The Security and Privacy of Unimodal and Multimodal Biometrics

Lee Ming Jie

A thesis submitted for the degree of Doctor of Philosophy at

Monash University in 2021

School of Information Technology

Monash University Malaysia

Copyright notice

© Lee Ming Jie 2021.

I certify that I have made all reasonable efforts to secure copyright permissions for third-party content included in this thesis and have not knowingly added copyright content to my work without the owner's permission.

TABLE OF CONTENTS

ABSTRACT

Biometric-based authentication has been massively deployed and played an essential part in our daily applications attributed to its convenience and decent verification performance. With the increasing deployment of biometric template storage, the security and privacy of biometric data have become more critical. Specifically, a stolen biometric template could lead to damaging events, e.g., permanent identity loss. Therefore, we must consider biometric template protection (BTP) to address potential threats. Although many BTP methods can be found in the literature, BTP is still an open issue, and there are still many unsolved problems. This thesis was established to study the security and privacy of the biometric system in terms of biometric template security. Throughout this research, there are three research outcomes. This thesis covers different mainstream biometric modalities, i.e., face, fingerprint, and iris. Proposals of this thesis are validated on several benchmarking datasets, including Fingerprint FVC, Face LFW, and Iris CASIA.

In the first work, the main issue in the irisCode template protection, i.e., alignment-issue, is studied. Despite there are many iris template protection schemes reported, many schemes are not capable of handling the misalignment of the iris. As such, many iris BTP schemes require a pre-alignment process in which the computation overhead is increased. In this case, a new irisCode template protection scheme, namely, Random Augmented Histogram of Oriented Gradient (R·HoG), is introduced. The R·HoG is an alignment-robust biometric template protection scheme that could directly produce a cancellable template from the unaligned irisCode. Experiments are carried out to examine the verification performance of the biometric system after applying the proposed R·HoG. The results show the proposed R·HoG could maintain the matching performance, with the EER=0.62%. Other than that, the authentication process of R·HoG is efficient, with 0.0916 seconds in the enrollment stage and 0.0811 seconds in the verification stage.

In the second work, the problems of token management and feature incompatibility in the face and fingerprint-based template protection are addressed. A BTP scheme is usually designed as a two-factor authentication approach that is inconvenient when the user has to keep multiple tokens that are used for corresponding systems. Another problem in this work is the performance skewness of the feature incompatibility problem in which the verification performance of the fused cancellable template could be similar to the biometric feature that

holds wider value distribution. Motivated by these problems, two tokenless template protection schemes: Extended Feature Vector (EFV) hashing and Multimodal Feature Vector (M·EFV) hashing are introduced for the face and fingerprint modalities. The proposed schemes are tokenless template protection in which the original transformation key is never stored or distributed. Experiments are conducted, and the results show both EFV and M·EFV hashing possess decent verification performance. In particular, M·EFV hashing could achieve the best matching accuracy with EER= $0.24\% \pm 0.10$ in FVC2002 + LFW dataset.

In the third work, the “tradeoff between security and performance” problem in biometric template protection is addressed. This work is divided into two parts corresponding to the contributions iii and iv in this thesis, i.e., an enhanced matching mechanism (contribution iii) and authentication attack (contribution iv). For the first part, the problem is the weak decision environment problem (low decidability) in which the overlap region between the genuine and impostor score distributions is large. An enhanced matching mechanism is introduced to improve the decidability of the cancellable biometric schemes. The results show the verification performance of the tested schemes is improved. For instance, in M·EFV hashing-based multimodal system, the matching accuracy of FVC2004 DB1 + LFW is improved from $\mathrm{EER} = 0.38\%$ to $\mathrm{EER} = 0.11\%$; while the decidability is improved from $d' = 5.37$ to $d' = 9.62$. It is observed that the enhanced matching mechanism enables the selection of a high matching threshold in the cancellable biometric scheme. For example, in M·EFV hashing-based multimodal system, the system threshold could be increased from 0.6400 to 0.8000 with a 5% reduction of GAR after applying the enhanced matching mechanism. For the second part, an automated authentication attack, namely the Whale Optimization Algorithm-based Authentication Attack (WO3A), is formalized to testify and quantify the security of the cancellable biometric schemes and enhanced matching mechanism experimentally.

Since the subject of the study is biometric template protection, the proposed biometric template protection schemes are examined based on the irreversibility, unlinkability, renewability .and performance preservation as listed in the ISO/IEC Standard 24745 and 30136. Various major security attacks are considered when evaluating the proposed schemes. Template inversion attacks via single and multiple records (ARM) are studied. Unlinkability and renewability of the template protection schemes are evaluated based on the benchmarking analysis framework.

DECLARATION

This thesis is an original work of my research and contains no material which has been accepted for the award of any other degree or diploma at any university or equivalent institution and that, to the best of my knowledge and belief, this thesis contains no material previously published or written by another person, except where due reference is made in the text of the thesis.

Signature: ……………………

Print Name: Lee Ming Jie ………………….

Date: 19-11-2021 ………………………….

LIST OF PUBLICATIONS AND OUTPUTS

Publications directly relevant to this thesis

[1] **M. J. Lee**, Z. Jin, and A. B. J. Teoh, “One-factor Cancellable Scheme for Fingerprint Template Protection: Extended Feature Vector (EFV) Hashing,” in **2018 IEEE International Workshop on Information Forensics and Security (WIFS)**, 2018, pp. 1-7

[2] **M. J. Lee**, Z. Jin, M. Li, and D. BW. Chen “Mixing Binary Face and Fingerprint based on Extended Feature Vector (EFV) Hashing” in **2019 International Symposium on Intelligent Signal Processing and Communications Systems (ISPACS)**, 2019

[3] **M.J. Lee**, A.B.J. Teoh, A. Uhl, S.-N. Liang, Z. Jin, A Tokenless Cancellable Scheme for Multimodal Biometric Systems, **Computers & Security**. 108 (2021) 102350. https://doi.org/https://doi.org/10.1016/j.cose.2021.102350.

Submitted manuscript directly relevant to this thesis

M. J. Lee, S.-N. Liang, M. Tistarelli, and Z. Jin, “Alignment-robust Cancellable Biometric Scheme for Iris Verification”, Submitted to **IEEE Transaction on Information Forensics and Security (TIFS) (2021)**.

M. J. Lee, S.-N. Liang, Y.-L. Lai, Z. Jin, and M. Li, “Authentication attack and enhancement on cancellable biometrics in decision environment”, Submitted to **IEEE Transaction on Information Forensics and Security (TIFS) (2021)**.

Award and achievement

Recipient of Monash Merit Scholarship (2018)

Recipient of Monash SoIT High Impact Publication (HIP) Award (2021)

ACKNOWLEDGEMENTS

I would like to express my most profound appreciation to everyone I met during my venture of postgraduate study. I would like to thank my research advisors: Dr. Jin Zhe and Dr. Liang Shiuan-Ni, for their continuous support throughout this research study. Their guidance helped me in all the research, thesis writing, and my growth as a researcher. Without the expertise of Dr. Jin Zhe and Dr. Liang Shiuan-Ni, the completion of this study could not have been possible. I would also like to express my gratitude to my previous co-supervisors: Dr. David Albrecht and Professor Anthony Guo, for once being part of my supervisory team and providing their advice to me. I would acknowledge milestone review panels: Dr. Lim Mei Kuan, Dr. Yuan Xingliang and Dr. Maxine Tan for their precious time to review my progress and give feedback during my milestone reviews.

I would like to express my gratitude to Prof. Andrew Teoh Beng Jin, Prof. Andreas Uhl, Prof. Massimo Tistarelli, A/Prof Wong Kok Sheik, Dr. Li Minyi and Dr. Daniel Chen Bo-Wei for their advice and support on the research. Apart from that, I would like to thank Dr. Soon Lay Ki for her support as GRS coordinator. I would like to thank Dr. Suleman Khan, Dr. Lin Chern Hong and Dr. Vishnu Monn A/L Baskaran for giving me the opportunity to handle tutoring tasks in their unit and build my skills as an academic. Additionally, I would like to acknowledge Ms. Misha, Ms. Wan Nurul, Ms. Wan Adleen, Ms. Azizun Sallehuddin, Ms. Tang Wai Mun, Mr. Philip Chan and Mr. Prabagaran Magendran for their professional assistance.

I want to thank my friend, Dr. Lai Yen Lung, for his willingness to share his experience when I encountered difficulties. Other than that, I want to express my gratitude to my fellow friends and colleagues: Chia Kai Lin, Dilshani Hansika Mallikarachchi, Ryoma Ito, Trọng Tín Trần, Choong Han Sheng and Jasmine Lim. More importantly, a big thank you to my family members for their continuous support and understanding. Without encouragement from my family, I would not decide to start pursuing this study.

I would acknowledge IEEE and Elsevier for reviewing my manuscript and sharing my knowledge with the world. I also thank the reviewers for their professional suggestions during the peer-review process.

I would acknowledge the support from EU Horizon 2020 – Marie Sklodowska-Curie Actions (Project No. 690907, Acronym: IDENTITY), the project SPADA from the Italian Ministry for Research (MIUR), Ministry of Higher Education (MOHE) through the Fundamental Research Grant Scheme (FRGS) (FRGS/1/2018/ICT08/MUSM/03/3) and NVIDIA Corporation donation of the Titan Xp GPU in the research conducted in this thesis. Lastly, I would like to acknowledge Monash University Malaysia (and Monash University) for providing opportunities (financial and professional) and support in my journey as a researcher and academic.

Portions of the research in this thesis use the CASIA-IrisV3 collected by the Chinese Academy of Sciences' Institute of Automation (CASIA). Benchmarking datasets, such as FVC and LFW datasets are also employed in this thesis.

LIST OF TABLES

LIST OF FIGURES

GLOSSARY OF ABBREVIATIONS

AI	Artificial Intelligence
ARM	Attack via Record Multiplicity
BF	Bloom Filter
BOW	Bag-of-Words
BTP	Biometric Template Protection
CASIA	Chinese Academy of Sciences' Institute of Automation
CB	Cancellable Biometrics
CNN	Convolutional Neural Network
CV	Computer Vision
DNN	Deep Neural Network
EER	Equal Error Rate
EEG	Electroencephalogram
EFV	Extended Feature Vector
FAR	False Acceptance Rate
FMR	False Match Rate
FNMR	False Non-match Rate
FR	Face Recognition
FRR	False Rejection Rate
FVC	Fingerprint Verification Competition
GAR	Genuine Acceptance Rate
HD	Hamming Distance
HE	Homomorphic Encryption
HoG	Histogram of Oriented Gradient
ID	Identity
IdM	Identity Management
KPCA	Kernel Principal Component Analysis
LFW	Labeled Faces in The Wild
LSH	Locality Sensitive Hashing
MCC	Minutia Cylinder Code
M·EFV	Multimodal Extended Feature Vector
MFA	Multi Factor Authentication
NIR	Near Infrared

PED	Portable Electronic Device
P-MCC	Protected Minutia Cylinder Code
R·HoG	Random Augmented Histogram of Oriented Gradient
SOTA	State-of-the-art
WO3A	Whale Optimization Algorithm Authentication Attack

GLOSSARY OF NOTATIONS

Chapter 3

$\mathbf{Z} \in [0,1]^{m\times n}$	Unaligned irisCode
$\ddot{\mathbf{Z}} \in [0,1]^{d\times n}$	Random augmented biometric matrix
$\acute{\mathbf{Z}} \in \mathbb{R}^{d\times n}$	Gradient orientation matrix
$\dddot{\mathbf{Z}} \in \mathbb{R}^{d\times n}$	Gradient magnitude matrix
$\mathbf{X} \in [-1,1]^{d\times n}$	Neighbour horizontal difference
$\mathbf{Y} \in [-1,1]^{d\times n}$	Neighbour vertical difference
$\mathbf{p} \in [1,m]^{d}$	Random augmentation seed
$\mathbf{t} \in \mathbb{R}^{h}$	Local histogram vector
$\mathbf{c} \in \mathbb{R}^{ho}$	Alignment-robust biometric vector (cancellable template)
$a \in \mathbb{Z}$	Segment column size
$b \in \mathbb{Z}$	Segment row size
$h \in \mathbb{Z}$	Local histogram vector bins
$o \in \mathbb{Z}$	Number of partitioned biometric vector
$\beta = \frac{d}{b}$	Feature dimension for each z-score normalization

Chapter 4

$\mathbf{x} \in \mathbb{R}^{2d}$	Original Bio. Vector
$\mathbf{h} \ \in [0,1]^{2d}$	IoM Bio. Vector
$\hat{\mathbf{h}} \in [0,1]^{2dn}$	Augmented Bio. Vector
$\dddot{\mathbf{h}} \in [1,2^{k}]^{2dn}$	Integer Bio. Vector
$\mathbf{c} \in [0,1]^{2dn}$	Cancellable Template
$\mathbf{r} \in [0,1]^{2d}$	Transformation Key (Random String)
$\mathbf{e} \in [0,1]^{\mathbf{2d}}$	Encrypted String
$\mathbf{P} = \{\mathbf{P}_1, \mathbf{P}_2 \dots \mathbf{P}_q\}$	Projection Seed, each $\mathbf{P}_i \in \mathbb{R}^{m\times \mathbf{2}d}$
$\alpha \in \mathbb{R}, \alpha > 0$	Rescale ratio
$n \in \mathbb{Z}, n > 1$	Number of Appending Round
$s \in \mathbb{Z}, s \geq 1$	Number of Bit Shifting
$k \in \mathbb{Z}, k \geq 2$	Sub-Block Size
$\beta \in \mathbb{Z}, 1 \leq \beta \leq 2^{k}$	Many-to-One Modulo Threshold

Chapter 5 (Enhanced Matching Mechanism)

$\mathbf{X} \in \mathbb{R}^{a \times b}$	Original biometric feature
$\mathbf{R} \in \mathbb{R}^{q \times e}$	Auxiliary data of the cancellable biometrics
$\mathbf{C} \in \mathbb{R}^{k \times m}$	Cancellable biometric template
$f(.)$	Cancellable transformation function, $f(\mathbf{X}, \mathbf{R}) \rightarrow \mathbf{C}$
n	Number of local cancellable template
$\mathbf{P} = \{\mathbf{P}_1, \mathbf{P}_2, \dots, \mathbf{P}_n\}$	Permutation seed, each $\mathbf{P} \in \mathbb{R}^{l \times o}$
τ_{L}	Local quantization threshold
τ_{G}	System matching threshold
$\mathbf{s} \in \mathbb{R}^n$	Local score vector, each $0 \leq s_i \leq 1$
s_{G}	Global score (matching score)

Chapter 5 (Authentication Attack)

$\mathbf{X} \in \mathbb{R}^{a \times b}$	Original biometric feature
$\mathbf{R} \in \mathbb{R}^{q \times e}$	Auxiliary data of the cancellable biometrics
$\mathbf{C} \in \mathbb{R}^{k \times m}$	Cancellable biometric template
$f(.)$	Cancellable transformation function, $f(\mathbf{X}, \mathbf{R}) \rightarrow \mathbf{C}$
$\mathbf{X}' = \{\mathbf{X}'_1, \mathbf{X}'_2, \dots, \mathbf{X}'_u\}$	Guessed biometric features, each $\mathbf{X}' \in \mathbb{R}^{a \times b}$
$\mathbf{s} = [s_1, s_2, \dots, s_u]$	Similarity score vector, each $0 \leq s_i \leq 1$
u	Number of guessed templates
$t_{\max}$	Maximum attack iteration
τ	System threshold

Chapter 1 INTRODUCTION

This thesis aims to study the security and privacy of biometric verification in terms of biometric template protection and feature injection attack (type-4 attack). Section 1.1 provides an overview of biometrics and biometric template protection. After that, the following three sections, i.e., 1.2 to 1.4, further discuss the research background, including biometric modalities, biometric system infrastructure, performance metrics, and threats. Followed by section 1.5 to discuss the motivation, research objectives & questions, contributions, and scope of the study. Lastly, section 1.6 outlines the thesis structure.

1.1 Overview

Identity management (IdM) is the process of verifying, authenticating and authorizing the user for gaining access to the application/ service by associating access rights with the user's identity (e.g., user account, name, etc.) [4]. As digital technology continues to enhance and gradually replace physical items/ services in many sectors (e.g., internet financial, digital currency), the demand to provide an effective authentication solution has become more prevalent towards the individual or organization. In 2018, Monash University implemented Okta multi-factor authentication (MFA) as the IdM solution to ensure staff and student login credentials and combat cyber-attack [5]. In IdM, linking user identity with the authentication factor(s) is the fundamental task. Generally, there are three types of authentication factors that can be employed in an IdM system [4]:

- **Knowledge factor ("What you know?")**: User proves the identity by providing the "information" that is shared with the applications/ services. For example, a password system requires the user to provide a valid username and a string of characters (commonly known as a password) for gaining access. The authentication process of this *model* depends on the secrecy of the knowledge factor. This shows that if the knowledge factor was once disclosed to others or can be easily guessed, the security of the authentication process will be weakened.

- **Possession factor ("What you have?")**: Authentication process of this method relies on a physical item, e.g., physical keys, security tokens or access card. An example is an individual providing a USB drive (e.g., YubiKey [6]) to the computer system for logging into the web-service account. However, anyone with the possession factor can claim to be a genuine user and access the applications/ services. This shows that the user must manage the possession factor very carefully.

- **Inherence factor ("Who are you?")**: This authentication factor is characterized by the uniqueness of the individual, including *biological* measurements from the individual. This method is usually known as biometrics. Compared to knowledge or possession factors, the inherence factor is more secure as it requires a high (financial or computational) cost to collect and forge the inherence factor. Yet, a drawback of using the inherence factor is the template is not changeable.

Among the above authentication factors, *knowledge* and *possession* factors are deployed in many conventional IdM, e.g., password authentication in an organization's smartphone or ID-card system [4]. Yet, it is not reliable when identity management is purely relying on the knowledge and possession factors. First, frequent change of the password is always required to maintain a high-security level, but such a "secure" password is the one that the user cannot remember. On the other hand, these methods require the user to manage the authentication factor by himself. The individual must hold many authentication factors (e.g., physical key, password, ID-card) for accessing their daily applications (e.g., house, digital services, company building). It is not convenient to manage many external authentication factors as it requires additional physical space or human memory. Moreover, these authentication methods cannot precisely recognize the user, and the authentication factor can be easily forged or shared [4]. Unlike biometrics that can deploy liveness detection technology (e.g., [7]) to distinguish *real* or *fake* biometric features (inherence factor), anyone with the (real or fabricated) knowledge or possession factor can claim to be the genuine user. This could cause a severe issue involving privacy-sensitive information (e.g., financial statement or e-mail record).

To overcome the limitations of knowledge and possession factors, biometrics was introduced. Integration of biometric recognition into identity management gains the following advantages and characteristics [4], [8], [9]:

- **Uniqueness**: Biometric features are unique, making the biometric system more precise in recognizing the user than the sharable knowledge and possession-based system.

- **Permanence**: Biometric feature is always with the owner and remains constant for a very long period (probably owner's lifespan) unless minor perturbation, e.g., burn or cut. Therefore, the biometric feature is a reliable authentication factor compared to passwords or tokens.

- **Improved user experience**: This is the key reason that biometrics is so popular. First, the user does not need to manage the authentication factor because it is a body part. Moreover, the authentication process is swift and easy, where the user only needs to provide biometric features to the sensor and gain access.

- **Privacy-preserving and improved security**: Biometric features, e.g., fingerprint or iris, are nearly impossible to be shared, stolen or lost compared to possession and knowledge factors. Therefore, only the owner with the biometric feature can gain access. This is very important, especially in a privacy-sensitive application, e.g., internet financial services, workstation device, email account, personal device, etc.

Biometrics (or biometric recognition) refers to the identity management solution that recognizes the person by means of traits that are directly derived from the person (biometric modality) [10]. Traditional biometric modalities involve fingerprint, face, iris, etc. With the advancement of technological tools, emerging biometrics, e.g., *brain* and *heart* signals, are introduced to human identification. A basic biometrics framework comprises the biometric reader, feature extractor, matcher, decision module and biometric storage [4], [11]. A biometric reader is an interface for the user to provide biometric data to the system. A feature extractor is then used to filter and extract the biometric feature set from the input biometric data. During enrollment, the extracted biometric feature set is stored in biometric storage as the template for comparison purposes. During authentication, the user provides the biometric feature to the system and generates the query template. The query and pre-stored biometric template are then passed to the matcher to perform similarity checking (e.g., hamming similarity). There are two types of authentication: biometric identification and verification [4]. If the individual provides a biometric feature without a claimed identity (e.g., passport or account), the system will compare the query template with all pre-stored templates in the database (1-to-n matching). As a result, the system returns a list of similarity checking results, and this process is called biometric identification. On the other hand, biometric verification is the process of comparing to the pre-stored template that is associated with the claimed identity (1-to-1 matching) [4]. This study focuses on security and privacy in the biometric verification system.

With the popularity of biometrics, the massive deployment of biometrics is a known fact. A recent article from Okta reveals the use of biometrics increases the security of identity management and suggests the industry implements biometrics into multi-factor authentication for best practice [12]. There are also many biometric applications in our daily life, e.g., automated cross-border checking also requires the user to provide a passport and fingerprint/ face for identity verification. Moreover, many digital devices manufacturers deploy biometrics for logical access control, e.g., Apple Touch ID [13], Microsoft Windows Hello [14]. However, there are still some security and privacy issues in biometric applications that need to be overcome before biometrics can be a reliable solution. Particularly, the security of the biometric data in storage is questionable because biometric data is unchangeable. When the biometric data is compromised, many serious problems will occur, including permanent loss of identity and privacy invasion. A real-life example is that in 2015, about 1.1 - 5.6 million of biometric data (many with secret clearances) from the U.S federal Office of Personnel Management were stolen by hackers and this cost a minimum of $133 million for providing identity theft protection to all victims [15].

The cryptographic hashing method [16] is the preemptive method in protecting the data because the original information is not recoverable from its protected instance. In cryptographic hashing, a one-way transformation transforms the input data into a non-invertible hash code. However, this approach requires the consistency of the input data, which means the user needs to provide the (exactly) same biometric data every time. Otherwise, the authentication process will fail even if there is a minor change in the input biometric data. Due to the wide variations of biometric data during different acquisitions, it is impossible that the feature extractor can extract the same biometric data in each authentication. Therefore, it is not suitable to directly use the cryptography hashing method to protect biometric data. With the urgent need for protecting biometric data, a research area, namely “Biometric Template Protection” is getting attention.

Biometric template protection was first introduced by Ratha *et al.* [16], where they applied a repeatable distortion process onto the biometric signal to generate a non-invertible template. Until now, existing biometric template protection (BTP) methods can be broadly divided into biometric cryptosystems [17] and cancellable biometrics [18]. Biometric cryptosystem (or helper data-based approach) was initially designed to use biometrics to protect a cryptographic key or directly derive the cryptographic key from biometric data. It can also be used as biometric template protection [11]. In biometrics, there is public information called *helper data* derived from input data. Biometric Cryptosystem can be sub-categorized into key binding and key generation based on the usage of the helper data [17]. If the helper data is used to bind/ release a pre-existing cryptographic key, this method is called a key binding scheme. On the other hand, if the helper is used to derive a cryptographic key, this method is called a key generation scheme.

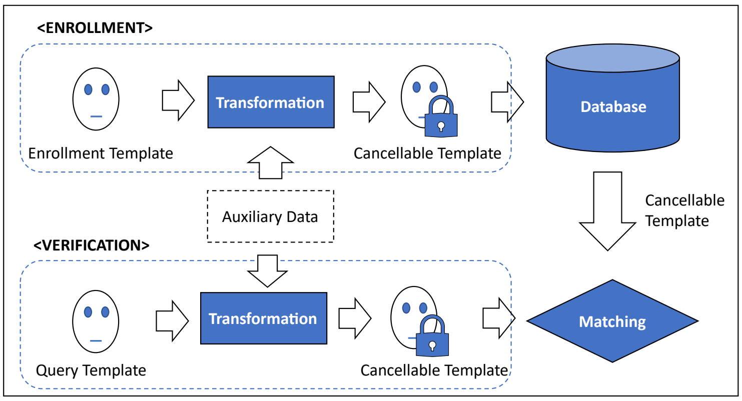


Fig 1.1. Overview of cancellable biometrics (adopted from [19])

Cancellable Biometrics (or transformation-based template protection approach) is similar to cryptographic hashing in the sense that it transforms the input data into distorted data [19]. As depicted in Fig 1.1, the overarching idea of cancellable biometrics is to convert the biometric data into distorted data and then store it as the authentication template (usually known as cancellable template). In a cancellable biometric method, a one-way transformation function (f) is applied onto the input biometric data (x) to generate a cancellable template ($c = f(x, r)$) where r refer to the transformation key (a form of auxiliary data) [20]. During authentication, a query cancellable template ($c' = f(x', r)$) is generated using the same transformation function and key where the symbol $'$ is used to distinguish the variables between enrollment and authentication. The components in cancellable biometrics are explained as below [20]:

- **One-way transformation function** (f): A series of mathematical operations (e.g., many-to-one modulo, substitution, etc.) to conceal the biometric information and produce a non-invertible output (cancellable template).

- **Transformation key** (r): Auxiliary data that is usually derived from a pseudo-random number generator (PRNG) or password [11]. The transformation key is used to randomize the biometric information and diversity the output cancellable template during the transformation.

The resultant cancellable template is irreversible and renewable, so the user can use the biometric applications without exposing the original biometric template. If the pre-stored cancellable template is compromised, the user can always re-issue a new cancellable template generated by the same biometric feature and a new transformation key. With the simplicity and excellent verification performance, cancellable biometrics is preferable among the community.

Ideally, a cancellable biometric scheme should achieve four requirements as specified in ISO/IEC Standard 24745 [21] and 30136 [22]:

- **Irreversibility (or Non-reversibility):** Restoration of the original biometric template from the protected template should be computationally hard. This is to prevent the original biometric data from being recovered and abused for attacks, e.g., spoofing or replay attacks.

- **Unlinkability (or Non-linkability):** It is computationally hard for the adversary to distinguish those multiple protected templates that originated from the same biometric feature. This is to prevent cross-matching of the templates across different biometric storages, and thus, protect users' privacy.

- **Renewability (or Revocability):** It should enable the user to re-issue a new protected template when the biometric storage is compromised. Moreover, it is computationally hard to recover the original biometric data from multiple protected templates that are generated from the same biometric data.

- **Performance preservation:** The template protection method should not degrade the verification performance (e.g., Equal Error Rate) of the original biometric system to a large degree to ensure the usability of the biometric system.

Although various cancellable biometric methods are designed, biometric template protection is still an unsolved problem. Most of the existing template protection methods suffer from weaknesses, e.g., performance degradation, token management, template linkage and security weakness [23]. In particular, massive information loss is required to achieve strong irreversibility, reducing the verification performance of the biometric feature. For example, the well-known Biohashing [24] is reported to suffer major performance degradation (High Equal Error Rate) compared to the original biometric counterpart [25]. On the other hand, most of the existing methods are still vulnerable to major attacks, e.g., attack via record multiplicity, false acceptance attack etc. On the other hand, existing cancellable biometric methods are designed as a tokenized template protection method which requires the user to manage the transformation key as a token. The practicability for having the external token with the user is questionable since the token is easy to be stolen. Furthermore, there are still many other shortcomings in the existing cancellable biometric schemes, e.g., high computation overhead caused by the feature alignment problem or verification performance skewness caused by the feature incompatibility.

On the other hand, injection of the biometric preimage before the matcher module is another potential issue towards a biometric system. Regardless of unprotected and protected, a biometric system is manifested as a thresholding-based decision system that grants access when the matching score (between the query and enrolled instances) surpasses the system threshold. Therefore, the adversary could launch authentication attacks [26] and attempt to get authenticated as the genuine user. In this attack, the adversary (i) sends the biometric primage to the matcher, (ii) randomly or strategically modifies the biometric preimage based on the matching score and (iii) repeats the former processes until the matching score surpasses the matching threshold. This could lead to the reconstruction of biometric information if the original biometric template is stored in the enrollment database. This attack is also applicable to the cancellable biometrics-enabled system where the adversary can just input the biometric preimage to the cancellable biometric scheme during the verification stage and perturb the biometric preimage until the access is granted. It is damaging, especially since the adversary does not need to have the knowledge of the cancellable biometric scheme and does not need to compromise the template storage. Moreover, due to the higher false acceptance rate raised by the performance degradation problem [27] in biometric template protection, it is easier to launch this kind of attack towards a cancellable biometrics-enabled system. Although many studies (e.g., [26], [28]–[32]) can be found in the literature, to the author's best knowledge, there is a limited number of studies of this kind of attack on a cancellable biometrics-enabled biometric system. Moreover, the method to increase the resistance of the biometric system towards this attack still remains unanswered. The details of the problems observed are further expanded in Section 1.5.1. In short, biometrics provides a convenient solution where the user just needs to show his fingerprint for accessing applications. Yet, there are still many security and privacy challenges needed to be addressed before biometrics can be a reliable authentication mechanism.

1.2 Biometric modalities, feature, and dataset

This section first revisits biometrics (or biometric recognition), followed by discussing the biometric modalities that have been employed in this thesis. Among various biometric modalities, iris, fingerprint, and face are the popular modalities that are widely adopted in today's biometric-based authentication system (e.g., Apple Touch ID [13], etc.). Therefore, this study focuses on enhancing the security and privacy aspects of the iris, face, and fingerprint systems.

When we have a glance at the term "biometrics", we notice that it originated from two Greek words: "*bios*" and "*metron*", with the *bio* meaning *life* and *metric* meaning measure [33]. While the initial use of biometrics can be traceback to 500BC in Babylon, the systematic biometric identification process first appeared in the 1870s when a French law enforcement officer - *Alphonse Bertillon,* invented a set of tools (known as the Bertillon System) to identify the individual based on the measurements, e.g., head diameter (length and breadth), length of the middle finger, left foot and cubit [34]. Later, with Sir Francis Galton's discovery of valuable traits, e.g., fingerprint pattern, biometric recognition based on fingerprint matching was introduced [34]. Since then, the advancement of digital signal processing has resulted in the explosive growth of biometric recognition [34]. Until now, there are more and more biometric modalities (e.g., iris [35], face [36], electrocardiogram [37] etc.) being studied and introduced to today's biometric recognition system. The following subsections further discuss the feature and datasets for the iris, fingerprint, and face that are employed in this thesis. In addition, a brief discussion on other biometric modalities is also covered.

1.2.1 Iris recognition

Iris recognition refers to the biometric method that identifies or verifies the individual based on the unique features within the ring-shaped region in the eye iris [35]. Eye iris is one of the strong biometric traits due to its rich entropy [38]. Based on the statistical studies done by Daugman [39], [40], it shows that the iris biometric enjoys the merit of uniqueness, and the iris feature is highly discriminated among identical twins; thus, guaranteeing a high recognition performance. Structure-wise, the iris is a multilayered structure that can be broadly divided into epithelial, muscle, stromal and anterior border layers that serve different purposes [41]. For instance, the epithelial layer serves the purpose of rendering the color of the iris. The existing iris recognition relies on the visual appearance of the iris surface and the pattern that is manifested by stromal [41].

There are two (external and internal) areas that can be observed in an iris image [41], [42], which are as follows:

- **(Internal) Pupillary zone:** An internal area of the iris that is between the pupillary boundary and collarette.

- **(External) Ciliary zone:** The external area of the iris extending from the collarette to the limbus.

In between the pupillary and ciliary zones, there is a line, so-called the collarette, that separates both zones [41], [42]. Speaking of the generation of the human iris pattern, the formation of the iris is initially found in the third month of gestation, and then the pattern of the iris continues to be formed until the eighth month [43], [44]. Next, the pigment accumulation can continue until the 1st year after birth. The complex structure allows us to find many high discriminative features from an iris image, e.g., furrows, ring and collarette [44]. For instance, we could observe some circular line patterns in the boundary of the ciliary zone [41]. Iris is highly popular among the community due to the following advantages. First, the iris is a very stable biometric feature such that the pattern remains the same over a human’s lifetime [35]. Second, the iris is an internal organ that is not exposed to external perturbation [41]. The iris is highly unique in the sense that the iris pattern is not the same among twins [39], [40]. Furthermore, the acquisition of an iris image does not require the individual to touch the scanner physically. In addition, the iris patterns of different eyes (from the same person) can be completely unrelated, and this made the iris a strong modality in a verification system [41], [42].

A. Iris Feature

Based on [35], Iris recognition is a set of processes that first use an iris scanner (e.g., Near Infrared (NIR) light iris sensor) to capture an iris image from the individual. Followed by processing the image by locating the circular structure outside the boundaries of the iris and pupil and, lastly, converting the iris texture into the iris feature (e.g., IrisCode [45]) for matching. Among various iris features, this thesis focuses on protecting the IrisCode-based verification system. This is because IrisCode is still the promising iris feature despite various alternative iris features being introduced [38]. IrisCode is an iris feature that was introduced by Daugman [45] in 1993 and has been continuously developed until now [46]. Structure-wise, IrisCode is a binary feature that is extracted by encoding and quantizing the iris data onto the Gabor wavelets [45]. Therefore, it is easy to adapt the irisCode into the existing template protection method.

The general process of extracting irisCode from an iris image is briefly discussed in this subsection. Given an iris image, the iris region is first detected, and then the iris and pupil boundaries are segmented. After that, rubbersheet transform is applied to normalize the segmented iris feature. Lastly, the normalized iris feature is encoded by means of Gabor wavelets [45]. Throughout this process, a compact binary iris feature (irisCode) is generated. Attributed to the rich entropy of the iris patterns, the irisCode-based verification system enjoys a high recognition performance [47], [48]. This is also supported by a recent statistical study conducted by Daugman and Downing [48], where a total of 3000 irisCodes were involved. Given the fine-tuned system threshold $\tau = 0.280$ (based on the normalized Hamming distance), the iris system can achieve 1 in 1 million of False Acceptance Rate (FAR) and a very low False Rejection Rate that is near to 0 (FRR) [48]. This implies a strong matching performance for a recognition system. This thesis mainly employs the methods from [49], [50] to extract the irisCode for realizing the proposed schemes.

B. Iris Dataset

In the existing iris template protection studies, the experiments were usually carried out using the iris database collected by the “Chinese Academy of Sciences’ Institute of Automation CASIA”. Until now, there are 4 editions of CASIA iris databases, namely the CASIA-Iris{V1, V2, V3 and V4}. The reader can refer to [51] for more details of every version of the databases. To be noted, CASIA-IrisV4 is an extension of the CASIA-IrisV3 with additional subsets.

Among the four versions of the database, this thesis employed the subset from the CASIA-IrisV3 database [52] to evaluate the schemes that are designed in this thesis. The CASIA-IrisV3 consists of three subsets: “CASIA-Iris-Internal, CASIA-Iris-Lamp and CASIA-Iris-Twins” [52]. Among the subsets, CASIA-IrisV3-Internal is mainly used for studying detailed iris features (e.g., furrows) since the iris images were captured using a close-up camera that is based on a fine-tuned circular Near-Infrared Ray (NIR) [52]. Therefore, the captured iris image is in high resolution and widely used in the existing BTP research [52]. On the other hand, iris images in CASIA-IrisV3-Lamp were taken using a hand-held iris sensor manufactured by Oki [52]. When capturing the iris images from each subject, the lamp was toggled to infuse more intra-class variations towards the subset. In particular, the intra-class variation of iris images in this subset is caused by the elastic deformation of iris texture [52]. Hence, CASIA-IrisV3-Lamp is mainly used for investigating the normalization and robust feature extraction problems [52]. In CASIA-IrisV3-Twins, the iris images were collected from a total of 100 pairs of twins using an Oki hand-held iris sensor. This subset is designed for studying the uniqueness of the iris traits among twins.

As a summary, the entire CASIA-IrisV3 database consists of 22035 iris images and the iris images in this database are all in the specification of an 8-bit grayscale jpeg format [52]. A summary of the CASIA-IrisV3 database is also provided in the table below. In this thesis, CASIA-IrisV3-Internal is chosen for the experiments since the main theme of this thesis is to study biometric template protection in iris verification. More importantly, it is easier for benchmarking purposes since CASIA-IrisV3-Internal is employed by most of the existing iris template protection works (e.g., [53], [54]).

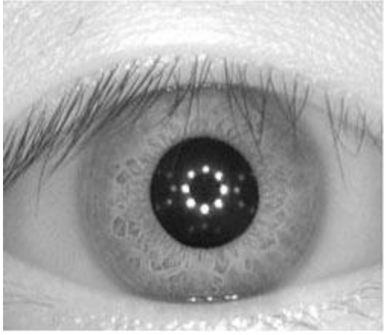


Fig 1.2. Sample iris image from CASIA-IrisV3 Internal (quoted from [52]) (available in: http://biometrics.idealtest.org/findTotalDbByMode.do?mode=Iris#/datasetDetail/3

Table 1.1: Summary of CASIA-IrisV3 (adopted from [52]) (available in: http://biometrics.idealtest.org/findTotalDbByMode.do?mode=Iris#/datasetDetail/3)

Dataset	**Iris Sensor**	**Acquisition Environment**	**Number of Subjects**	**Number of Classes**	**Total Images**	**Image Size ($W \times H$)**
CASIA-IrisV3-Internal	Self-developed Sensor	Indoor	249	395	2639	320×280
CASIA-IrisV3-Lamp	Oki IRISPASS-h	Indoor (Lamp on/off)	411	819	16212	640×480
CASIA-IrisV3-Twins	Oki IRISPASS-h	Outdoor	200	400	3183	640×480

1.2.2 Fingerprint recognition

A fingerprint recognition system refers to a biometric system that is based on the comparison between a pair of fingerprints [10]. The fingerprint is considered the oldest yet most popular biometric modality in a recognition system due to its permanence and uniqueness [55]. The fingerprint pattern is arguably to remain the same over time unless external perturbation, e.g., cut or burn, occurs [33]. Until now, fingerprint systems have been widely implemented in industry, e.g., Apple Touch ID [13], Microsoft Windows Hello [14], Zwipe payments solution [56] etc. The fingerprint is the feature that can be found in the fingertips, and it is formed by the pattern of valleys and ridges [57]. Instead of using raw fingerprint images, many existing fingerprint systems rely on the fingerprint representations that are observed from the fingerprint pattern [57].

A fingerprint can be analyzed into three levels of representation, i.e., coarsest (or global) level, middle (or local) level and finest (or very-fine) level [10]:

- **First level representation:** The fingerprint is represented in the form of a ridge orientation map and ridge frequency map at the first level [10]. The features that can be observed in this level are singular points and coarse ridge shape [58]. Typically, the level-1 features are used for fingerprint indexing and classification [58]. Since only the flow and frequency of the ridgeline are observed, a fingerprint scanner with a low hardware specification is sufficient to observe the features [10].

- **Second level representation:** At the second level, a ridge skeleton image represents the fingerprint [10]. The features that can be observed in this level are different characteristics of the local ridge, so-called minutiae (e.g., ridge ending) [58]. The level-2 features are very stable; hence, it is used by many conventional fingerprint recognition systems. A fingerprint scanner with 500 PPI is sufficient to observe level-2 features [10].

- **Third level representation:** In this level, the fingerprint is represented in intra-ridge details, e.g., edge and sweat pores in the finest level [10]. At this level, the features that are observed are sweat pores and ridge shapes [58]. However, the level-3 features are not suitable for commercial recognition systems due to the high hardware requirement for a fingerprint scanner [10]. In fact, the level-3 features are usually used for forensic applications.

