that can compromise their security, potentially allowing for the reconstruction of the original fingerprint data. The proposed attack takes advantage of the improperly isolated information shared across different fingerprint templates belonging to the same individual. By exploiting this gap, we were able to reconstruct the secret key and consequently regenerate the protected fingerprint templates.

7.1 Perspectives and future researche

The current work paves the way for many future research directions, including :

- The use of hybrid systems and multibiometric approaches represents a critical area for future research, aiming to enhance the security and robustness of biometric systems. By combining different biometric modalities, such as fingerprints, facial recognition, and iris scans, with non-invertible transformations, these systems can provide stronger protection against attacks like forgery and identity theft. Moreover, hybrid systems can improve security by making it significantly harder to reverse-engineer biometric templates or track users, thereby mitigating the severity of potential attacks.

- Addressing the trade-off between security and accuracy remains a critical challenge in cancelable biometrics that demands significant attention. Enhancing security measures often comes at the expense of system performance, potentially reducing accuracy and usability, while prioritizing accuracy can leave systems vulnerable to attacks. Future research should focus on developing a protection method that ensures both high security and reliable performance.

- A future research direction is to investigate cancelable protection systems to identify vulnerabilities and safeguard against a broader range of potential attacks. Additionally, it is essential to develop advanced protection mechanisms specifically designed to counteract the types of attacks discussed in this thesis.

- Most attacks on cancelable biometrics rely on the attacker's knowledge of specific parameters, such as the secret key, transformation function, or transformed template. Therefore, it is crucial to address this issue by enhancing the security of cancelable systems and by developing attack models that are independent of these parameters.

Bibliography

[1] Amanpreet A Kaur and Khurram K Mustafa. A critical appraisal on password based authentication. *International Journal of Computer Network and Information Security*, 11(1):47, 2019.

[2] Hilarie Orman. The morris worm: A fifteen-year perspective. *IEEE Security & Privacy*, 1(5):35–43, 2003.

[3] Anil K Jain, Arun Ross, and Salil Prabhakar. An introduction to biometric recognition. *IEEE Transactions on circuits and systems for video technology*, 14(1):4–20, 2004.

[4] Davide Maltoni, Dario Maio, Anil K Jain, Salil Prabhakar, et al. *Handbook of fingerprint recognition*, volume 2. Springer, 2009.

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

[6] Manisha and Nitin Kumar. Cancelable biometrics: a comprehensive survey. *Artificial Intelligence Review*, 53(5):3403–3446, 2020.

[7] IEC ISO and Partie CEI. Iso/iec directives part1. 2009.

[8] Nalini K Ratha, Sharat Chikkerur, Jonathan H Connell, and Ruud M Bolle. Generating cancelable fingerprint templates. *IEEE Transactions on pattern analysis and machine intelligence*, 29(4):561–572, 2007.

[9] AK Jain. Handbook of biometrics. *Springer google schola*, 2:114–116, 2007.

[10] Suo Jidong and Liu Xiaoming. Fusion of radar and ais data. In *Proceedings 7th International Conference on Signal Processing, 2004. Proceedings. ICSP'04. 2004.*, volume 3, pages 2604–2607. IEEE, 2004.

[11] Karthik Nandakumar, Arun Ross, and Anil K Jain. Biometric fusion: Does modeling correlation really matter? In *2009 IEEE 3rd International Conference on Biometrics: Theory, Applications, and Systems*, pages 1–6. IEEE, 2009.

[12] Zaheer Ahmad, Muhammad Ajmal, Farooq Ahmad, Muhammad Hasanain Chaudary, and Mudasser Naseer. Comparative analysis of biometric recognition techniques. *Bahria University Journal of Information & Communication Technologies (BUJICT)*, 11(1):21–30, 2018.

[13] Nikolaos V Boulgouris, Konstantinos N Plataniotis, and Evangelia Micheli-Tzanakou. *Biometrics: theory, methods, and applications*. John Wiley & Sons, 2009.

[14] Dario Maio, Davide Maltoni, Raffaele Cappelli, Jim L Wayman, and Anil K Jain. Fvc2004: Third fingerprint verification competition. In *International conference on biometric authentication*, pages 1–7. Springer, 2004.