Table 1.2: Summary of 3 levels fingerprint representation (summarized from [10], [58])

Fingerprint Representation Level	**Features**	**Required Fingerprint Scanner Resolution (PPI)**	**Application**
Level 1	Singular points and coarse ridge shape	≥ 250	Fingerprint indexing and classification
Level 2	Minutiae points	≥ 500	Commercial fingerprint recognition
Level 3	Pores and ridge shape	≥ 1000	Law enforcement and forensics

The table above summarizes three levels of fingerprint representations. This thesis employed the fingerprint feature descriptor that is generated based on the level 2 fingerprint representation (minutiae point) since this feature has been widely adopted in the commercial system. A minutia refers to the discontinuous point of the ridge in a fingerprint pattern. Each extracted minutia can be represented as a point-based feature that consists of coordinates (or position) of the minutiae in fingerprint and orientation (or direction) of the minutiae. Usually, a minutia is treated as a point $\boldsymbol{m} = \{x, y, \theta\}$ where x, y are the coordinates and θ is the orientation [10], [57], [59].

A. Fingerprint Feature

Despite the coordinates (x, y) and the orientation (θ) of the minutiae can be directly used for similarity comparison, the minutiae-based template faces several limitations, especially when the bio-cryptographic applications or template protection is required [55], [60]–[62]. It is known that a minutiae-based template is a point set data that is unordered and variable-size due to the position change of the fingerprint during the acquisition process. Although the variable-size minutiae-based template can achieve decent verification performance, it usually requires complex algorithms (e.g., Lagrangian Relaxation strategy [63]) during the matching process; thus, resulting in a higher time complexity for the authentication process compared to a fixed-length representation. On the other hand, many existing biometric cryptosystem techniques (e.g., fuzzy commitment [64], symmetric key-ring encryption [65]) and cancellable biometrics (e.g., [53], [66], [67]) requires a fixed-length representation as input. This has limited the application of these schemes when the input fingerprint template is variable-size. There are many fixed-length fingerprint representations that can be found in the existing studies, e.g., [55], [60]–[62], [68]–[70].

The general process of extracting the fixed-length fingerprint representation is outlined in this subsection. Given a fingerprint image, the initial step is to extract the minutiae points $M = \{\boldsymbol{m}_1, \boldsymbol{m}_2, \dots, \boldsymbol{m}_n\}$ where each $\boldsymbol{m} = \{x, y, \theta\}$. After that, the minutiae points are converted into a set of local structures, so-called the minutiae descriptor (e.g., Minutia Cylinder Code MCC [63], Multi-line Code MLC [71]). Lastly, a learning-based point-to-string conversion method, e.g., bags-of-words (BOW) [55], kernel principal component analysis (KPCA) [62], K-means clustering [61], is applied to extract a fixed-length fingerprint representation from the minutiae descriptor. The generated fixed-length fingerprint representation enjoys the following merits:

- The fixed-length fingerprint template can be easily adopted in many existing template protection schemes and biometric cryptosystems without the need to redesign the schemes.

- Since the fingerprint representation is extracted based on the minutia local structures, the fixed-length fingerprint representation is an alignment-robust feature. Thus, a similarity comparison between a pair of fixed-length fingerprint templates can be made with a simple matcher.

This thesis employs the fixed-length fingerprint vector extraction technique originated from [62] for the experiments.

B. Fingerprint Dataset

Fingerprint verification competition (FVC) databases are widely deployed in fingerprint template protection studies. Until now, there are up to four editions of (Fingerprint Verification Competition (FVC) databases: FVC2000, FVC2002, FVC2004 and FVC2006. The reader can refer to [72] for more details of every edition of the database. Among the four editions, six datasets from FVC2002 [73] and FVC2004 [74] are employed in this thesis because these databases are employed in most of the existing fingerprint template protection works; and hence, can be used for benchmarking purposes. These databases are collected with the aim of providing an environment that allows the developers to testify and benchmark their designed method [74]. For FVC2002 and FVC2004 databases, each dataset consists of 100 subjects with 8 fingerprint samples per subject; thus, a total of 800 fingerprint images are available for the experiment. Table 1.3 tabulates the information of each dataset in terms of the number of fingerprint images, specification of image and sensor used for collecting the dataset.

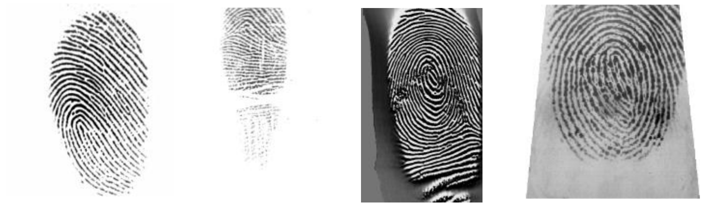


Fig 1.3. Sample fingerprint images from FVC2002 and FVC2004 datasets (quoted from [73], [74]) (available in: http://bias.csr.unibo.it/fvc2002/ and http://bias.csr.unibo.it/fvc2004/)

Table 1.3: Summary of FVC datasets employed in this thesis (adopted from [73]–[75]) (available in: http://bias.csr.unibo.it/fvc2002/ and http://bias.csr.unibo.it/fvc2004/)

Dataset	**Fingerprint Sensor**	**Number of Subjects**	**Samples per Subject**	**Total Images**	**Image Size ($W \times H$)**	**Image Resolution**
FVC2002						
DB1	Optical Sensor	100	8	800	388 × 374	500 dpi
DB2	Optical Sensor	100	8	800	296 × 560	568 dpi
DB3	Capacitive Sensor	100	8	800	300 × 300	500 dpi
DB4	*Synthetic Fingerprint*	100	8	800	288 × 384	≈ 500 dpi
FVC2004						
DB1	Optical Sensor	100	8	800	640 × 480	500 dpi
DB2	Optical Sensor	100	8	800	328 × 364	568 dpi
DB3	Thermal Sweeping Sensor	100	8	800	300 × 480	512 dpi
DB4	*Synthetic Fingerprint*	100	8	800	288 × 384	≈ 500 dpi

1.2.3 Face recognition

Face recognition (FR) is the process of using the face pattern as the authentication identifier to identify or verify one's identity. The face is one of the widely deployed biometric modalities in today's world attributed to the highly distinctive and contactless acquisition [76]. The face acquisition process is highly convenient in the sense that there is no close contact between the user and the face scanner. Due to the explosive advancement of image capture technology (e.g., integrated camera in smartphone), face recognition has become a huge part of our daily applications.

The face is a three-dimensional object that is easily affected by external factors, e.g., illumination, expression, pose during the capturing process; thus, face recognition is considered as a visual pattern recognition problem to recognize an individual in an image by face pattern [76]. A face system comprises 4 processes [76], as illustrated in Fig 1.4:

- **Face Detection:** Given an image, this process first detects the face by segmenting the face from the background. After that, the landmarks of the face (e.g., face outline, eyes, etc.) are localized in this process [76]. Hence, a processed face image with face detected is produced.

- **Normalization:** Given processed face image, this process normalizes the face image such that the face image is geometrically and photometrically standardized. For geometrical normalization, the face image is usually cropped into a fixed-size image frame, while the photometric normalization processes the images such that the properties, e.g., color scale of the images, are consistent in different authentication [76].

- **Feature Extraction:** The task of feature extraction is to convert the useful traits from the normalized face image into a face feature that is useful for similarity comparison. Attributed to the face detection and normalization processes, a face feature is usually invariant towards the geometric and photometric changes [76].

- **Matching:** The main task of this process is to determine the identity of the individual based on the query face feature. At first, the query face feature is compared to the enrolled face feature to compute the similarity score. When the similarity score surpasses the system threshold, the individual is recognized as the genuine user.

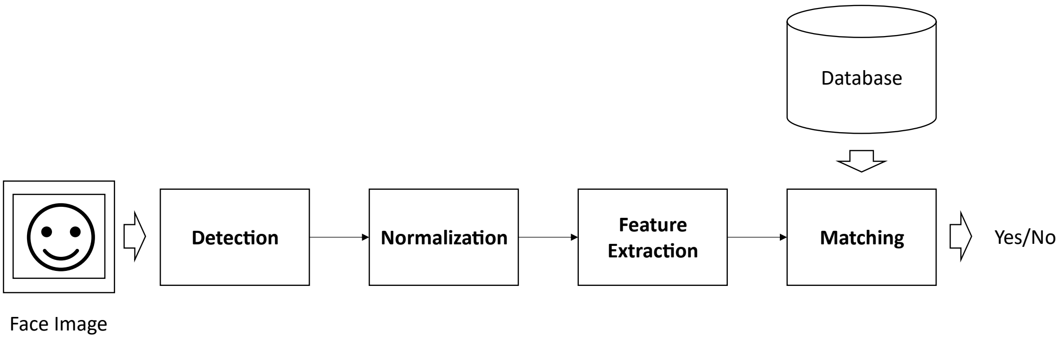


Fig 1.4. Overview of a face recognition system (adopted from [76])

A. Face Feature

Face recognition (FR) has been a frequently discussed topic in the computer vision (CV) research area over the past decades [77]. Due to the success of the deep learning-based method, i.e., AlexNet in the image classification [78], deep learning-based approaches are then extensively studied in face recognition [77], [79]. Since then, there have been many notable deep learning-based face feature extraction methods introduced in the literature, e.g., DeepID3 [80], FaceNet [36], etc. Typically, a deep learning-based face feature extraction involves the use of the convolutional neural network (CNN) [78] that employs multiple layers of operation units to learn a unique feature from the input face image [77]. The hierarchical design of the CNN enables the deep learning-based method to extract multiple levels of facial features from different abstracts where the extracted feature is typically invariant to the illumination, expression, pose problem [77]. Briefly, the lowest layer(s) of the deep learning-based method extracts a rather coarse face feature that is equivalent to the handcrafted Gabor feature that was developed in the earlier stage of Face Recognition. With the increment of CNN's layer, the deep learning-based method is able to extract a more precise face feature, e.g., facial emotion. Furthermore, the combination of face features extracted from different high layers produces a more stable face feature [77].

A notable work is the DeepFace introduced by the Taigman *et al.* [81] from the Facebook AI Research, where the DeepFace is the first deep learning-based method that can nearly achieve human-level recognition performance with 97.35% accuracy on the benchmarking LFW dataset. Later, GaussianFace [82] shows the possibility that a deep learning-based method could surpass human-level performance. The continuous development of the DeepID series [80], [83] shows the prominence recognition performance of 99.53% that can highly surpass the human-level performance of 97.53%. Attributed to these preemptive works, the research focus of the community has leaped into the era of deep learning. The later works, e.g., FaceNet [36], employed different network architecture or conducted training with other datasets to increase the recognition performance of the extracted face feature. A summary of these deep features can be found in [77]. The focus of this thesis is to design a scheme that enhances the security and privacy of a biometric system; hence, this thesis adopts FaceNet [36] to extract the face feature from the face image for experimentation purposes.

B. Face Dataset

Labeled Faces in the Wild (LFW) [84] is a publicly available dataset that was collected for providing a public benchmark environment for face verification. It is widely employed in the experimentations of recent face recognition research. The LFW dataset is formed by collecting face images over the web. In particular, the dataset consists of the face images taken from 5749 persons, with 1680 out of 5749 having more than two images [84]. Since the purpose of employing the face modality is to study the biometric fusion problem (with fingerprint modality) in the biometric template protection, a subset from the LFW dataset is formed to match the numbers of fingerprint images from the FVC databases. The details will be provided in the experiment section of the respective chapter. A summary of the LFW dataset is provided in Table 1.4. The reader can refer to [84], [85] for more information regarding the LFW dataset.

Fig 1.5. Sample face images from Labeled Faces in the Wild (LFW) dataset (quoted from [84]) (available in: http://vis-www.cs.umass.edu/lfw/

Table 1.4: Summary of LFW dataset (adopted from [84]) (available in: http://vis-www.cs.umass.edu/lfw/)

Total face images	13233
Total subject	5749
Subject with two or more face images	1680

1.2.4 Other biometric modalities

Other than iris, fingerprint and face, there are a lot of biometric modalities being used in human recognition. Based on [86] and [87], these modalities can be broadly categorized into *traditional* and *emerging* biometrics. Traditional biometrics refers to the modalities that are widely deployed in the conventional biometric system while emerging biometrics refers to the modalities that are introduced due to the uprising of the portable electronic device (PED) [87]. While the use of emerging modalities is an attractive idea, there are several challenges to be overcome before the emerging modalities can be widely deployed in the commercial biometric system [87]:

- Certain emerging modalities, e.g., keyboard, are highly unstable and not available for everyone [87]. Therefore, the acceptance of emerging modalities is lower than traditional biometrics.

- There is a limited selection of public datasets that can be used for testifying the designed scheme [87]. Hence, it is hard for the researcher to benchmark the performance of the proposed schemes.

- Although the advancement of technological tools has reduced the cost of biometric sensors, it is still hard to find a biometric sensor (for some emerging modalities) that can be directly integrated into our daily application. One example is the acquisition process of the Electroencephalogram (EEG) requires the user to wear a head-mounted sensor [87].

On the other hand, face, fingerprint and iris are heavily used in commercial applications, and the deployment of the database is massive compared to the emerging modalities. Therefore, this thesis puts the focus on the face, fingerprint and iris.

1.3 Biometric system and performance metrics

This section presents the basic biometric system and performance metrics that are commonly used in the BTP research area as well as this thesis. The reader is also encouraged to refer to [21], [22], [33], [35], [76], [88]–[90] for more in-depth knowledge of biometrics.

1.3.1 Biometric system

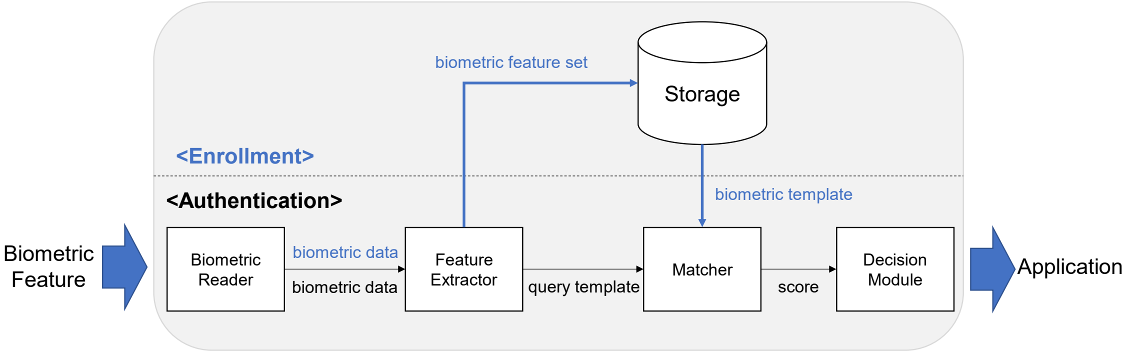


Fig 1.6. Graphical Illustration of a basic biometric system with five components (adopted from [4], [11])

A Biometric system refers to the automated tools to recognize the individual by means of the biometric characteristic. A biometric system can be operated into *identification* and *verification* modes [4], [11], and the terms *identification* and *verification* are listed as below:

- **Identification:** The operation to identify the identity of the individual by searching and comparing the query biometric feature with all enrolled biometric instances in the database. In this case, the biometric system conducts 1-to-many matchings.

- **Verification:** The operation to verify the claimed identity by comparing the query biometric feature with the enrolled biometric instance that is associated with the claimed identity. In this case, the biometric system conducts a 1-to-1 matching.

A biometric system, regardless of identification and verification, is a process that establishes the connection between identity and authentication factors (biometric feature) and examines the identity of the individual that presented the biometric feature to the system [4]. This is achieved by the *enrollment* and *authentication* processes [4] (see Fig 1.6), which are explained below:

- **Enrollment:** A process to link the identity and biometric feature(s). The biometric feature is stored as the authentication identifier at the end of enrollment.

- **Authentication:** A process to determine the identity of the individual by comparing the query biometric feature and the enrolled authentication identifier. This process can be operated as verification or identification based on the matching approaches (1-to-1 or 1-to-many).

A basic biometric system consists of five modules that are used to complete the process of enrollment and authentication [11]. These five modules are:

- **Biometric Reader:** A biometric sensor or reader is operated as the user interface to acquire the digitized biometric data from the biometric feature presented.

- **Feature Extractor:** A software to analyze the useful traits from the biometric data (e.g., minutiae point) and transform the traits into the feature descriptor (e.g., Minutia Cylinder Code [63]).

- **Storage (or biometric database):** A mechanism that allows the computation unit (server or computer) to keep the enrollment information, i.e., biometric template.

- **Matcher:** A logical module to calculate the similarity degree (e.g., hamming distance or normalized Euclidean similarity) between a pair of biometric templates. Typically, the result is returned as a matching score.

- **Decision Module:** A logical module to decide whether the individual is the genuine user based on the matching score calculated from the matcher. A Biometric system is a thresholding-based system, such that the decision module recognizes the individual as the genuine user when the matching score surpasses the system threshold τ.

1.3.2 Performance evaluation metrics

In BTP research, performance evaluation of a biometric system is usually conducted based on the recognition performance that is quantified by the genuine matching score distribution and impostor score distribution of a testing set [89]. Both distributions are generated through the *genuine* and *impostor* comparisons, which are as follows:

- **Genuine comparison**: Comparison between a pair of biometric features originated from the *same* individual (mated biometric pairs). The similarity score generated from this comparison is known as the genuine matching score.

- **Impostor comparison**: Comparison between a pair of biometric features that are extracted from *different* individuals (non-mated biometric pairs). The similarity score from this comparison refers to an impostor matching score.

Given a dataset with m numbers of subject and n biometric samples per subject, both genuine and impostor score distributions consist of $m * ({}^{n}C_2)$ numbers of genuine matching scores and ${}^{m}C_2$ numbers of impostor matching scores. Given the score distributions, the following performance metrics can be calculated [4]:

- **False Acceptance Rate (FAR):** It is also rebranded as a false match rate (FMR). It is the possibility that the biometric system falsely recognizes the individual (impostor) as the user [4]. FAR is calculated by quantifying the numbers of false matches (the case that the matching score ≥ threshold) over the non-mated (impostor) biometric pairs:

$$\mathrm{FAR} = \frac{\text{number of false matches}}{\text{total impostor comparison}} \tag{1.1}$$

- **False Rejection Rate (FRR):** It is also rebranded as false non-match rate (FNMR). FRR is the case of false declaration of genuine matching as an impostor matching [4]. This metric is calculated based on the ratio between the number of false rejections (the case that the matching score< threshold) and total mated (genuine) comparison:

$$\mathrm{FRR} = \frac{\text{number of false rejects}}{\text{total genuine comparison}} \tag{1.2}$$

In addition to the false rejection rate (FRR), there is another performance metric, so-called the *genuine acceptance rate* (GAR) (or True Acceptance Rate, TAR), to quantify the level of genuine matches in a biometric system [4]. After acquiring the FRR, the GAR is calculated as $\mathrm{GAR} = 1 - \mathrm{FRR}$ [4]. In this thesis, GAR is mainly used for estimating the system threshold τ and quantifying the security strength of the proposed works. With the computed values of

FAR and FRR, the performance metric, namely the Equal Error Rate (EER), can be estimated as [4]:

- **Equal Error Rate (EER):** Performance metric of a biometric system that is inferred from the intersection of the FAR and FRR.

Evaluation-wise, the lower the FAR, FRR and EER, the better the verification performance of the biometric system [27]. Therefore, it is always desirable when the biometric system (with and without template protection) can achieve a low EER$< 1\%$. An example of the genuine and impostor score distributions is depicted in Fig 1.7. In the figure, the red curve denotes the genuine score distribution, and the blue curve denotes the impostor score distribution. Any impostor matching score beyond the right side of the system threshold τ is considered as a false acceptance. On the contrary, a false rejection refers to the genuine matching score that drops at the left side of the τ. The genuine and impostor curves can also be used to visualize the verification performance of the biometric system. Specifically, a large overlap region between the genuine and impostor curves indicates the undesirable matching performance of the system (high EER). The overlapping can also be quantified by the decidability (d') [89], which is calculated by the mean and variance of both curves (see equation (5.3)). In short, it is desirable when observing a small overlap region between both curves (low EER and high d').

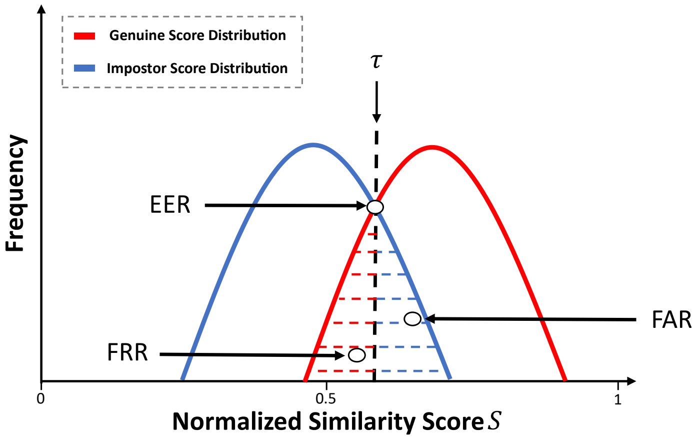


Fig 1.7. Example of genuine/ impostor score distributions (adopted from [4])

1.4 Security and privacy of biometric authentication

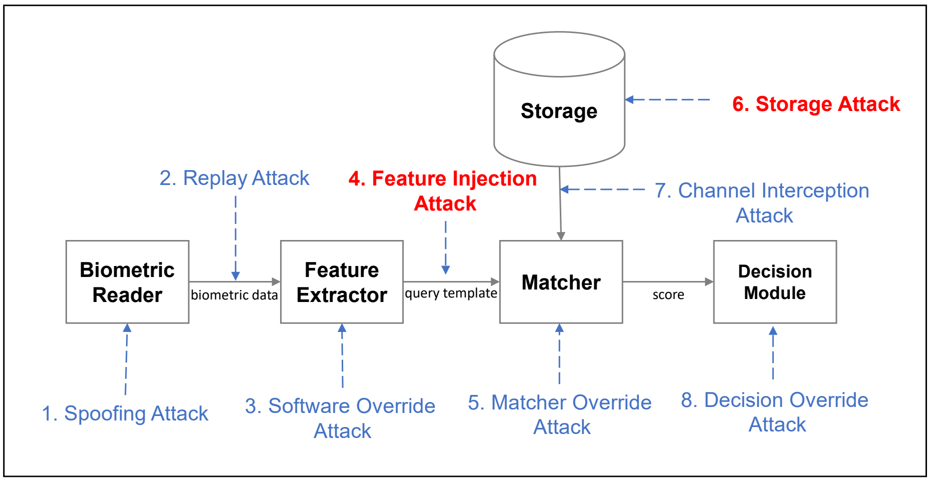


Fig 1.8. A basic biometric system with eight possible attacks in the system (adopted from [11])

There are still many problems needed to be addressed so that a biometric system can be a reliable authentication mechanism. Specifically, the adversary could identify any security and privacy vulnerabilities in the biometric system to disrupt the biometric system (e.g., denial-of-service), which is also illustrated in Fig 1.8, where there are 8 possible attacks in a biometric system [11], [20]. It is noted that Fig 1.8 illustrates the components in a basic biometric system, while the actual implementation of the biometric system depends on the functionality of the system, e.g., key binding system, on-device verification system, etc.

This thesis is established to study the security and privacy problems raised by the type-4 attack (feature injection attack) and type-6 attack (storage attack) in a biometric system. In BTP research, a type-6 attack usually refers to the attack on the biometric template that is stored in storage [11]. Due to the fact that the biometric template is unique compared to the password or token, the following problems could occur when there is an exposure of the storage (type-6 attack in Fig 1.8) [11]:

- An impostor may synthesize a fake biometric feature from the stolen biometric template and launch a spoofing attack to gain illegitimate access to the system.

- An impostor may inject the stolen biometric template into the matcher module and gain illegitimate access to the application/ service.

- Since biometric data is highly distinctive, the adversary can abuse the biometric template by attempting to crossmatch with other applications or other events (e.g., repudiation) to invade victims' enrollment(s).

By uniqueness of biometric features, the biometric system may be more accurate than token or password systems in recognizing the person. However, the biometric data breach is a big problem because the biometric template is not changeable [20]. Once the original biometric template is compromised, there is no security to the biometric system. As an example, an adversary can steal the biometric template from the storage (centralized biometric database or mobile phone) and use the stolen template to search for the victim's private information in other applications, e.g., healthcare records or financial statements. It is noted that it is always easier to steal biometric data from digital storage than copy it from the physical biometric feature. A real-world example was in 2019, fingerprint and face data of over 1 million people were exposed on a publicly accessible database that is managed by a security company called Suprema [91]. More critically, many important organizations, e.g., UK Metropolitan police or banks, deploy biometric access control from Suprema [91]. Therefore, it is important to protect the biometric template that is stored in storage.

Other than the type-6 attack (storage attack), the type-4 attack (feature injection attack) is another damaging attack in a biometric system. The type-4 attack is a type of communication channel attack that aims to penetrate the security and privacy of a biometric system by means of a guessed query biometric feature [11]. Once the impostor manages to find a suitable guessed query biometric feature (or biometric preimage) and be granted as the user (using the biometric preimage), the impostor can access the system for the following harmful events [11]:

- **Privacy Leakage:** Sensitive information disclosure occurs when the impostor can access the system and view the records that are stored in the system.

- **Service Disruption:** The impostor can alter/ delete the system information/ configuration and make the victim (genuine user) being prohibited from accessing the system.

This attack resembles a feature reconstruction attack when the pre-stored template is unprotected. In this sense, it enables the adversary to use the biometric preimage to perform a replay attack [11]. Although a mechanism, e.g., time-out lock-out policy [92], [93] can be used to mitigate the effect of the type-4 attack and prevent the impostor from attempting the authentication attack, it is insufficient when the system purely relies on this type of mechanism. Since the lock-out penalization is applied for everyone (genuine user and impostor), the impostor could abuse the policy and attempt to lock the account with massive tries of authentication [93]. In addition, denial-of-service (dos) could occur when multiple accounts are locked [93]. Moreover, this mechanism is ineffective, especially when the adversary reduces the frequency of the attack within the authentication threshold [93]. Since the pre-stored templates are highly distinctive, it is also feasible to invade multiple accounts of the same victim. Therefore, it requires biometric template protection in the biometric system to provide an additional layer of security to the biometric-based authentication and prevent the replay attack.

1.5 Problems, objectives, and outcomes

This section starts by discussing the shortcomings that are identified in the existing biometric template protection works, followed by the formulated research questions and objectives that drive the research in this thesis. With the question and objectives, the following section expands the research goals and scope of this thesis. Lastly, this section outlines the outcomes and main contributions of this thesis.

1.5.1 Problem statement

Provided that storage and feature injection attacks lead to many serious problems and biometric-based authentication is heavily implemented in today’s applications, biometric template protection (BTP) is essential. In particular, the research in this thesis is mainly motivated by the following observations from the existing BTP studies:

- **Security and privacy vulnerabilities**: Many existing template protection methods are subject to different attacks, e.g., authentication attack, preimage attack, birthday attack etc. Since the protected templates are stored as public information, the adversary may compromise one or multiple protected templates and attempt security and privacy attacks. For example, the Bloom filter-based template protection method [94] was reported that two protected templates generated from the same biometric data could be cross-matched [95]. BioEncoding suffers from the risk of original template recovery attack when the transformation key and the protected biometric template are known to the adversary [96]. Another example is the adversary could estimate a biometric preimage and use it to bypass the BioHashing-based system [97]. Therefore, the cancellable biometric methods need to be strengthened to provide more resistance to different attacks.

- **Token management**: Most of the existing template protection methods are designed as a tokenized authentication method that distributes the transformation key into an external factor, e.g., token or password. However, the necessity for having the user manage the transformation key invites several issues. First, since the method requires two inputs (biometric feature and transformation key) from the user, it requires the user to bear the inconvenience of keeping an external factor with them. This is serious when the user enrolls in multiple systems. Besides, the user might lose or forget the external transformation key, and this leads to the *stolen-token scenario* [19]*.* In the stolen-token scenario, the adversary could use the compromised key to conduct a zero-effort false acceptance attack and gain access to the system. This is critical when the performance degradation of the template protection is large. Additionally, the exposure of the transformation key could cause the recovery of the original biometric template from the protected template(s), especially in the salting-based template protection method [17], [19]. Therefore, a tokenless authentication approach is desirable.

- **Performance degradation**: Performance degradation is another open issue in template protection [27]. The fundamental task of template protection is to distort the original biometric template and store the distorted template for future authentication [27]. To achieve the high irreversibility of the protected template, a large distortion of the input biometric data (information loss) is usually required. This would impact the biometric system and increase the rate that valid users get rejected (False Rejection Rate). Many existing template protection methods, e.g., [24], [54], are reported from suffering performance degradation issues. For instance, the well-known BioHashing [24] was reported from major performance degradation. Therefore, it requires the produced cancellable template to maintain the matching accuracy of the original biometric template.

- **Biometric fusion in template protection**: Biometric fusion is the approach to improve the verification performance by integrating two or multiple biometric features into a biometrics system [9]. In recent years, biometric fusion has been getting attention in template protection research as it compensates for the performance degradation issue of the unimodal template protection method [98]. In the biometric template protection context, there are three fusion approaches: score-level, decision-level and feature-level [99]. Among three fusion approaches, feature-level fusion is the most suitable in template protection because it requires lesser processing overhead and storage space. Yet, it is a non-trivial task when trying to combine multiple biometric features into a protected template. As feature-level fusion is not merely a concatenation process, it requires a transformation that can cope with different biometric features. Incompatibility between different biometric features (value distribution, alignment issue, data type, etc.) would highly impact the matching accuracy of the system (or cancellable biometric method in this thesis) [9]. As an example, the value distribution problem between two input biometric features will result in the matching accuracy of the protected template biased to the biometric feature that holds a wider range of value distribution. Therefore, it requires a cancellable biometric method that can overcome this issue.

- **Alignment issue:** The alignment issue is a well-known problem in the irisCode feature, and this is due to the displacement (e.g., rotation or position) during the acquisition of the biometric feature [4]. In iris verification, the correlation-based strategy is used for template matching to compensate for the misaligned issue. For example, the irisCode requires a horizontal shifting for $\pm n$ bits of the templates during matching [53]. This would require a total of $2n + 1$ shifting. However, this invites an efficiency problem when applying for biometric template protection. Most of the existing template protection methods are worked with a fixed-sized and aligned biometric feature. Therefore, it will lead to failure in recognizing the user when directly applying the template protection method onto the unaligned biometric feature. The straightforward solution is to apply the template protection method to multiple shifted instances of the biometric template during the enrollment/ verification stage (e.g., [53]). However, this could increase the processing overhead to repeatedly executing the cancellable transformation and the storage space to store the output cancellable templates. Therefore, it requires an alignment-robust cancellable biometric method that can directly encode the unaligned irisCode template into an aligned template while providing strong concealment to the biometric information.

- **Weak decision environment:** Recognition performance of a (protected or unprotected) biometric system is characterized by the decision environment that is based on the score distributions from the *genuine* and *impostor* comparisons [89]. Typically, a biometric system is a thresholding-based decision system that relies on a predefined matching threshold τ to determine the identity of the individual. For instance, the individual is recognized as the *genuine user* when the similarity score S between the *enrolled* and *query* biometric features surpasses the matching threshold (i.e., $S \geq \tau$). In this case, the adversary could apply the feature injection attack and get authenticated as the genuine user. Although adjusting the matching threshold τ could increase the resistance against this kind of attack, it is not the best solution, especially when high overlapping between the genuine/ impostor score distributions is observed in the system. Despite the feature injection attack being harder to be conducted when the τ is set to a high value, it will lead to a situation that the genuine user easily gets rejected (higher *false rejection rate*), and the verification performance is degraded. On the other hand, a lower τ increases the false acceptance of the impostor as well as the feasibility of the feature injection attack. Therefore, it urges for a solution that can improve the decision environment as well as enhance the security resistance against the security attack.

1.5.2 Research questions and objectives

Based on the observations from the existing studies, the following research questions are devised:

- How to resolve alignment issues in iris template protection?

- How to resolve token management issues in the fingerprint protection method?

- How to combine multiple biometric features using the proposed template protection method?

- Can a cancellable biometrics-enabled system get attacked by a type-4 (authentication) attack, and how to perform this attack?

- How to improve the biometric decision environment and improve the security resistance of the cancellable biometrics-enabled system against the authentication attack?

To address the above questions, the research objectives are formulated as follows:

- Design an alignment-robust iris template protection scheme that can directly derive a protected biometric template that is robust towards the alignment issue of the biometric feature.

- Design a tokenless fingerprint template protection method that satisfies the template protection requirements: irreversibility, unlinkability, renewability and performance preservation.

- Integrate additional feature transformation and another biometric modality to reduce performance degradation of the unimodal tokenless template protection

- Formalize an automated authentication (type-4) attack towards the cancellable biometrics-enabled biometric system

- Design an enhanced matching mechanism to improve the decision environment and security resistance of the cancellable biometrics-enabled biometric system.

1.5.3 Research goal and scope

Based on the formulated questions and objectives, the goal of this thesis is to

"Enhance the security and privacy of biometric authentication systems."

This thesis focuses on the protection of the biometric template in the storage and the enhanced matching mechanism. The research aims to provide strong concealment towards the biometric information, such that the original biometric information is hard to obtain even though the protected template is stolen by the adversary. Other than that, the user is allowed to use the same biometric feature in different systems where the resultant templates in different systems are non-correlated. Besides that, this research also studies the trade-off between security and performance issue led by the canonical matching mechanism and designs an enhanced matching mechanism that can improve the decision environment of the cancellable biometrics-enabled biometric system. With the improved decision environment, developers of the biometric system are allowed to choose a higher system threshold without sacrificing the verification performance so much. With the increment of the system threshold, security resistance towards the authentication attack is increased. This thesis also formalizes an optimization-driven authentication attack to experimentally study the security resistance of the cancellable biometrics-enabled biometric system that is enhanced by the proposed enhanced matching mechanism.

In short, this thesis studies the potential security and privacy threats in a biometric system and proposes several techniques that can be considered when building the biometric system. The proposed techniques are mainly examined based on biometric security criteria as listed in the ISO/IEC Standard *24745* [21] and *30136* [22]: irreversibility, unlinkability, renewability and performance preservation. Since the schemes are mainly designed for the fixed-length *matrix* and *vector*-based biometric feature, the schemes can be easily propagated to the biometric modalities other than the face, fingerprint and iris that are covered in this thesis. Implementation-wise, the proposed techniques can be adapted to the existing biometric-based authentication mechanism to provide another layer of security and privacy.

1.5.4 Research outcomes and contributions

This thesis focuses on the prevention of the original biometric template being recovered for abusive activity and enhancing the secure matching process. The outcomes and contributions of this thesis are highlighted as follows:

- Contribution i: An alignment-robust biometric template protection method, namely the *Random Augmented Histogram of Gradients (R·HoG),* is designed to protect the iris feature. The proposed *R·HoG* overcomes the misalignment issue in the iris feature and directly transforms the unaligned iris feature (with ± 16 bits displacement) into the protected template. The generated protected template is robust towards the alignment, and thus, the authentication process is efficient compared to the existing iris template protection methods. Analysis based on the four biometric template protection requirements: irreversibility, unlinkability, renewability and performance preservation are conducted to justify the feasibility of adopting the proposed R·HoG in the real-world application. Besides that, major security attacks, i.e., false acceptance and birthday attacks, are carried out to examine the security aspect of the produced cancellable template.

- Contribution ii: Two tokenless biometric template protection methods, namely the *Extended Feature Vector (EFV) Hashing* and *Multimodal Extended Feature Vector (M·EFV) Hashing* are introduced for face and fingerprint-based biometric systems. The former method is a unimodal fingerprint template protection method, while the latter method is a feature-level fusion-based multimodal (face and fingerprint) template protection method. It is worth noting that the proposed M·EFV Hashing is the first tokenless multimodal template protection method in the literature. Both methods are tokenless template protection methods such that the user does not need to manage the transformation key. Specifically, the XOR encryption/ decryption notions are operated on the transformation key for producing the auxiliary information that can be stored alongside the enrolled cancellable template, which achieves the tokenless property. Rigorous analyses are conducted, and it is shown that the recovery of the original key is impossible even if multiple cancellable templates and auxiliary data are present. Moreover, the empirical results show that both the EFV and M·EFV hashing satisfy the biometric template protection requirements as specified in the ISO/IEC Standard 24745 [21] and 30136 [22].

- Contribution iii: An enhanced matching mechanism is proposed to enhance the decision environment of a cancellable biometrics-enabled system. The proposed enhanced matching mechanism is a dual-phase score quantization mechanism that could produce a matching score in which the gap between the mean of genuine/ impostor matching scores is increased. As such, the proposed matching mechanism could improve the verification performance and decidability of the system. Comprehensive experiments are carried out to justify the system performance after applying the enhanced matching mechanism. Experiment results suggest the enhanced matching mechanism could increase the verification performance of the system as well as separate the mean of genuine/ impostor score distributions. The proposed enhanced matching mechanism can be considered as a matching strategy in the sense that it can be applied to any cancellable biometric scheme.

- Contribution iv: An automated authentication attack, namely the whale optimization algorithm authentication attack (WO3A), is formalized to testify the security resistance of a cancellable biometrics-enabled system (with and without the enhanced matching mechanism) towards the type-4 attack. The formalized attack is designed with the inspiration of the recently introduced whale optimization algorithm (WOA) [100]. Two mechanisms, namely the uni-step binarization function and adaptive mutation mechanism, are applied to improve the efficiency and genericity of the WO3A. The experiments are carried out on the existing biometric template protection scheme, namely the Index-of-Max (IoM) hashing [66]. Furthermore, the M·EFV hashing and R·HoG introduced in this thesis are also being tested. The result suggests that the formalized WO3A could compromise the security of the tested scheme (in its original form) in a short time, which is not favorable since the user could not respond to the attack and renew the cancellable template. The result also suggests the enhanced matching mechanism could improve the security resistance of the tested scheme towards the WO3A.

1.6 Thesis organization

This subsection summarizes the contents of each chapter in this thesis. The main theme of this thesis is the security and privacy of the face, fingerprint, and iris verification. Fig 1.9 provides an overview of the organization of this thesis. In particular, this thesis consists of 6 chapters. Chapters 1 and 2 provide a background study on the research context and an overview of this thesis. After that, chapters 3, 4 and 5 present the works that have been accomplished in this thesis, with each chapter discussing the scheme design and evaluation. Lastly, chapter 6 concludes the findings of the thesis.

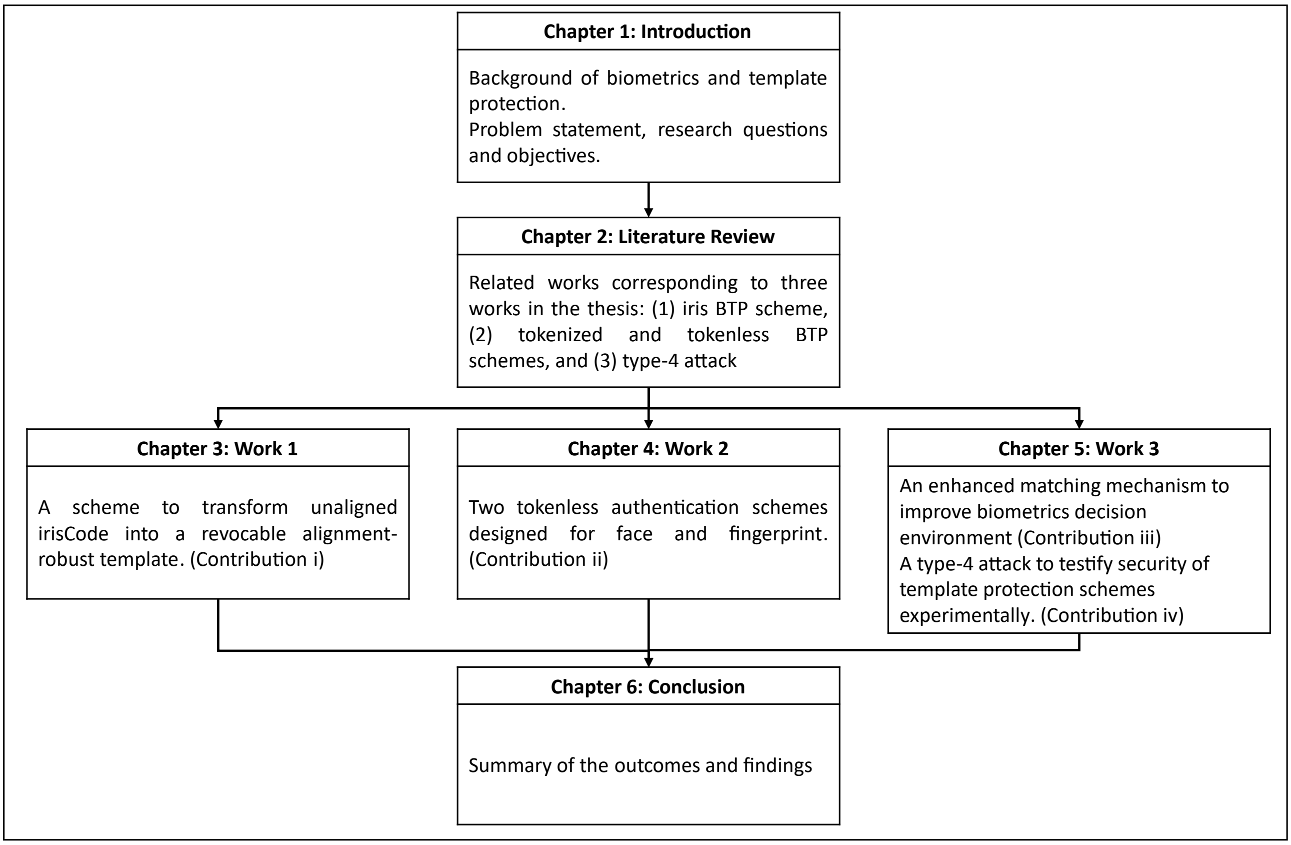

Chapter 1: Introduction
Background of biometrics and template protection.
Problem statement, research questions and objectives.
Chapter 2: Literature Review
Related works corresponding to three works in the thesis: (1) iris BTP scheme, (2) tokenized and tokenless BTP schemes, and (3) type-4 attack
Chapter 3: Work 1
A scheme to transform unaligned irisCode into a revocable alignment-robust template. (Contribution i)
Chapter 4: Work 2
Two tokenless authentication schemes designed for face and fingerprint. (Contribution ii)
Chapter 5: Work 3
An enhanced matching mechanism to improve biometrics decision environment (Contribution iii)
A type-4 attack to testify security of template protection schemes experimentally. (Contribution iv)
Chapter 6: Conclusion
Summary of the outcomes and findings

Fig 1.9. Overview of thesis organization

The remaining parts of this thesis are organized as follow:

- Chapter 2 revisits the existing works that are related to the research carried out in this thesis. Chapter 2 first reviews the existing iris template protection schemes in terms of the alignment-based and alignment-robust approaches. The chapter then discusses the token management in the face and fingerprint template protections and reviews the works that are related to the (unimodal and multimodal) Extended Feature Vector (EFV) hashing that will be presented in chapter 4. Lastly, this chapter reviews the related works on the type-4 attack that is targeted on the protected and unprotected biometric system.

- Chapter 3 presents the proposal of alignment-robust template protection for iris verification that overcomes the alignment problem of the irisCode feature in biometric template protection. The chapter first discusses the shortcomings of the current biometric template protection for the well-known iris feature, irisCode. The chapter then introduces the proposal of alignment-robust template protection, namely the Random Augmented Histogram of Gradients (R·HoG). After that, the experimental results and analyses are presented to demonstrate the R·HoG achieved four design criteria of biometric template protection. The chapter is concluded by discussing the findings of the research.

- Chapter 4 presents the proposal of tokenless template protection for face and fingerprint-based biometric systems that reduce the token management burden of a user. The chapter starts off by discussing the token management and performance degradation faced by the face and fingerprint template protection. After that, the chapter presents the proposal tokenless template protection, namely the Extended Feature Vector (EFV) hashing and Multimodal Extended Feature Vector (M·EFV) hashing. The following section of this chapter discusses the experimental results and analyses. Lastly, the findings of this research are outlined.

- Chapter 5 presents the proposal of the enhanced matching mechanism that aims to improve the decision environment of the cancellable biometrics-enabled system. The chapter begins with an introduction to the transformation-based biometric template protection (or cancellable biometrics) and the potential security threats towards the thresholding-based decision-making mechanism. After that, the chapter introduces the enhanced matching mechanism that can replace the canonical matching mechanism to improve the verification performance of a cancellable biometric scheme and allow the matching process to produce the genuine/ impostor matching scores that are highly separated. Other than the matching mechanism, this chapter also formalizes an automated type-4 attack to testify the security resistance of the BTP-enabled biometric system. The chapter then presents the experimental results. Lastly, this chapter discusses the findings.

- Chapter 6 summarizes this thesis by first discussing the outcomes and findings from the research conducted. This chapter first presents the summary of the thesis chapter with the focus on presenting the original contributions and impacts made in this thesis. Future recommendations are also discussed.

Chapter 2 LITERATURE REVIEW

This chapter reviews the existing works that are related to the proposals section by section. Since the first proposal in this thesis is an alignment-robust iris template protection, this chapter first revisits the existing iris template protection works in section 2.1. After that, section 2.2 revisits the template protection works that are relevant to the token management problem identified in the face and fingerprint template protection. Lastly, section 2.3 presents the existing works that are associated with the security and privacy of the biometric system in regard to thresholding-based decision-making.

2.1 Alignment problem in iris template protection

In this section, several iris cancellable biometrics primitives are revisited in terms of (a) *alignment-based* and (b) *alignment-robust* approaches. In an alignment-based approach, the cancellable biometric scheme requires a feature alignment process to compensate for the alignment issue of the iris. In general, there are two types of feature alignment processes. The first type of feature alignment is to create multiple shifted instances from the input iris feature. After that, the shifted instances are transformed into the cancellable templates for storing or matching purposes. Another feature alignment process is to extract a robust biometric feature based on reference biometric feature(s) from the user and then transform the robust biometric feature into the cancellable biometric template. On the other hand, the alignment-robust approach refers to the BTP scheme that can produce a similar cancellable template for two unaligned biometric features without the feature alignment process. The time complexity of the alignment-robust approach is usually lower than the alignment-based approach.

2.1.1 Alignment-based iris template protection

Random Projection (RP) is a well-known biometric salting technique due to its performance preservation property. In the RP approach, the cancellable template is generated by projecting the original biometric features onto a random subspace via randomly generated auxiliary data. In RP, the formula to form cancellable template $\mathbf{x}'$ can be simplified as below

$$\mathbf{x}' = \mathbf{R}\mathbf{x} \tag{2.1}$$

where $\mathbf{x}$ denote the biometric data, and $\mathbf{R}$ denote the transformation key. From equation (2.1), the re-issue of a new cancellable template $\mathbf{x}'$ can be done by replacing the $\mathbf{R}$. Pillai *et al*. [101], [102] propagate RP into iris template protection. Due to the outliers remaining in the iris vector, e.g., eyelids and specular reflections., application of the linear transformation (i.e., RP) to the entire iris vector will corrupt the iris data; thus, the result cancellable template is less discriminative. Therefore, the sectored random projection process in [101] was introduced to solve this issue. In [101], the iris vector is firstly divided into several sectors, and RPs are applied to the sectors independently; hence the cancellable iris template is generated by combining and encoding the transformed sectors. To handle the misalignment issue that is caused by the rotating iris images, a two-stage alignment process is merged with the proposed cancellable biometric scheme to obtain the final matching result [102]. Later work of Pillai *et al.* [102] extends the methodology in [101] so that the RP works in video-based iris recognition. One drawback of using the random projection-based template protection method is that it requires the user to keep the transformation key $\mathbf{R}$ securely as the transformation process is vulnerable to the template inversion attacks (e.g., [97]).

Ouda *et al.* [103] proposed a cancellable iris scheme, namely "BioEncoding". In [103], the consistent bits $\mathbf{c} \in [0,1]^n$ are first determined from multiple IrisCode of each user where the consistent bits refer to the bits that remained the same in different irisCode samples for the same user. After that, $\mathbf{c}$ is partitioned into multiple m-bits binary blocks and the binary blocks are then converted into integer values. This yields an integer vector $\mathbf{x} \in [0,2^{m-1}]^{n/m}$. Lastly, the cancellable iris template (BioCode $\mathbf{b} \in [0,1]^{n/m}$) is generated by substituting each of the element in the integer vector $\mathbf{x} \in [0,2^{m-1}]^{n/m}$ by the element in a randomly generated transformation key $S \in [0,1]^{2^m-1}$. As such, the same integer value (x) will be substituted by the same bit and this achieves a many-to-one mapping. To handle the irisCode misalignment issue, BioEncoding based schemes (e.g., [103]–[105]) require a pre-alignment process to obtain the consistent bit vector from the irisCode [103]. In particular, the pre-alignment process requires the user to perform scanning and shifting multiple times to have the several aligned irisCodes to be extracted. After that, the most consistent bits from the aligned irisCodes are extracted to form the consistent bit vector. The pre-alignment process increases computation overhead where multiple rounds of iris scanning are involved.

Hämmerle-Uhl *et al.* [106] obtain the revocable wavelet-based iris feature using the key-dependent wavelet transforms. In their work, there are two schemes: parameterized wavelet filter and wavelet packets [106]. In the parameterized wavelet filter approach, the parameterized filters are used to replace the quadratic spline wavelet (QWS) of the iris feature extraction technique (i.e., [107]). As for the wavelet packets approach, the decomposition of the iris image is limited to 8 stages to generate up to 510 different sub-bands. After that, 20 sub-bands are randomly selected to form the revocable iris template, which will then be encoded into the cancellable irisCode. In [106], a key-dependent wavelet transform is directly applied to the feature extraction stage to avoid the data loss and alignment problem which usually occurs in the image warping process (i.e., [108]). Although the transformation process could avoid the alignment problem, the produced cancellable irisCode is not alignment-robust since iris mask shifting is required during the matching process. Furthermore, the security of the cancellable irisCode is an issue because both schemes are biometric-salting approaches such that the iris template is invertible if the transformation key is presented [106].

Dwivedi and Dey [109] utilize the concept of a lookup table to create a cancellable iris template. In [109], a pre-alignment process is applied to generate a rotation-invariant iris template as the input for the cancellable transformation. The pre-alignment process performs horizontal shifting on input irisCode with reference to a sample irisCode from the same user. After that, all rows of the rotation-invariant iris template are concatenated into a single bit-vector $\mathbf{c} \in [0,1]^n$. The bit-vector $\mathbf{c}$ is then partitioned into several sub-bit blocks with the size of m-bits where m can be user-specific to improve security [109]. A binary-to-decimal conversion is applied to all the sub-bit blocks and yield a decimal vector $\mathbf{d} \in [0,2^{m-1}\ ]^{m/n}$. With a randomly generated lookup table $\mathbf{M} \in [0,1\ ]^{2^m \times m}$, each $d \in \mathbf{d}$ is used to look up $\mathbf{M}$ for selecting d numbers of bits in a certain row and combine the selected bits to produce the final cancellable template. The follow-up study done by Dwivedi *et al.* [110] applied the consistent bit extraction to the bit-vector $\mathbf{c}$ to improve the matching accuracy. One drawback of this scheme is the lookup table $\mathbf{M}$ must be kept secretly, otherwise the iris template can be easily recovered by reverse lookup the $\mathbf{M}$ and a cancellable template [53].

Lai *et al.* [53] proposed a locality-sensitive hashing inspired scheme, namely the *Indexing First One (IFO) Hashing* in iris template protection. The concept of the IFO hashing is to record the index value of the first $'1'$ in the binary iris vector. The procedures of IFO hashing to transform the binary iris vector $\mathbf{x} \in [0,1]^d$ to the cancellable iris template $\mathbf{c} \in [1, k - \tau]^q$ are explained as follows: 1) Given the randomly generated permutation matrices $\mathbf{P}_i \in [0,1]^{d \times d}$ where $i = 1 \dots n$, transform the $\mathbf{x}$ via the following formula to generate p numbers of permuted vectors $\mathbf{x}^{\mathrm{perm}}{}_i \in [0,1]^d$:

$$\mathbf{x}^{\mathrm{perm}}{}_i \ = \mathbf{x}\mathbf{P}_i; \tag{2.2}$$

2) Calculate the Hadamard product of the permuted vectors via the formula $\mathbf{h} = \prod_{i=1}^{p} \mathbf{x}^{\mathrm{perm}}{}_i$ where $i = 1 \dots n$; 3) Record the index value of the first $'1'$ in the Hadamard product $\mathbf{h} \in [0,1]^d$ as c_j; 4) Re-calculate the $c_j{}' = c_j \mathrm{mod}(k - \tau)$ where k and τ are the pre-defined parameters; and 5) Repeat steps $1 - 4$ for $(q - 1)$ times until every $c_j \in \mathbf{c}$ are recorded where $j = 1 \dots q$. In IFO hashing, the use of q numbers of random matrices $\mathbf{P} \in [0,1]^{d \times d}$ in step 1 enables the revocation of the cancellable template. Despite [53] achieving a good matching accuracy with the Jaccard similarity matcher, it requires a pre-alignment process to alleviate the alignment issue [53]. Specifically, the original irisCode is horizontally shifted for $\pm n$ bits to produce up to $2n + 1$ shifted instances. Then, all the shifted instances are transformed into the IFO hashed codes and matched to the enrolled IFO hashed code. The highest similarity score from the many-to-one matching process is returned as the matching result. Although this can achieve a desired matching result, the pre-alignment process increases the computation time for the entire matching process since multiple rounds of irisCode shifting and IFO transformations are involved.

2.1.2 Alignment-robust iris template protection

Zuo *et al.* [18] proposed two alignment-robust cancellable biometric schemes, i.e., GRAY-COMBO and BIN-COMBO. The underlying concept of the COMBO approach is to randomly shift and combine the given rows in the iris template. Briefly, an iris template is transformed to the cancellable iris template through the following steps: 1) Each row of the input template is circularly shifted according to a key (or random offset), and 2) A pair of selected rows are combined via mathematical operation, e.g., XOR according to another key (or row selection). Due to the mixing nature, the generated template could resist template inversion attacks [18]. If the cancellable template is compromised, GRAY-COMBO and BIN-COMBO allow the renewal of the new cancellable template by applying a new key in steps 1 and 2, as mentioned above. Among the two approaches, BIN-COMBO is designed for the irisCode feature, while GRAY-COMBO is designed for unwrapped iris image [18]. Both GRAY-COMBO and BIN-COMBO are claimed to be registration-free (or alignment-robust) BTP schemes where the shifted rows of the iris template usually possess the same orientation regardless of rotation difference in the input iris image. This is validated by the experiment in [18] where multiple randomly shifted iris templates are involved. However, a good quality iris image is required to achieve the desired matching result [111].

Rathgeb *et al.* [54], [94] introduced the Bloom filter-based BTP scheme that can transform the unaligned irisCode into an alignment-robust protected template. In [54], the irisCode $\mathbf{I} \in [0,1]^{H\times W}$ is first partitioned into K numbers of sub-matrix with column size of $l = \frac{W}{K}$. Each sub-matrix $\mathbf{B}_i \in [0,1]^{H\times l}$ is then used to generate a Bloom filter vector $\mathbf{b}_i \in [0,1]^{2^w}$ where $i = 1,2,\dots,K$ and $w \leq H$. Generation of each Bloom filter $\mathbf{b}_i$ is done by setting 1 in $\mathbf{b}_i$ according to the position(s) pointed by the codeword $x_j \in [0,2^{\mathrm{w}}-1]^w$ converted from $\mathbf{B}_i \in [0,1]^{H\times l}$ where $j = 1,2,\dots l$. During the transformation process, [54], [94] only consider the codeword x_j converted from the upper w-bits of each column in $\mathbf{B}_i$. Since multiple codewords point to the same position in the Bloom filter vector, a many-to-one effect is achieved, and this enables the alignment-robust transform. Lastly, K numbers of Bloom filters are generated as the cancellable template. To achieve renewability, Bloom filter-based approach generates the final cancellable template by applying XOR operation between the codeword $x_j \in [0,2^{\mathrm{w}}-1]^w$ and an application-specific secret T. As such, a new cancellable template can be obtained by applying a new application-specific secret onto the XOR operation. Despite the Bloom filter approach possesses a good irreversibility property (many-to-one mapping), it was not satisfying non-linkability criteria [95]. Security analysis done by Hermas *et al.* [95] showed that it is possible that two protected templates generated from the same iris input (with different T) are highly correlated. Later, Gomez-Barrero *et al.* [112] resolve the correlation issue of the Bloom filter approach by applying a row-wise permutation onto the biometric feature before the Bloom filter-based transformation takes place. Bringer *et al.* [113] showed that the original irisCode can be recovered via brute force attack (preimage attack) when the size of the application-specific secret (T) is very small. Therefore, T should be sufficiently large to provide security resistance. Yet, this could increase the performance degradation of the Bloom filter-based transformation [113].

Lai *et al.* [114] propose an alignment-robust IFO hashing to directly transform the unaligned irisCode into the alignment-robust cancellable template. The underlying concept of the alignment-robust IFO hashing is to integrate an alignment-robust transformation (Bloom Filters [54]) into the IFO transformation function. In this sense, the pre-alignment process that involves multiple shifted instances generation and transformation is not required. Specifically, [114] first utilizes the Bloom Filters to first transform the unaligned irisCode into a Bloom Filter vector $\mathbf{b}$. It is noted the $\mathbf{b}$ is generated without using any auxiliary data. After that, $\mathbf{b}$ is passed to the IFO [53] to have the cancellable template be generated. Attributed to the Bloom Filters transformation, the generated cancellable template can be directly used for matching without pre-alignment. [114] also shows the alignment-robust IFO hashing is more efficient than the original IFO hashing by comparing the authentication time. However, the performance degradation is higher than the alignment-based counterpart [53].

Ajish and AnilKumar [115] propose the Double Bloom Filter to improve the performance preservation of the Bloom Filter [54], [94] approach. Similar to Bloom Filter, the input irisCode is first partitioned into multiple sub-matrix $\mathbf{B}_i \in [0,1]^{H\times l}$. After that, each $\mathbf{B}_i$ is converted to the bloom filter vector $\mathbf{b}_i \in [0,1]^q$ by setting 1 that is pointed by the codeword where $q = 2^{w/2}$. In contrast to the canonical Bloom Filter, [115] further divide each column vector in $\mathbf{B}_i$ into upper and lower columns, and then convert each column into the codeword. The codeword converted from the upper-column is used for setting 1 in the first $q/2$ part of the $\mathbf{b}_i$; while the lower-column is used for setting another part of the $\mathbf{b}_i$. Similar to Bloom Filter, an application secret T is applied to each codeword to enable the renewability. Since the transformation function is derived from Bloom Filter, [115] is naturally alignment-robust. Despite the [115] improves the matching accuracy, the correlation between cancellable templates from the same iris is high, with the global linkage indicator $D_{\underleftrightarrow{sys}} = 0.68$ when $w = 10$.

2.2 Token management in unimodal and multimodal BTP

In this section, related works on existing (mainly face and fingerprint) template protection methods are reviewed in terms of *tokenized unimodal*, *tokenized multimodal* and *tokenless unimodal* template protection methods. A tokenized approach refers to the template protection scheme that is designed in the sense that the scheme distributes a user-specific token (storage for the transformation key) during the enrollment process. Users are required to keep the token securely where disclosure of the user-specific token could lead to many problems, e.g., zero-effort false acceptance attack [27]. On the other hand, a tokenless approach, sometimes rebranded as “one-factor template protection”, refers to the template protection approach that does not require the user to manage the user-specific key. Typically, the tokenless scheme transforms the transformation key into public information (auxiliary data) that is independent of the cancellable template and store it in the enrollment database. In this case, the user does not need to manage anything other than their biometric trait for the authentication. To the author’s best knowledge, until now, there is no *tokenless* template protection method for multimodal cancellable biometrics.

Additionally, the proposed tokenless template protection scheme demonstrates a *hybrid* characteristic (cancellable biometrics + biometric cryptosystems) where XOR notions are employed in generating the auxiliary data. Thus, this section also reviews the existing hybrid template protection works. The difference between the scheme and the existing approach will be discussed in Chapter 4.

2.2.1 Tokenized unimodal template protection

A special instance of RP, namely the *Biohashing* [24], was proposed in fingerprint template protection. Briefly, the Biohashing accepts a biometric vector $\mathbf{x} \in \mathbb{R}^n$ and a random matrix $\mathbf{R} \in \mathbb{R}^{n \times q}$ $q \leq n$. Then, the Biohashing constructs $\mathbf{y}$ by projecting $\mathbf{x}$ via inner product, i.e., $\mathbf{y} = \mathbf{xR}$, and followed by a binarization process to convert $\boldsymbol{y}$ into the bioCode $\mathbf{b} = [0,1]^q$ (cancellable template). The binarization process is shown as below:

$$b_i = \begin{cases} 0 & ,\text{if } y_i \leq \tau \\ 1 & ,\text{otherwise} \end{cases} \tag{2.3}$$

where $i = 1, \dots, q$ and τ is a binarization threshold. With the generic property, Biohashing has been propagated to other biometric modalities, e.g., face, iris, palmprint, as reported in [116]–[120]. However, the user of the Biohashing must keep the random matrix $\mathbf{R}$ (i.e., user-specific token) securely due to the problems identified in [25], [97]. In [25], the experiments showed that the Biohashing is suffering from significant performance degradation when the same random matrix $\mathbf{R}$ is applied to every user. Therefore, the adversary can break into the system easily with a false accept attack when the random matrix $\mathbf{R}$ is revealed. Other than that, the original biometric vector $\mathbf{x}$ can be recovered when the random matrix $\mathbf{R}$ is compromised. Despite the binarization process can effectively prevent the adversary to attempt for reversing the bioCode $\mathbf{b}$ to original biometric vector $\mathbf{x}$, the $\mathbf{x}$ can be recovered by a preimage attack. In [97], a pseudo-inverse operation (preimage attack) was demonstrated to estimate the original biometric vector $\mathbf{x}$ from the bioCode $\mathbf{b}$ and random matrix $\mathbf{R}$.

Wang and Hu [121] proposed a fingerprint cancellable biometric scheme that does not require an alignment process during matching. This scheme utilizes many-to-one transform machinery, so-called the "densely infinite-to-one mapping (DITOM)" to generate a cancellable template for matching. Briefly, this scheme quantizes every minutia pair into a binary string, followed by a Discrete Fourier Transformation (DFT) to transform the binary string into a complex vector $\boldsymbol{C}$. The cancellable template $\boldsymbol{T}$ is then generated by combining a randomly generated parameter key $\mathbf{R}$ with the complex vector. The combination function is described as follow:

$$\boldsymbol{T} = \mathbf{R}\boldsymbol{C} \tag{2.4}$$

Different from Biohashing, this approach generates an irreversible instance from biometric data, then combines the irreversible instance with the key to generate the cancellable template. Later in [122], Wang and Hu proposed another non-invertible transformation-based cancellable scheme on the fingerprint system that demonstrates enhanced security and accuracy compared to DITOM. In [122], the curtailed circular convolution is applied to the paired-minutiae vector to generate an alignment-free cancellable template for matching. Wang and Hu [122] also pointed out the DITOM required high memory storage due to the large key size of the auxiliary data.

Savviddes *et al.* [123] proposed the *cancelable biometric filters* (CBF) in the face template protection, which is based on the random convolution method. In this work, a randomly generated number (or PIN) is employed as the seed to form a random convolution kernel (or random kernel). After that, a set of convolved training images are generated by convolving the random kernel with a set of training facial images. A *minimum average correlation energy* (MAGE) filter $\mathbf{f}$ is then generated by the convolved training images with the formula as below:

$$\mathbf{f} = \mathbf{R}^{-1}\mathbf{X}(\mathbf{X}^{+}\mathbf{R}^{-1}\mathbf{X})^{-1}\mathbf{c} \tag{2.5}$$

where $^{+}$ denote the complex conjugate transpose, $\mathbf{X}$ denote the matrix with consist of n training images with $w \times h$ pixels, $\mathbf{R}$ denote the average power spectrum of the training images, and $\mathbf{c}$ is a vector with size n consist of the correlation values for n training images [123]. The generated MAGE filter is then stored in storage as the verification/ identification identifier. During the authentication stage, the user presents their face (to generate a facial image) and the PIN (to generate the random kernel). The given facial image and random kernel are convolved to generate a convolved facial image, which is matched to the pre-stored MAGE filter for recognition [123]. In the CBF approach, cancellability is achieved by replacing the PIN number for the kernel generation. Later, Takahashi and Hirata [124] applied a similar approach to the fingerprint system, which is based on the famous chip matching algorithm.

Cappelli *et al.* [63] proposed a state-of-art fingerprint minutiae descriptor, namely Minutia Cylinder Code (MCC). MCC is the technique to convert minutiae point set $M = \{\boldsymbol{m}_1, \boldsymbol{m}_2, \dots, \boldsymbol{m}_n\}$ to a set of cylinder $C = \{\boldsymbol{c}_1, \boldsymbol{c}_2, \dots, \boldsymbol{c}_n\}$ where each $\boldsymbol{m} = \{x, y, \theta\}$ and n is the amount of minutiae extracted, A cylinder refer to the data structure that records the directional (orientation) and spatial (position) relationships between the central minutia and its neighbourhood minutiae within a fixed radius r [63]. Despite MCC possessing superior matching performance, it is possible to obtain the original minutiae point set from the MCC template [125]. Therefore, the protected minutia cylinder code (P-MCC) was proposed to protect the MCC template. General speaking, the P-MCC method converts the MCC template $C = \{\boldsymbol{c}_1, \boldsymbol{c}_2, \dots, \boldsymbol{c}_n\}$ to P-MCC template $V = \{\boldsymbol{v}_1, \boldsymbol{v}, \dots, \boldsymbol{v}_n\}$ via a one-way transformation function so-called “B-KL projection” [125]. Although P-MCC generated an irreversible instance that ensures the security of the MCC template, users of P-MCC cannot use the same fingerprint to re-issue the P-MCC template [126]. Due to the cancellability issue, a permutation-based cancellable scheme, i.e., the two-factor protected minutia cylinder code (2P-MCC), was proposed [126]. In 2P-MCC, a user-specific secret key s is used to perform partial permutation onto the P-MCC template to generate the 2P-MCC template [126]. Therefore, renewal of a 2P-MCC template can be done by replacing the s.

In the concept of ranking-based transformation, the cancellable template is generated by replacing the value in the original biometric feature with the “index value” during transformation. A Locality Sensitive Hashing (LSH) [127] inspired cancellable scheme, namely the *Index-of-Max (IoM) Hashing* [66], was proposed to protect the fingerprint template which is generated via [62]. In the literature, LSH refers to a dimensionality reduction technique to hash the input high dimension data and map similar data to the same "bucket" [127]. In [66], there are two transformation strategies in the IoM hashing, i.e., Gaussian Random Projection (GRP) and Uniformly Random Permutation (URP). For GRP-based IoM: 1) After IoM takes input $\mathbf{x}$, the scheme generates a set of random projection matrices $\mathbf{R} = \{\mathbf{R}_1, \dots, \mathbf{R}_q\}$ where each $\mathbf{R}_i \in \mathbb{R}^{l \times d}$ and d denotes the size of $\mathbf{x}$ 2) After that, project the $\mathbf{x}$ into multiple random sub-spaces and this yields a set of projected vectors $\mathbf{v} = \{\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_q\}$ where each $\mathbf{v}_i = \mathbf{x}\mathbf{R}_i$ and $i = 1, \dots, q$; 3) Lastly, record the index value that is corresponding to the maximum value of each $\mathbf{v}_i$ and this form the IoM hashed code $\mathbf{t}_{\mathrm{GRP}} \in [0, l-1]^q$. While for URP-based IoM: 1) Generates m independent hash functions $h_i(\mathbf{x}) \in [1, k]$ where $i = 1, \dots, m$ and each $h_i(\mathbf{x})$ consist of p-order Hadamard product; 2) The IoM hashed code $\mathbf{t}_{\mathrm{URP}} \in [1, k]^m$ is then formed by concatenating the output from the m hash functions $h(\mathbf{x})$. To achieve cancelability, IoM applied the replace token: gaussian projection matrices $\mathbf{R}$ (for GRP-based IoM) and p-order Hadamard product (for URP-based IoM) during the enrollment of IoM hashed codes [66].

2.2.2 Tokenless unimodal template protection

Ouda *et al.* [103] proposed the tokenless template protection scheme, namely "*BioEncoding*". The BioEncoding was discussed earlier in section 2.1 by focusing on the pre-alignment process required in the scheme. This scheme is revisited in this subsection because it is the preemptive tokenless cancellable biometric scheme in the literature. Apart from the discussion in section 2.1, this subsection focuses on the tokenless property of the scheme. In [49], the two required inputs to generate the BioCode $\mathbf{b} \in [0,1]^{\mathrm{n/m}}$ are the irisCode $\mathbf{c} \in [0,1]^n$ and a randomly generated transformation key $S \in [0,1]^{2^m - 1}$ where m is a system parameter which will be discussed later. After $\mathbf{c}$ and S are inputted to the scheme, the following procedures are carried out to embed the two entities into the $\mathbf{b}$: 1) $\mathbf{c}$ is segmented into several binary blocks with m-bits; 2) The binary blocks are then converted to a set of integer value which yields an integer vector $\mathbf{x} \in [0, 2^{m-1}]^{n/m}$; and 3) Each $x \in \mathbf{x}$ is transformed into the binary value via following Boolean function $f(.)$:

$$f(x_i) = S[x_i] \tag{2.6}$$

where $S[x_i]$ returns the x_i-th binary value in S. In this sense, the S is used to build the Boolean function. The BioCode $\mathbf{b}$ is formed after each of $x \in \mathbf{x}$ are converted to the binary vector. With the many-to-one mapping process, it is hard for the adversary to recover the original irisCode $\mathbf{c}$ from the BioCode $\mathbf{b}$ even if the transformation key S is publicly known. Therefore, the transformation key S is directly stored in the database as a publicly accessible system parameter to realize the tokenless authentication [103]. However, Lacharme [96] revealed that the original biometric data $\mathbf{b}$ can be recovered when multiple sets of transformation key S and BioCode $\mathbf{b}$ is known to the adversary. Specifically, the adversary could perform cross-correlation analysis between multiple sets of S and $\mathbf{b}$ to recover the original irisCode $\mathbf{c}$. Thus, the tokenless property of BioEncoding is questionable.

Inspired by LSH-based iris template protection - IFO hashing [53], Kim and Teoh [128] propose tokenless IFO hashing for fingerprint systems. In the tokenless IFO, two independent IFO transformation functions are deployed to generate the cancellable template [53]. During the enrollment stage, the biometric input $\mathbf{x}$ is transformed into the IFO hashed code $\mathbf{h}_1$ with a randomly generated permutation seed. In the meantime, a random bit-string $\mathbf{r}$ is transformed in the second IFO hashed code $\mathbf{h}_2$ with the second permutation seed. The $\mathbf{h}_2$ is served as the pseudo-identifier for matching. After that, the $\mathbf{h}_1$ and $\mathbf{h}_2$ are XOR-ed and yield a XOR vector $\mathbf{c} = \mathbf{h}_1 \oplus \mathbf{h}_2$. At the end of enrollment, every information including $\mathbf{h}_2$, $\mathbf{c}$, permutation seed 1 and permutation seed 2 are stored in the database. During the verification, the $\mathbf{h}_2{}'$ is recovered by the $\mathbf{h}_1{}'$ generated from the user. After that, the recovered $\mathbf{h}_2{}'$ is processed by IFO hashing and yields the query template $\mathbf{c}'$ for matching. Since the $\mathbf{h}_1{}'$ can only be re-generated by the genuine user, all the auxiliary information could be stored in the database for realizing tokenless authentication.

2.2.3 Tokenized multimodal template protection

With the drawback of unimodal *Biohashing* that degrades the matching performance, Nanni and Lumini [129] extended the Biohashing to a multimodal system [129]. In [129], Biohashing was used to transform the face and fingerprint templates separately. During the verification stage, a fused matching score is calculated by using the mean rule on the outcomes of face authentication and fingerprint authentication [129]. On the other hand, Maiorana *et al.* [130] proposed another score-level fusion cancellable scheme, namely the *Bioconvolving* in an online signature-based biometric system. Instead of fusing the matching score of different biometric features, Bioconvolving fuses matching scores of different matchers for the same signature feature. In Bioconvolving, the two widely used signature matchers, i.e., Hidden Markov Models (HMMs) and Dynamic Time Warping (DTW), are employed during the cancellable template matching [130]. After that, the outcomes of two matches are fused together to estimate the fused matching score. As reported in [129], [130], the matching performance of score-level fusion is outperforming the unimodal cancellable system.

Paul and Gavrilova [131] proposed a feature-level fusion cancellable scheme that is based on *random projection* and the *feature extraction and selection in the transformed domain*. At first, the ear and face images are divided into two parts (e.g., ear fold 1 and ear fold 2) via a pseudorandom function. The parts of ear and face images are then combined to form two fused images (e.g., ear-face fold 1). After that, the two fused images are transformed into a single cancellable template through the following procedures: 1) The fused images are transformed to low-dimension features via random projection and principal component analysis (PCA); 2) With k-means clustering, a distance-based feature is extracted from each low-dimension feature; and 3) The two distance-based features are then combined by the linear discrimination analysis (LDA) to form the final cancellable template. As shown in [131], the matching performance of the fused cancellable template is better than the unimodal cancellable template. Since the biometric source is represented in an image, the incompatible issue of biometric feature vectors (e.g., feature type, feature-length) does not exist in [131].

Chin *et al.* [132] proposed feature-level fusion on fingerprint and palmprint-based biometric systems. Briefly, [132] is a three-stage hybrid method that transforms fingerprint and palmprint templates into a single cancellable template. At first, the normalized fingerprint and palmprint images are integrated into a fused feature by an XOR operation. Then, the fused feature is transformed into another form, so-called the *RT feature,* by a parameterized function (known as Random Tiling, RT). Generally speaking, with a user-specific key, the Random Tiling extracts a set of random rectangles (RT feature) from the fused feature; thus, the renewability property of [132] is achieved by replacing the key for RT transformation. Lastly, the RT feature is binarized to produce a bit-string template as the final cancellable template.

In [133], Rathgeb *et al.* proposed a *multimodal Bloom filter* that performs feature-level fusion on face and iris templates to generate the cancellable template. Briefly, the multimodal Bloom filter [133] performs Bloom filter transformation (refer to [94]) on the binary face feature and irisCode separately to generate a cancellable face template $\mathbf{C}_{\text{face}}$ and cancellable iris template $\mathbf{C}_{\text{iris}}$. After that, the two entities are fused together to generate the final cancellable template $\mathbf{C}$ as below:

$$\mathbf{C} = \text{OR}(\mathbf{C}_{\text{face}}, \mathbf{C}_{\text{iris}}) \tag{2.7}$$

where the OR(.) denotes the bitwise-OR operation. Recently, Gomez *et al.* [99] enhanced the multimodal Bloom filter framework and propagated the methodology to face + finger-vein and face + iris-based systems. In [99], a weighted fusion strategy was proposed for the enhanced multimodal Bloom filter transformation, and it can increase the matching accuracy when fusing multiple biometric features in different sizes [99]. During the Bloom filter transformation, a weight α_i is allocated to each cancellable template $\mathbf{C}_i$ where $i = 1 \ldots n$ indicates the number of different biometric characteristics. After that, the weighted sum (i.e., weight × similarity score) is calculated as the fused score. The formula is re-written as below:

$$S = \sum_{i=1}^{n} (\alpha_i \times HD(\mathbf{C}_i, \mathbf{C}_i')) \tag{2.8}$$

where $HD(.)$ denotes the Hamming distance function, n represents the number of biometric characteristics and $\mathbf{C}_i'$ denote the query template.

Recently, Yang *et al.* [134] proposed a non-invertible transformation-based cancellable scheme, namely the *enhanced partial discrete Fourier transform (EP-DPT)* in the fingerprint and fingervein-based biometric system. In general, the EP-DPT performs feature-level fusion on the minutiae-based fingerprint feature and image-based finger-vein feature into a single cancellable template. In [134], the bit-string fingerprint template $\mathbf{x}_{\text{face}} \in [0,1]^d$ and finger-vein template $\mathbf{x}_{\text{vein}} \in [0,1]^d$ are transformed into a single cancellable template $\mathbf{c} \in [0,1]^m$ where d is the size of the bit-string template and m is the size of the cancellable template.

2.2.4 Hybrid template protection

Ao and Li [135] proposed a key binding scheme that integrates the cancellable biometric scheme (*Biohashing* [24]) and a key binding scheme (*Bose-Chaudhuri-Hocquenghem*, BCH) in face biometrics. The primary goal of [135] is to bind the cancellable template (generated by Biohashing) with a cryptographic key. Initially, [135] followed the Biohashing technique to transform the near-infrared (NIR) face image to a binary string $\mathbf{b}$ (or Biohashed code) for the cancellability. Then, the binary string $\mathbf{b}$ is used as the input for the BCH scheme to bind a cryptographic key. Due to the fact that ECC algorithm cannot be applied on the binary string $\mathbf{b}$, [135] enhanced the Biohashing by applying a NXOR mask onto the binary string $\mathbf{b}$ before it is input to the Error Correction Code (ECC) (a component of BCH key binding scheme). During authentication stage, the same NXOR mask is applied to the binary string $\mathbf{b}'$ before the key release process. Application of the NXOR mask provides a more reliable binding process for a biometric key where the performance degradation was minimized to 1~2% degradation rate [135].

Feng *et al.* [136] proposed another hybrid cancellable biometric scheme to protect the face templates. Briefly, [136] is a three-stage transformation scheme that integrates the cancellable transformation (i.e., *random projection*) and biometric cryptosystem (i.e., *fuzzy commitment*) in generating a secure face template. At first, the random projection (RP) transforms the input face template $\mathbf{x}$ to a projected vector $\mathbf{v}=\mathbf{xR}$ to achieve the *cancellability* where $\mathbf{R}$ is the projection matrix (in the form of *user-specific token*). After that, the projected vector $\mathbf{v}$ is binarized by the discriminability preserving (DP) transformation and yield a binary vector $\mathbf{b}$. Lastly, the $\mathbf{b}$ is passed to the *fuzzy commitment* (with ECC enabled) to produce an encrypted template $\mathbf{e}$ and auxiliary data $\mathbf{a}$, During authentication, the input face template $\mathbf{x}'$ is firstly used to release a binary vector $\mathbf{b}'$ from $\mathbf{a}$ via fuzzy commitment. Lastly, the $\mathbf{b}'$ is encrypted to the query template $\mathbf{e}'$ for matching.