[15] Ruud M Bolle, Jonathan H Connell, and Nalini K Ratha. Biometric perils and patches. *Pattern recognition*, 35(12):2727–2738, 2002.

[16] RT Pratyush, A Dhruv, J Prakhar, D Swagam, D Preetha, R Vineet, et al. India's aadhaar biometric id: Structure, security, and vulnerabilities', 2022.

[17] Vidar Ajaxon Grønland, Havard Hasli, and Jon Fredrik Pettersen. Challenging fingerprint scanner. *October16*, 2005.

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

[19] Nalini K Ratha, Jonathan H Connell, and Ruud M Bolle. An analysis of minutiae matching strength. In *Audio-and Video-Based Biometric Person Authentication: Third International Conference, AVBPA 2001 Halmstad, Sweden, June 6–8, 2001 Proceedings 3*, pages 223–228. Springer, 2001.

[20] Claude Barral and Assia Tria. Fake fingers in fingerprint recognition: Glycerin supersedes gelatin. *Formal to Practical Security: Papers Issued from the 2005-2008 French-Japanese Collaboration*, pages 57–69, 2009.

[21] Tsutomu Matsumoto, Hiroyuki Matsumoto, Koji Yamada, and Satoshi Hoshino. Impact of artificial" gummy" fingers on fingerprint systems. In *Optical security and counterfeit deterrence techniques IV*, volume 4677, pages 275–289. SPIE, 2002.

[22] EA Maro and MM Kovalchuk. Bypass mobile lock systems with gelatin artificial fingerprint. *Int. J. Comput. Sci. Eng*, 6(6):32–36, 2018.

[23] Rubal Jain and Chander Kant. Attacks on biometric systems: an overview. *International Journal of Advances in Scientific Research*, 1(07):283–288, 2015.

[24] Umut Uludag and Anil K Jain. Attacks on biometric systems: a case study in fingerprints. In *Security, steganography, and watermarking of multimedia contents VI*, volume 5306, pages 622–633. SPIE, 2004.

[25] Javier Galbally. *Vulnerabilities and attack protection in security systems based on biometric recognition*. Javier Galbally, 2009.

[26] Colin Soutar, Danny Roberge, Alex Stoianov, Rene Gilroy, and Bhagavatula Vijaya Kumar. Biometric encryption using image processing. In *Optical Security and Counterfeit Deterrence Techniques II*, volume 3314, pages 178–188. SPIE, 1998.

[27] Vishal M Patel, Nalini K Ratha, and Rama Chellappa. Cancelable biometrics: A review. *IEEE signal processing magazine*, 32(5):54–65, 2015.

[28] Juan Carlos Bernal-Romero, Juan Manuel Ramirez-Cortes, Jose De Jesus Rangel-Magdaleno, Pilar Gomez-Gil, Hayde Peregrina-Barreto, and Israel Cruz-Vega. A review on protection and cancelable techniques in biometric systems. *Ieee Access*, 11:8531–8568, 2023.

[29] Anil K Jain, Arun Ross, and Umut Uludag. Biometric template security: Challenges and solutions. In *2005 13th European signal processing conference*, pages 1–4. IEEE, 2005.

[30] Karthik Nandakumar, Abhishek Nagar, and Anil K Jain. Hardening fingerprint fuzzy vault using password. In *Advances in Biometrics: International Conference, ICB 2007, Seoul, Korea, August 27-29, 2007. Proceedings*, pages 927–937. Springer, 2007.

[31] Prabhjot Kaur, Nitin Kumar, and Maheep Singh. Biometric cryptosystems: a comprehensive survey. *Multimedia Tools and Applications*, 82(11):16635–16690, 2023.

[32] Ari Juels and Madhu Sudan. A fuzzy vault scheme. *Designs, Codes and Cryptography*, 38:237–257, 2006.

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

[34] SP Ragendhu, Tony Thomas, and Sabu Emmanuel. Cancelable biometric template generation using random feature vector transformations. *IEEE Access*, 2024.

[35] Christophe Rosenberger. Evaluation of biometric template protection schemes based on a transformation. In *ICISSP*, pages 216–224, 2018.