Jin *et al.* [137] proposed a biometric key binding scheme using cancellable transform for fingerprint templates. Given a binary key, the binding/release idea is to encode 1s with true templates while encodes 0s with synthetic templates. Cancellable transform is used to generate multiple cancellable templates in order to encode multiple 0s and 1s in the cryptographic key. Error correction code (ECC) is abandoned in this proposal. Hence, vulnerabilities, e.g., performance-key size trade-off and statistical attack associated with

ECCs no longer exist. Although the primary goal of this proposal is meant to bind/release a cryptographic key (key protection), cancellable transform enables the secure templates generation (template protection).

2.3 Security and privacy of thresholding-based decision making

A (protected and unprotected) biometric system is manifested as a thresholding-based decision system that determines the identity of the individual based on the similarity score that is acquired from the similarity comparison between the enrolled and query instances. In this case, the adversary could exploit the similarity score obtained from the matching process and launch an attack that aims to breach the security and privacy of the biometric system. In the biometric research area, this attack is sometimes rebranded as a type-4 attack in a biometric system [27]. In this kind of attack, the adversary aims to acquire a guessed biometric template (or preimage) that is highly similar to the enrolled biometric template by means of trial-and-error towards the matcher module. More deadly, this attack does not require the adversary to compromise the template storage. This consequence of this attack is further exacerbated in a biometric system that directly stores the original biometric feature in the storage since a high similarity score usually indicates that the guessed template is approximately close to the original biometric template, which leads to the reconstruction of the biometric template in the existing studies. This enables the adversary to conduct a replay attack (to other applications) due to the irrevocable trait of the biometric feature. In this section, the existing works that are related to the injection of the guessed biometric template before the matcher module are revisited. To the author’s best knowledge, there are limited works to improve the security resistance of the biometric system towards this type of attack in terms of the matching mechanism. Therefore, the literature review in this section focuses on the type-4 attack, which corresponds to the contribution iv of this thesis.

A brute-force attack is the most straightforward approach that performs trial-and-error on every possible combination of guessed query biometric templates towards the biometric system until access is granted. In [138], a brute-force attack model is formalized towards a minutiae point-based fingerprint system. In the naïve approach, the attack complexity of the brute-force attack is determined by the probability that each guessed minutia is matched to one of the minutiae in the enrolled fingerprint template. The probability p is calculated as below

$$p = \frac{N}{K * d} \tag{2.9}$$

where N is the total number of minutiae in the fingerprint template, d denotes the total possible value for the minutia orientation, and K is the possible value for the minutia position. In addition to the naïve approach, [138] factors in the probability of minutia are counted as the middle point of the fingerprint to leverage a more realistic scenario. Nevertheless, the exhaustive search manner of the brute-force attack requires high attack complexity for a successful attempt, which is infeasible for a biometric template that is sufficiently large in terms of template space. This is pointed out by [138], where the brute-force attack is plausible when the number of the information for the fingerprint template is small. By increasing the number of information, the attack complexity for the brute-force attack is increasing drastically.

Knowing that high complexity is required for a brute-force approach, the hill-climbing approach is then introduced in the literature. Hill climbing is a mathematical local optimization technique that employs iterative modification onto the guessed instance until an optimal result is achieved. In a biometric system, a hill climbing-based attack model usually starts by randomly guessing a biometric template and injecting it into the matcher module. After that, the attack model intercepts the similarity score from the matching process and factors it into the modification scheme to improve the guessed template. In [26], Uludag and Jain devise a hill climbing-based attack model that is targeted towards an (unprotected) minutiae-based fingerprint system. In this work, the adversary aims to bypass the authentication process using a guessed minutiae template that is sufficient to be recognized as a genuine user. The five steps procedures of the attack framework in [26] are: 1) The attack framework initializes n numbers of guessed minutiae template, each with m numbers of minutiae points; 2) Iteratively inject the n numbers of guessed minutiae template into the system and intercept the matching scores for each comparison; 3) Based on the matching scores intercept, the attack framework selects the best matching template as the initial guessed template for the modification attempt; 4) After acquiring the initial guessed template, a series of operations, i.e., perturbation, insertion, replacement and deletion are performed towards the guessed template; 5) Inject the modified template to the matcher module to obtain the matching result. The step 4-5 repeats until the matching score surpass the system threshold. Since the minimum distance between the ridges is identified as 9 pixels, a rectangular grid (with 9×9 cells) is applied to avoid the creation of minutiae points that are close to each other during the step 1. Besides that, the orientation for each guessed minutiae point is selected from 16 possible values that are quantized from the range of $[0,2\pi)$. Attributed to the grid formulation and the orientation quantization, the total numbers of possible values for each guessed minutiae point are greatly reduced; and thus, this attack framework is more efficient than the brute-force approach.

Marta *et al.* [139], [140] proposed another hill climbing-based attack to exploit the privacy aspect of the online signature and face verification system in the sense that the biometric feature is reconstructed via the attack framework. In [139], [140], the Nelder-Mead (or Downhill Simplex) algorithm [141] is adopted as the modification scheme to update the guessed biometric feature that is in the format of the fixed-dimensional real-valued vector. In this attack, the operation to obtain a similarity score between the enrolled biometric template and the guessed instance refers to evaluating an objective function $F(.)$. Since the biometric comparison of the targeted biometric system relies on a normalized similarity score (not distance), the Downhill Simplex algorithm is operated inversely such that the modification scheme is maximizing the $F(.)$. Thus, this attack is rebranded as Uphill Simplex Hill Climbing. Suppose a biometric feature $\mathbf{x} \in \mathbb{R}^n$ with n dimensions, this attack framework is formed by a series of iterative process are as follow: 1) the attack framework first establish $n+1$ numbers of guessed instances (simplex vertices) $\mathbf{x}_v$ where $v = 1,2,\dots,n+1$ and each $x \in \mathbf{x}_v$ is randomly chosen from the statistical model of a pool of users; 2) Compute the centroid $\mathbf{c}$ of the vertices by averaging the value of every $\mathbf{x}_v$ where $v = 1,2,\dots,n+1$; 3) After that, the attack framework evaluate the $F(.)$ of $\mathbf{x}_v$ where $v = 1,2,\dots,n+1$ to identify the $\mathbf{x}_h$ (vertex with highest matching score) and $\mathbf{x}_l$ (vertex with lowest matching score); 4) The computed $\mathbf{c}$, $\mathbf{x}_h$ and $\mathbf{x}_l$, are then inputted to the Nelder-Mead algorithm [141] to update each $\mathbf{x}_v$ with a series of processes, i.e., expansion and contraction. The step 2-4 repeat until the maximum iteration is reached or the matching score surpasses the system threshold. Since the attacks were targeted onto the biometric system that directly stores the original biometric feature in the template storage, a successful attack attempt means the reconstruction of the original biometric feature. As such, the estimated template can be used for replay attack due to the irrevocable traits of biometrics. This also shows the importance of employing biometric template protection (BTP) in a biometric system to mitigate the effect of the type-4 attack.

Hill climbing is an optimization technique that finds the best solution by means of local search. The output guessed feature of a hill climbing-based attack is the best solution (*hereafter* refer as local optimum) bounded by its neighboring candidature solutions. As such, it could lead to the situation that there is no feasible guessed feature throughout the attack (refer to as the local optimum problem). To overcome this problem, Pashalidis [142] devised another variation of hill climbing-based attacks, namely the simulated annealing attack, to bypass the authentication process of a minutiae-based fingerprint system. The attack is optimized for the fingerprint system that employs the vicinity-based matcher, where it is not required to explore the entire search space during the attack attempt. Furthermore, this work demonstrates the possibility of conducting the type-4 attack in biometric template protection (BTP)-enabled system since the experiments in [142] were conducted on the PMCC [125] enabled fingerprint system. Similar to the aforementioned attacks, the simulated annealing attack is an iterative modification process of improving the guessed biometric template until a desirable authentication outcome is achieved. The initial step of this attack is to create an initially guessed fingerprint template T which contains $a \times b$ numbers of vicinities. Each vicinity is formed by n numbers of minutiae where n is randomly chosen within the range from $n_{\min}$ until $n_{\max}$, and the attributes of the minutiae (i.e., location and orientation) are randomly generated. After that, the attack create a candidature guessed fingerprint template T' by replacing one vicinity in the T with a randomly generated vicinity and inject the T' to the system for matching. The attack then set $T = T'$ if the matching score of T' is higher than the T. Differ to the classical hill climbing-based attack, the simulated annealing attack occasionally replace the T to a T' that possesses a lower matching score based on a configurable probability to reduce the local optimal problem. Although the aforementioned works show the possibility of obtaining a guessed biometric template with sufficient matching score in a BTP-enabled system, the works never show the guessed biometric template can compromise the privacy of the system especially when the stored template is a cancellable template that can be revoked and renewed.

Although the brute-force, hill climbing, and simulated annealing-based attacks can be used to obtain a guessed biometric template with a sufficient matching score, the attack complexity tends to be higher when the template space is sufficiently large. Knowing the bottleneck of the local search algorithm (e.g., hill climbing), the population-based search algorithm (e.g., genetic algorithm) is then explored to study the security and privacy of biometric authentication. A genetic algorithm (GA) is an optimization algorithm that imitates the biological genetic development process that can be divided into natural selection, genetics and evolution [143]. Differ from the local search approaches that iteratively modify a guessed biometric template, the GA modifies a list of guessed biometric templates (so-called population) within a fixed interval of attack iterations. Given a list of guessed biometric templates that are randomly initialized, the GA performs a series of processes in each attack iteration: selection, crossover and mutation. In each iteration, the selection process is first conducted to choose the template with the high matching score as the parents. After that, the crossover process creates the children by mixing a portion of the parent with randomly generated information. The children refer to the list of guessed biometric templates (population) for the next iteration of the attack. The last step in each attack iteration is the mutation process that randomly perturbs the children to diversify the population. The attack continues until the best matching score from the population is higher than the system threshold or the maximum attack iteration is reached. Galbally *et al.* [31] demonstrate the utilization of the genetic algorithm in reconstructing the iris image without prior knowledge towards the binary irisCode that is stored in the system. Specifically, the attack framework utilizes the genetic algorithm that aims to minimize the pairwise irisCodes distance by iteratively modifying the guessed iris image until the desired result (i.e., high similarity score) is achieved. In [31], the necessity of having biometric template protection is mentioned so that the possibility of the original biometric template being reconstructed can be reduced.

Knowing that biometric template protection is essential in preventing the original biometric template from being reconstructed, [29] studies both security and privacy aspects of a fingerprint system that is enforced by the Protected Minutia Cylinder Code (PMCC) [125]. In [29], security refers to the case that the guessed fingerprint template can achieve a sufficient matching score and bypass the authentication process, while privacy refers to the case that the guessed fingerprint template is identical to the original fingerprint template. Since PMCC is a transformation-based template protection scheme, the attack is conducted by guessing the input for the PMCC scheme. Specifically, the attack framework utilizes the population-based modification traits of the genetic algorithm to first populate a group of guessed fingerprint templates. After that, the guessed templates are fed to the PMCC to have the transformed templates to be generated and matched to the pre-stored template. Similar to most of the aforementioned attacks, the attack is an iterative modification scheme that continues until the authentication is granted or the max iteration is reached. Due to the thresholding decision-making nature of the PMCC, the attack framework is able to obtain a guessed fingerprint template that can be used to bypass the authentication process. Despite the [29] is able to compromise the security (authentication process) of the system, the privacy aspect of the system is protected where the guessed fingerprint template is not identical to the original fingerprint template. This also shows that it is important to employ biometric template protection in a biometric system.

2.4 Summary

In this chapter, the existing biometric template protection (BTP) related works are revisited, and the revisited works are mostly associated with the face, fingerprint and iris modalities. The works are presented in section-by-section based on the main issue identified: (i) alignment problem in iris template protection, (ii) token management in unimodal and multimodal BTP and (iii) security and privacy of thresholding-based decision making. Despite there are various numbers of work introduced in the literature, biometric template protection is still an open issue with a few concerns, e.g., verification performance, alignment issue, token management and security vulnerabilities that have yet to be fully solved. For a quick overview, the reviewed works are summarized in the three tables below in the respective categories, with Table 2.1 summarizing the existing iris template protection scheme. The iris template protection schemes are revisited in regard to the capability of handling the unaligned iris feature during the transformation process. Although a number of works showed the capability of directly transforming the unaligned iris feature, it is noticed that certain vulnerabilities are yet fully resolved. Table 2.2 covers the existing unimodal and multimodal template protection works in terms of tokenized and tokenless authentications. It is observed that there are limited studies on the template protection scheme that can address token management and biometric fusion problems simultaneously. Lastly, Table 2.3 outlines the compromisation of the security and privacy aspects in a biometric matching process through the type-4 attack. The reviewed works demonstrate the importance of biometric template protection to conceal the original biometric feature in the sense that the original biometric feature cannot be fully recovered even if the matching process of a BTP-enabled system is compromised. Yet, there is limited study on a solution that can further enhance the security resistance of the BTP-enabled system in terms of the threshold selection. This drove the author to explore the type-4 attack as well as a solution that can further improve the security resistance of the BTP-enabled system.

Enlightened from these impactful works, the author carried out research, and the outcomes of this thesis are: (i) an iris template protection scheme with the alignment-robust property, (ii) two tokenless face and fingerprint-based template protection schemes, (iii) a robust matching mechanism that improves the security resistance of the system and (iv) an automated type-4 attack scheme that aims to bypass the authentication process. The proposals are presented in the remaining parts of this thesis on a chapter-by-chapter basis, with Chapter 3 presenting the work (i), Chapter 4 presenting the work (ii), and Chapter 5 presenting the works (iii) and (iv).

Table 2.1: Summary of reviewed works in section 2.1

Method	Alignment Mechanism	Technique	Observation(s)
Alignment-based approach			
Pillai *et al.* [101], [102]	- Two-stage alignment estimation	- Biometric Salting - Random Projection with partitioning approach	- Increased computation overhead due to the two-stage pre-alignment process - User-specific token required
Ouda *et al* [103] (BioEncoding)	- Shifting-based consistent bit vector generation	- Random many-to-one mapping - Random XOR/ permutation before BioEncoding [105]	- Increased computation overhead due to multiple irisCode extractions for handling irisCode misalignment
Hämmerle-Uhl *et al.* [106]	- Shifting bit-mask during matching	- Biometric Salting - Key-dependent wavelet transform	- Token management issue [106]
Dwivedi *et al.* [109], [110]	- Rotation invariance mechanism - Consistent bit generation	- Lookup table mapping	- Performance degradation when transforming unaligned irisCode - Reference images required for generating rotation invariant code
Lai *et al.* [53] (IFO hashing)	- Consistent bit vector generation	- Locality Sensitive Hashing (LSH) - Min-Hash	- High computation overhead and increased matching time due to the shifting-based alignment process [114]
Alignment-robust approach			
Zuo *et al.* [18]	- The shifted row of iris feature share the same orientation	- Biometric Salting - Random offset shifting - Combination of features via multiplication/ addition (GRAY-COMBO) or XOR/ XNOR (BIN-COMBO)	- High quality of input iris image required [18]
Rathgeb *et al.* [54], [94] and Marta *et al.* [112] (Bloom Filters)	- Many-to-one mapping	- Bloom Filter mapping	For [54], [94]: - Unlinkability not satisfied [95]

		- Binary-to-decimal conversion (many-to-one) - Row-wise permutation [112]	- Vulnerable to preimage attack when key space is small [113] For [112]: - Resolves linkage issue of previous works
Lai *et al.* [114]	- Integration of Bloom Filter	- Bloom Filter - IFO	- Higher performance degradation
Ajish and AnilKumar [115]	- Bloom Filter transform	- Divide a bloom filter into upper and lower parts	- High template linkage

Table 2.2: Summary of reviewed works in section 2.2

Method	Biometric Modality	Technique	Observation(s)
Tokenized (or two-factor) unimodal template protection			
Teoh *et al.* [24] (BioHashing)	Fingerprint	- Random Projection - Uni-step binarization	- Token management issue [25], [97] - Performance degradation [25]
Wang and Hu [121] (densely infinite-to-one mapping, DITOM)	Fingerprint	- Discrete Fourier Transformation - Random Projection	- The large size of the auxiliary data [122]
Savviddes *et al.* [123] (Cancelable biometric filters, CBF)	Face	- Random convolution	- Training required - The user needs to memorize the PIN
Cappelli *et al.* [63], [126] (2P-MCC)	Fingerprint	- KL projection + Binarization - Full/ partial permutation	- Specific for fingerprint minutia descriptor (MCC [63])
Jin *et al.* [66] (IoM hashing)	Fingerprint	- Ranking-based locality-sensitive hashing	- Performance degradation
Tokenless (or one-factor) unimodal template protection			
Ouda *et al.* [103] (BioEncoding)	Iris	- Consistent bit vector generation - Random many-to-one mapping - Random XOR/ permutation before BioEncoding [105]	- Vulnerable to cross-correlation attack [105] - IrisCode is recoverable when the random key is disclosed [96]
Kim and Teoh [128] (One-factor IFO hashing)	Fingerprint	- Two-stages IFO hashing - Locality sensitive hashing	- Performance degradation - Specific for binary input
Tokenized (or two-factor) multimodal template protection			
Nanni and Lumini [129]	- Face - Fingerprint	- Biohashing transformation - Score-level fusion	- User-specific token required - Increased computation overhead and storage space due to multiple
Maiorana *et al.* [130] (Bioconvolving)	On-line signature templates	- Random mapping - Score-level fusion via Hidden Markov Models	- The user-specific token is required

		(HMMs) and Dynamic Time Warping	
Paul and Gavrilova [131]	- Ear - Face	- Random projection and principal component analysis (PCA) - Feature-level fusion via linear discrimination analysis (LDA)	- The user-specific token is required
Chin *et al.* [132]	- Fingerprint - Palmprint	- Feature fusion via XOR operation - User-specific key guided random rectangle extraction	- The user-specific token required
Rathgeb *et al.* [133]	- Face - Iris	- Bloom Filter transformation - Weighted sum-based score-level fusion	- User-specific token required - Increased computation overhead due to multiple Bloom Filter transformations is required
Yang *et al.* [134]	- Finger-vein - Fingerprint	- Discrete Fourier Transform	- User-specific token required
Hybrid scheme (cancellable biometrics + biometric cryptosystems)			
Ao and Li [135]	Fingerprint	- Biohashing - BCH key binding	- Error Correction Code (ECC) required
Feng *et al.* [136]	Face	- Random projection - Fuzzy commitment - Discriminability preserving transformation	- User-specific token required
Jin *et al.* [137]	Fingerprint	- Random permutation - Minutiae vicinity decomposition (MVD) - Randomized GHE	- Error Correction Code (ECC) is not required for the key binding

Table 2.3: Summary of reviewed works in section 2.3

Method	Targeted System	Technique	Observation(s)
Ratha *et al.* [138]	Unprotected fingerprint minutiae-based system	- Brute-force attack	- High attack complexity due to exhaustively search manner
Uludag and Jain [26]	Unprotected fingerprint minutiae-based system	- Manual hill-climbing	- Quantize the search space (e.g., fingerprint orientation) to reduce attack complexity - Specific for fingerprint minutiae-based system
Marta *et al.* [139], [140]	Unprotected face and online signature systems	- Uphill simplex algorithm	- The estimated feature can be used for a replay attack - The importance of biometric template protection is highlighted
Pashalidis [142]	PMCC protected fingerprint system	- Simulated annealing algorithm	- Optimized for fingerprint vicinity-based system

			- The possibility of bypassing the authentication in a protected system is demonstrated - The attack scheme is not tested for compromising the privacy aspect of the targeted system
Galbally *et al.* [31]	Unprotected Iris system	- Genetic algorithm	- Possibility of recovering the input irisCode - The importance of biometric template protection is highlighted
Rozsa *et al.* [29]	PMCC protected fingerprint system	- Genetic algorithm	- The possibility of bypassing the authentication in a protected system is evidenced with experimental results - Highlights the biometric template protection guarantee the privacy aspect because the estimated template is not identical to the original input biometric template

Chapter 3 Alignment-robust Iris Template Protection

In this chapter, the alignment problem (bit-displacement) of the irisCode template protection is addressed, and a Histogram of Oriented Gradient (HoG) inspired cancellable biometrics, coined as Random Augmented Histogram of Gradients (R·HoG) is proposed. The proposed R·HoG is constructed based on two main mechanisms: 1) column vector-wise random augmentation and 2) gradient orientation grouping to protect the irisCode. The essence of the proposed R·HoG is an alignment-robust scheme that can produce an alignment-robust cancellable template, which is crucial for an efficient authentication process. The experimental result shows reasonable performance on the benchmarking CasiaV3 iris dataset with the lowest EER= 0.62% in the protected system. It is worth noticing that the performance preservation is acceptable as compared to the original counterpart (EER= 0.50%). Other than that, the irreversibility and security properties are studied with major security and privacy attacks in the biometric system, e.g., false acceptance attack and birthday attack. With the quantitative evaluation framework, the proposed scheme is shown to satisfy the unlinkability property.

3.1 Background

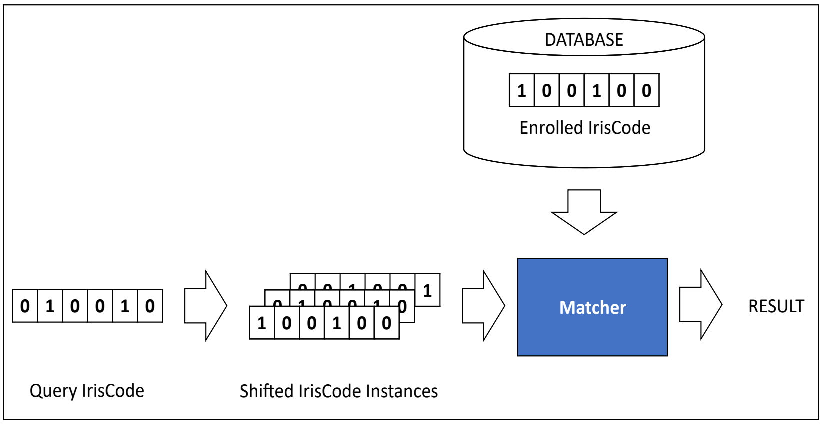


Fig 3.1. Graphical representation of shifting-based matching for unaligned IrisCode with horizontal ± 1 bit shifting (adopted from [144])

Iris is one of the most promising biometric traits for identity verification because of the rich entropy in the iris pattern [44]. In iris recognition, IrisCode is the well-known iris feature descriptor although many alternatives are introduced in the literature [38], [145]. Due to the rotational inconsistency of the iris image (caused by head tilt) during the acquisition process, it is known that the extracted irisCode possesses a bit-displacement (or alignment) issue. For instance, the query irisCode cannot be directly matched to the enrolled irisCode even the irisCodes are extracted from the same iris. To achieve the optimal verification result, pre-alignment of the IrisCode templates is required during the authentication process [144], [146], [147]. One common approach is to perform horizontal shift for $\pm n$ bits on the query IrisCode to produce up to $2n + 1$ shifted instances (e.g., [53], [94], [144], [147]). The final verification result is done by obtaining the highest matching score from the comparison between the enrolled irisCode and the shifted instances. One drawback of the pre-alignment process is that it increases the processing overhead for the iterative shifting process. This problem is amplified when an additional mechanism, e.g., biometric template protection is applied to the iris verification system. Despite a number of iris template protection methods, iris template protection is still an unsolved issue. For instance, the recently developed IFO hashing [53] is identified from suffering the high processing overhead where multiple rounds of transformation and matching are required. Hence, it urges for a new alignment-robust solution to protect the iris feature.

In this chapter, a cancellable biometric scheme, namely the Random Augmented Histogram of Gradients (R·HoG) is introduced to protect the irisCode. Unlike existing biometric works that consider HoG as a feature extraction method [148]–[150], this chapter demonstrates a new variant of HoG that can directly transform the unaligned irisCode feature into an *alignment-robust* cancellable template. The motivations that HoG is a suitable descriptor to enable the cancellable biometric scheme are outlined as below:

- HoG is derived by statistical readings of the local information, which possesses the alignment-free property. Hence, this mechanism can be used to eliminate the irisCode bit-shifting process (alignment) when performing the cancellable transformation.

- A many-to-one mapping was utilized in HoG to offer the concealment of the original feature vector, which is critical for the non-invertible property.

Since the resultant cancellable template is robust towards the alignment issue, feature alignment is not required during the authentication process, and this increases the efficiency of the authentication process. Contributions of this chapter are explained as follows:

- A new cancellable biometric scheme, namely the random augmented histogram of gradients (R·HoG) is introduced to protect the iris feature. The proposed scheme is inspired by the well-known histogram of oriented gradients in object detection [151]–[153] to directly transform the unaligned irisCode feature into a renewable and irreversible template. The generated template is alignment-robust.

- Verification performance is justified on the benchmarking CASIA-IrisV3 dataset and compared to the state-of-the-art iris cancellable biometric schemes. Other than that, benchmarking evaluation frameworks are employed to validate unlinkability property

- Rigorously analysis of the security and privacy aspects of R·HoG is carried out in both qualitative and quantitative manners. Particularly, existing major attacks, e.g., attack via input enumerations, brute force attack, false acceptance attack and birthday attack, are conducted, and the attack complexity is calculated.

This chapter is organized as follows: Section 3.2 discusses the preliminaries relevant to the proposed scheme, followed by the methodology (i.e., enrollment and verification phases) in section 3.3. Section 3.4 presents the experiment result in terms of parameters estimation and computation efficiency. After that, section 3.5 evaluates the proposed scheme. Lastly, the findings of this chapter are summarized in section 3.6.

3.2 Preliminary

This section presents the histogram of oriented gradient (HoG) on which the proposed cancellable biometric scheme is built upon.

3.2.1 Histogram of oriented gradient (HoG)

Histogram of oriented gradient (HoG) [151]–[153] is a feature descriptor that has been widely used within the field of computer vision (CV) to detect an object in an image. In general, a HoG descriptor is formed by characterizing the local structure and shape of the object by means of gradient magnitudes and orientations. For a simple view of HoG feature extraction, a histogram is used to statistically record the frequency distribution (gradient magnitude) of the gradient orientations in localized portions of an image. The implementation of a classical HoG feature extraction is described as follows:

1) Given an image I, the HoG extraction technique divides the I into several overlapping regions called cells and computes a histogram of gradient orientations for each cell. Each histogram bin is defined by a fixed-range orientation across $0° - 180°$ or $0° - 360°$.

2) After that, each cell adds the gradient magnitude to the corresponding histogram bin.

3) Lastly, normalization of the histograms is applied to improve the robustness of the HoG feature towards the illumination variation. In the HoG algorithm, several overlapping cells are grouped as a block, and the normalization is done in each block. In the end, the normalized block histograms represent the HoG descriptor.

3.3 Methodology

This section is devoted to presenting the proposed alignment-robust biometric template protection scheme. Notations being used in the methodology are provided in the table below.

Table 3.1: NOMENCLATURE

Notation(s)	Description
$\mathbf{Z} \in [0,1]^{m \times n}$	Unaligned irisCode
$\ddot{\mathbf{Z}} \in [0,1]^{d \times n}$	Random augmented biometric matrix
$\acute{\mathbf{Z}} \in \mathbb{R}^{d \times n}$	Gradient orientation matrix
$\dddot{\mathbf{Z}} \in \mathbb{R}^{d \times n}$	Gradient magnitude matrix
$\mathbf{X} \in [-1,1]^{d \times n}$	Neighbour horizontal difference
$\mathbf{Y} \in [-1,1]^{d \times n}$	Neighbour vertical difference
$\mathbf{p} \in [1, m]^{d}$	Random augmentation seed
$\mathbf{t} \in \mathbb{R}^{h}$	Local histogram vector
$\mathbf{c} \in \mathbb{R}^{ho}$	Alignment-robust biometric vector (cancellable template)
$a \in \mathbb{Z}$	Segment column size
$b \in \mathbb{Z}$	Segment row size
$h \in \mathbb{Z}$	Local histogram vector bins
$o \in \mathbb{Z}$	Number of partitioned biometric vector
$\beta = \frac{d}{b}$	Feature dimension for each z-score normalization

To be noted, symbol $'$ (e.g., $\mathbf{z}$ and $\mathbf{z}'$) is used to distinguish the same variable during the enrollment and verification phase

3.3.1 Overview

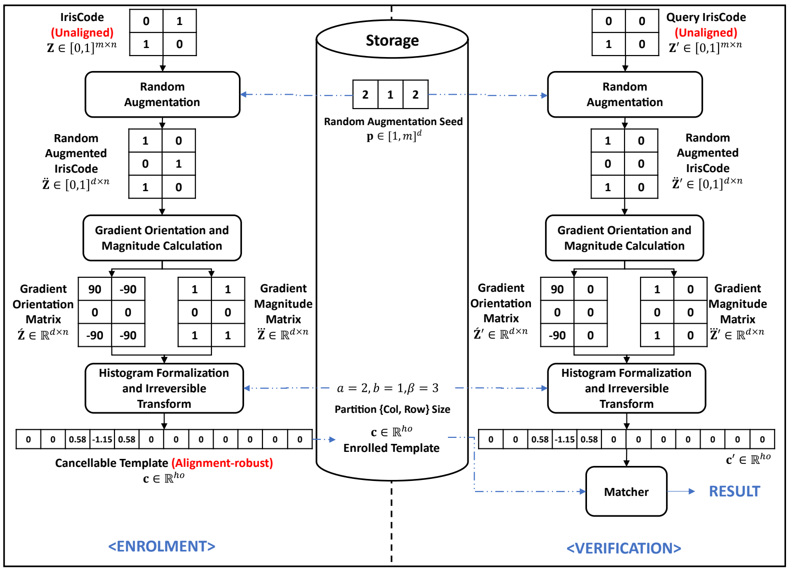

IrisCode
(Unaligned)
$\mathbf{Z} \in [0,1]^{m \times n}$
Storage
Query IrisCode
(Unaligned)
$\mathbf{Z}' \in [0,1]^{m \times n}$
Random Augmentation
2 1 2
Random Augmentation Seed
$\mathbf{p} \in [1, m]^d$
Random Augmented IrisCode
$\hat{\mathbf{Z}} \in [0,1]^{d \times n}$
$\hat{\mathbf{Z}}' \in [0,1]^{d \times n}$
Gradient Orientation and Magnitude Calculation
Gradient Orientation Matrix
$\acute{\mathbf{Z}} \in \mathbb{R}^{d \times n}$
$\acute{\mathbf{Z}}' \in \mathbb{R}^{d \times n}$
Gradient Magnitude Matrix
$\ddot{\mathbf{Z}} \in \mathbb{R}^{d \times n}$
$\ddot{\mathbf{Z}}' \in \mathbb{R}^{d \times n}$
Histogram Formalization and Irreversible Transform
$a = 2, b = 1, \beta = 3$
Partition {Col, Row} Size
$\mathbf{c} \in \mathbb{R}^{ho}$
Enrolled Template
Cancellable Template (Alignment-robust)
$\mathbf{c} \in \mathbb{R}^{ho}$
$\mathbf{c}' \in \mathbb{R}^{ho}$
Matcher
RESULT
<ENROLMENT>
<VERIFICATION>

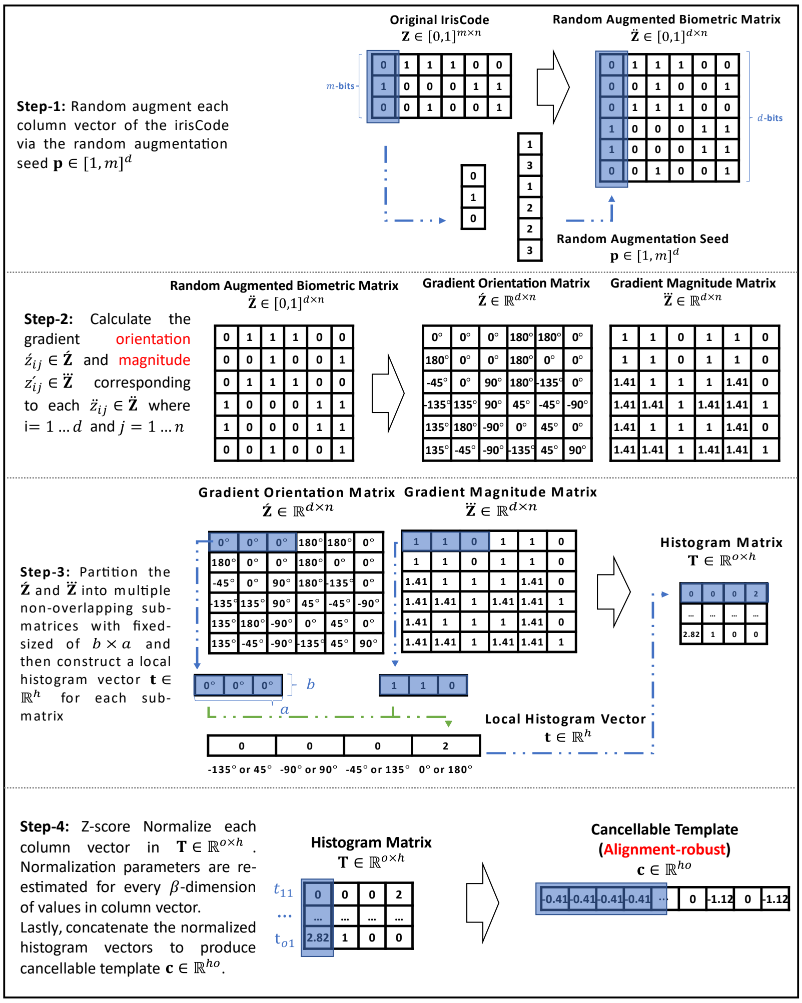
Fig 3.2. Overview of Random Augmented Histogram of Gradients (R·HoG)

The proposed template protection methodology can be decomposed into two main processes: a) a randomize and discriminative feature transformation of the input irisCode. This involves the use of a randomly generated transformation key to augment the input irisCode in a column vector-wise manner. b) a many-to-one mapping and non-invertible transformation process to transform the randomized irisCode feature into an alignment-robust cancellable template. This involves the gradient occurrence count in each non-overlapped segment of the randomized irisCode feature. Since two unaligned irisCode ($\pm n$ bits bit displacement) can produce similar cancellable templates, the matching between the enrolled and query templates can be done efficiently without a pre-alignment strategy (e.g., [144], [146], [147]).

3.3.2 Detailed approach

A. Alignment-robust cancellable transformation

In iris verification, the head tilt, camera tilt, or eye rotation during the iris image capturing cause the horizontal bit-displacement issue in the extracted irisCode [144]. The bit-displacement issue could result in a severe matching performance degradation, and thus, many existing iris cancellable biometric schemes require a pre-alignment process to deal with this issue. However, the pre-alignment process might increase the time complexity for the matching process. This section demonstrates a novel usage of Histogram of Oriented Gradients (HoG) to construct an alignment-robust cancellable template from the unaligned irisCode feature. Histogram of Oriented Gradient (HoG) was originally designed for the statistical record of the frequency distribution of the pixel gradient to detect an object in an image [151]–[153]. In contrast to the existing HoG related works that consider HoG as the feature extraction (e.g., [149], [150]), an unconventional usage of HoG is explored to overcome the pre-alignment issue in iris template protection and directly transform the irisCode feature into an irreversible and renewable template.



Step-1: Random augment each column vector of the irisCode via the random augmentation seed $\mathbf{p} \in [1, m]^d$

Step-2: Calculate the gradient orientation $\acute{z}_{ij} \in \acute{\mathbf{Z}}$ and magnitude $\ddot{z}_{ij} \in \ddot{\mathbf{Z}}$ corresponding to each $\dot{z}_{ij} \in \dot{\mathbf{Z}}$ where i= $1 \dots d$ and $j = 1 \dots n$

Step-3: Partition the $\acute{\mathbf{Z}}$ and $\ddot{\mathbf{Z}}$ into multiple non-overlapping sub-matrices with fixed-sized of $b \times a$ and then construct a local histogram vector $\mathbf{t} \in \mathbb{R}^h$ for each sub-matrix

Step-4: Z-score Normalize each column vector in $\mathbf{T} \in \mathbb{R}^{o \times h}$. Normalization parameters are re-estimated for every β-dimension of values in column vector. Lastly, concatenate the normalized histogram vectors to produce cancellable template $\mathbf{c} \in \mathbb{R}^{ho}$.

Original IrisCode
$\mathbf{Z} \in [0,1]^{m \times n}$
m-bits
Random Augmented Biometric Matrix
$\dot{\mathbf{Z}} \in [0,1]^{d \times n}$
d-bits
Random Augmentation Seed
$\mathbf{p} \in [1, m]^d$
Random Augmented Biometric Matrix
$\dot{\mathbf{Z}} \in [0,1]^{d \times n}$
Gradient Orientation Matrix
$\acute{\mathbf{Z}} \in \mathbb{R}^{d \times n}$
Gradient Magnitude Matrix
$\ddot{\mathbf{Z}} \in \mathbb{R}^{d \times n}$
Histogram Matrix
$\mathbf{T} \in \mathbb{R}^{o \times h}$
b
a
Local Histogram Vector
$\mathbf{t} \in \mathbb{R}^h$
-135° or 45°
-90° or 90°
-45° or 135°
0° or 180°
t_{11}
t_{o1}
Cancellable Template
(Alignment-robust)
$\mathbf{c} \in \mathbb{R}^{ho}$
-0.41 -0.41 -0.41 -0.41 ... 0 -1.12 0 -1.12

Fig 3.3. Process of the proposed R·HoG to transform the irisCode to the alignment-robust cancellable template

The proposed Random Augmented Histogram of Gradients (R·HoG) is an extension of Histogram of Oriented Gradients (HoG) coupled with random augmentation and gradient orientation grouping mechanisms, which are explained as below:

- In the proposed scheme, the alignment-robust biometric vector (cancellable template) is produced by using the histogram vector to record the frequency distribution of the gradient orientations in the irisCode. It is known that biometric feature (irisCode) is noisy data that has the intra/ inter-class similarity issue [8]. To increase the intra-class similarity, the feature augmentation process is applied to the input irisCode. As such, the population of the gradient orientations is increased, and this improves the similarity of the output cancellable template for the similar input irisCodes. Thus, the matching performance of the biometric system is largely preserved. Due to the horizontal bit-displacement of the irisCode, the random augmentation is carried out in a column vector-wise manner. Since randomly generated information is involved, this enables the proposed scheme to produce multiple independent cancellable templates for the same input irisCode; and thus, guarantee the renewability and unlinkability properties.

- In R·HoG, each of the histogram vectors is constructed by using an orientation-based histogram to record the gradient magnitude for each $z_{ij} \in \mathbf{Z}$ where $\mathbf{Z} \in [0,1]^{m \times n}$ denotes the biometric feature. Since $\mathbf{Z}$ is a binary matrix with only $'0'$ and $'1'$, the possible gradient orientations are $-135°$, $-90°$, $-45°$, $0°$, $45°$, $90°$, $135°$ and $180°$. To improve the concealment towards the biometric information, the approach that spread the histogram bins over $0 - 180°$ is considered in the proposed R·HoG. In particular, the gradient orientations with $180°$ difference (e.g., $-45°$ and $135°$) are grouped into the same histogram bin. The imposed gradient orientation grouping mechanism induced a many-to-one mapping effect where gradient magnitudes from different orientations are mapped into the same histogram bin; thus, strengthening the irreversibility properties. Besides that, the orientation grouping reduces the affection of the random augmentation towards the size of the cancellable template where the histogram vector in R·HoG is a compact data structure.