[36] Abhishek Nagar, Karthik Nandakumar, and Anil K Jain. Biometric template transformation: a security analysis. In *Media Forensics and Security II*, volume 7541, pages 237–251. SPIE, 2010.

[37] Andrew Teoh Beng Jin and Lim Meng Hui. Cancelable biometrics. *Scholarpedia*, 5(1):9201, 2010.

[38] Tohari Ahmad, Jiankun Hu, and Song Wang. Pair-polar coordinate-based cancelable fingerprint templates. *Pattern recognition*, 44(10-11):2555–2564, 2011.

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

[40] Chulhan Lee, Jeung-Yoon Choi, Kar-Ann Toh, Sangyoun Lee, and Jaihie 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.

[41] Huijuan Yang, Xudong Jiang, and Alex 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.

[42] Matteo Ferrara, Davide Maltoni, and Raffaele Cappelli. Noninvertible minutia cylinder-code representation. *IEEE Transactions on Information Forensics and Security*, 7(6):1727–1737, 2012.

[43] Raffaele Cappelli, Matteo Ferrara, and Davide 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.

[44] Osama Ouda, Norimichi Tsumura, and Toshiya Nakaguchi. Tokenless cancelable biometrics scheme for protecting iris codes. In *2010 20th international conference on pattern recognition*, pages 882–885. IEEE, 2010.

[45] Dongdong Zhao, Shu Fang, Jianwen Xiang, Jing Tian, and Shengwu Xiong. Iris template protection based on local ranking. *Security and Communication Networks*, 2018(1):4519548, 2018.

[46] Ragendhu SP and Tony Thomas. Cancelable biometric scheme based on dynamic salting of random patches. *Multimedia Tools and Applications*, 82(10):14337–14366, 2023.

[47] Gourav Siddhad, Pritee Khanna, and Aparajita Ojha. Cancelable biometric template generation using convolutional autoencoder. In *International Conference on Computer Vision and Image Processing*, pages 303–314. Springer, 2020.

[48] Wencheng Yang, Song Wang, Jiankun Hu, Xiaohui Tao, and Yan Li. Feature extraction and learning approaches for cancellable biometrics: A survey. *CAAI Transactions on Intelligence Technology*, 9(1):4–25, 2024.

[49] Christian Rathgeb, Frank Breitinger, and Christoph Busch. Alignment-free cancelable iris biometric templates based on adaptive bloom filters. In *2013 international conference on biometrics (ICB)*, pages 1–8. IEEE, 2013.

[50] David CL Ngo, Andrew BJ Teoh, and Alwyn Goh. Biometric hash: high-confidence face recognition. *IEEE transactions on circuits and systems for video technology*, 16(6):771–775, 2006.

[51] Zhe Jin, Jung Yeon Hwang, Yen-Lung Lai, Soohyung Kim, and Andrew Beng Jin 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.

[52] Jaishanker K Pillai, Vishal M Patel, Rama Chellappa, and Nalini K Ratha. Sectored random projections for cancelable iris biometrics. In *2010 IEEE International Conference on Acoustics, Speech and Signal Processing*, pages 1838–1841. IEEE, 2010.

[53] Xingbo Dong, KokSheik Wong, Zhe Jin, and Jean-luc Dugelay. A cancellable face template scheme based on nonlinear multi-dimension spectral hashing. In *2019 7th International Workshop on Biometrics and Forensics (IWBF)*, pages 1–6. IEEE, 2019.

[54] Yen-Lung Lai, Zhe Jin, Andrew Beng Jin Teoh, Bok-Min Goi, Wun-She Yap, Tong-Yuen Chai, and Christian Rathgeb. Cancellable iris template generation based on indexing-first-one hashing. *Pattern Recognition*, 64:105–117, 2017.

[55] Jinyuan Liu, Yong Wang, Kun Wang, and Zhuo Liu. An irreversible and revocable template generation scheme based on chaotic system. *Entropy*, 25(2):378, 2023.

[56] T Boult. Robust distance measures for face-recognition supporting revocable biometric tokens. In *7th International Conference on Automatic Face and Gesture Recognition (FGR06)*, pages 560–566. IEEE, 2006.