Given an unaligned irisCode $\mathbf{Z} \in [0,1]^{m \times n}$ and the random augmentation seed $\mathbf{p} \in [1, m]^d$, with the transformation parameters {segment row size $b \in \mathbb{Z}$, segment column size $a \in \mathbb{Z}$ and histogram bin $h \in \mathbb{Z}$ }, the procedures (Algorithm 1) to generate an alignment-robust biometric vector $\mathbf{c} \in \mathbb{R}^{ho}$ are described as follows:

1) For each of the column vector $\mathbf{z}_j = [z_{1j}, z_{2j}, \dots, z_{mj}]$ in the $\mathbf{Z} \in [0,1]^{m \times n}$ where $j = 1 \dots n$ indicates the j-th column, the random augmentation seed $\mathbf{p} \in [1, m]^d$ is applied onto the $\mathbf{z}_j$ to produce a random augmented column vector $\ddot{\mathbf{z}}_j = [\ddot{z}_{1j}, \ddot{z}_{2j}, \dots, \ddot{z}_{dj}]$. Specifically, the random augmentation process first initializes an empty $\ddot{\mathbf{z}}_j$. With each $p \in \mathbf{p}$ act as the

index value for $\mathbf{z}_j$, each $z \in \mathbf{z}_i$ are then randomly chosen with replacement and added into the $\ddot{\mathbf{z}}_j$. Lastly, n numbers of $\ddot{\mathbf{z}}_j$ are horizontal concatenated to produce the random augmented biometric matrix $\ddot{\mathbf{Z}} = \ddot{\mathbf{z}}_1 ||\ddot{\mathbf{z}}_2|| \dots ||\ddot{\mathbf{z}}_n$. To be noted, random augmentation is a form of permutation. Involvement of the randomly generated data (i.e., $\mathbf{p}$) induces a randomization effect towards the proposed scheme; and hence enables the renewal of the cancellable template.

2) In this step, the gradient orientation and magnitude corresponding to each $\ddot{z}_{ij} \in \ddot{\mathbf{Z}}$ are calculated and stored in the orientation matrix $\acute{\mathbf{Z}} = \mathbb{R}^{d\times n}$ and magnitude matrix $\dddot{\mathbf{Z}} = \mathbb{R}^{d\times n}$. Particularly, the horizontal and vertical difference of the neighboring elements for each $\ddot{z}_{ij} \in \ddot{\mathbf{Z}}$ are first calculated with:

$$\mathbf{X} = \mathrm{rcirshift}(\ddot{\mathbf{Z}}, -1) - \mathrm{rcirshift}(\ddot{\mathbf{Z}}, 1) \tag{3.1}$$

$$\mathbf{Y} = \mathrm{ccirshift}(\ddot{\mathbf{Z}}, 1) - \mathrm{ccirshift}(\ddot{\mathbf{Z}}, -1) \tag{3.2}$$

where $\mathbf{X}$ is the horizontal difference matrix and $\mathbf{Y}$ is the vertical difference matrix, while $\mathrm{rcirshift}(.)$ and $\mathrm{ccirshift}(.)$ are the *row-wise* and *column-wise* circular shifting functions, e.g., $\mathrm{rcirshift}(\ddot{\mathbf{Z}}, 1)$ means shift the $\ddot{\mathbf{Z}}$ row-wise by 1 (i.e., right shift). After obtaining the $\mathbf{X}$ and $\mathbf{Y}$, the orientation matrix $\acute{\mathbf{Z}}$ and magnitude matrix $\dddot{\mathbf{Z}}$ are calculated as follow:

$$\dddot{z}_{ij} = \sqrt{(x_{ij})^2 + (y_{ij})^2} \text{ , } \dddot{z}_{ij} \in \dddot{\mathbf{Z}} \tag{3.3}$$

$$\acute{z}_{ij} = \arctan\,(y_{ij}/x_{ij}),\ \acute{z}_{ij} \in \acute{\mathbf{Z}} \tag{3.4}$$

where $i = 1 \dots d$ and $j = 1 \dots n$ indicate the position (row and column) of the elements in the matrices.

3) The core of the alignment-robust transformation is to use a histogram feature to record the occurrence (sum of gradient magnitude) of gradient orientation corresponding to each $\ddot{z}_{ij} \in \ddot{\mathbf{Z}}$. To increase the matching accuracy, the feature matrix is partitioned into o numbers of non-overlapping sub-matrices with equal size of $b \times a$, and then be

transformed to a local histogram vector $\mathbf{t} \in \mathbb{R}^h$ where $o = \frac{d}{b} * \frac{n}{a}$. Let $\ddot{\mathbf{Z}}^{\text{part}} \in [0,1]^{b\times a}$ be each of the non-overlapped partitioned matrix, a local histogram vector $\mathbf{t} \in \mathbb{R}^h$ is constructed by adding the gradient magnitude $\ddot{z}_{ij} \in \ddot{\mathbf{Z}}$ to the $\mathbf{t}$ according to the gradient orientation $\acute{z}_{ij} \in \acute{\mathbf{Z}}$, where h refers to the number of histogram bins; while the $\ddot{z}_{ij}$ and $\acute{z}_{ij}$ are the magnitude and orientation values corresponding to each $\left(\ddot{z}^{\text{part}}\right)_{ij} \in \ddot{\mathbf{Z}}^{\text{part}}$ respectively, where i and j are the *row* and *column* number of elements in $\ddot{\mathbf{Z}}$ and $\acute{\mathbf{Z}}$ respectively. As mentioned previously, the histogram bins are defined as: $\{-135° \text{ or } 45°\}$, $\{-90° \text{or } 90°\}$, $\{-45° \text{ or } 135°\}$ and $\{0° \text{ or } 180°\}$. After o numbers of the (unnormalized) histogram vector $\mathbf{t} \in \mathbb{R}^h$ are constructed, the histogram vectors (i.e., $\mathbf{t}$) are vertically concatenated and yield a histogram matrix $\mathbf{T} = \begin{bmatrix} \mathbf{t}_1 \\ \dots \\ \mathbf{t}_o \end{bmatrix}$.

4) For each of the column vector $\mathbf{t}_j = \left[t_{1j}, t_{2j}, \dots, t_{oj}\right]$ in the $\mathbf{T} \in \mathbb{R}^{o\times h}$ where $j = 1 \dots h$ indicates the j-th column. A z-score normalization (irreversible transformation) is applied onto the $\mathbf{t}_j$ to produce a normalized histogram vector $\hat{\mathbf{t}}_j$. Each $\hat{t}_{ij} \in \hat{\mathbf{t}}_j$ is computed based on the following formula:

$$\hat{t}_{ij} = \frac{t_{ij} - \mu}{\sigma} \tag{3.5}$$

where $i = 1 \dots o$ indicates the i-th element in the $\hat{\mathbf{t}}$, $\{\mu$ and $\sigma\}$ are the normalization parameters. The z-score normalization (with the same μ and σ) is applied to every β-dimension of values in $\hat{\mathbf{t}}_j$ where $\beta = \frac{d}{b}$. Therefore, the μ and σ are re-calculated after normalizing every β-dimension of values in $\hat{\mathbf{t}}_j$. Since $\mathbf{t}_j$ is transformed from biometric information, μ and σ are biometric dependent information; thus, only the genuine user can regenerate the correct μ and σ and produce the $\hat{\mathbf{t}}_j$. In this case, the normalization could be operated as an irreversible transformation where μ and σ are disposed of after the normalization process. Without storing μ and σ, normalization is merely a many-to-one transformation that could map different data into the normalized data with a similar scale. This offers another layer of the many-to-one mapping effect.

Lastly, h numbers of $\hat{\mathbf{t}} \in \mathbb{R}^o$ are concatenated to produce the alignment-robust biometric vector (cancellable template) $\mathbf{c} \in \mathbb{R}^{ho}$ where $\mathbf{c} = \hat{\mathbf{t}}_1{}^\top || \hat{\mathbf{t}}_2{}^\top || \ldots || \hat{\mathbf{t}}_h{}^\top$. Fig 3.3 depicts the R·HoG transformation to generate the alignment-robust cancellable template $\mathbf{c} \in \mathbb{R}^{ho}$ for the irisCode $\mathbf{Z} \in [0,1]^{3\times5}$ with the parameters setting of $a = 3$, $b = 1$ and $d = 6$. Besides that, algorithm 3.1 shows the pseudo-code of the R·HoG transformation. Whenever $\mathbf{c}$ is compromised, a new cancellable template ($\mathbf{c}^*$) can be always be generated by transforming the same irisCode $\mathbf{Z}$ with a new random augmentation seed $\mathbf{p}^* \in [1, m]^d$. Since $\mathbf{c}$ is a large real-valued and randomized vector, it is unlikely that the new cancellable template $\mathbf{c}^*$ can be collided with the old cancellable template $\mathbf{c}$. Hence, renewability property is demonstrated. The proposed scheme is essentially an alignment-robust transformation scheme that transforms the unaligned irisCode $\mathbf{Z} \in [0,1]^{m\times n}$ into an alignment-robust cancellable template $\mathbf{c} \in \mathbb{R}^{ho}$. Thus, the proposed scheme can perform the matching for the cancellable templates without additional pre-alignment.

Suppose $RHOG(.)$ is the transformation function for the proposed scheme, the following case is used to describe the alignment-robust property in the proposed R·HoG generally.

Case 3.1: Given two vectors $\mathbf{x} \in [0,1]^m$ and $\mathbf{x}' \in [0,1]^m$ that possess n element-wise horizontal displacement, i.e., $\mathrm{cirshift}(\mathbf{x}', n) = \mathbf{x}$ where $\mathrm{cirshift}(.)$ refers to circular left shift function. The $RHOG(.)$ produce the same output for the $\mathbf{x}$ and $\mathbf{x}'$, such that $RHOG(\mathbf{x}) = RHOG(\mathbf{x}')$.

***Discussion**:* In step-3 transformation, the proposed scheme transforms the biometric feature into a histogram vector $\mathbf{t} \in \mathbb{R}^h$ that statistically counts the gradient magnitude corresponding to the gradient orientation. In this case, a many-to-one mapping is achieved where gradient magnitudes for the same gradient orientation are mapped to the same histogram bin. Considering an example of two vectors: $\mathbf{x}_1 = [0,1,0]$ and $\mathbf{x}_2 = [1,0,0]$ where $\mathrm{cirshift}(\mathbf{x}_1, 1) = \mathbf{x}_2$. The gradient magnitude and orientation for $\mathbf{x}_1$ are $\ddot{\mathbf{z}}_1 = [1,0,1]$ and $\acute{\mathbf{z}}_1 = [0°, 0°, 180°]$; as for $\mathbf{x}_2$, $\ddot{\mathbf{z}}_2 = [0,1,1]$ and $\acute{\mathbf{z}}_2 = [0°, 0°, 180°]$. To be noted, the proposed scheme pad $'0'$ to the top and bottom of the vectors during the calculation of gradient magnitude and orientation if the vectors do not have neighboring *top* and *bottom* elements. Given the gradient magnitude (i.e., $\ddot{\mathbf{z}}_1$ and $\ddot{\mathbf{z}}_2$) and orientation (i.e., $\acute{\mathbf{z}}_1$ and $\acute{\mathbf{z}}_2$), the proposed scheme generates the histogram vectors $\mathbf{t}_1 = [0,0,0,2]$ and $\mathbf{t}_2 = [0,0,0,2]$ where the histogram bins are:$\{-135° \text{ or } 45°\}$, $\{-90° \text{ or } 90°\}$, $\{-45° \text{ or } 135°\}$, and $\{0° \text{ or } 180°\}$. Since $\mathbf{t}_1 \approx \mathbf{t}_2$, the step-4 transformation will produce the similar output $\mathbf{c}$ for $\mathbf{x}_1$ and $\mathbf{x}_2$. Hence, given $\mathbf{x} \in [0,1]^m$ and $\mathbf{x}' \in [0,1]^m$ where $\mathrm{cirshift}(\mathbf{x}', n) = \mathbf{x}$, the proposed Random Augmented Histogram of Gradients (R·HoG) overcomes the misalignment issue and generates similar output, such that $RHOG(\mathbf{x}) \approx RHOG(\mathbf{x}')$.

With the statement above, it is shown that the proposed scheme can transform the irisCode $\mathbf{Z} \in [0,1]^{m\times n}$ into an alignment-robust cancellable template $\mathbf{c} \in \mathbb{R}^{ho}$. To compensate for the performance degradation that is caused by the many-to-one transformation in the scheme, two strategies are employed in the proposed scheme. (a) In step 3, the $\ddot{\mathbf{Z}}$ is partitioned into multiple parts and then transformed into the histogram vector (i.e., $\mathbf{t}$), which will be used to form the cancellable template $\mathbf{c}$. (b) Data augmentation is carried out onto the input $\mathbf{Z} \in [0,1]^{m\times n}$ to increase the information for histogram formalization. In addition, experiments are carried out to validate the performance preservation effect of the two strategies.

B. Cancellable Template Matching

Typically, similarity comparison between normalized histogram features can be made by calculating the Euclidean distance. In the proposed scheme, the cancellable iris template is a concatenated histogram vector; and thus, *normalized Euclidean similarity* is used to perform similarity comparison between the cancellable templates. Given the enrolled cancellable iris template $\mathbf{c} \in \mathbb{R}^{ho}$ and the query cancellable iris template $\mathbf{c}' \in \mathbb{R}^{ho}$, the similarity score $S \in [0,1]$ is obtained via the following formula:

$$S = 1 - \frac{||\mathbf{c} - \mathbf{c}'||_2}{||\mathbf{c}||_2 + ||\mathbf{c}'||_2} \tag{3.6}$$

where $||.||_2$ is a norm function. S ranged from 0 to 1, which indicates the similarity level between $\mathbf{c}$ and $\mathbf{c}'$. Since the generated cancellable iris template is an alignment-robust feature, there is no pre-alignment (e.g., horizontal shifting [144]) required throughout the matching process, which guarantees an efficient authentication process.

Algorithm 3.1. The pseudocode of alignment-robust biometric vector generation

```
Input: Unaligned irisCode $\mathbf{Z} \in [0,1]^{m\times n}$, Random augmentation seed $\mathbf{p} \in [1, m]^d$
Transformation parameter: Histogram bins $h \in \mathbb{Z}, h \geq 2$, Segment column size $a \in \mathbb{Z}, 0 < a \leq n,$ Segment row size $b \in \mathbb{Z}, 0 < b \leq d$, $\beta = \frac{d}{b}$
Output: Alignment-robust biometric vector $\mathbf{c} \in \mathbb{R}^{ho}$
Step 1: Column-wise Random Augmentation
  Initialize $\ddot{\mathbf{Z}} = [0]^{d\times n}$, $\mathbf{c} = []$
  for $i \leftarrow 1$ to $d$ and $j \leftarrow 1$ to $n$
      $\ddot{z}_{ij} = z_{p_i j}$
  end for
Step 2: Gradient Orientation and Magnitude Calculation
  $\mathbf{X} = \mathrm{rcirshift}\big(\ddot{\mathbf{Z}}, -1\big) - \mathrm{rcirshift}(\ddot{\mathbf{Z}}, 1)$ // horizontal difference
  $\mathbf{Y} = \mathrm{ccirshift}\big(\ddot{\mathbf{Z}}, 1\big) - \mathrm{ccirshift}(\ddot{\mathbf{Z}}, -1)$ // vertical difference
  Initialize $\acute{\mathbf{Z}} = [0]^{d\times n}$ // orientation matrix
  Initialize $\dddot{\mathbf{Z}} = [0]^{d\times n}$ // magnitude matrix
  for $i \leftarrow 1$ to $d$ and $j \leftarrow 1$ to $n$
      $\dddot{z}_{ij} = \sqrt{(x_{ij})^2 + (y_{ij})^2}$
      $\acute{z}_{ij} = \arctan\,(y_{ij}/x_{ij})$
  end for
Step 3: Histogram Formalization
  Initialize $\mathbf{T} = []$ //  HoG feature
  Partition the $\acute{\mathbf{Z}}$ and $\dddot{\mathbf{Z}}$ into $o$ numbers of non-overlapped sub-blocks with size of $b \times a$
  for $i \leftarrow 1$ to $o$
      Initialize $\mathbf{t} = [0]^{\mathrm{h}}$ // local histogram vector
      Let $\acute{\boldsymbol{Z}}^{\mathrm{part}} \in \mathbb{R}^{b\times a}$ be a partitioned orientation matrix
      Let $\dddot{\boldsymbol{Z}}^{\mathrm{part}} \in \mathbb{R}^{b\times a}$ be a partitioned magnitude matrix
      for $j \leftarrow 1$ to $a$ and $k \leftarrow 1$ to $b$
          Add the value of $\dddot{z}_{kj} \in \dddot{\mathbf{Z}}_{\mathrm{block}}$ into $\mathbf{t}$ according to the bins value pointed by $\acute{z}_{kj} \in \acute{\mathbf{Z}}_{\mathrm{block}}$
      end for
      vertical concatenate $\mathbf{t}$ to $\mathbf{T}$
  end for
Step 4: Z-score transformation
  for $j \leftarrow 1$ to $h$
      Initialize $\hat{\mathbf{t}} = [0]^o$
      Get each column vector $\mathbf{t}_j$ from $\mathbf{T}$
      Calculate mean $(\mu)$ of first $\beta$-dimension values in $\mathbf{t}_j$
      Calculate standard deviation $(\sigma)$ of first $\beta$-dimension values in $\mathbf{t}_j$
      for $i \leftarrow 1$ to $o$
          Compute each $\hat{t}_i = (t_{ij} - \mu)/\sigma$ // z-score normalization
          if $(i-1)\%\,\beta == 0$
              Re-calculate $\mu$ and $\sigma$ based on next $\beta$-dimension of values in $\mathbf{t}_j$
          end if
      end for
      $\mathbf{c} = \mathbf{c}||\hat{\mathbf{t}}$
  end for
return c
```

To be noted, $\mathrm{rcirshift}(.)$ and $\mathrm{ccirshift}(.)$ represent the *row-wise* and *column-wise* circular shift functions. For example, $\mathrm{ccirshift}(\mathbf{Z}, 1)$ means to shift the matrix $\mathbf{Z}$ column-wise by 1.

3.4 Experiments and discussions

This section is devoted to presenting the experimental result of the proposed method in terms of verification performance via parameter estimation.

3.4.1 Experimental setup

This subsection presents the experimental setup for the experiments in terms of the dataset, matching protocol and feature extraction. The implementation of the proposed scheme is written using MATLAB and being executed in a PC with the hardware specification of Solid-State Drive (SSD)@480GB, Intel Core i7 7th-Gen CPU and Memory DDR4@20GB.

A. Dataset and matching protocol

The benchmarking *CASIA-IrisV3-Internal* [52] dataset is used for the experiment. Briefly, this dataset consists of 249 subjects with different amounts of iris images per subject. To be consistent with the existing iris cancellable biometrics works (e.g., [53], [54]) and standardize the matching numbers for each subject, the experiments are conducted based on the left iris image. The dataset is a subset by choosing the subjects with 7 iris images. In short, a total of 868 irisCodes (124 subjects $\times$ 7 irisCodes) are extracted for the experiment.

In the experiment, the assessment of the matching accuracy is based on the Equal Error Rate (EER) (%) of the intra/ inter-class matching score distributions. Both score distributions are generated from the following matching attempts:

- **Intra-class (or Genuine) matching attempt**: Crossmatch all the cancellable iris templates generated from the same subject; and thus, a total of $^{7}\mathrm{C}_2 = 21$ intra-class matching scores are generated for each subject with 7 cancellable iris templates.

- **Inter-class (or Impostor) matching attempt:** Crossmatch all the cancellable iris templates generated from the first iris image of different subjects; and thus, a total of $^{124}\mathrm{C}_2 = 7626$ inter-class matching scores are generated for 124 cancellable iris templates generated from different subjects.

In each experiment, the intra-class score distribution consists of 2604 matching scores, while inter-class score distribution contains 7626 matching scores. Since randomly generated information (e.g., random augmentation seed $\mathbf{p} \in [1, m]^d$) is involved in the proposed scheme, a total of 5 experiments are conducted with different sets of $\mathbf{p} \in [1, m]^d$ for more precise reading of the matching accuracy. To be noted, the experiments are conducted under the worst-case (stolen token) scenario by assuming the transformation key or parameters is compromised by the impostor. Therefore, one $\mathbf{p} \in [1, m]^d$ is shared among every subject in each experiment.

B. IrisCode extraction

This chapter focuses on the proposal of the cancellable biometric scheme that can transform the unaligned irisCode into the alignment-robust cancellable iris template. Therefore, the methods from [49], [50] are adopted to extract the irisCode $\mathbf{Z} \in [0,1]^{20\times512}$ as the input for the proposed scheme. Given an iris image, the irisCode extraction process is as follows:

1) In this step, Weighted Adaptive Hough Transform is first applied to locate the iris [154]. After that, iris and pupil boundaries are segmented by means of Ellipsopolar Transforms [154]. Next, the rubbersheet transform [44] is employed to normalize the iris texture into a fixed-size matrix $\ddot{\mathbf{Z}}^{50\times512}$.

2) The $\ddot{\mathbf{Z}}^{50\times512}$ is divided into 10 stripes, and then each stripe in the normalized iris texture is averaged into a 1-D signal vector [155]. The Gabor filter is then applied to convolute the signal vectors and produce a complex iris feature $\bar{\mathbf{Z}}^{10\times512}$.

Lastly, the complex iris features $\bar{\mathbf{Z}}^{10\times512}$ is converted into the irisCode $\mathbf{Z} \in [0,1]^{20\times512}$ [155]. The table below tabulates the summary of the tested iris dataset in terms of verification performance and the total number of irisCode $\mathbf{Z} \in [0,1]^{20\times512}$ extracted. Summary of the employed iris dataset and the extracted irisCode are tabulated in the table below.

Table 3.2: Summary of the iris subset

	CASIA-IrisV3-Internal
Number of iris images per user	7
User	124
Total irisCode extracted	868
Equal Error Rate (EER) (%) **(±16 bit shifting)**	0.50

3.4.2 Parameter estimation

This subsection presents the experimental result of selecting the best-tuned parameters for the proposed method, i.e., random augmentation size d, partition column a and row size b. Notice that the parameter h is fixed to 4; while β is fixed as $\frac{d}{b}$.

A. Effect of random augmentation size d

In this subsection, the effect of the random augmentation size d towards the verification performance of the proposed method is examined. Recall the methodology, a random augmentation process is applied onto the input irisCode to increase the information for the gradient orientation binning as well as improve the uniqueness of the produced cancellable template. In here, the random augmentation size d is used to control the column size of the augmentation irisCode. To examine the d, experiments are conducted by setting d from $20 - 250$, with an increment interval of 25*,* and the remaining parameters are fixed at $a = 32$, $b = 1$. Since the row size of the irisCode is 20, the proposed method under $d = 20$ achieves only a random shuffle effect. In the table below, the EERs and cancellable template dimensions under different settings of d are tabulated. The experimental results show the verification performance is improved (lower EER) when d is set to a higher value; hence, the random augmentation is taking effect. In $d = 250$, the equal error rate reaches the lower point where EER= 0.62%. Although the result suggests that it is possible to obtain lower EER when $d > 250$, the setting beyond 250 is not considered because of the increment of template size as well as computing overhead. With the slight increment of 56% in the template size from $20 \times 512 = 10240$ dimensions to 16000 dimensions and reasonable verification performance of EER= 0.62%, $d = 250$ is chosen as the best setting.

Table 3.3: EERs and template size of the cancellable template under different d

Augmentation Column Size d	**EER (Unprotected) (%)**	**EER (Protected) (%)**	**Original irisCode Dimension**	**Cancellable Template Dimension**
20	0.50	3.01 ± 0.51	20×512	1280
50		1.48 ± 0.35		3200
75		1.04 ± 0.28		4800
100		1.01 ± 0.18		6400
125		0.85 ± 0.16		8000
150		0.84 ± 0.22		9600
175		0.74 ± 0.18		11200
200		0.70 ± 0.13		12800
225		0.69 ± 0.17		14400
$\mathbf{250}$		$\mathbf{0.62 \pm 0.14}$		$\mathbf{16000}$

B. Effect of partition column and row size (a, b)

In the proposed scheme, the shift-invariant biometric vector is formed by concatenating the local histogram vectors for multiple non-overlapping partitioned blocks of the irisCode. Parameters a and b are used to determine the *column* and *row* size for each partitioned block. The effect of parameters a and b is examined by testing the verification performance of the cancellable template generated using different scales of partition size (a and b). In the experiments, the a and b are tested under different values while the d is fixed at 250. The table below tabulates the EERs of the proposed method under different settings of a and b. As expected, partitioning the biometric feature into multiple non-overlapping sub-blocks can improve the matching accuracy of the alignment-robust biometric vector. From the table, the EER is at the highest degree when $a = 512$ and $b = 125$. From the table, the EERs of the proposed method decrease with the lower value of a and b, which shows the partitioning strategy is taking effect for improving verification performance. It is observed that the histogram formulation serves the best performance preservation effect when $b = 1$ with different settings of a. On the other hand, a cannot be set to a lower value (≤ 16) as the EERs start to increase. Hence, it is concluded that $a = 32$ and $b = 1$ are the best settings.

Table 3.4: EERs (%) under different settings of a and b

Partition Column Size a	**Partition Row Size** b						
	1	**2**	**5**	**10**	**25**	**50**	**125**
8	3.28	2.98	3.28	3.98	5.84	7.89	18.80
16	0.95	1.07	1.35	1.82	3.31	6.63	20.57
32	**0.62**	0.69	1.06	1.65	3.83	7.93	26.16
64	1.23	1.37	1.95	3.22	7.71	13.52	30.30
128	2.65	3.00	4.55	6.46	13.15	21.04	37.54
256	5.88	6.34	8.08	11.33	19.93	28.32	41.29
512	7.94	9.10	11.62	1.575	24.49	31.38	48.48

C. Summary of parameter estimation

Throughout the experiments, observations of the result are concluded as below:

1) Increment of the random augmentation size d can effectively reduce the Equal Error Rate (EER) (%) of the generated alignment-robust biometric vector (cancellable template) $\mathbf{c} \in \mathbb{R}^{ho}$. This is because of the increment of the gradient orientations for the similar biometric feature (irisCode) during the histogram formulation process; thus, the intra-class variance of $\mathbf{c} \in \mathbb{R}^{ho}$ can be reduced.

2) Increment of random augmentation size d resulting in the increment of template size for the alignment-robust biometric vector as well as time complexity for generating the template. Hence, the trade-off between template size and matching accuracy must be considered when choosing a suitable value for d.

3) The matching accuracy of the original irisCode is well preserved by partitioning the irisCode into multiple sub-blocks and then converting the sub-blocks into a local histogram vector. Parameters a and b are used to determine the *column* and *row* size for the sub-block. As observed, smaller values of a and b lead to a better matching accuracy of the alignment-robust biometric vector. It should take note that a cannot be set to a low value to prevent insufficient gradient orientations of each sub-block for histogram formulation.

Table 3.5: Optimal parameter setting for R·HOG

Parameters	**Value**
d	250
a	32
b	1
h	4
β	$\frac{d}{b}$

3.4.3 Verification performance and comparison

It is noticed that existing iris template protection studies have no standardized experiment matching protocols and the numbers of testing iris images; hence, it is impossible to perform a fair comparison between the proposed scheme and the existing works. Nevertheless, the verification performance of the proposed method and the existing iris template protection methods are presented for benchmarking purposes. Table 3.6 tabulates the summary of different iris template protection methods, and it is observed that:

- The verification degradation rate of the proposed scheme is 0.12% compared to the original iris counterpart, which indicates the proposed scheme has reasonable performance preservation property.

- Verification performance of the proposed scheme (refer to EER with protection) is comparable to existing iris template protection methods. This is attributed to the original irisCode and the nice performance preservation property.

Table 3.6: Verification performance of existing iris template protection methods under CASIA-IrisV3-Internal

Method	Pre-alignment	Total Iris Images Used	EER (%) without protection	EER (%) with protection
Proposed Scheme	**Not required**	**868 (Left eye)**	**0.50**	**0.62**
IFO Hashing [53]	**Required**	868 (Left eye)	0.38	0.54
BioEncoding [103]	**Required**	740	6.02	6.27
Dwivedi *et al.* [110]	**Required**	2639	0.39	0.43
Bin-Combo [18]	Not required	1332 (Left eye)	0.81	4.41
Adaptive Bloom Filters [54]	Not required	1332 (Left eye)	1.19	1.14
Lai *et al.* [114]	Not required	868 (Left eye)	0.38	0.69

3.4.4 Computation efficiency

The computation efficiency of the proposed scheme is also examined in terms of the machine runtime (in second) to transform the irisCode into the cancellable template. The processing time of the proposed scheme in *enrollment* and *verification* stages are tabulated in the table below. From the table, the average enrollment time is 0.0916 seconds, and the verification time is 0.0811 seconds. This shows that it is feasible to adapt the proposed scheme to real-world applications. On the other hand, it is observed that the enrollment stage is slightly higher compared to the verification stage. This is mainly due to the initialization of the auxiliary information (i.e., random augmentation seed $\mathbf{p} \in [1, m]^d$) in the enrollment. However, initialization is required once in the enrollment stage.

Table 3.7: Time complexity for R·HoG in enrollment and verification stages

Process	Experiment 1	Experiment 2	Experiment 3	Experiment 4	Experiment 5	Average
Enrollment Stage (sec)						
R·HoG	0.0782	0.0849	0.0845	0.1099	0.1007	0.0916
Verification Stage (sec)						
R·HoG	0.0716	0.0822	0.0749	0.0813	0.0945	0.0809
Matching	0.0003	0.0002	0.0001	0.0001	0.0002	0.0002
Total	0.0719	0.0824	0.0750	0.0814	0.0947	0.0811

3.5 Security and privacy analysis

Security and privacy are the important aspects of the biometric template protection method. The analyses are based on the biometric template protection requirements as listed in the ISO/IEC Standard 24745 [21] and 30136 [22], i.e., irreversibility, unlinkability and renewability. Other than that, the security property is analyzed by evaluating the attack complexity required for the attack to guess the cancellable template and use it for matching.

3.5.1 Irreversibility analysis

Irreversibility refers to the infeasibility in recovering the original irisCode $\mathbf{Z} \in [0,1]^{m \times n}$ from the cancellable iris template $\mathbf{c} \in \mathbb{R}^{ho}$. In this subsection, the irreversibility is evaluated using three attacks where the attacker aims to recover the input irisCode $\mathbf{Z} \in [0,1]^{m \times n}$ from single/ multiple compromised cancellable iris template(s) $\mathbf{c} \in \mathbb{R}^{ho}$ and random augmented seed(s) $\mathbf{p} \in [1, m]^d$.

A. Template inversion via single record

The transformation procedure of the proposed scheme is revisited before commencing the discussion of the inversion attack. Suppose there is an input irisCode $\mathbf{Z} \in [0,1]^{m \times n}$, the proposed scheme first applied $\mathbf{p} \in [1, m]^d$ onto each column vector of $\mathbf{Z}$ and this produce a random augmented irisCode $\ddot{\mathbf{Z}} \in [0,1]^{d \times n}$. After that, $\ddot{\mathbf{Z}} \in [0,1]^{d \times n}$ is partitioned into o numbers of sub-blocks $\ddot{\mathbf{Z}}^{\text{part}} \in [0,1]^{b \times a}$, which is then be converted into a histogram vector $\mathbf{t} \in \mathbb{R}^h$ where $a = 32$ and $b = 1$. The histogram vectors are then vertically concatenated into a histogram matrix $\mathbf{T} = [\mathbf{t}_1 \dots \mathbf{t}_o]^\top$. Lastly, a z-score normalization is applied to each column vector $\mathbf{t}_j \in \mathbf{T}$ and the normalized vector $\hat{\mathbf{t}}_j$ are concatenated to produce the cancellable template $\mathbf{c} = \hat{\mathbf{t}}_1{}^\top || \hat{\mathbf{t}}_2{}^\top || \dots || \hat{\mathbf{t}}_h{}^\top$, where $j = 1 \dots h$ and the normalization parameters are re-calculated for every β-dimension of values in $\mathbf{t}_j$.

Knowing the cancellable template $\mathbf{c}$ is formed by a set of normalized histogram vectors in which $\mathbf{c} = \hat{\mathbf{t}}_1{}^\top || \hat{\mathbf{t}}_2{}^\top || \dots || \hat{\mathbf{t}}_h{}^\top$, the attacker can attempt to reverse each $\hat{\mathbf{t}}_i$ instead of reversing each entry of the cancellable template. Given a $\hat{\mathbf{t}}_i$, the attacker must traverse through the process of recovering the unnormalized $\mathbf{t}_i$ from $\hat{\mathbf{t}}_i$, then recover the gradient magnitudes and orientations from $\mathbf{t}_i$ and eventually, recover the $\ddot{\mathbf{Z}}^{\text{part}}$. After o numbers of $\ddot{\mathbf{Z}}^{\text{part}}$ are acquired, the attacker can use $\mathbf{p} \in [1, m]^d$ to perform reverse permutation and recover the original irisCode feature $\mathbf{Z} \in [0,1]^{m\times n}$. In the inversion attack, the first step is to recover the original $\mathbf{t} \in \mathbb{R}^o$ from the normalized $\hat{\mathbf{t}} \in \mathbb{R}^o$. The following cases are used to discuss the feasibility of reverse transform $\hat{\mathbf{t}} \in \mathbb{R}^o$.

Case 3.2: Given a z-score normalized vector $\hat{\mathbf{t}} \in \mathbb{R}^o$, mean μ and standard deviation σ, the attacker can recover the original vector $\mathbf{t} \in \mathbb{R}^o$.

Discussion: Suppose there is a vector $\mathbf{t} \in \mathbb{R}^o$, the z-score normalization constructs a normalized vector $\hat{\mathbf{t}} \in \mathbb{R}^o$ with the following formula:

$$\hat{t}_i = \frac{t_i - \mu}{\sigma} \tag{3.7}$$

where $i = 1, \dots, o$. The recovery of **t** (de-normalization) can be carried out by inverting the normalization process. In this case, Equation (3.7) can be inverted to calculate $t_i \in$ **t**. The reverse transformation is written as below:

$$t_i = (\hat{t}_i * \sigma) + \mu \tag{3.8}$$

where $i = 1, \dots, o$. Knowing $\hat{\mathbf{t}}$, μ and σ, it is feasible for the attacker to calculate each t_i and reconstruct the original vector **t** $\in \mathbb{R}^o$.

Case 3.3: Without knowing μ and σ, it is infeasible to reconstruct the original vector $\mathbf{t} \in \mathbb{R}^h$ from the z-score normalized vector $\hat{\mathbf{t}} \in \mathbb{R}^h$.

***Discussion**:* Z-score normalization is a process that utilizes the probability distribution of the input data to transform the input data to re-scaled (normalized) data. In general, z-score normalization could produce the normalized data with a similar scale for different inputs. Given three vectors, i.e., $\mathbf{t}_1 = [1,0,1]$, $\mathbf{t}_2 = [2,0,2]$ and $\mathbf{t}_3 = [3, 0, 3]$, a z-score normalization is applied with μ and σ set to the mean and standard deviation of the respective vector. Despite the $\mathbf{t}_1$, $\mathbf{t}_2$ and $\mathbf{t}_3$ are different, the z-score normalization produces a similar normalized vector, i.e., $\hat{\mathbf{t}}_1 = \hat{\mathbf{t}}_2 = \hat{\mathbf{t}}_3 = [0.58, -1.15, 0.58]$. Therefore, it is difficult to recover the original vector **t** without knowing the exact values of μ and σ. In this case, the z-score normalization can be operated as an irreversible transformation function.

The above cases discuss the feasibility of recovering the original vector from the normalized vector in a reverse transform manner. It clearly demonstrates that a normalization process is irreversible when the normalization parameters (i.e., μ and σ) are not known. In the proposed scheme, μ and σ are biometric dependent information, and the genuine user can regenerate μ and σ during the verification stage. Therefore, μ and σ are disposed and not stored after the cancellable template $\mathbf{c}$ is generated. Since μ and σ are not stored, it is difficult to reveal the original vector $\mathbf{t}_j \in \mathbb{R}^o$ for further inversion attempts. Besides that, knowing the transformation key (i.e., random augmented seed $\mathbf{p} \in [1, m]^d$) is helpless towards the inversion attack as there is no direct link between $\mathbf{p}$ and $\mathbf{t}_j \in \mathbb{R}^o$, where $\mathbf{p}$ is not directly involved in the z-score normalization process. In short, it is difficult for the attacker to attempt the inversion attack via a single cancellable template $\mathbf{c} \in \mathbb{R}^{ho}$ and random augmented seed $\mathbf{p} \in [1, m]^d$.

B. Template inversion via multiple records

In this attack, the attacker attempts to recover the irisCode feature $\mathbf{Z} \in [0,1]^{m \times n}$ based on multiple compromised cancellable templates $\mathbf{c} \in \mathbb{R}^{ho}$ and random augmented seeds $\mathbf{p} \in [1, m]^d$. In biometric template protection, this attack is also rebranded as an attack via record multiplicity [156]. This attack is more damaging than the previous attack, where the attacker had gained extra information and can try to exploit the privacy linkage of multiple compromised information and reconstruct the irisCode $\mathbf{Z} \in [0,1]^{m \times n}$.

Recall the methodology, $\mathbf{p}$ is first applied to random augment $\mathbf{Z} \in [0,1]^{m \times n}$ into a random augmented irisCode $\ddot{\mathbf{Z}} \in [0,1]^{d \times n}$. To be noted, random augment is a form of permutation to provide randomness towards the irisCode in different applications. After that, an irreversible transformation is applied on $\ddot{\mathbf{Z}} \in [0,1]^{d \times n}$ to produce a cancellable template $\mathbf{c} \in \mathbb{R}^{ho}$. As stated above, the irreversibility of $\mathbf{c} \in \mathbb{R}^{ho}$ is based on the z-score normalization and the disposable parameters (i.e., μ and σ). With the extra information of multiple cancellable templates $\mathbf{c} \in \mathbb{R}^{ho}$, the attacker could proceed with the inversion attack by trying to estimate the normalization parameters, i.e., μ and σ, from the cancellable templates. In this attack, the attacker can attempt to use multiple $\mathbf{c}$s to infer the value of μ and σ to perform a further inversion attack. Given $\mathbf{c} = \hat{\mathbf{t}}_1{}^{\top} || \hat{\mathbf{t}}_2{}^{\top} || \ldots || \hat{\mathbf{t}}_h{}^{\top}$, the following case is used to discuss the feasibility to recover μ and σ from $\hat{\mathbf{t}}$ of multiple cancellable templates $\mathbf{c}s$.

Case 3.4: Given two z-score normalized vector $\hat{\mathbf{t}}_1 \in \mathbb{R}^o$ and $\hat{\mathbf{t}}'_1 \in \mathbb{R}^o$ from different $\mathbf{c}/\mathbf{c}'$ that are generated from the same input $\mathbf{Z} \in [0,1]^{m\times n}$, it is difficult to obtain μ and σ for recovering the original $\mathbf{t}_1$ and $\mathbf{t}'_1$.

Discussion: In the proposed scheme, a random augmentation process is applied onto the input $\mathbf{Z}$ to produce $\ddot{\mathbf{Z}}$. Since the randomization process is involved, different $\ddot{\mathbf{Z}}$s are formed in different applications; hence, $\hat{\mathbf{t}}_1$ and $\hat{\mathbf{t}}'_1$ are independent of each other and have different values of μ and σ. Thus, the attacker cannot use $\hat{\mathbf{t}}_1$ and $\hat{\mathbf{t}}'_1$ to estimate μ and σ. Given an irisCode $\mathbf{Z} = \begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \end{bmatrix}$ with two random augmentation seeds, i.e., $\mathbf{p} = [1,3,2,1]$ and $\mathbf{p}' = [3,2,2,1]$, the proposed scheme first augment $\mathbf{Z}$ into $\ddot{\mathbf{Z}} = \begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{bmatrix}$ and $\ddot{\mathbf{Z}}' = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{bmatrix}$. With the parameter $\{a = 4, b = 1, \beta = \frac{d}{b} = 4\}$, the $\mathbf{t}_1 = [0, 1.4142, 0, 0]$ and $\mathbf{t}'_1 = [1.4142, 0, 1.4142, 0]$ are derived from the $\ddot{\mathbf{Z}}$ and $\ddot{\mathbf{Z}}'$. Since β is same as the dimension of $\mathbf{t}_1$/$\mathbf{t}'_1$, there is only 1 set of $\{\mu, \sigma\}$ calculated for the $\mathbf{t}_1$/$\mathbf{t}'_1$. Given $\mathbf{t}_1$ and $\mathbf{t}'_1$, μ and σ are calculated as $\mu = 0.3536$, $\sigma = 0.7071$, $\mu' = 0.7071$ and $\sigma' = 0.8165$. Therefore, $\hat{\mathbf{t}}_1 \in \mathbb{R}^o$ and $\hat{\mathbf{t}}'_1 \in \mathbb{R}^o$ from the same input $\mathbf{Z}$ are normalized using different μ, σ, $\mathbf{t}_1$ and $\mathbf{t}'_1$. Since the normalized parameters (i.e., μ and σ) and the value of the unnormalized vectors ($\mathbf{t}_1$ and $\mathbf{t}'_1$) are different for $\hat{\mathbf{t}}_1$ and $\hat{\mathbf{t}}'_1$, it is unlikely that the resultant $\hat{\mathbf{t}}_1$ and $\hat{\mathbf{t}}'_1$ are collided. Therefore, it is difficult for the attacker to use $\hat{\mathbf{t}}_1$ and $\hat{\mathbf{t}}'_1$ to infer the values of μ and σ, and recover the original $\mathbf{t}_1$ and $\mathbf{t}'_1$. Moreover, the μ, σ, $\mathbf{t}_1$ and $\mathbf{t}'_1$ are not stored.

The above statements discuss the inversion attempt of using multiple $\hat{\mathbf{t}}$ to recover μ and σ for recovering the original vector $\mathbf{t}$. Since the cancellable template $\mathbf{c}$ is formed as $\mathbf{c} = \hat{\mathbf{t}}_1^{\top} || \hat{\mathbf{t}}_2^{\top} || \ldots || \hat{\mathbf{t}}_h^{\top}$, the attacker cannot attempt to recover each $\hat{\mathbf{t}}_i$ to $\mathbf{t}_i$ even the attacker has compromised multiple cancellable templates $\mathbf{c}$ from different applications. This prohibits the attacker from further inversion attacks to recover the irisCode $\mathbf{Z} \in [0,1]^{m\times n}$. In practical, $\ddot{\mathbf{Z}} \in [0,1]^{d\times n}$ is a large binary feature with the dimension of 250×512; thus, it is unlikely that $\ddot{\mathbf{Z}}$s in different systems can collide. Since multiple $\ddot{\mathbf{Z}}$s are randomized independent instances, the generated $\mathbf{c}$s are uncorrelated to each other. Moreover, as stated previously, there is no direct link between $\mathbf{c}$ and $\mathbf{p}$. Hence, given multiple $\mathbf{c}$s and $\mathbf{p}$s, it is clueless for the attacker to attempt the inversion attack and restore $\ddot{\mathbf{Z}} \in [0,1]^{d\times n}$ (or even the original $\mathbf{Z} \in [0,1]^{m\times n}$). This also shows that $\mathbf{p}$ can be stored alongside with $\mathbf{c}$ and reduce the user's burden of managing $\mathbf{p}$. To sum up, the analysis shows the proposed scheme satisfies irreversibility as the original biometric feature (i.e., $\mathbf{Z} \in [0,1]^{m\times n}$) is not recoverable with the inversion attacks.

C. Attack via input enumeration

In this attack, the attacker aims to recover the original irisCode $\mathbf{Z} \in [0,1]^{m\times n}$ via *attack via input enumeration*. This attack differs from the previous attacks that attempt to recover the original irisCode $\mathbf{Z} \in [0,1]^{m\times n}$ by reverse processing the cancellable iris template $\mathbf{c} \in \mathbb{R}^{ho}$, the attacker guesses a fake $\mathbf{Z}^*$ and inject $\mathbf{Z}^*$ to the proposed scheme to produce a cancellable iris template $\mathbf{c}^*$. The template $\mathbf{c}^*$ is then matched to the compromised $\mathbf{c}$. This attack is simple and effective as it does not require prior knowledge of the transformations function. In this attack, recovery of $\mathbf{Z}$ is considered successful when the attacker can produce $\mathbf{c}^*$ that is equal to $\mathbf{c}$ ($\mathbf{c}^* = \mathbf{c}$). The attack complexity of this attack can be calculated using the below formula:

$$\text{Attack Complexity} = \text{Guess Attempt} \times \text{Time Complexity} \tag{3.9}$$

where guess attempt refers to the total rounds required to guess a $\mathbf{Z}^*$ that can produce a $\mathbf{c}^*$ which is equal to the compromised $\mathbf{c}$ and the time complexity refers to the time required to transform a guessed $\mathbf{Z}^*$ into $\mathbf{c}^*$. Since the matching is done using a simple matcher, the matching time is not factored into the formula. In the proposed scheme, the original irisCode $\mathbf{Z} \in [0,1]^{m\times n}$ is a binary matrix; hence, the guess complexity for each correct entry $z \in \boldsymbol{Z}$ is $2/2 = 1$, where the possible values of z are 0 and 1. Therefore, the guess attempt for the entire $\mathbf{Z}$ is equal to $2^{20\times 512}/2$, where 20×512 is the dimension of the extracted irisCode in the proposed scheme. Based on section 0, the time complexity is referred from the average processing time for the verification stage. To sum up, this attack requires a total of $(2^{20\times 512}/2) \times 0.0811\ (\text{seconds})$ to recover the entire $\mathbf{Z}$. From the calculated value, it is computation infeasible for the attacker to recover the original irisCode $\mathbf{Z}$; and hence, the proposed scheme shows resistance against attack via input enumeration.

3.5.2 Security analysis

Security refers to the feasibility of a method to withstand the attack, which is used to gain illegal access with a fake query cancellable template that is similar to the pre-stored enrolled template. In this subsection, the security aspect of the proposed method is examined using three main attacks in biometric-based authentication.

A. Brute-force attack

In this attack, the attacker guesses the cancellable template $\mathbf{c}^*$ exhaustively and compare $\mathbf{c}^*$ to the enrolled cancellable template $\mathbf{c}$. The brute-force (BF) attack succeed when the attacker obtains the $\mathbf{c}^*$ that is the same as the enrolled $\mathbf{c}$ ($\mathbf{c}^* = \mathbf{c}$). In the proposed scheme, $\mathbf{c} \in \mathbb{R}^{ho}$ is a real-valued vector with a size of $ho = 16000$ (generating using the best-tuned parameters) and value distribution of $[LB_\mathbf{c}, UB_\mathbf{c}]$, where UB and LB denote the *upper* and *lower* value bounds for each $c_i \in \mathbf{c}$. In this attack, the attacker is required to guess each $c_i \in \mathbf{c}$, where $i = 1, \dots, 16000$ is the i-th element in $\mathbf{c}$ and 16000 is the size of $\mathbf{c}$. The guess attempt for each $c^*{}_i \in \mathbf{c}^*$ is determined by the value range (i.e., $LB_\mathbf{c}$ and $UB_\mathbf{c}$) and the guess precision for the real-valued c_i in decimal points. For instance, given $c \in [-0.02, 0.02]$ and a guess precision of 2 decimal points, it requires 5 guess attempts to guess a correct c out of -0.02, -0.01, 0.00, 0.01 and 0.02. In short, the guess attempt for a correct guess of $c_i \in \mathbf{c}$ is formulated as below:

$$\text{Guess Attempt } = \|UB_\mathbf{c} - LB_\mathbf{c}\| \times 10^{\text{decimal points}} + 1 \tag{3.10}$$

The guess complexity for the entire $\mathbf{c}^*$ is calculated as $\text{Guess Complexity} = \text{Guess Attempt}^{\text{size}}$ where size refers to the size of $\mathbf{c}^*$. Since $\mathbf{c}^*$ is a vector with the size of $ho = 16000$, is it unlikely that the attacker can guess the entire $\mathbf{c}^*$ within a feasible time.

The guess complexity with different guess precisions is calculated and evidenced in the table below. The cancellable template $\mathbf{c} \in \mathbb{R}^{ho}$ is generated using the best-tuned parameters $\{d = 250, a = 32, b = 1\}$. In the table, the lowest guess precision requires a total of 87^{16000} guess attempts. Thus, it is clearly infeasible for the attacker to carry out the BF attack onto the proposed scheme. Therefore, the analysis shows the proposed scheme can resist the BF attack.

Table 3.8: Brute force attack complexity with different guess precisions

Transformation Parameters			Value Distribution of $\mathbf{c}$	Guess Precision	Guess Complexity for each $c_i \in \mathbf{c}$	Guess Complexity for $\mathbf{c}$
d	a	b				
250	32	1	$[-2.6668, 5.9799]$	1	87	87^{16000}
				2	865	865^{16000}
				3	8647	8647^{16000}
				4	86468	86468^{16000}

B. False acceptance attack

A Biometric system is a thresholding-based decision system that grants access when the matching score can surpass the system's pre-defined threshold τ. The attacker can exploit the false acceptance rate (FAR) of the biometric system and gain illegal access to the system. Unlike the brute-force attack that manually guesses each entry of the cancellable iris template, a false acceptance attack (or dictionary attack) requires less guess complexity where it only requires the fake cancellable template $\mathbf{c}^*$ to surpass the minimal system threshold τ [157]. Typically, a false acceptance (FA) attack is analyzed by calculating the attack complexity for generating $\mathbf{c}^*$ that surpass the τ, where τ is the point when False Acceptance Rate (FAR) = False Rejection Rate (FRR) (refer to [66] for the analysis). However, this is not secure, especially when the attacker initially generates $\mathbf{c}^*$ which drops in the upper-bound (UB_{imp}) of impostor scores distribution, where the matching score is initially higher than τ**.** Thus, τ should always be tuned under the case that FAR$= 0\%$ to maintain sufficient security. However, higher τ leads to a lower genuine acceptance rate (GAR), which is the trade-off between security and matching performance. In this subsection, the false acceptance attack is analyzed towards the proposed scheme and choose a suitable system threshold τ.

The FA attack is conducted in the worst-case scenario by assuming the attacker first generate a $\mathbf{c}^*$**,** where the similarity score between $\mathbf{c}$ and $\mathbf{c}^*$ is equal to UB_{imp}. After that, the attacker perturbs $\mathbf{c}^*$ by guessing each correct $c^* \in \mathbf{c}^*$ until $S(\mathbf{c}, \mathbf{c}^*) = \tau$. For the security consideration, τ is a *secure matching threshold* that sacrifices a certain level of GAR and always higher than UB_{imp}. Given the guessed template $\mathbf{c}^*$ and enrolled template $\mathbf{c}$, the attack complexity required to increase the matching score $S(\mathbf{c}, \mathbf{c}^*)$ from UB_{imp} to τ and is calculated with the following formula:

$$\text{Attack complexity} = (N_{\mathrm{c}})^{SIZE_{\mathrm{c}} \times (\tau - UB_{\mathrm{imp}})} \tag{3.11}$$

where $N_{\mathbf{c}}$ is the possible value for each $c \in \mathbf{c}$ and $SIZE_{\mathbf{c}}$ denotes the size of $\mathbf{c}$. Since $\mathbf{c}$ is a real-valued vector with value distribution of $[LB_{\mathbf{c}}, UB_{\mathbf{c}}]$, the $N_{\mathbf{c}}$ is calculated based on the formula as discussed in Section 3.5.2A using different guess precisions. The formula is as below:

$$N_{\mathbf{c}} = \, \|UB_{\mathbf{c}} - LB_{\mathbf{c}}\| \times 10^{\text{decimal points}} + 1 \tag{3.12}$$

where $SIZE_{\mathbf{c}} = 2ho = 16000$. Since the main purpose of this evaluation is to find a suitable τ, the analysis is carried out using different τs with respect to the GAR.

Table 3.9: False acceptance attack complexity under different settings of τ

Value Distribution of c	**Guess Precision**	**System Threshold** τ	UB_{imp}	$\tau - UB_{\mathrm{imp}}$	$N_{\mathbf{c}}$	**FA Attack Complexity**
GAR= $\mathbf{95\%}$						
$[-2.6668, 5.9799]$	1	0.4021	0.3938	0.0083	87	$87^{16000\times0.0083} \approx 87^{132}$
	2				865	$865^{16000\times0.0083} \approx 865^{132}$
	3				8647	$8647^{16000\times0.0083} \approx 8647^{132}$
	4				86468	$86468^{16000\times0.0083} \approx 86468^{132}$
GAR= $\mathbf{90\%}$						
$[-2.6668, 5.9799]$	1	0.4151	0.3938	0.0213	87	$87^{16000\times0.0213} \approx 87^{340}$
	2				865	$865^{16000\times0.0213} \approx 865^{340}$
	3				8647	$8647^{16000\times0.0213} \approx 8647^{340}$
	4				86468	$86468^{16000\times0.0213} \approx 86468^{340}$
GAR= $\mathbf{85\%}$						
$[-2.6668, 5.9799]$	1	0.4219	0.3938	0.0281	87	$87^{16000\times0.0281} \approx 87^{449}$
	2				865	$865^{16000\times0.0281} \approx 865^{449}$
	3				8647	$8647^{16000\times0.0281} \approx 8647^{449}$
	4				86468	$86468^{16000\times0.0281} \approx 86468^{449}$

Table 3.9 tabulates FA attack complexity for the proposed scheme under different matching thresholds τ. From the table, it is observed that the minimum attack complexity is reduced from 87^{16000} to 87^{132} compared to the brute force attack. Besides that, another observation is that UB_{imp} and τ are consistent under different guess precisions, and this shows it is not required to guess $\mathbf{c}^*$ with high guess precision. Yet, a minimum of 87^{132} attempts are still required to gain access to the system, which is computationally infeasible for the attacker to carry out the FA attack towards the proposed scheme. With the minimum attack complexity of 87^{132} attempts and GAR= 95%, the verification rate is still reasonable.

C. Birthday attack

Birthday attack [158] is the well-known cryptanalytic technique that exploits the birthday problem [158] to find the collision likelihood between the ciphertexts of different clear texts. In the biometrics context, a birthday attack refers to the scenario where the attacker aims to generate a fake cancellable template $\mathbf{c}^* \in \mathbb{R}^{ho}$ using the collisions of the input irisCode $\mathbf{Z} \in [0,1]^{m \times n}$ and use $\mathbf{c}^*$ to gain access to the system. In other words, the attacker aims to obtain a fake input irisCode $\mathbf{Z}^*$, such that $RHOG(\mathbf{Z}^*) = RHOG(\mathbf{Z})$ where $RHOG(.)$ refers to the transformation function for the proposed scheme. In this case, $\mathbf{Z}$ and $\mathbf{Z}^*$ is the collision pair and $\mathbf{Z} \neq \mathbf{Z}^*$. This attacker requires less attack complexity than the BF and FA attacks because the estimated $\mathbf{Z}^*$ does not need to be the same as the $\mathbf{Z}$.

This analysis is determined by calculating the birthday bound [158] in terms of the guess attempts. Here, a brief description of the birthday bound [158] is given, followed by the formalization of the birthday attack. Suppose a transformation function $f(x)$ that can produce H numbers of possible outputs, the minimum attack attempts (birthday bound) required to obtain x^*, such that $f(x) = f(x^*)$ can be calculated

$$\text{Birthday bound} = \sqrt{2H \cdot \ln(1/(1-p))} \tag{3.13}$$

where p is the collision rate between x and x^*, and H refers to the possible combinations for the output of $f(x)$.

The birthday attack is conducted as an extension of the FA attack where the attacker initially guessed $\mathbf{Z}^*$ that can produce $\mathbf{c}^*$ which is initially drops in the upper-bound (UB_{imp}) of impostor scores distribution. Then, the attacker perturb each $z_{ij} \in \mathbf{Z}^*$ until $S(\mathbf{c}, \mathbf{c}^*) = \tau$, where τ is the system threshold. Since there are $(N_{\text{c}})^{SIZE_{\text{c}}}$ of possible $\mathbf{c}'$s where $SIZE_{\mathbf{c}} = ho = 16000$ is the template size for $\mathbf{c}$; the birthday attack complexity can be estimated as follows:

$$\text{Attack Complexity} = \sqrt{2(N_{\text{c}})^{SIZE_{\text{c}} \times (\tau - UB_{\text{imp}})} \cdot \ln(1/(1-p))} \tag{3.14}$$

where p is the collisions rate for $\mathbf{Z}^*$ that is falsely recognized as the genuine $\mathbf{Z}$. In this case, p is calculated based on the False Acceptance Rate (FAR) in genuine/ impostor score distributions. N_c is the number of possible $c \in \mathbf{c}$, which is calculated based on the Eq. (3.12) in Section 3.5.2B with the guess precision $= 1$. As observed from FA attack analysis, the attacker is not required to perform the attack with high guess precision. Thus, the analysis is not considering the attack under guess precision > 1. In this subsection, analysis of the birthday attack is conducted towards the proposed scheme under different GARs and choose the suitable system threshold τ.

Table 3.10 tabulates the attack complexity for the CASIAv3 dataset under different GARs. From the table, we observed the minimum attack complexity is reduced from 87^{132} to $(87^{132/2} \cdot 0.110)$ (attempts) compared to the false acceptance attack. However, the attack complexity is sufficient to resist the birthday attack. The security strength can be further increased by adjusting τ to a higher value. With the minimum attack complexity of $(87^{132/2} \cdot 0.110)$ attempts and GAR= 95%, the verification performance remains reasonable.

Table 3.10: Birthday attack complexity under different settings of τ

N_c **(Guess precision =1)**	p	**System Threshold** τ	UB_{imp}	$\tau - UB_{\text{imp}}$	$\ln(1/(1-p))$	**Birthday Attack Complexity**
GAR= 95%						
87	0.0060	0.4021	0.3938	0.0083	≈ 0.006	$\approx 87^{132/2} \cdot 0.110$
GAR= 90%						
87	0.0060	0.4151	0.3938	0.0213	≈ 0.006	$\approx 87^{340/2} \cdot 0.110$
GAR= 85%						
87	0.0060	0.4219	0.3938	0.0281	≈ 0.006	$\approx 87^{449/2} \cdot 0.110$

3.5.3 Unlinkability and renewability analysis

Unlinkability and renewability properties are important towards a cancellable biometric scheme to allow the reproduction of cancellable templates for the same biometric input while minimizing the linkage between multiple cancellable templates generated from the same biometric input. This section examines the unlinkability and renewability properties of the proposed scheme via quantitative experiments. Throughout the experiments, the cancellable templates $\mathbf{c}$s are generated using best-tuned parameters as listed in Section 3.4.2C.

A. Unlinkability analysis

In this section, the benchmarking unlinkability analysis framework [159] is employed to examine the unlinkability of the proposed scheme. Particularly, this assessment framework relies on the two indicators, $D_{\leftrightarrow}(s)$ and $D_{\underset{\longleftrightarrow}{sys}}$, to quantify the unlinkability level of a biometric system [159]:

- **Local measure**, $D_{\leftrightarrow}(s)$: $D_{\leftrightarrow}(s)$ is a local score-wise indicator that is found between mated/ non-mated score distributions according to the likelihood ratio [159].

- **Global Measure**, $D_{\underset{\longleftrightarrow}{sys}}$: $D_{\underset{\longleftrightarrow}{sys}}$ assesses the unlinkability of the whole system [159]; thus, $D_{\underset{\longleftrightarrow}{sys}}$ is usually used for benchmarking purpose [159].

Specifically, the indicators are calculated based on the mated/non-mated samples score distributions that are generated from the following matching attempts [126], [159]:

- **Mated-samples matching attempt**: Cross-matching multiple cancellable templates $\mathbf{c}$s which are generated from the same iris instance of the same subject.

- **Non-mated samples matching attempt**: This matching attempt is conducted by matching $\mathbf{c}$s generated from the first sample of different subjects

In both matching attempts, every $\mathbf{c}$s is generated using different $\mathbf{p} \in [1, m]^d$ to simulate the situation that the cancellable templates $\mathbf{c}$s are from different system databases. Particularly, 5 random augmentation seeds $\mathbf{p}$s are used to generate up to 5 $\mathbf{c}$s for each iris. $D_{\leftrightarrow}(s)$ and $D_{\underset{\longleftrightarrow}{sys}}$ ranged from 0 to 1, which indicates the linkage level of the cancellable templates [159]. The computed $D_{\leftrightarrow}(s)$ and $D_{\underset{\longleftrightarrow}{sys}}$ should remain as low as possible to provide a considerable level of unlinkability. Besides that, $D_{\underset{\longleftrightarrow}{sys}}$ can also be used to verify the renewability property. Particularly, the low linkage between the cancellable templates for the same user (low $D_{\underset{\longleftrightarrow}{sys}}$) shows that the newly generated cancellable template is indistinguishable from other users.

Throughout the unlinkability assessment, the cancellable templates are generated with respect to the best-tuned parameters, as discussed in Section 3.4.2C. The parameter of the evaluation framework ϖ is set to 1 to evaluate the linkage of cancellable templates under the worst-case scenario [159]. Fig 3.4 shows the result of the unlinkability analysis in terms of mated/ non-mated score distributions and $D_{\underset{\longleftrightarrow}{sys}}$. The plotted score distributions show the proposed scheme is achieving a nearly unlinkable scenario where both score distributions are highly overlapped. Other than that, the calculated global measure $D_{\underset{\longleftrightarrow}{sys}} \approx 0.04$ shows that the proposed scheme meets the unlinkability requirement.

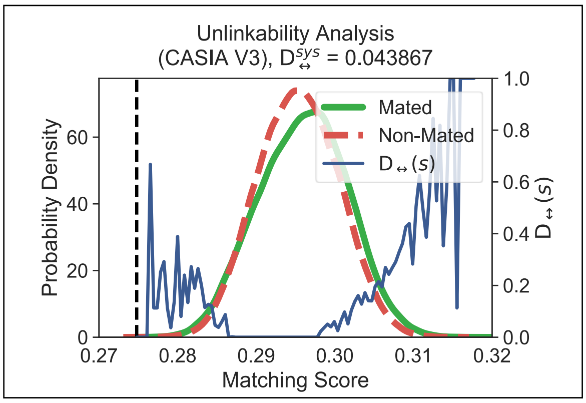


Fig 3.4. Unlinkability analysis of CASIAv3 dataset with best-tuned parameters

B. Renewability (or revocability) analysis

Renewability refers to the reproduction of the cancellable templates $\mathbf{c}$ using the same input biometric feature $\mathbf{Z}$ [19]. $D_{\underset{\longleftrightarrow}{sys}} = 0.04$ calculated from the unlinkability analysis shows the proposed scheme having renewability property where multiple cancellable templates $\mathbf{c}$s from the same $\mathbf{Z}$ have low linkage. This subsection further investigates the renewability by performing a quantitative experiment as suggested in [66]. This experiment is built upon three score distributions: *Genuine*, *Impostor* and *Pseudo-impostor* Score distributions by assuming the cancellable templates are generated under different cases. The matching attempts, as discussed in Section 3.4.1A, are followed to generate the genuine and impostor score distributions. Differ from the experiment in Section 3.4.1A, the renewability property is evaluated under the real-world scenario where the cancellable templates for different users are generated using different transformation keys. Hence, different random augmentation seed $\mathbf{p}$s are assigned to different users during the impostor matching attempt. Besides that, the pseudo-impostor matching attempt is followed to generate the pseudo-impostor score distributions:

- **Pseudo-impostor matching attempt:** Different random augmentation seed $\mathbf{p}$s are used to generate up to 51 cancellable templates $\mathbf{c}$s for the same input irisCode $\mathbf{Z}$. Then, the first $\mathbf{c}$ is matched to the 50 $\mathbf{c}s$ and form the mated-sample score distribution.

This pseudo-impostor matching attempt is carried out by matching the "compromised" (or old) cancellable template to many "renewed" cancellable templates. In this case, each renewed cancellable template is assumed as the impostor template that does not belong to the enrolled user. Therefore, the pseudo-impostor score distribution should not highly overlap with the genuine matching score distribution to demonstrate the renewability property of the scheme. Fig 3.5 shows the genuine, impostor and mated samples score distributions of the cancellable templates $\mathbf{c}$s generated via the proposed R·HoG scheme. From the figure, it is observed that the impostor and genuine score distributions are not overlapped, and this implies the newly generated cancellable template $\mathbf{c}$ are not same as the “old” template. In conclusion, this shows that the proposed scheme satisfies the renewability property.

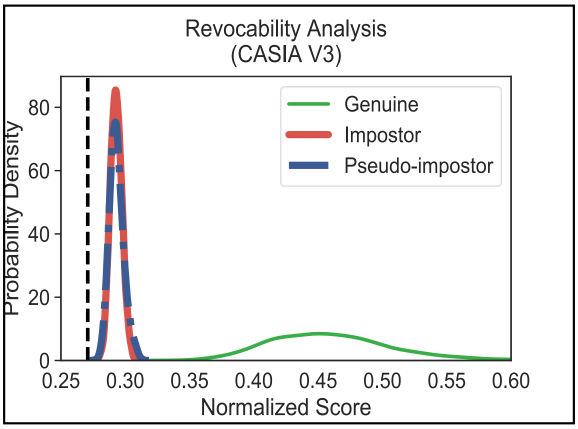


Fig 3.5. Renewability of CASIAv3 dataset with best-tuned parameter

3.5.4 Summary of security and privacy analysis

Throughout the security and privacy analyses, the observations are summarized as below:

- The key ingredients (i.e., μ and σ) to form the cancellable template $\mathbf{c} \in \mathbb{R}^{ho}$ are biometric dependent parameters that are not stored in the storage. Therefore, it is hard for reverse transforming the $\mathbf{c} \in \mathbb{R}^{ho}$ to the irisCode $\mathbf{Z} \in [0,1]^{m \times n}$ even the random augmented seeds $\mathbf{p} \in [1, m]^d$ are known. Whenever the $\mathbf{c}$ is compromised, the user can renew the template by using a different $\mathbf{p}$, thus, shows renewability.

- The proposed scheme can withstand major security attacks (e.g., false acceptance and birthday attacks) while maintaining reasonable verification performance.

- The unlinkability evaluation result suggests the proposed scheme allows the user to enroll/ re-enroll into different applications with the same iris feature. The renewability analysis shows the renewed cancellable template is independent of the old cancellable template.

3.6 Summary and contributions

In this chapter, the main problem in the irisCode template protection is perceived as the degraded authentication efficiency that is caused by the alignment issue in the irisCode feature. The main research outcome in this chapter is an alignment-robust cancellable biometric scheme dubbed the Random Augmented Histogram of Gradients (R·HoG) that could overcome the pre-alignment issue of the iris feature and produce an alignment-robust cancellable iris template for efficient matching. Two mechanisms: column vector-wise random augmentation and gradient orientation grouping, are used to consolidate this proposal in terms of performance preservation and irreversibility. Matching performance is validated under the worst-case (stolen token) scenario, and it shows reasonable matching accuracy. With the comprehensive analysis that is supported by the empirical data, the R·HoG cancellable biometric scheme is proved to withstand major security and privacy attacks, e.g., false acceptance attack and birthday attacks. By sacrificing a certain level of genuine acceptance rate for the higher system threshold τ, the proposed scheme can resist the birthday attack, with the minimum attack complexity of $87^{132/2} \cdot 0.110$ attempts and GAR=95%. Besides that, the quantitative analysis framework suggests the proposed scheme achieve unlinkability requirement with the calculated $D_{\underset{\longleftrightarrow}{sys}}$ close to 0. Renewability is enabled by using a different random augmentation seed during the re-enrollment. More importantly, the R·HoG enjoys the merit of the fast similarity comparison where the generated cancellable template does not require pre-alignment during the matching process, which is crucial for the efficient authentication process.

Chapter 4 TOKENLESS FINGERPRINT AND FACE TEMPLATE PROTECTION

Most of the face and fingerprint cancellable biometric schemes are commonly designed to protect biometric templates with two input factors, i.e., biometrics and a token used in template replacement. However, the token is often required to be kept secretly; otherwise, the protected template could be vulnerable to several security attacks and breaches of privacy. In this chapter, two tokenless cancellable biometric schemes, namely the Extended Feature Vector (EFV) Hashing and the Multimodal Extended Feature Vector (M·EFV) Hashing, are proposed for the face and fingerprint-based biometric systems. The former scheme is a unimodal fingerprint cancellable biometric scheme that focuses on resolving token management issues. The EFV hashing utilizes a permuted key that is separated from the biometric data to serve as an identifier for matching. The crux that enables the tokenless authentication in EFV hashing is the permutation seed of the key is derived from the biometric features of the user, but not from the external factor (e.g., token). The latter scheme is essentially an enhanced version of the former scheme that explores biometric fusion to resolve the performance degradation issue. The proposed M·EFV hashing stresses on multimodal biometrics where the real-valued face and fingerprint vectors are fused and embedded into a binarized cancellable template. Several benchmarking datasets, i.e., fingerprint {FVC2002, FVC2004} and face {LFW}, are used in experiments to evaluate the proposed schemes. The verification performance is validated by employing the FVC matching protocol. Several major attacks are simulated and analyzed in the worst-case scenario. Lastly, unlinkability and renewability properties are examined experimentally.

4.1 Background

In this chapter, the problems of biometric template protection in the face and fingerprint verification is mainly perceived as *key management* and *feature incompatibility problems*: Face and fingerprint-based cancellable biometrics are commonly designed as a *two-factor authentication scheme* that requires to present the *biometric feature* and a *token* (storage for the transformation key) where the token is used for the template revocation and renewal. The two-factor authentication mechanism has distorted the usability of biometric systems. First of all, the token could be stolen and utilized for unfavorable events, e.g., impersonation, original template inversion attack and cross-matching [27]. Most of the existing multimodal cancellable biometric schemes, i.e., [99], [129], [132], [134], are designed to be a *two-factor scheme*. Although the use of a user-specific key (i.e., token) satisfies the renewability and unlinkability requirements, a failure in managing the key can lead to several security-related problems, as mentioned. In this sense, a sole biometric instance-enabled tokenless scheme is preferable. However, a tokenless scheme produces additional auxiliary data, which is derived from the transformation key and stored alongside the cancellable template after enrollment, which is absent for tokenized schemes. Moreover, a tokenless scheme requires an additional process to recover the transformation key from the auxiliary data in the verification stage. In short, a tokenless scheme trades extra storage and additional processing costs for better usability due to the absence of the key.

Multimodal biometric systems are gaining the public's interest as they compensate for issues of unimodal systems such as recognition performance limitation [27], [98], [160]. However, multimodal biometric systems do suffer from the same privacy issues mentioned above, yet it could even be more severe due to multiple templates of different modalities being stored (and compromised eventually). Therefore, multimodal biometric template protection deserves urgent attention. In multimodal biometrics, there are three major fusion strategies available, i.e., feature, score and decision level fusion [9]. Although score and decision level fusion gain better accuracy performance, they require cancellable templates to be generated and stored separately, which may prompt complications in template and storage management [99], [134]. Therefore, the *feature-level fusion* that integrates multiple biometric modality features into a single cancellable template is preferred. Yet, it is challenging to design a feature-level fusion cancellable biometric scheme. This is due to the incompatibility issue of different biometric modalities, such as different biometric feature types (e.g., fingerprint minutiae point and face deep feature) [9].

To address the above challenges, this chapter introduces two tokenless cancellable biometric schemes, namely the *Extended Feature Vector (EFV) Hashing* and *Multimodal Extended Feature Vector (M·EFV) Hashing* for both unimodal and multimodal biometric systems without requiring the user to manage the key, as the key is released upon the presence of the biometrics. The proposed schemes are salted by an XOR encryption/ decryption machinery, which is adopted from the fuzzy commitment scheme (an instance of a biometric cryptosystem). Specifically, XOR is used to bind or retrieve the transformation key, which enables the “tokenless” property for both EFV hashing and M·EFV hashing. The proposed schemes are distinguishable from the existing hybrid schemes (cancellable biometrics + biometric cryptosystems) in the sense that:

1) The existing hybrid schemes (e.g., [135]–[137], [161], [162]) are primarily used for binding/releasing a key, while the proposed tokenless schemes are meant to generate secure and revocable templates while avoiding a two-factor approach.

2) As the hybrid schemes are key binding, the *exact* key must be recovered in these schemes. In contrast, the tokenless scheme might never produce the exact key. Instead, given genuine query biometrics, recovery of a ‘*similar’* random string is to facilitate secure template generation.

3) Error correction codes (ECCs) [135], [161], [162] or other mechanisms [136] (e.g., thresholding [137]) are applied to correct the errors in the reviewed hybrid schemes, while the tokenless scheme does not require error correction.

In short, the contributions made in this chapter are highlighted as follows:

- A new tokenless authentication mechanism that addresses the *key management* issue for unimodal and multimodal cancellable biometrics is introduced. As the token is abandoned, the associated attacks are therefore no longer considered a threat. Other than that, tokenless authentication reduces the burden for users to manage an external token for authentication.

- A feature-level fusion method is proposed to embed the real-valued face and fingerprint feature vectors into a binarized feature vector without sacrificing the discriminative traits of the face and fingerprint features. In addition, with the generic property of accepting real-valued, fixed-length face and fingerprint vectors as input, the proposed scheme can be transferred to other biometric traits exhibiting the same form factor. To the author's best knowledge, there is no existing tokenless multimodal biometric template protection in the literature.

- Security and privacy aspects of the resultant cancellable template are examined in both quantitative and qualitative manner. Supported by the empirical results, it is proved that the proposed M · EFV hashing satisfies the major biometric template protection requirements. In addition, major security attacks are carried out to examine the security strength of the proposed schemes and choose the suitable secure system threshold.

- This chapter further analyses the birthday attack, which was a new type of attack and first proposed by [66] for cancellable biometrics. Specifically, the analyses in this chapter factor in the worst-case scenario that the adversary is able to obtain a good guessed biometric input which drops at the upper bound of impostor matching score distributions. Other than that, the birthday attack is launched in a different manner from [66], where it estimates the input which is used for generating the cancellable template. As such, attack complexity is shown to be much lower compared to attacking the large cancellable template.

This chapter is organized as follows: Section 4.2 discusses the proposed EFV hashing, which was designed in the earlier stage and the preliminary in which the stage-2 transformation of the proposed M · EFV hashing is built upon. After that, section 4.4 introduces the methodology of the proposed M·EFV hashing, followed by section 4.5 to present the experiment results in terms of parameters estimation, analysis on stage-1 transformation and computation efficiency. Section 4.6 examines the irreversibility, security and unlinkability properties of the proposed M·EFV hashing. Lastly, section 4.7 concludes the findings of this chapter.

4.2 Preliminaries

This section is devoted to presenting the preliminary works (i.e., Index-of-Max (IoM) Hashing and Extended Feature Vector (EFV) Hashing), which the proposed Multimodal Extended Feature Vector (M·EFV) Hashing is built upon.

4.2.1 Index-of-Max (IoM) Hashing

Index-of-Max (IoM) hashing is a ranking-based cancellable biometric scheme that was originally proposed for fingerprint template protection [66]. In the proposed scheme, the IoM hashing plays an important role in the stage-2 transformation in the proposed scheme where it transforms the original biometric vector $\mathbf{x} \in \mathbb{R}^d$ into a binary vector (refer to IoM Bio. Vector $\mathbf{h} \in [0,1]^{2d}$) where the value of the binary vector represents the index of the maximum value of the feature vector during the IoM transformation. This subsection gives a brief account of the Gaussian Random Projection (GRP) based IoM hashing function. Given a set of random projection matrices $\mathbf{P} = \{\mathbf{P}_1, \ldots, \mathbf{P}_q\}$ where each $\mathbf{P}_i \in \mathbb{R}^{m \times d}$, the procedures to transform the original biometric vector $\mathbf{x} \in \mathbb{R}^d$ to the IoM hashed code $\mathbf{h} \in [0, m-1]^q$ are described as below:

1) Project $\mathbf{x}$ onto a random sub-space and form a *projected vector* $\mathbf{v}_i \in \mathbb{R}^m$ by computing $\mathbf{v}_i = \mathbf{x} \cdot \mathbf{P}_i$.

2) Record the index value which corresponds to the maximum value in the $\mathbf{v}_i$ as the IoM hashed code h_i:

$$h_i = \operatorname{argmax}(\mathbf{v}_i) \tag{4.1}$$

where $\operatorname{argmax}(.)$ is the argument maximum function.

Repeat step 1-2 for $i = 1 \ldots q$ rounds until the IoM hashed code $\mathbf{h} \in [0, m-1]^q$ is constructed.

4.3 Methodology – Extended Feature Vector (EFV) hashing

This section is devoted to presenting the methodology of the Extended Feature Vector (EFV) hashing.

Extended feature vector (EFV) hashing [1] is the preemptive tokenless cancellable biometric method that was introduced in the earlier stage of the research in this thesis. EFV hashing was originally designed for unimodal fingerprint template protection. Since the EFV hashing is a part of the Multimodal EFV hashing, this section gives a brief description of the EFV hashing. Briefly, EFV hashing is a permutation-based template protection method that utilizes a permuted key as a reference (cancellable template) for verification [1]. Unlike existing template protection methods that store the transformation key in a token or password, the proposed method transforms the transformation key into the form of an encrypted key and stores it alongside the cancellable template. In particular, during enrollment, the transformation key is derived from the pseudo-random number generator. After the cancellable template is generated, the transformation key will be encrypted into the encrypted key via XOR encryption. Therefore, the original biometric data and genuine transformation key are not stored. During verification, after the biometric data is accepted by the EFV hashing, an *approximate transformation key* is released by XOR-ing the input biometric feature and the encrypted key. The approximate transformation key is then used to generate the query template for matching. In a nutshell, EFV hashing only requires the user to provide a biometric feature for enrollment/ verification.

EFV hashing consists of a 4-step procedure to transform the fingerprint vector into a cancellable template [1]. Given a fingerprint vector $\mathbf{x} \in [0,1]^p$ and a randomly generated transformation key $\mathbf{r} \in [0,1]^{pn}$, the below procedures are followed to generate the EFV hashed code $\mathbf{t} \in [0,1]^{pn}$:

1) *Feature Augmentation:* The $\mathbf{x}$ is augmented by repeatedly appending the $\mathbf{x}$ to the *extended feature vector* $\bar{\mathbf{x}}$ for $n-1$ times. Throughout this process, a $\bar{\mathbf{x}} \in [0,1]^{pn}$ is yield.

2) *Sub-block Construction:* Each $\bar{x}_i \in \bar{\mathbf{x}}$, it is appended with the corresponding $(k-1)$ element(s) from the $\bar{\mathbf{x}}$; a *sub-bits block* $[\bar{x}_i \,|\bar{x}_{i+1}| \dots |\bar{x}_{i+(k-1)}]$ is constructed where | denotes the concatenation.

3) *Binary-to-Decimal Conversion*: Each sub-bits block $[\bar{x}_i\ |\bar{x}_{i+1}|\ ...\ |\bar{x}_{i+(k-1)}]$ is converted to an integer number $\hat{x}_i \in \mathbb{Z}$. After pn numbers of sub-bits blocks are converted, an integer vector $\hat{\mathbf{x}} \in [1, pn]^{pn}$ is formed. To be noted, each $\hat{x}_i \in \hat{\mathbf{x}}$ is re-calculated as $\hat{x}_i$=$((\hat{x}_i + 1) \times i)\text{mod}(pn + 1)$ to ensure the value of $\hat{x}_i$ is bounded from 1 until pn.