[57] Terrance E Boult, Walter J Scheirer, and Robert Woodworth. Revocable fingerprint biotokens: Accuracy and security analysis. In *2007 IEEE Conference on Computer Vision and Pattern Recognition*, pages 1–8. IEEE, 2007.

[58] Wei Jing Wong, ML Dennis Wong, and Andrew Beng Jin Teoh. A security-and privacy-driven hybrid biometric template protection technique. In *2014 International Conference on Electronics, Information and Communications (ICEIC)*, pages 1–5. IEEE, 2014.

[59] Padma Polash Paul and Marina Gavrilova. Multimodal cancelable biometrics. In *2012 IEEE 11th international conference on cognitive informatics and cognitive computing*, pages 43–49. IEEE, 2012.

[60] Padma Polash Paul and Marina Gavrilova. Rank level fusion of multimodal cancelable biometrics. In *2014 IEEE 13th International Conference on Cognitive Informatics and Cognitive Computing*, pages 80–87. IEEE, 2014.

[61] Padma Polash Paul, Marina Gavrilova, and Stanslav Klimenko. Situation awareness through multimodal biometric template security in real-time environments. In *2013 International Conference on Cyberworlds*, pages 82–88. IEEE, 2013.

[62] Yong Jian Chin, Thian Song Ong, Andrew Beng Jin Teoh, and Michael KO Goh. Multimodal biometrics based bit extraction method for template security. In *2011 6th IEEE Conference on Industrial Electronics and Applications*, pages 1971–1976. IEEE, 2011.

[63] Harkeerat Kaur and Pritee Khanna. Random distance method for generating unimodal and multimodal cancelable biometric features. *IEEE Transactions on Information Forensics and Security*, 14(3):709–719, 2018.

[64] P Suresh and KR Radhika. Bio-metric credential system: Multimodal cancelable anonymous identity management. In *2015 IEEE International Advance Computing Conference (IACC)*, pages 353–356. IEEE, 2015.

[65] Andrew BJ Teoh, Alwyn Goh, and David CL Ngo. Random multispace quantization as an analytic mechanism for biohashing of biometric and random identity inputs. *IEEE transactions on pattern analysis and machine intelligence*, 28(12):1892–1901, 2006.

[66] Andrew Teoh Beng Jin, David Ngo Chek Ling, and Alwyn Goh. Biohashing: two factor authentication featuring fingerprint data and tokenised random number. *Pattern recognition*, 37(11):2245–2255, 2004.

[67] Matteo Ferrara, Davide Maltoni, and Raffaele 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.

[68] Priyanka Das, Kannan Karthik, and Boul Chandra Garai. A robust alignment-free fingerprint hashing algorithm based on minimum distance graphs. *Pattern Recognition*, 45(9):3373–3388, 2012.

[69] M Aydar, SC Cetin, S Ayvaz, and B Aygun. Private key encryption and recovery in blockchain. arxiv 2019. *arXiv preprint arXiv:1907.04156*.

[70] Sang Wook Shin, Mun-Kyu Lee, Daesung Moon, and Kiyoung Moon. Dictionary attack on functional transform-based cancelable fingerprint templates. *ETRI journal*, 31(5):628–630, 2009.

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

[72] Feng Quan, Su Fei, Cai Anni, and Zhao Feifei. Cracking cancelable fingerprint template of ratha. In *2008 International Symposium on Computer Science and Computational Technology*, volume 2, pages 572–575. IEEE, 2008.

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

[74] Osama Ouda, Norimichi Tsumura, and Toshiya Nakaguchi. On the security of bioencoding based cancelable biometrics. *IEICE TRANSACTIONS on Information and Systems*, 94(9):1768–1777, 2011.

[75] Dongdong Zhao, Wenjian Luo, Ran Liu, and Lihua Yue. Negative iris recognition. *IEEE Transactions on Dependable and Secure Computing*, 15(1):112–125, 2015.

[76] X Dong, Z Jin, ABJ Teoh, M Tistarelli, and K Wong. On the security risk of cancelable biometrics. *arXiv preprint arXiv:1910.07770*, 2019.