4) *EFV Hashed Code formalization*: Given the $\mathbf{r} \in [0,1]^{pn}$ and $\hat{\mathbf{x}} \in [1, pn]^{pn}$, each $t_i \in \mathbf{t}$ is computed as $t_i = r_{\hat{x}_i}$ where $i = 1 \ldots pn$. Lastly, the EFV hashed code $\mathbf{t}$ = $[r_{\hat{x}_2}, \ldots, r_{\hat{x}_{pn}}] \in [0,1]^{pn}$ is formed.

Since the EFV hash code $\mathbf{t} \in [0,1]^{pn}$ is a binary vector, comparison between the enrolled $\mathbf{t}$ and query $\mathbf{t}'$ can be made using the *normalized hamming similarity* [1]. Despite the EFV hashing resolved token management issue in biometric template protection, there are two shortcomings observed in the original construction of EFV hashing [1]:

- Performance degradation is observed in the unimodal EFV hashing. From [1], the Equal Error Rate (EER) (%) of the fingerprint system in FVC2002 DB2 is observed to be increased from 4.39% to 6.27%.

- Despite EFV hashing showing a strong irreversibility property when there is only one set of the cancellable template and encrypted string are compromised, it is potentially that the original fingerprint vector can be recovered if multiple cancellable templates and encrypted string are involved. Particularly, the attacker could perform correlation analysis between multiple cancellable templates and encrypted string [1].

4.4 Methodology – Multimodal EFV (M·EFV) hashing

This section is devoted to presenting the proposal face and fingerprint-based multimodal template protection scheme, i.e., Multimodal Extended Feature Vector (M·EFV) hashing. Mathematical notations of the proposed M·EFV hashing are listed in the table below.

Table 4.1: NOMENCLATURE

Notation(s)	Description
$\mathbf{x} \in \mathbb{R}^{2d}$	Original Bio. Vector
$\mathbf{h} \in [0,1]^{2d}$	IoM Bio. Vector
$\hat{\mathbf{h}} \in [0,1]^{2dn}$	Augmented Bio. Vector
$\ddot{\mathbf{h}} \in [1, 2^k]^{2dn}$	Integer Bio. Vector
$\mathbf{c} \in [0,1]^{2dn}$	Cancellable Template
$\mathbf{r} \in [0,1]^{2d}$	Transformation Key (Random String)
$\mathbf{e} \in [0,1]^{\mathbf{2d}}$	Encrypted String
$\mathbf{P} = \{\mathbf{P}_1, \mathbf{P}_2 \dots \mathbf{P}_q\}$, each $\mathbf{P}_i \in \mathbb{R}^{m\times \mathbf{2}d}$	Projection Seed
$\alpha \in \mathbb{R}, \alpha > 0$	Rescale ratio
$n \in \mathbb{Z}, n > 1$	Number of Appending Round
$s \in \mathbb{Z}, s \geq 1$	Number of Bit Shifting
$k \in \mathbb{Z}, k \geq 2$	Sub-Block Size
$\beta \in \mathbb{Z}, 1 \leq \beta \leq 2^k$	Many-to-One Modulo Threshold

Note that the symbol $'$ is used to differentiate the same variable in the enrollment/ verification stage, e.g., $\mathbf{x}$ and $\mathbf{x}'$.

4.4.1 Overview

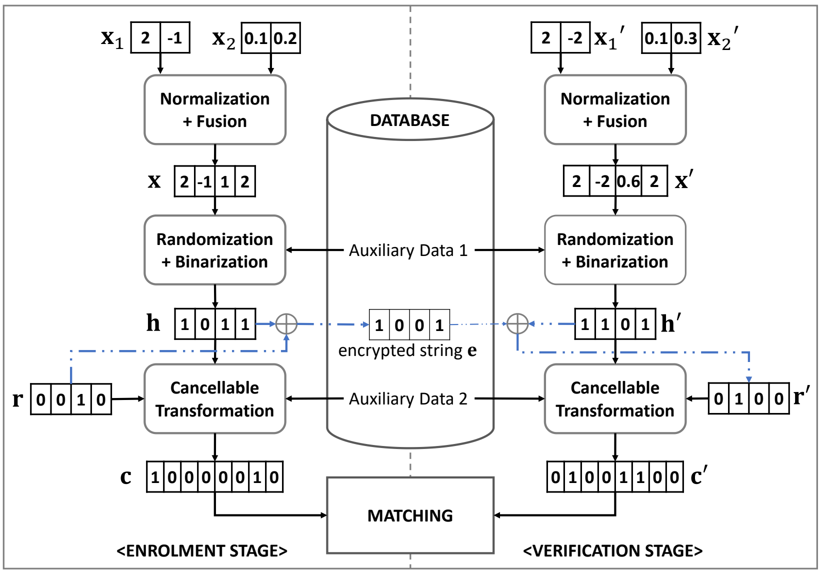


Fig 4.1. Overview of M·EFV hashing in enrollment and verification stages [3]

M·EFV hashing is essentially an extension of EFV hashing where it integrates an additional face modality and additional mechanism (refer to stage-2 and stage-3 transformation) to realize the biometric fusion for tokenless biometric template protection and enhance the irreversibility property. In essence, M·EFV hashing is a feature-level fusion-based biometric template protection scheme that fuses face and fingerprint features into a cancellable template. As shown in Fig 4.1, M·EFV hashing is a multi-stage transformation method that combines the real-valued face and fingerprint vectors into a cancellable template, the staged transformations are briefly explained as below:

1) In the first stage, M·EFV hashing normalizes and combines the input face and fingerprint vectors into a fused vector. In this stage, the value distribution of the face or fingerprint vector is rescaled, such that the domination of the face or fingerprint vector during the fusion process is reduced, and the resultant fused template is robust.

2) The second stage randomizes and binarizes the fused biometric template into an *IoM hashed vector* that is essential for the third stage transformation.

3) Lastly, the *IoM hashed vector* is passed to the irreversible transformation function to yield the cancellable template. In this stage, the XOR encryption/ decryption notion is used to convert the transformation key into auxiliary data and achieve the tokenless property.

Given the real-valued face vector $\mathbf{x}_1$ and fingerprint vector $\mathbf{x}_2$, the three-stage transformation can be briefly explained as follows: During the stage-1 transformation, $\mathbf{x}_1$ and $\mathbf{x}_2$ are normalized and concatenated to form the fused biometric vector $\mathbf{x} = \mathbf{x}_1|\mathbf{x}_2$. The $\mathbf{x}$ is then transferred to the stage-2 transformation for randomization and binarization, yielding the *binary IoM hashed vector* $\mathbf{h}$. Lastly, $\mathbf{h}$ is further processed in the stage-3 transformation to generate **c,** which is the cancellable biometric template in the proposed scheme. The random transformation key $\mathbf{r}$ is encrypted by **h** yielding the encrypted string **e,** which will be stored in the database. As such, the original $\mathbf{r}$ is never kept in the system, and there is no additional information needed to be managed by the user.

Differ from the EFV hashing, the XOR operation to generate the encrypted string $\mathbf{e}$ is conducted on the transformation key $\mathbf{r}$ and the *IoM hashed vector* $\mathbf{h}$ (the randomized biometric vector). Since the $\mathbf{h}$ is a randomized vector, multiple $\mathbf{h}$s (from the same biometric feature) in different applications are independent of each other, and the attacker could not perform correlation analysis on multiple encrypted string $\mathbf{e}$s and attempt to reveal the $\mathbf{r}$, which resolves the shortcoming of EFV hashing.

4.4.2 Generation of cancellable template

This subsection presents the details of the M·EFV hashing to transform the input face vector $\mathbf{x}_1 \in \mathbb{R}^d$ and fingerprint vector $\mathbf{x}_2 \in \mathbb{R}^d$ into a cancellable template $\mathbf{c} \in [0,1]^{2dn}$.

A. Stage-1 transformation (feature rescaling and concatenation)

The main task of stage-1 transformation is to rescale and combine the face and fingerprint vectors into a fused template (original bio. vector $\mathbf{x}$). As there is a value-distribution difference between the input face and fingerprint vectors, it will affect the matching accuracy of the cancellable template. In particular, the matching result (similarity score) will bias to the biometric vector that holds a larger value scale as the calculation of scalar product for the biometric feature is involved in the proposed scheme.

Example 4.1: Let $\mathbf{x}_1 \in [-50{,}50]^d$ be the face vector and $\mathbf{x}_2 \in [-5{,}5]^d$ be the fingerprint vector where there is a huge scale difference between the $\mathbf{x}_1$ and $\mathbf{x}_2$. Suppose a feature-level fusion transformation first *combines* both $\mathbf{x}_1$ and $\mathbf{x}_2$ into the fused vector $\mathbf{x} = \mathbf{x}_1|\mathbf{x}_2$ where the | denote the concatenation process. Then, the $\mathbf{x}$ is randomly projected into a random vector $\mathbf{v} = \mathbf{xR}$ where **R** is the projection matrix. Due to the fact that the value distribution $\mathbf{x}_1$ is higher than the $\mathbf{x}_2$, the magnitude of the $\mathbf{v}$ is skewed to the $\mathbf{x}_1$. In other words, the biometric vector with larger value distribution (refer as $\mathbf{x}_\mathrm{L}$) is dominance throughout the transformation process and resulting the verification performance produced cancellable template is *biased* towards the $\mathbf{x}_\mathrm{L}$. This is unfavorable, especially when the dominant biometric feature is low in verification performance. To support this reasoning, a detailed experiment is conducted in Section 4.5.3 to study the effect of stage-1 transformation towards the proposed method.

Based on the reasoning above, rescaling is essential towards a feature-level fusion multimodal biometric template protection scheme, especially when fusing multiple biometric vectors with huge scale differences. Instead of using a fixed-valued parameter to rescale the two vectors into a fixed scale, the proposed method employs a dynamic parameter, coined as the *rescale ratio* $\alpha \in \mathbb{R}$ in the feature rescaling process. Given the face vector $\mathbf{x}_1 \in \mathbb{R}^d$ and fingerprint vector $\mathbf{x}_2 \in \mathbb{R}^d$, the procedure (also shown in Algorithm 4.1) to fuse the $\mathbf{x}_1$ and $\mathbf{x}_2$ into the original bio. vector $\mathbf{x} \in \mathbb{R}^{2d}$ is as follow:

1) Calculate the rescale ratio α**,** which is then used for the rescaling process. α is calculated based on the following formula:

$$\alpha = \begin{cases} \mathrm{Max}(\mathbf{x}_1)/\mathrm{Max}(\mathbf{x}_2) & \text{if } \mathrm{Max}(\mathbf{x}_1) \geq \mathrm{Max}(\mathbf{x}_2) \\ \mathrm{Max}(\mathbf{x}_2)/\mathrm{Max}(\mathbf{x}_1) & \text{otherwise} \end{cases} \tag{4.2}$$

2) Rescale the biometric vector with the smaller Max(.) value by multiplying it with the rescale ratio α. For example, if $\mathrm{Max}(\boldsymbol{x}_1) \geq \mathrm{Max}(\boldsymbol{x}_2)$, the $\mathbf{x}_2$ will be re-scaled as $\mathbf{x}_2 = \mathbf{x}_2 * \alpha$.

3) Generate the original bio. vector $\mathbf{x}$ by computing $\mathbf{x} = \mathbf{x}_1|\mathbf{x}_2$**.**

Algorithm 4.1. Stage-1 Transformation

```
Input (From User): Face vector $\mathbf{x_1} \in \mathbb{R}^{\boldsymbol{d}}$, Fingerprint vector $\mathbf{x_2} \in \mathbb{R}^{\boldsymbol{d}}$
Output: Original bio. vector $\mathbf{x} \in \mathbb{R}^{\boldsymbol{2d}}$
if $\mathrm{Max}(\mathbf{x}_1) \geq \mathrm{Max}(\mathbf{x}_2)$
    $\alpha = \mathrm{Max}(\mathbf{x}_1)/\mathrm{Max}(\mathbf{x}_2)$
    $\mathbf{x}_2 = \mathbf{x}_2 \times \alpha$
else
    $\alpha = \mathrm{Max}(\mathbf{x_2})/\mathrm{Max}(\mathbf{x}_1)$
    $\mathbf{x}_1 = \mathbf{x}_1 \times \alpha$
end if
compute $\mathbf{x} = \mathbf{x}_1|\mathbf{x}_2$
return $\mathbf{x}$
```

B. Stage-2 transformation (binarization and prior-randomization)

After the original bio. Vector $\mathbf{x} \in \mathbb{R}^{2d}$ is generated, $\mathbf{x} \in \mathbb{R}^{2d}$ is passed to stage-2 transformation to yield the *IoM bio. vector* $\mathbf{h} \in [0,1]^{2d}$*.* Briefly, the main task of stage-2 transformation is to binarize and increase the randomness of the $\mathbf{x}$ before non-invertible transformation, or XOR encryption is applied. To counter the attack via record multiplicity (ARM), a prior-randomization process is always needed in a template protection method. The example below is given to present the reason for applying prior randomization in template protection.

Example 4.2: Assume there is a biometric feature $\mathbf{x}$ and a transformation key $\mathbf{r}$, a template protection method $f(.)$ is applied to takes $\mathbf{x}$ and $\mathbf{r}$ as input to produce a cancellable template $\mathbf{c}$. For simplicity, an XOR-encryption will be used as the example for $f(.)$. Therefore, this process is re-written as $\mathbf{c} = \mathbf{x} \oplus \mathbf{r}$. If the $\mathbf{c}$ is compromised, the user can re-issue a new cancellable template $\mathbf{c}_2$ using a new transformation key $\mathbf{r}_2$. To sum up, the new cancellable template $\mathbf{c}_2 = \mathbf{x} \oplus \mathbf{r}_2$. Now, assume that the attacker compromised one $\mathbf{c}$ and attempted to recover the $\mathbf{x}$. Not to mention the $\mathbf{r}$, it computationally hard for the attacker to recover the $\mathbf{x}$ from a single $\mathbf{c}$. However, if the attacker compromised multiple $\mathbf{c}$s, it is possible for the attacker to perform cross-XOR on multiple $\mathbf{c}$ to first cancel out the $\mathbf{x}$ since each $\mathbf{c} = \mathbf{x} \oplus \mathbf{r}$, $\mathbf{c}_2 = \mathbf{x} \oplus \mathbf{r}_2$, etc. Then, the attacker could analyze the cross-XOR products of $\mathbf{r}$s with the $\mathbf{c}$s and recover $\mathbf{x}$. This scenario is known as *Attack via Record Multiplicity* (ARM) [156]. To counter the ARM, one can reduce the redundancy of the input $\mathbf{x}$ among different applications by converting the $\mathbf{x}$ into multiple independent randomized vector $\mathbf{h}$s so that each $\mathbf{c} = \mathbf{h} \oplus \mathbf{r}$, $\mathbf{c}_2 = \mathbf{h}_2 \oplus \mathbf{r}_2$.

Other than randomization, binarization is another important aspect of the M·EFV hashing. Since the stage-3 transformation accepts only a binary vector as input, a binarization process is required. In the proposed scheme, the concept of locality-sensitive hashing from IoM hashing [66] is adapted to perform binarization and randomization at once. As [66] can be adjusted to arbitrary size, it can be used to handle unequal size or different data types (matrix/ vector) of different biometric features and produce a fixed-sized binary vector. The procedure in Algorithm 4.2 is followed to transform the original bio. vector $\mathbf{x}$ into the IoM bio. vector $\mathbf{h}$. Since the purpose of the stage-2 transformation is merely randomization and binarization, the parameter m is fixed as $m = 2$, and $q = 2d$ (the size of $\mathbf{x}$).

Algorithm 4.2. Stage-2 Transformation

```
Input (From User): Original bio. vector $\mathbf{x} \in \mathbb{R}^{2d}$
Parameter: Desired upper limit $m$, Projection round $q$, Random projection matrices $\mathbf{P} = \{\mathbf{P}_1, \dots, \mathbf{P}_q\}$ where each $\mathbf{P}_i \in \mathbb{R}^{m \times 2d}$
Output: IoM bio. vector $\mathbf{h} \in [0, m-1]^q$
Initialize $\mathbf{h} = [0]^q$
for $i \leftarrow 1$ to $q$
    $\mathbf{x} = \mathbf{x}\mathbf{P}_i$
    Set $v$ equal to the index of $\mathrm{ArgMax}(\boldsymbol{x})$
    $h_i = v$
end if
return h
```

C. Stage-3 transformation (non-invertible transformation)

Lastly, the IoM bio. Vector $\mathbf{h} \in [0,1]^{2d}$ is passed to the irreversible transformation function generate a cancellable template $\mathbf{c} \in [0,1]^{2dn}$ for matching. The stage-3 transformation is essentially an enhanced version of [1] where it requires a smaller n to achieve a competitive verification performance. The enhanced version introduces bit-shifting and many-to-one modulo mappings during the transformation. In the stage-3 transformation, a hashed vector augmentation is carried out to transform $\mathbf{h}$ into the augmented IoM hashed vector $\hat{\mathbf{h}}$. The notion of bit-shifting is to demolish the repetition of $\mathbf{h}$ in $\hat{\mathbf{h}}$, which can improve the matching performance. For clarification, an example is given.

Example 4.3: Given $\mathbf{h} = [0,1,1,0]$, $n = 3$ and $\hat{\mathbf{h}}$ is initially equal to $\mathbf{h}$. Suppose the augmentation process appends $\mathbf{h}$ to $\hat{\mathbf{h}}$ for n rounds, there are two scenarios to be considered:

- **Scenario-1**: No bit-shifting for $\mathbf{h}$ during the augmentation; and thus, the final $\hat{\mathbf{h}}$ is formed as $\hat{\mathbf{h}} = [0,1,1,0,0,1,1,0,0,1,1,0]$. The repetition pattern in $\hat{\mathbf{h}}$ is obvious as it is formed by three sub-groups "$0,1,1,0$". Accordingly, the cancellable template $\mathbf{c}$ also possesses the same pattern, and verification performance is constant under different ns.

- **Scenario-2**: $\mathbf{h}$ is circularly right shifted for 1-bit during each appending round and $\hat{\mathbf{h}}$ is formed as $\hat{\mathbf{h}} = [0,1,1,0,0,0,1,1,1,0,0,1]$. In this case, there is no repetition pattern observed.

From the scenarios above, bit-shifting is important when performing the hashed vector augmentation as it affects the verification performance of the cancellable template $\mathbf{c}$. To support the reasoning, an experiment is conducted in Section 4.5.2B to investigate the effect of bit-shifting. Given the IoM bio. vector $\mathbf{h} \in [0,1]^{2d}$ and transformation key $\mathbf{r} \in [0,1]^{2d}$, process below (Algorithm 4.3) is followed to generate the cancellable template $\mathbf{c} \in [0,1]^{2dn}$:

1) *Hashed vector augmentation*: Generate $\hat{\mathbf{h}}$ by computing $\hat{\mathbf{h}} = \hat{\mathbf{h}}|\mathbf{h}$ for $(n-1)$ rounds where | is the concatenation process. In the proposed method, scenario-1 is followed, and $\mathbf{h}$ is circularly right shifted for s-bits in each round of concatenation.

2) *Sub-blocks formalization*: A *sub-block* is constructed for each $\hat{h}_i \in \hat{\mathbf{h}}$ where $i = 1 \dots dn$. This is done by appending its following $\hat{h}$s to it until the size of the sub-block equals to k-bits. The process is repeated until $2dn$ numbers of sub-blocks are constructed.

3) *Binary-to-Decimal conversion*: Each sub-block is converted to the integer number $\dddot{h}_i$ where $i = 1 \dots dn$. After $2dn$ numbers of sub-blocks are converted, $\dddot{\mathbf{h}} \in [0{,}2^k - 1]^{2dn}$ is formed.

4) *Many-to-One modulo*: Modulate each $\dddot{h}_i \in \dddot{\mathbf{h}}$ by a pre-fixed threshold $\beta \in \mathbb{Z}$. By doing so, the range of $\dddot{\mathbf{h}} \in [0{,}2^k - 1]^{2dn}$ is remapped to $\dddot{\mathbf{h}} \in [0, \beta - 1]^{2dn}$. Since the β is always a small value, a many-to-one mapping is taking effect, and the security of the transformation function is enhanced.

5) *Index Rescaling*: Transform each $\dddot{h}_i \in \dddot{\mathbf{h}}$ with the equation below:

$$\dddot{h}_i = \big((\dddot{h}_i + 1) \times i\big) \bmod 2d \tag{4.3}$$

where d is the size of the random string $\mathbf{r}$ and $i = 1 \dots dn$. Then set each $\dddot{h} \in \dddot{\mathbf{h}}$ to $2d$ if $\dddot{h} = 0$. As a result, $\dddot{\mathbf{h}} \in [0, \beta - 1]^{2dn}$ is rescaled to $\dddot{\mathbf{h}} \in [1, 2d]^{2dn}$.

6) *Index-to-Binary substitution:* The cancellable template is first initialized as $\mathbf{c} = \dddot{\mathbf{h}}$. After that, each $c_i \in \mathbf{c}$ is transformed in accordance with $c_i = \pi(\mathbf{r}, c_i)$ where $\pi(.)$ is a substitution box and $\mathbf{r} \in [0{,}1]^{2d}$ is the transformation key. The function $\pi(.)$ is defined as follows:

Given $\mathbf{r} \in [0{,}1]^{2d}$ the substitution table of the substitution function, $\pi(.)$ returns $r \in \mathbf{r}$ where c_i indicates the index of r, which is simplified as $\pi(\mathbf{r}, c_i) \to r_{c_i}$. Since the size of $\mathbf{r}$ is smaller than $\mathbf{c}$, multiple c_i will be substituted by the same r, which achieves another many-to-one mapping. As a result, a *cancellable template* $\mathbf{c} \in [0{,}1]^{2dn}$ is generated.

Apart from $\mathbf{h}$ (or $\mathbf{x}$), the $\mathbf{r} \in [0{,}1]^d$ is another piece of information required to generate $\mathbf{c}$. Since $\mathbf{r}$ is sensitive data and should not be disclosed, $\mathbf{r}$ is encrypted to the encrypted string

$\mathbf{e} = \mathbf{r} \oplus \mathbf{h}$ where $\oplus$ is the XOR operator. In particular, during enrollment $\mathbf{r}$ is generated by a PRNG and input to transform the *iom bio. vector* $\mathbf{h}$ into the cancellable template $\mathbf{c}$. After that, an XOR operation is applied to $\mathbf{h}$ and $\mathbf{r}$ to produce the encrypted string $\mathbf{e} = \mathbf{h} \oplus \mathbf{r}$. Lastly, $\mathbf{c}$ and $\mathbf{e}$ are stored in storage. Since $\mathbf{h}$ and $\mathbf{e}$ are distorted from different processes, $\mathbf{h}$ and $\mathbf{e}$ are independent of each other. During verification, the *iom bio. vector* $\mathbf{h}'$ is first generated from the input biometric feature and be used to compute the approximated transformation key $\mathbf{r}' = \mathbf{h}' \oplus \mathbf{e}$. The $\mathbf{r}'$ is then be used to generate the query template $\mathbf{c}'$ for verification. This ensures there is the only valid user can generate the approximated transformation key $\mathbf{r}'$ for generating cancellable templates. However, due to the inconsistency of the biometric input, the genuine user cannot fully recover $\mathbf{r}$ and induces large intra-class variation between the cancellable template $\mathbf{c}$ and query template $\mathbf{c}'$. Step-1 transformation is used to reduce the discrepancy of the generated $\mathbf{c}/\mathbf{c}'$ and overcome the performance degradation problem.

Algorithm 4.3. Stage-3 Transformation

```
Input (From User): IoM bio. vector $\mathbf{h} \in [0,1]^{2d}$
Input (From System): Transformation key $\mathbf{r} \in [0,1]^{2d}$
Parameter: Duplicative factor $n$, Shifting factor $s$, Sub-block Size $k$, Modulo threshold $\beta$
Output: Cancellable template $\mathbf{c} \in [0,1]^{2dn}$
Initialize $\hat{\mathbf{h}} = \mathbf{h}$
for $l \leftarrow 1$ to $(n-1)$
    Circular right shift $\mathbf{h}$ for $s$-bit(s)
    $\hat{\mathbf{h}} = \hat{\mathbf{h}}|\mathbf{h}$
end for
Initialize $\mathbf{c} = [0]^{dn}$
for $i \leftarrow 1$ to $dn$
    for $j \leftarrow 1$ to $(k-1)$
        $\hat{h}_i = \hat{h}_i|\hat{h}_j$
    end for
    Convert $\hat{h}_i$ to $\dddot{h}_i \in \mathbb{Z}$
    $\dddot{h}_i = \dddot{h}_i \bmod \beta$
    $\dddot{h}_i = (\dddot{h}_i \times i) \bmod 2d$
    if $\dddot{h}_i = 0$ then
        $\dddot{h}_i = 2d$
    end if
    $c_i = r_{\ddot{h}_i}$
end for
return $\mathbf{c}$
```

4.4.3 Matching of cancellable template

Since the protected template is a fixed-length and aligned binary vector, similarity comparison between the query template and the pre-stored template is based on the *normalized Hamming similarity*. Assume the pre-stored template to be $\mathbf{c} \in [0,1]^d$ and query template to be $\mathbf{c}' \in [0,1]^d$ where d refer to the dimension of both vectors, matching process of $\mathbf{c}$ and $\mathbf{c}'$ is as follow:

a) Compute XOR-product $\mathbf{z} = \mathbf{c} \oplus \mathbf{c}'$

b) Calculate similarity score $S = 1 - (\frac{\sum_{i=1}^{d} z_i}{d})$

Similarity score $S = [0,1]$ indicates the similarity degree between $\mathbf{c}$ and $\mathbf{c}'$. The higher the S, the more similar for $\mathbf{c}$ and $\mathbf{c}'$. After the S is calculated, S is passed to the decision module for getting the final result. Given the pre-defined threshold τ, the final decision is computed as:

$$\text{final decision} = \begin{cases} \text{genuine user}, & S \geq \tau \\ \text{impostor}, & S < \tau \end{cases} \tag{4.4}$$

4.4.4 Renewal of cancellable template

Renewal of the cancellable template is an important part of a cancellable biometrics-enabled system. Whenever the pre-stored cancellable template $\mathbf{c}$ and encrypted string $\mathbf{e}$ are compromised, the user can re-issue a new cancellable template $\mathbf{c}$ with different projection matrices $\mathbf{P}$ and transformation key $\mathbf{r}$. This process is outlined as follows:

1) The system/ application deletes the old cancellable template $\mathbf{c}$, projection matrices $\mathbf{P}$ and transformation key $\mathbf{r}$.

2) The user provides face and fingerprint to the biometric reader and has the *face* and *fingerprint* vectors ($\mathbf{x}_1$ and $\mathbf{x}_2$) to be extracted.

3) At the same time, the system/ application employs PRNG to generate the new projection matrices $\mathbf{P}$ and transformation key $\mathbf{r}$.

4) $\mathbf{x}_1$, $\mathbf{x}_2$, $\mathbf{P}$ and $\mathbf{r}$ are passed to M·EFV hashing to generate the cancellable template $\mathbf{c}$ and encrypted string $\mathbf{e}$.

Lastly, the system stores $\mathbf{c}$ and $\mathbf{e}$ in the storage for authentication purposes. Since there are two randomization processes are involved in the M·EFV hashing, it is unlikely that the new cancellable template can collide with the old cancellable template.

4.5 Experiments and discussions

This section presents the experimental studies of the proposed scheme in terms of matching performance and time complexity. Comparison with the state-of-the-art cancellable biometric schemes is conducted for benchmarking purposes. In addition, an analysis on the stage-1 transformation is conducted to support the reasoning discussed earlier.

4.5.1 Experimental setup

This subsection presents the experimental setup to realize the proposed scheme, including the datasets, matching protocol and feature extraction methods. The implementation of the proposed scheme is written using MATLAB (Ver. R2017b) and being executed in a PC with the hardware specification of Solid-State Drive (SSD)@128GB, Intel Core i7 7th-Gen CPU@2.80Hz and Memory DDR4@8GB.

A. Dataset and matching protocol

Eight datasets from Fingerprint Verification Competition (FVC) are chosen as the test datasets for fingerprint modality. These datasets include FVC2002 (DB1, DB2 and DB3) [73] and FVC2004 (DB1, DB2 and DB3) [74]. Each sub-dataset from FVC2002 and FVC2004 datasets consists of 100 users with 8 fingerprint samples for each user. Labeled Faces in the Wild (LFW) [84], [85] is the test dataset for face modality. There are a total of 13233 facial images and 5749 users in the dataset. Among 5749 users, 1680 users have two or more face images in the dataset. For experiment purposes, the first 100 users with 5 face images are chosen to pair with the FVC2002 and FVC2004 fingerprint datasets.

To evaluate the matching performance of the M·EFV hashing, the FVC full matching protocol is followed to generate the *Equal Error Rate (EER) (%)* for each dataset. FVC matching protocol [163] is the benchmarking performance evaluation method in a verification system. The assessment of this matching protocol is based on the Equal Error Rate (EER) (%), which is calculated from the *genuine* and *impostor* score distributions. Both score distributions are generated via the following matching attempts [163]:

- **Genuine matching attempt**: All biometric samples of the same user are cross-matched, and the similarity scores are recorded. For a user with m numbers of samples, this attempt generated ${}^{m}\mathrm{C}_2$ genuine matching scores.

- **Impostor matching attempt**: The first biometric samples of all users are cross-matched, and the similarity scores are recorded. For a dataset with n numbers of users, this attempt generated ${}^{n}\mathrm{C}_2$ impostor matching scores.

The genuine matching attempt is formulated by assuming the user performs the matching process during different scanning, while the impostor matching attempt is formulated by assuming the attacker attempts to use their biometric feature for performing matching with the pre-stored biometric template. Both matching attempts of this matching protocol avoid the symmetric matching, that is, the case where a is matched to b at first, b matched to a is the symmetric matching [163]. Finally, for a dataset with n numbers of users and m numbers of samples per user, this matching protocol generate a total of $(n * {}^{m}\mathrm{C}_2)$ numbers of genuine matching scores and ${}^{n}\mathrm{C}_2$ numbers of impostor matching scores. In this paper, a total of 1000 genuine scores and 4950 impostor scores are generated for each experiment. 5 repetitions with 5 sets of auxiliary data $\{\mathbf{P}, \mathbf{r}\}$ are carried out for each experiment to have a precise reading on matching accuracy. Since the proposed scheme is a tokenless scheme, there is no genuine-token/ stolen-token scenario. All experiments are conducted by assuming every individual uses the pre-stored information to generate the query instance for matching, which is similar to the stolen-token scenario in two-factor schemes.

B. Face vector extraction

For the face modality, this chapter adopted the well-known FaceNet [36] to extract a real-valued face vector $\mathbf{x}_1 \in \mathbb{R}^d$ from the facial image. Specifically, FaceNet [36] is a deep convolutional network based method that transforms the facial image into a compact Euclidean space [36]. This subsection focuses on the face vector generation (i.e., testing phase) of FaceNet since the pre-trained models are publicly available on GitHub. The procedure for generating the face vector is explained as below:

1) MTCNN [36] is employed to align and crop the input image into the size of 160×160.

2) The processed face image is then input to FaceNet [36] for extracting the real-valued face vector.

Lastly, a real-valued face vector with dimensions of 256 is extracted to represent the input face image. In this thesis, the feature extraction is conducted using the pre-trained model that was trained based on the MS-Celeb-1M dataset [164]. The extraction and pre-trained model are adopted from David Sandberg's open-source implementation [165]. The reader may refer to [36] for the detailed process of FaceNet. Summary of the employed face dataset and the extracted face vector are tabulated in the table below.

Table 4.2: Summary of LFW datasets

	LFW dataset
Total face images	13233
User	5749
User with two or more face images	1680
EER(%)	0.60

C. Fingerprint vector extraction

The fingerprint vector extraction technique originated from [62] is adopted to extract a fixed-length and aligned fingerprint vector as the input for the proposed method. Briefly, [62] utilize kernel principal component analysis (KPCA) to transform the fingerprint minutiae point set into a compact real-valued vector $\mathbf{x}_2 \in \mathbb{R}^d$ with the following procedures:

1) The open-source minutiae extraction tool, namely the FingerJetFXOSE [166], is adopted to extract minutiae point set $M = \{\mathbf{m}_1, \mathbf{m}_2, \dots \mathbf{m}_j\}$ from a fingerprint image where each $\mathbf{m}_i = \{x_i, y_i, \theta_i\}$ with x, y the spatial position and θ the orientation of the minutia within the fingerprint.

2) The M is then converted to a minutiae descriptor $\mathbf{\Omega}$. In this research, the state-of-the-art MCC descriptor [63] is chosen due to its superior matching performance. To be noted, the MCC descriptor is generated using the transformation parameters as reported in [63].

Since [62] is a learning-based method, the following procedures are separated into *training-phase* and *testing-phase*. During training-phase,

1) Given a set of training samples (i.e., MCC minutiae descriptors) $\mathbf{\Omega} = \{\mathbf{\Omega}^t(i)|i = 1, \dots, N_t\}$, a kernel matrix $\mathbf{K} \in \mathbb{R}^{N_t \times N_t}$ is first computed by cross-matching the training samples. This step is summarized as below:

$$\mathrm{K}(i,j) = \exp\left(-0.5(1 - S_{\mathrm{MCC}}(\mathbf{\Omega}^t(i), \mathbf{\Omega}^t(j)))^2/\sigma^2\right) \tag{4.5}$$

where σ denote the spread factor [62], and $S_{\mathrm{MCC}} = [0,1]$ denote the MCC matching score. Note that MCC matching score is computed based on the matching parameters reported in [63].

2) Kernel Principal Component Analysis (KPCA) is then applied to compute the eigenvectors $\mathbf{E} \in \mathbb{R}^{N_t \times d}$ from the kernel matrix $\mathbf{K}$, where the parameter d controls the desired dimension of the output fingerprint vector ($d = 256$ in this thesis).

3) The training samples $\mathbf{\Omega^t}$ and the eigenvectors $\mathbf{E}$ are then stored for fingerprint vector generation (i.e., testing phase).

During testing-phase,

1) A query MCC descriptor is $\mathbf{\Omega}^q$ is extracted and be matched to pre-stored training samples $\mathbf{\Omega^t}$; a score vector $\mathbf{s} \in [0,1]^{N_t}$ is generated with each $s_i = \mathrm{S}_{\mathrm{MCC}}(\mathbf{\Omega}^q, \mathbf{\Omega}^t(i))$ where $i = 1 \dots N_t$.

2) The score vector $\mathbf{s}$ is then transformed to $\bar{\mathbf{s}} \in \mathbb{R}^{N_t}$ with the formula $\bar{\mathbf{s}} = \exp\left(-(1 - \mathbf{s})^2/2\sigma^2\right)$ where σ denote the spread factor [62].

3) Finally, an *ordered* and *fixed-length* fingerprint vector $\mathbf{x}_2 \in \mathbb{R}^d$ is generated by computing $\mathbf{x}_2 = \bar{\mathbf{s}}\mathbf{E}$ where $\mathbf{E}$ denote the pre-stored eigenvectors.

Lastly, a real-valued fingerprint vector with 256 dimensions is generated for the experiments. To extract the fingerprint vector from each dataset, the first three samples of each user will be used for the training phase, while the remaining samples will be used for generating fingerprint vectors. Summary of the employed fingerprint dataset and the extracted fingerprint vector are tabulated in the table below.

Table 4.3: Summary of fingerprint vector extracted from FVC2002 and FVC2004 datasets

	FVC2002			FVC2004		
	DB1	DB2	DB3	DB1	DB2	DB3
Number of fingerprint vector	500	500	500	500	500	500
Dimension of fingerprint vector	256	256	256	256	256	256
EER (%)	0.15	0.49	2.47	2.11	5.08	3.62

4.5.2 Parameter estimation

This subsection examines the matching performance of the proposed scheme in terms of testifying the scheme under different settings of transformation parameters. The experiments are mainly focusing on the parameters of the stage-3 transformation, i.e., n, s and k. Stage-1 and stage-2 parameters (i.e., α, q and m) are not examined due to the following reasons: (i) the *rescale ratio* α is a dynamic parameter and (ii) the parameters q and m are constant in the sense that q=$2d$ and m are fixed at 2.

A. Effect of parameter n

In the proposed scheme, n controls the hashed vector augmentation, which turns a binary IoM hashed vector $\mathbf{h} \in [0,1]^{2d}$ into its augmented counterpart $\hat{\mathbf{h}} \in [0,1]^{2dn}$. As a result, the cancellable template $\mathbf{c} \in [0,1]^{2dn}$ is large when n is large. As stated in Section 4.4.2C, the intra-class variation of the template and query instance is large since $\mathbf{r}$ cannot be fully recovered. The use of $\hat{\mathbf{h}}$ can reduce the discrepancy of $\mathbf{c}$ and $\mathbf{c}'$; and thus, improve the verification performance. To testify the effect of n, n varies from 10 until 250 with a step size of 15, $k = 3,4,5,6,7$ and other parameters are fixed at $s = 1$ and $\beta = 3$. Fig 4.2 depicts the curves of EER vs n for the FVC2002+LFW dataset pair under different settings of k. The highest EERs is observed when $n = 10$. Then, the EERs decrease significantly from $n = 10$ to 40. The decline of EERs becomes slower for $40 \leq n \leq 55$. The EERs become lowest when $n = 55$ in most of the tested datasets. After that, the EERs level off when $n \geq 55$. For certain datasets such as FVC2002 DB3+LFW, the EERs remain decreasing slowly even for $n \geq 55$. To sum up, high n offers decent verification performance. Yet, the large n will induces large template size due to $\mathbf{c} \in [0,1]^{2dn}$.

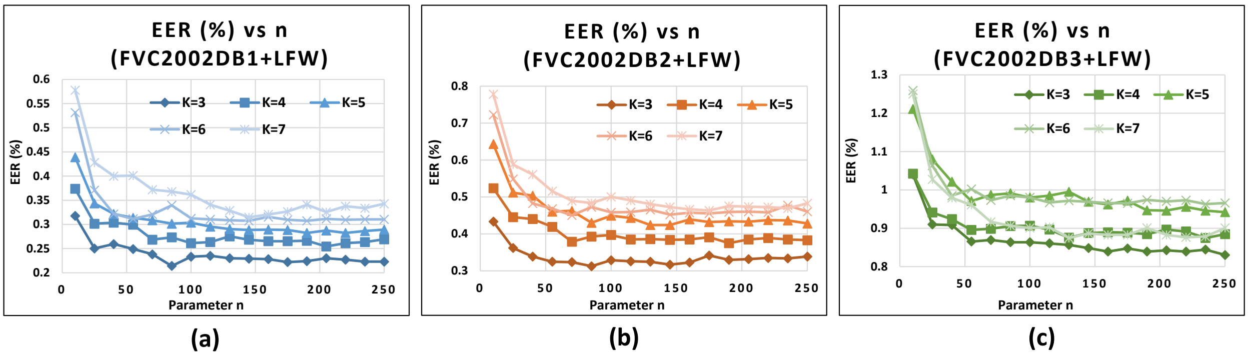


Fig 4.2. Curves of EER (%) vs n in FVC2002+LFW datasets

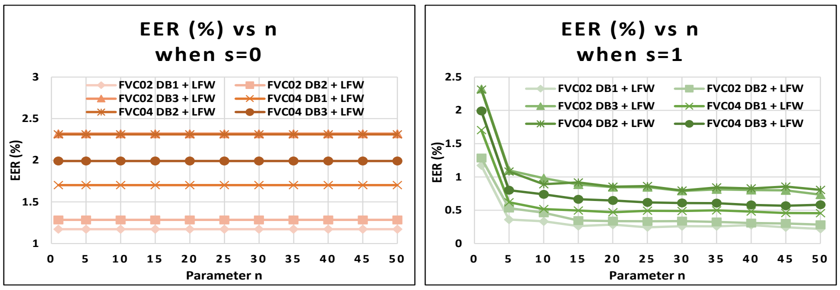
B. Effect of parameter s

Other than n, s is another parameter used in the hashed vector augmentation. Briefly, the augmentation produces the $\hat{\mathbf{h}}$ by appending $\mathbf{h}$ to $\hat{\mathbf{h}}$ for $(n-1)$ times. In each round of augmentation, the proposed scheme circularly right shifts $\mathbf{h}$ before it is appended to $\hat{\mathbf{h}}$. In this case, s is used to define the bit-shifting interval and demolish the repetition pattern of $\mathbf{h}$ in $\hat{\mathbf{h}}$. To validate the reasoning, the effect of the bit-shifting during the augmentation process is examined. Given the $\mathbf{h} \in [0,1]^{2d}$, n and s, two experiments are conducted by considering the below scenarios:

- **Scenario-1 (without bit-shifting):** An augmented IoM hashed vector $\hat{\mathbf{h}}$ is generated by computing $\hat{\mathbf{h}} = \hat{\mathbf{h}}|\mathbf{h}$ for $(n-1)$ times where | is the concatenation where there is no bit-shifting for $\mathbf{h}$ throughout the augmentation process.