[77] Saloni Nanwate and Debanjan Sadhya. Similarity attack on cancelable biometric templates using particle swarm optimization. In *2020 IEEE International Conference on Computing, Power and Communication Technologies (GUCON)*, pages 693–697. IEEE, 2020.

[78] Hanrui Wang, Xingbo Dong, Zhe Jin, Andrew Beng Jin Teoh, and Massimo Tistarelli. Interpretable security analysis of cancellable biometrics using constrained-optimized similarity-based attack. In *Proceedings of the IEEE/CVF Winter Conference on Applications of Computer Vision*, pages 70–77, 2021.

[79] Xingbo Dong, Zhe Jin, and Andrew Teoh Beng Jin. A genetic algorithm enabled similarity-based attack on cancellable biometrics. In *2019 IEEE 10th International Conference on Biometrics Theory, Applications and Systems (BTAS)*, pages 1–8. IEEE, 2019.

[80] Patrick Lacharme, Estelle Cherrier, and Christophe Rosenberger. Preimage attack on biohashing. In *2013 International Conference on Security and Cryptography (SECRYPT)*, pages 1–8. IEEE, 2013.

[81] Yongjin Lee, Yunsu Chung, and Kiyoung 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.

[82] Loubna Ghammam, Koray Karabina, Patrick Lacharme, and Kevin Thiry-Atighehchi. A cryptanalysis of two cancelable biometric schemes based on index-of-max hashing. *IEEE Transactions on Information Forensics and Security*, 15:2869–2880, 2020.

[83] Yi C Feng, Meng-Hui Lim, and Pong C Yuen. Masquerade attack on transform-based binary-template protection based on perceptron learning. *Pattern Recognition*, 47(9):3019–3033, 2014.

[84] Berkay Topcu, Cagatay Karabat, Matin Azadmanesh, and Hakan Erdogan. Practical security and privacy attacks against biometric hashing using sparse recovery. *EURASIP Journal on Advances in Signal Processing*, 2016:1–20, 2016.

[85] Andras Rozsa, Albert E Glock, and Terrance E Boult. Genetic algorithm attack on minutiae-based fingerprint authentication and protected template fingerprint systems. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops*, pages 100–108, 2015.

[86] Walter J Scheirer and Terrance E Boult. Bipartite biotokens: Definition, implementation, and analysis. In *International Conference on Biometrics*, pages 775–785. Springer, 2009.

[87] Osama Ouda. On the practicality of local ranking-based cancelable iris recognition. *IEEE Access*, 9:86392–86403, 2021.

[88] Patrick Lacharme. Analysis of the iriscodes bioencoding scheme. *Int. J. Comput. Sci. Softw. Eng.(IJCSSE 2012)*, 6(5):315–321, 2012.

[89] Foudil Belhadj and Adel Moussaoui. Attack via missed record synchronization on transformation-based fingerprint template protection algorithms. *Multimedia Tools and Applications*, 83(9):27543–27563, 2024.

[90] Tetsuya Izu, Yumi Sakemi, Masahiko Takenaka, and Naoya Torii. A spoofing attack against a cancelable biometric authentication scheme. In *2014 IEEE 28th International Conference on Advanced Information Networking and Applications*, pages 234–239. IEEE, 2014.

[91] Mitsuhiro Hattori, Nori Matsuda, Takashi Ito, Yoichi Shibata, Katsuyuki Takashima, and Takeshi Yoneda. Provably-secure cancelable biometrics using 2-dnf evaluation. *Information and Media Technologies*, 7(2):749–760, 2012.

[92] Axel Durbet, Pascal Lafourcade, Denis Migdal, Kevin Thiry-Atighehchi, and Paul-Marie Grollemund. Authentication attacks on projection-based cancelable biometric schemes. *arXiv preprint arXiv:2110.15163*, 2021.

[93] Jens Hermans, Bart Mennink, and Roel Peeters. When a bloom filter is a doom filter: security assessment of a novel iris biometric template protection system. In *2014 international conference of the biometrics special interest group (BIOSIG)*, pages 1–6. IEEE, 2014.

[94] Christian Rathgeb, Frank Breitinger, Christoph Busch, and Harald Baier. On application of bloom filters to iris biometrics. *IET Biometrics*, 3(4):207–218, 2014.

[95] Javier Ortega-Garcia, Julian Fierrez, Fernando Alonso-Fernandez, Javier Galbally, Manuel R Freire, Joaquin Gonzalez-Rodriguez, Carmen Garcia-Mateo, Jose-Luis Alba-Castro, Elisardo Gonzalez-Agulla, Enrique Otero-Muras, et al. The multiscenario multienvironment biosecure multimodal database (bmdb). *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 32(6):1097–1111, 2009.

[96] Dilip Kumar Vallabhadas, Mulagala Sandhya, Sudireddy Dinesh Reddy, Davala Satwika, and Gatram Lakshmi Prashanth. Biometric template protection based on a cancelable convolutional neural network over iris and fingerprint. *Biomedical Signal Processing and Control*, 91:106006, 2024.

[97] Gerges M Salama, Safaa El-Gazar, Basma Omar, and AA Hassan. Multimodal cancelable biometric authentication system based on eeg signal for iot applications. *Journal of Optics*, 53(3):1839–1853, 2024.

[98] Quang Nhat Tran and Jiankun Hu. A multi-filter fingerprint matching framework for cancelable template design. *IEEE Transactions on Information Forensics and Security*, 16:2926–2940, 2021.

[99] Wencheng Yang, Song Wang, Muhammad Shahzad, and Wei Zhou. A cancelable biometric authentication system based on feature-adaptive random projection. *Journal of Information Security and Applications*, 58:102704, 2021.

[100] Hengyi Ren, Lijuan Sun, Jian Guo, Chong Han, and Fan Wu. Finger vein recognition system with template protection based on convolutional neural network. *Knowledge-based systems*, 227:107159, 2021.

[101] Zineb Maaref, Abdelouahab Attia, and Foudil Belhadj. Generating cancelable multispectral palmprint templates based on cartesian transformation. In *2023 5th International Conference on Pattern Analysis and Intelligent Systems (PAIS)*, pages 1–7, 2023.

[102] Ziyuan Yang, Ming Kang, Andrew Beng Jin Teoh, Chengrui Gao, Wen Chen, Bob Zhang, and Yi Zhang. A dual-level cancelable framework for palmprint verification and hack-proof data storage. *arXiv preprint arXiv:2403.02680*, 2024.

[103] Hanaa S Ali, Eman I Elhefnawy, and Mohammed Abo-Zahhad. Cancelable palmprint: intelligent framework toward secure and privacy-aware recognition system. *EURASIP Journal on Information Security*, 2024(1):31, 2024.

[104] David Zhang, Wangmeng Zuo, and Feng Yue. A comparative study of palmprint recognition algorithms. *ACM computing surveys (CSUR)*, 44(1):1–37, 2012.

[105] Vahid K Alilou. Fingerprint matching: A simple approach. *Mathwork*, 2020.

[106] David Zhang, Zhenhua Guo, Guangming Lu, Lei Zhang, and Wangmeng Zuo. An online system of multispectral palmprint verification. *IEEE transactions on instrumentation and measurement*, 59(2):480–490, 2009.

[107] Zineb Maaref, Foudil Belhadj, Abdelouahab Attia, Zahid Akhtar, Muhammed Basheer Jasser, Athirah Mohd Ramly, and Ali Wagdy Mohamed. A comprehensive review of vulnerabilities and attack strategies in cancelable biometric systems. *Egyptian Informatics Journal*, 27:100511, 2024.

[108] Dario Maio, Davide Maltoni, Raffaele Cappelli, James L Wayman, and Anil K Jain. Fvc2002: Second fingerprint verification competition. In *2002 International conference on pattern recognition*, volume 3, pages 811–814. IEEE, 2002.

[109] Sani M Abdullahi, Shuifa Sun, Hongxia Wang, and Beng Wang. The reversibility of cancelable biometric templates based on iterative perturbation stochastic approximation strategy. *Pattern Recognition Letters*, 172:221–229, 2023.