- **Scenario-2 (with bit-shifting):** The $\hat{\mathbf{h}}$ is generated by computing $\hat{\mathbf{h}} = \hat{\mathbf{h}}|\mathbf{h}$ for $(n-1)$ rounds. The $\mathbf{h}$ is circularly right shifted for s-bits during each round of augmentation.

In the experiment, n is examined from 1 through 55 with step size 5, $k = 3$ and $\beta = 3$. As observed from Fig 4.3 (a), EERs remain constant under different settings of n if there is no bit-shifting ($s = 0$). From Fig 4.3 (b), it is observed that the bit-shifting notion $(s = 1)$ is taking effect as the EERs decrease with respect to the n. Therefore, it is proven that the repetitive sub-groups jeopardize the hashed vector augmentation as well as the verification performance of the produced cancellable template. Since the repetitive sub-groups (refer to scenario-1) make no difference for matching accuracy, the case that $\mathbf{h}$ shifts back to the starting position must be avoided. Hence, sn should be smaller than the size of $\mathbf{h}$, which is $2d$ in this context.

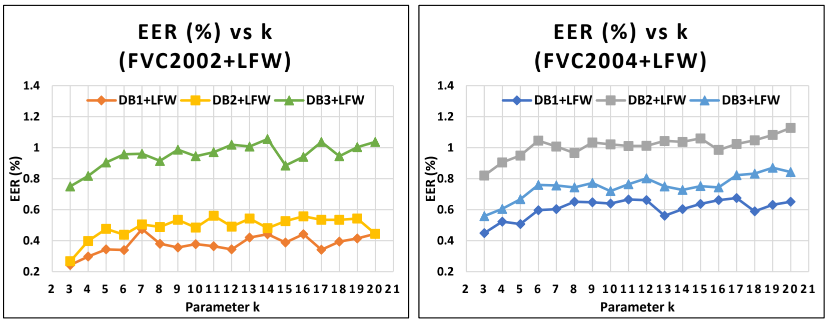


(a) (b)

Fig 4.3. Curves of EEF (%) vs n in every dataset under the two scenarios where (a) does not perform shifting and (b) performs bit-shifting with $s = 1$

C. Effect of parameter k

One of the important procedures in the stage-3 transformation is to substitute the $r \in \mathbf{r}$ with the integer value from $\ddot{\mathbf{h}} \in [1,2^k]^{2dn}$. As stated in Section 4.4.2C, $\ddot{\mathbf{h}}$ is converted by sub-blocks with k-bits; and hence, the upper limit of each converted $h \in \ddot{\mathbf{h}}$ is equal to 2^k. Despite a large k can increase the upper limit of $h \in \ddot{\mathbf{h}}$, the possibility that a sub-block consists of an error bit is also increased. This implies the verification performance of the proposed scheme will decrease for large k. In the experiments, k varies from 3 through 20 with step size 1, while $n = 55$, $s = 1$ and $\beta = 3$. Fig 4.4 presents the experimental results for all datasets. As observed, the lowest EER is found at $n = 3$, and EERs start to increase when n is varied from 3 until 6. When $n \geq 6$, the increments of EERs are getting slower. An interesting observation is that EERs reach the lowest point and increase afterward, e.g., at $k = 15$ in FVC2002 DB3+LFW dataset. Overall, the results suggest a low k to maintain the verification performance.



(a) (b)

Fig 4.4. Curves of EER (%) vs k in every dataset pairs where (a) is FVC2002+LFW and (b) is FVC2004+LFW

D. Summary of parameter estimation

Parameter setting is important in the M·EFV hashing as it will affect the matching accuracy of the generated cancellable template. The experiments conducted to estimate the parameters were actually done by testing each parameter under different settings. Then, the suitable parameter was observed from the curve of EERs plotted. In this subsection, the summarized effect of the parameters in M·EFV hashing is explained as below:

1) Increment of n is helpful to elevate performance. However, the performance is saturated and then degraded when n is set too large.

2) The larger the k, the poorer the matching accuracy of M·EFV hashing. This is due to the enlargement of intra-class variation in terms of error bits during the transformation.

3) The use of s promotes accuracy enhancement. However, larger s would limit n to be chosen since $sn < d$.

The best parameter setting from the experiments is shown in the table below. The remaining experiments in this chapter will follow the parameter setting. Other than that, the value distribution of the extracted face and fingerprint vector in each dataset is also tabulated.

Table 4.4: Best-tuned parameters for M·EFV hashing

Parameter	**Value**
Stage-1 Transformation	
α	-
Stage-2 Transformation	
m	2
q	*d* (size of the original bio. vector)
Stage-3 Transformation	
n	55
s	1
k	3
β	3

Table 4.5: Summary of value distribution of the extracted biometric feature in different datasets

Dataset		Distribution
Fingerprint	FVC2002 DB1	$[-0.21, 0.15]$
	FVC2002 DB2	$[-0.24, 0.24]$
	FVC2002 DB3	$[-0.23, 0.15]$
	FVC2004 DB1	$[-0.18, 0.13]$
	FVC2004 DB2	$[-0.19, 0.23]$
	FVC2004 DB3	$[-0.18, 0.19]$
Face	LFW	$[-0.34, 0.34]$

4.5.3 Analysis on Stage-1 Transformation

In the proposed scheme, rescaling of the real-valued biometric vectors is essential to eliminate the dominance of the huge scale vector during the transformation process. In this subsection, the effect of the rescaling process in stage-1 transformation is investigated (see Section 4.4.2A). Given $\mathbf{x}_1 \in \mathbb{R}^d$ the face vector and $\mathbf{x}_2 \in \mathbb{R}^d$ the fingerprint vector, the experiments are conducted in the following scenarios:

- **Scenario-1**: Fusion and transformation for the $\mathbf{x}_1$ and $\mathbf{x}_2$ are carried out without feature rescaling.

- **Scenario-2**: $\mathbf{x}_1$ and $\mathbf{x}_2$ are re-scaled according to a dynamic parameter, i.e., α during the transformation.

In the experiments, n is changed from 1 to 50 with step size 5, $k = 3$ and $\beta = 3$. From Fig 4.5 (a), the EERs from different dataset pairs are observed to have a similar value for different n. This is mainly attributed to the face vector which is larger in scale (refer to Table 4.5) dominates the transformation. This is unfavorable, especially when the dominant biometric, which is the face in this context, is less discriminative (refer to the results of FVC2002 DB1+LFW). On the other hand, the EERs in scenario-2 are not overlapping as observed from Fig 4.5 (b). This implies that rescaling is effective where the face vector is not dominating. The worst EER (FVC2004 DB2+LFW from Fig 4.5 (b)) in scenario-2 is still lower than the best EER (FVC2002 DB2+LFW from Fig 4.5 (a)). To sum up, the results of the experiments suggest that rescaling is essential for feature-level fusion on real-valued biometric vectors.

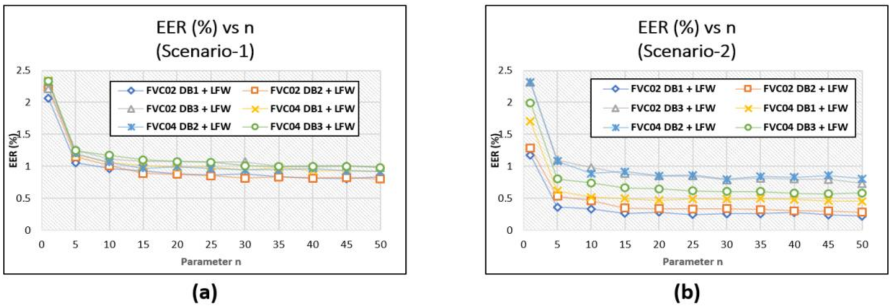


Fig 4.5. Curves of EER (%) vs n in two scenarios where (a) without rescaling, and (b) with feature rescale

4.5.4 Verification performance and comparison

This subsection presents the verification performance of the proposed scheme in unimodal and multimodal modes. The results presented are:

- Verification performance comparison between the proposed method (unimodal mode) and existing unimodal template protection methods is presented in Table 4.6.

- Verification performance comparison between the proposed method under *unimodal* and *multimodal* modes (blue, bold fonts represent the best performance) is presented in Table 4.7. Additionally, verification performance results of the multimodal system are also presented under different settings of k and n.

Note that it is hard to perform a fair comparison between the proposed multimodal cancellable biometric scheme and the existing schemes because the configurations, i.e., fusion strategy, biometric modalities and datasets selection, are different. From the tabulated results, it is observed that:

- The matching accuracy of the proposed scheme (unimodal mode) is slightly degraded compared to the original fingerprint and face counterparts [36], [62]. This is mainly attributed to the hashed vector augmentation in the proposed scheme. Nevertheless, the matching accuracy of the proposed scheme in the unimodal system is still comparable or even better than the existing unimodal template protection schemes.

- The proposed scheme achieves a good verification accuracy in unimodal and multimodal settings. This is due to the superior learning-based face and fingerprint vector extraction techniques [36], [62] and the exceptional performance preservation property.

- From Table 4.6 and Table 4.7, the matching accuracy of the multimodal system outperforms the unimodal system, e.g., EER in FVC2002DB1+LFW versus EER in FVC2002DB1/ LFW under the same parameter setting. Furthermore, the matching accuracy of the cancellable templates exceeds the original biometric input in certain dataset constellations such as FVC2004DB1+LFW.

Table 4.6: Verification performance of the proposed M·EFV hashing (unimodal mode) versus the state-of-the-arts unimodal template protection schemes

	FVC2002 (EER) (%)			FVC2004 (EER) (%)			LFW
	DB1	DB2	DB3	DB1	DB2	DB3	
Original counterpart [36], [62]	0.15	0.49	2.47	2.11	5.08	3.62	0.60
Proposed M·EFV hashing (unimodal mode)	0.40	0.86	4.61	**2.86**	6.27	5.38	**1.87**
Existing unimodal template protection schemes							
$2\mathrm{P}-\mathrm{MCC}_{64,64}$ [126]	3.3	1.8	7.8	6.3	−	−	−
Bloom Filter [167]	2.3	1.8	6.6	13.4	8.1	9.7	−
URP-based IoM hashing [66]	0.46	2.10	6.60	4.51	8.02	8.46	−
GRP-based IoM hashing [66]	**0.22**	**0.47**	**3.07**	4.74	**4.10**	**3.99**	−
Biohashing [24]	15	15	27	−	−	−	−
Yang *et al.* [168]	5.75	4.71	10.22	−	12	−	−
Wang and Hu [121]	3.5	−	−	−	5	7.5	−
Wang and Hu [122]	2	−	−	−	3	6.12	−

Table 4.7: Verification performance of proposed M·EFV hashing (multimodal mode) under different n and k

Parameter	FVC2002 + LFW (EER) (%)			FVC2004 + LFW (EER) (%)		
n	DB1	DB2	DB3	DB1	DB2	DB3
Parameter $k = 3$						
1	1.04 ± 0.23	1.23 ± 0.29	2.38 ± 0.23	1.62 ± 0.28	2.35 ± 0.31	2.07 ± 0.31
10	0.31 ± 0.11	0.43 ± 0.16	1.04 ± 0.13	0.46 ± 0.11	0.87 ± 0.11	0.74 ± 0.22
25	0.25 ± 0.09	0.36 ± 0.16	0.91 ± 0.11	0.39 ± 0.13	0.83 ± 0.16	0.68 ± 0.18
55	**0.24 ± 0.10**	**0.32 ± 0.15**	**0.91 ± 0.16**	**0.38 ± 0.13**	**0.78 ± 0.15**	**0.66 ± 0.19**
Parameter $k = 4$						
1	1.64 ± 0.18	1.82 ± 0.25	3.07 ± 0.37	2.26 ± 0.25	3.60 ± 0.47	2.78 ± 0.69
10	0.37 ± 0.12	0.52 ± 0.20	1.04 ± 0.13	0.65 ± 0.08	1.04 ± 0.19	0.74 ± 0.23
25	0.30 ± 0.11	0.45 ± 0.16	0.94 ± 0.14	0.54 ± 0.09	0.93 ± 0.28	0.67 ± 0.19
55	0.29 ± 0.13	0.42 ± 0.13	0.92 ± 0.18	0.54 ± 0.09	0.89 ± 0.18	0.65 ± 0.21
Parameter $k = 5$						
1	2.32 ± 0.44	2.62 ± 0.37	3.85 ± 0.52	3.28 ± 0.69	4.44 ± 0.68	3.63 ± 0.72
10	0.43 ± 0.11	0.64 ± 0.19	1.21 ± 0.19	0.67 ± 0.13	1.25 ± 0.23	0.98 ± 0.25
25	0.34 ± 0.14	0.51 ± 0.17	1.08 ± 0.18	0.54 ± 0.17	1.07 ± 0.20	0.77 ± 0.27
55	0.31 ± 0.14	0.46 ± 0.17	1.02 ± 0.20	0.53 ± 0.16	0.98 ± 0.14	0.69 ± 0.20

4.5.5 Computation efficiency

Apart from matching accuracy, the runtime of the M·EFV hashing in multimodal template protection mode is also evaluated to show the feasibility of deploying M·EFV hashing onto a biometric system. The runtime of the M·EFV hashing is evaluated in terms of the computation time (in second) to transform the input face and fingerprint vectors into the cancellable template during enrollment and verification (multimodal template protection). From the tabulated results, the average runtime for the M·EFV hashing in enrollment ≈ 0.006 seconds, while the average runtime during verification ≈ 0.0065 seconds. Therefore, the results suggest it is feasible to deploy the M·EFV hashing onto a biometric system.

Table 4.8: Computation efficiency for M·EFV hashing

Transformation Stage	FVC2002 + LFW			FVC2004 + LFW		
	DB1	DB2	DB3	DB1	DB2	DB3
Enrollment (in sec)						
1	0.000018	0.000016	0.000017	0.000017	0.000017	0.000017
2	0.004028	0.004008	0.004039	0.003863	0.003918	0.003960
3	0.002285	0.002130	0.002401	0.002273	0.002137	0.002212
Total	**0.006330**	**0.006155**	**0.006458**	**0.006153**	**0.006071**	**0.006189**
Verification (in sec)						
1	0.000014	0.000014	0.000015	0.000014	0.000013	0.000014
2	0.004008	0.003965	0.004043	0.003846	0.003912	0.003965
3	0.002532	0.002313	0.002600	0.002449	0.002355	0.002426
Total	**0.006555**	**0.006293**	**0.006659**	**0.006309**	**0.006281**	**0.006405**

4.6 Security and privacy analysis

This section is devoted to presenting the analyses of the security and privacy aspects of the produced cancellable template, including the irreversibility, security, unlinkability and renewability properties.

4.6.1 Irreversibility analysis

In biometric template protection, the irreversibility property ensures that it is hard to recover the original biometric feature if one or multiple cancellable templates and auxiliary data are presented. In this subsection, several inversion attacks are conducted towards the proposed method to justify the irreversibility property. In this subsection, the irreversibility is evaluated using three attacks where the attacker aims to recover the input face vector $\mathbf{x}_1 \in \mathbb{R}^d$ and fingerprint vector $\mathbf{x}_2 \in \mathbb{R}^d$ from single/ multiple compromised information, which includes cancellable fused template $\mathbf{c} \in [0,1]^{2dn}$, projection seed $\mathbf{P} = \{\mathbf{P}_1, \mathbf{P}_2 \ldots \mathbf{P}_q\}$ with each $\mathbf{P}_i \in \mathbb{R}^{m \times \mathbf{2}d}$ and encrypted string $\mathbf{e} \in [0,1]^{\mathbf{2d}}$.

A. Template inversion via Single Record

In this attack, the attacker attempts to obtain the original bio. vector $\mathbf{x}$ by reversing the cancellable template $\mathbf{c}$ with the compromised information, i.e., one set of projection matrices $\mathbf{P}$, cancellable template $\mathbf{c}$, and encrypted string $\mathbf{e}$. During the attack, the attacker can analyze the relation between the compromised data, i.e., cancellable template $\mathbf{c}$, transformation parameters and auxiliary data ($\mathbf{P}$ and $\mathbf{e}$).

Recall the methodology, the key process of generating $\mathbf{c}$ is to substitute the real-value elements in $\ddot{\mathbf{h}}$ with the binary element in $\mathbf{r}$. In other words, each $c \in \mathbf{c}$ is constructed as $c = \mathbf{r}_{\ddot{h}}$. The chief idea of this attack is: At first, $\mathbf{r}$ is revealed. A correlation analysis is conducted between $\mathbf{r}$ and $\mathbf{c}$ to estimate $\ddot{\mathbf{h}}$, which is to be reversed to $\mathbf{h}$. Lastly, $\mathbf{x}$ is recovered by $\mathbf{h}$ and $\mathbf{P}$. Since $\mathbf{r}$ is not stored, the adversary must recover $\mathbf{r}$ first. Among the compromised information, $\mathbf{e}$ is related to $\mathbf{r}$ as $\mathbf{e} = \mathbf{r} \oplus \mathbf{h}$. Therefore, the easiest way to recover $\mathbf{r}$ is to perform an XOR operation between the stolen $\mathbf{e}$ and $\mathbf{h}$. However, $\mathbf{h}$ is not accessible since $\mathbf{h}$ is a *randomized* vector generated from the biometric input. Thus, the adversary cannot recover $\mathbf{r}$ from $\mathbf{e}$ without $\mathbf{h}$. Nevertheless, the attacker may attempt to guess $\mathbf{r}$ from $\mathbf{e}$. However, it is infeasible since the adversary has no way to verify the guessed $\mathbf{r}$ ($\mathbf{c}$ is independent of $\mathbf{e}$).

Alternatively, the adversary attempts to guess both $\mathbf{h} \in [0,1]^{2d}$ and $\mathbf{r} \in [0,1]^{2d}$ based on $\mathbf{e} \in [0,1]^{2d}$. With two entities, the adversary can perform a preimage attack to generate a 'fake' cancellable template $\mathbf{c}^*$. After the adversary verified $\mathbf{c}^*$ with the compromised $\mathbf{c}$, the adversary uses $\mathbf{h}^*$ and the stolen $\mathbf{P}$ to recover $\mathbf{x}$. This attack is possible when the key space of $\mathbf{e}$ is small; however, $\mathbf{e}$ is always a large binary vector (≥ 512-bits). For each $e \in \mathbf{e}$, there are 2 possible $h \in \mathbf{h}$ and $r \in \mathbf{r}$; thus, a total of $2/2 = 1$ guess to reveal the correct $h \in \mathbf{h}$ and $r \in \mathbf{r}$. Since $\mathbf{e} \in [0,1]^{2d}$ and $d = 256$ (refer to Sections 4.5.1B and 4.5.1C), a total of $2^{512}/2 \approx 2^{511}$ guesses are required to recover the complete $\mathbf{h}$ and $\mathbf{r}$. Thus, it is infeasible to conduct this attempt before $\mathbf{h}$ is revealed for any further attempt. In short, the result implies restoring the original bio. vector $\mathbf{x}$ from a set of compromised information is not possible.

B. Template inversion via Multiple Records

Similar to the approach above, the adversary tries to inverse the cancellable template $\mathbf{c}$ and recover the original biometric vector $\mathbf{x}$. In contrast, this attack is more damaging and related to the Attack via Record Multiplicity (ARM) [168], [169] where multiple sets of cancellable template $\mathbf{c}$ and auxiliary data ($\mathbf{P}$ and $\mathbf{e}$) are involved.

As stated previously, the most straightforward way to obtain $\mathbf{x}$ is to recover the $\mathbf{r}$ and $\mathbf{h}$ from $\mathbf{e}$, then perform correlation analysis. Unlike the previous attack that can only guess the $\mathbf{r}$ and $\mathbf{h}$, this attack enables the attacker to analyze the relation between multiple $\mathbf{e}$s to reveal $\mathbf{h}$. The recovered $\mathbf{h}$ can be further used for the attempt to recover the original $\mathbf{x}$. In here, an assumption is made where the attacker compromised *three* sets of $\{\mathbf{c}, \mathbf{e}, \mathbf{P}\}$. During the analysis, the nominal value from A to C is used to differentiate multiple compromised information, e.g., $\mathbf{c}_{\mathrm{A}}$, $\mathbf{c}_{\mathrm{B}}$.

As described above, encrypted string $\mathbf{e}$ is the XOR product of $\mathbf{r}$ and $\mathbf{h}$. The attacker can perform correlation analysis on multiple $\mathbf{e}$s to reveal the $\mathbf{h}$. This attempt is possible when one of the key ingredients ($\mathbf{h}$ or $\mathbf{r}$) for the $\mathbf{e}$s is identical. In here, we first analyze the case where $\mathbf{e}$s are formed by the same $\mathbf{h}$, followed by the actual situation (different $\mathbf{h}$s) in the proposed scheme. Firstly, the generation of different $\mathbf{e}$s is summarized as follows:

$$\begin{gathered}\mathbf{e_A} = \mathbf{h_A} \oplus \mathbf{r_A} \\ \mathbf{e_B} = \mathbf{h_B} \oplus \mathbf{r_B} \\ \mathbf{e_C} = \mathbf{h_C} \oplus \mathbf{r_C}\end{gathered} \tag{4.6}$$

In the first case, $\mathbf{e}$s are formed by the same $\mathbf{h}$; therefore, $\mathbf{h}_{\mathrm{A}} = \mathbf{h}_{\mathrm{B}} = \mathbf{h}_{\mathrm{C}}$. Since $\mathbf{h}$s are the same, the attacker can perform cross-XOR on multiple $\mathbf{e}$s and generate XOR-ed vectors of different $\mathbf{r}$s. During the cross-XOR process, $\mathbf{h}$s are canceled out, e.g., $\mathbf{r}_{\mathrm{A}} \oplus \mathbf{r}_{\mathrm{B}} \oplus (\mathbf{h}_{\mathrm{A}} \oplus \mathbf{h}_{\mathrm{B}}) = \mathbf{r}_{\mathrm{A}} \oplus \mathbf{r}_{\mathrm{B}} \oplus \mathbf{0}$ where $\mathbf{h}_{\mathrm{A}} = \mathbf{h}_{\mathrm{B}}$; therefore, a set of correlated $\mathbf{r}$ is generated.

$$\begin{gathered}\mathbf{e_A} \oplus \mathbf{e_B} = \mathbf{r_A} \oplus \mathbf{r_B} \\ \mathbf{e_B} \oplus \mathbf{e_C} = \mathbf{r_B} \oplus \mathbf{r_C} \\ \mathbf{e_A} \oplus \mathbf{e_C} = \mathbf{r_A} \oplus \mathbf{r_C}\end{gathered} \tag{4.7}$$

After that, the attacker can perform frequency analysis on the correlated $\mathbf{r}$s and recover the $\mathbf{h}$ in a short time. This is unfavorable, especially when $\mathbf{h}$ is the original biometric input, not to mention the attack complexity of the frequency analysis attack. In the proposed scheme, a prior-randomization process is utilized to resist this attack. Using the prior-randomization process (stage-2 transformation), the $\mathbf{h}$ is a randomized binary vector generated from biometric input $\mathbf{x} \in \mathbb{R}^{2d}$ and randomly generated projection matrices $\mathbf{P}$. Thus, for each user, different $\mathbf{h}$s are generated and used for generating $\mathbf{c}$ and $\mathbf{e}$ in different applications, which achieve a One-Time-Pad (OTP) effect. Since $\mathbf{h}$ is usually a large binary vector (512-bits), it is unlikely the $\mathbf{h}$s of different applications can collide. In other words, to overcome the correlation analysis attack, the projection matrices $\mathbf{P}$ (for stage-2 transformation) and transformation key $\mathbf{r}$ (for stage-3 transformation) must not be *re-used* for the same user.

Besides that, an adversary can guess $\mathbf{h}$ and perform a preimage attack at the stage-3 transformation (as stated in the previous attack). Due to prior randomization, the adversary cannot use the $\mathbf{c}$s to verify the guessed $\mathbf{h}$. The attack complexity of this attempt is similar to the previous section, where it requires at least 2^{511} guesses to recover $\mathbf{h}$ before any further attempt; thus, $\mathbf{P}$ does not need to be kept secretly. To sum up, the analysis shows that the proposed scheme satisfies the irreversibility property as the original biometric input $\mathbf{x}$ (or $\mathbf{x}_1$ and $\mathbf{x}_2$) are not recoverable with the reverse transformation.

C. Attack via input enumeration

Apart from reverse processing the compromised information $\{\mathbf{c}, \mathbf{e}, \mathbf{P}\}$, the attacker can recover the original biometric input, i.e., *original bio. vector* $\mathbf{x}$ by performing a preimage attack. It is easier as the attacker just guess the input face and fingerprint vectors ($\mathbf{x}_1$ and $\mathbf{x}_2$) and transform it into $\mathbf{c}'$ without knowing the details of the transformation function. Recall the transformation function, the face vector $\mathbf{x}_1 \in \mathbb{R}^d$ and fingerprint vector $\mathbf{x}_2 \in \mathbb{R}^d$ are firstly rescaled according to the parameter α, followed by concatenation process to form $\mathbf{x} = \mathbf{x}_1 | \mathbf{x}_2$. Thus, the attacker can guess the $\mathbf{x}$ instead of $\mathbf{x}_1$ and $\mathbf{x}_2$. Assume the original bio. vector $\mathbf{x}$ is a real-valued vector with the distribution of $[LB_{\mathbf{x}}, UB_{\mathbf{x}}]$ where LB is upper bound (maximum value) and UB is upper bound (minimum value). The guess attempt of each $x \in \mathbf{x}$ is determined by the range between $UB_{\mathbf{x}}$ and $LB_{\mathbf{x}}$, and the guess precision (decimal point). As an example, given a vector $x \in [-0.02, 0.01]$, the distribution range is 0.03. If the guess precision is two decimal places (0.00, 0.01 … so on), the guess attempt will be 4. The calculation of attack complexity is summarized as Guess Attempt $= (\|UB_{\mathbf{x}} - LB_{\mathbf{x}}\| \times 10^{\text{decimal points}} + 1)^{\ SIZE_{\mathrm{x}}}$ where $SIZE_{\mathrm{x}}$ denote the size of the $\mathbf{x}$.

Here, the attack complexity is calculated and tabulated in the table below. During the calculation, the guess precision is set to 1 to determine the lowest attack complexity. From the result, it is hard to recover the full $\mathbf{x}$ even with the lowest guess precision. It is harder when the attacker tries to obtain a more precise biometric vector $\mathbf{x}$.

Table 4.9: Complexity for the attack via input enumeration where guess precision = 1 decimal place

Dataset	**Distribution of Biometric Inputs** $[LB_{\mathrm{x}}, UB_{\mathrm{x}}]$			**Attack Complexity (Attempt)**
	$\mathbf{x_1}$	$\mathbf{x_2}$	$\mathbf{x}$	
FVC02DB1+LFW	$[-0.21,0.15]$	$[-0.34,0.34]$	$[-0.34,0.34]$	$7.8^{512} \approx 8^{512}$
FVC02DB2+LFW	$[-0.24,0.24]$	$[-0.34,0.34]$	$[-0.34,0.34]$	$7.8^{512} \approx 8^{512}$
FVC02DB3+LFW	$[-0.23,0.15]$	$[-0.34,0.34]$	$[-0.34,0.34]$	$7.8^{512} \approx 8^{512}$
FVC04DB1+LFW	$[-0.18,0.13]$	$[-0.34,0.34]$	$[-0.34,0.34]$	$7.8^{512} \approx 8^{512}$
FVC04DB2+LFW	$[-0.19,0.23]$	$[-0.34,0.34]$	$[-0.34,0.34]$	$7.8^{512} \approx 8^{512}$
FVC04DB3+LFW	$[-0.18,0.19]$	$[-0.34,0.34]$	$[-0.34,0.34]$	$7.8^{512} \approx 8^{512}$

4.6.2 Security analysis

In biometric template protection, security refers to the resistance strength of the cancellable template toward the attacks that are attempted to bypass the system authentication. In this subsection, the security property of the proposed scheme is examined with several security attacks which are specifically targeted to the scheme.

A. Brute-force attack

Brute-force (BF) attack is the commonly known instance of security attack, with the intention to guess the cancellable template $\mathbf{c}'$ manually. This attack attempt is considered successful when the guessed $\mathbf{c}' = \mathbf{c}$. In the proposed scheme, $\mathbf{c}$ is a large binary with the size of $2dn$ where $2d$ is the size of original biometric input (fused face and fingerprint vectors), and n is the parameter. For each $c \in \mathbf{c}$, a total of $N_{\mathbf{c}}$ guess attempts are required where $N_{\mathbf{c}}$ denote the total possible value in $\mathbf{c}$ ($N_{\mathbf{c}} = 2$); thus, a total of $((N_{\mathbf{c}})^{2dn}/2)$ guess attempts are required before any correct $\mathbf{c}'$ is guessed. This subsection studies the attack complexity under different configurations of $n = 1,10,25,55$ and 100. The brute-force attack complexity is calculated and evidenced in Table 4.10. As observed from the tabulated result, the attack complexity is in the lowest degree (2^{511} attempts) when $n = 1$. The attack complexity increases when n is tuned to a higher value, i.e., from 2^{511} ($n = 1$) to 2^{5119} ($n = 10$). This implies the cancellable template is more secure with the increment of template size (n is high). For verification rate, the cancellable template achieves a low EER when n is high ,e.g., EER= 0.24 ± 0.10 % in FVC2002 DB1+LFW when $n = 55$. However, the verification performance is degraded when n too large.

Table 4.10: Brute-force (BF) attack complexity

Proposed Multimodal Cancellable Scheme			**Total Combinations of c**	**Attack Complexity (Attempt)**
n	d	$2dn$		
1	256	512	2^{512}	$(2^{512}/2) = 2^{511}$
10		5120	2^{5120}	$(2^{5120}/2) = 2^{5119}$
25		12800	2^{12800}	$(2^{25600}/2) = 2^{12799}$
55		28160	2^{28160}	$(2^{28160}/2) = 2^{28159}$

B. False acceptance attack

False acceptance (FA) attack (or Dictionary Attack) is another well-known security attack in a biometric system [157]. In a false acceptance attack, the adversary estimates an approximated cancellable template $\mathbf{c}'$ which can exceed the matching threshold. In other words, the adversary is recognized as the genuine user when the matching score between $\mathbf{c}'$ and the pre-stored $\mathbf{c}$ (refer to $S(\mathbf{c}, \mathbf{c}')$) surpasses the system threshold τ (or matching threshold). Traditionally, FA attack is analyzed by calculating the attack complexity (attempts) where the adversary manually guesses an *approximated* $\mathbf{c}'$ can surpass τ. In this case, τ is the matching threshold when False Acceptance Rate (FAR) = False Rejection Rate (FRR). However, such τ (when FAR=FRR) is yet to be secure especially when the adversary randomly generate a $\mathbf{c}'$ which drops in the upper-bound (UB_{imp}) of *impostor scores distribution*. Therefore, security-wise, the τ should always be higher than impostor scores distribution (FAR= 0%); however, this leads to another situation, so-called the trade-off between security and Genuine Acceptance Rate (GAR).

In this subsection, the FA attack is conducted by assuming the adversary randomly generate an approximated $\mathbf{c}'$ where $S(\mathbf{c}, \mathbf{c}') = UB_{\text{imp}}$ (worst-case scenario). Then, the value of the $\mathbf{c}'$ is increased in a fixed-degree (one-bit per attack attempt) until the $S(\mathbf{c}, \mathbf{c}') \geq \tau$. In this case, τ is defined as a *secure matching threshold* that sacrifices a certain degree of GAR. To summarize, the attack attempts required for the adversary to increase the matching score from UB_{imp} to τ is formulated as follows:

$$\text{Attack complexity} = (N_{\mathrm{c}})^{SIZE_{\mathrm{c}} \times (\tau - UB_{\mathrm{imp}})} \tag{4.8}$$

where $N_{\mathbf{c}}$ is the total value in $\mathbf{c}$ and $SIZE_{\mathbf{c}}$ denote the size of $\mathbf{c}$. In the implementation, $N_{\mathbf{c}} = 2$ and $SIZE_{\mathbf{c}} = 2dn$. Analysis of FA attack is conducted to find the most suitable τ based on the attack complexity and GAR. The evaluations are conducted in every dataset pair with the best-tuned parameters (see Section 4.5.2D) under different settings of τ (with respect to the GAR). To be noted, attack complexity is not calculated when $(\tau - UB_{\mathrm{imp}}) \leq 0$ since the $\mathbf{c}'$ can surpass the secure matching threshold τ.

Table 4.11: False acceptance (FA) attack complexity under different τs

Dataset	**Proposed Scheme**				$(N_{\mathrm{c}})^{SIZE_{\mathrm{c}}}$	$(\tau - UB_{\mathrm{imp}})$	**Attack Complexity (Attempt)**
	$2dn$	N_{c}	UB_{imp}	τ			$(N_{\mathrm{c}})^{SIZE_{\mathrm{c}} \times (\tau - UB_{\mathrm{imp}})}$
GAR = 95%							
FVC02 DB1+LFW	28160	2	0.555	0.582	2^{28160}	0.027	$2^{28160*0.027} \approx 2^{760}$
FVC02 DB2+LFW			0.569	0.579		0.010	$2^{28160*0.01} \approx 2^{282}$
FVC02 DB3+LFW			0.565	0.568		0.003	$2^{28160*0.003} \approx 2^{85}$
FVC04 DB1+LFW			0.567	0.573		0.006	$2^{28160*0.006} \approx 2^{169}$
FVC04 DB2+LFW			**0.568**	**0.565**		**−0.003**	**n/a**
FVC04 DB3+LFW			**0.571**	**0.567**		**−0.004**	**n/a**
GAR = 90%							
FVC02 DB1+LFW	28160	2	0.555	0.594	2^{28160}	0.039	$2^{28160*0.039} \approx 2^{1098}$
FVC02 DB2+LFW			0.569	0.593		0.024	$2^{28160*0.024} \approx 2^{676}$
FVC02 DB3+LFW			0.565	0.580		0.015	$2^{28160*0.015} \approx 2^{422}$
FVC04 DB1+LFW			0.567	0.587		0.020	$2^{28160*0.02} \approx 2^{563}$
FVC04 DB2+LFW			0.568	0.574		0.006	$2^{28160*0.006} \approx 2^{169}$
FVC04 DB3+LFW			0.571	0.578		0.007	$2^{28160*0.027} \approx 2^{197}$
GAR = 85%							
FVC02 DB1+LFW	28160	2	0.555	0.603	2^{28160}	0.048	$2^{28160*0.048} \approx 2^{1352}$
FVC02 DB2+LFW			0.569	0.599		0.03	$2^{28160*0.03} \approx 2^{845}$
FVC02 DB3+LFW			0.565	0.589		0.024	$2^{28160*0.024} \approx 2^{676}$
FVC04 DB1+LFW			0.567	0.595		0.028	$2^{28160*0.028} \approx 2^{789}$
FVC04 DB2+LFW			0.568	0.582		0.014	$2^{28160*0.014} \approx 2^{394}$
FVC04 DB3+LFW			0.571	0.587		0.016	$2^{28160*0.016} \approx 2^{451}$

Table 4.11 tabulates FA attack complexity against the proposed scheme under different matching thresholds τ with respect to the GAR. To be noted, the results with bold red indicate the system is not secure as the adversary is recognized as the genuine user without any attack attempt. From Table 4.11, the proposed scheme is not secure in some datasets, i.e., FVC2004{DB2, DB3}+LFW when GAR= 95%. On the other hand, the proposed scheme is considered secure after sacrificing a certain amount of GAR. The upper-bounds of impostor scores distributions do not exceed the matching threshold τ when GAR is reduced to 90%. For the complexity, it requires a minimum of 2^{169} attempts before the access can

be gained, which implies the scheme can resist the FA attack after sacrificing 10% of GAR. In addition, the attack complexity can be further increased by tuning the τ to a higher value. However, this will reduce the verification performance of the scheme (lower GAR). To sum up, with the best configurations of parameters, the proposed scheme can resist the FA attack with the minimum attack complexity of 2^{169} in the worst-case scenario with a certain sacrifice of GAR. Yet, the attack complexity can be further increased by tuning the parameter n.

C. Birthday attack

Apart from the BF and FA attacks that aim to estimate a $\mathbf{c}'$, birthday attack [158] in the analysis aims to estimate and inject the source input (refer to $\mathbf{x} \in \mathbb{R}^{2d}$ for stage-2 transformation or $\mathbf{h} \in [0,1]^{2d}$ for stage-3 transformation) for generating a $\mathbf{c}'$. In contrast to previous security attacks, a birthday attack is more damaging due to the small template size of input **x/** $\mathbf{h}$ and short transformation time. Briefly, a birthday attack [158] is a cryptanalytic technique that utilizes the birthday problem in probabilistic theory for finding the collisions between the ciphertexts (refer to the cancellable template) of different inputs.

In the analysis, the birthday attack is conducted by estimating an *IoM bio. vector* $\mathbf{h}_{\text{imp}} \in [0,1]^{2d}$ and injecting it for generating a $\mathbf{c}' \in [0,1]^{2dn}$. Let $\mathbf{c}$ be the pre-stored template, $\mathbf{h}_1$ denote the original input to generate $\mathbf{c}$ and $f(.)$ denote the stage-3 transformation function (in verification mode), i.e., $f(\mathbf{h}_1, \mathbf{e}) \rightarrow \mathbf{c}$ where $\mathbf{e}$ is the encrypted string from the database, the adversary aims to estimate a $\mathbf{h}_{\text{imp}}$ such that $f(\mathbf{h}_1, \mathbf{e}) = f(\mathbf{h}_{\text{imp}}, \mathbf{e})$ where $\mathbf{h}_{\text{imp}} \neq \mathbf{h}_1$. Such pair of $\mathbf{h}_{\text{imp}}$, $\mathbf{h}_1$ is a collision. Here, the analysis is conducted in every dataset pair with the best configuration of transformation parameters where the attack complexity is determined by the birthday bound [158] in terms of attack attempts.

Extended from false acceptance attack, birthday attack is conducted in the worst-case scenario where the initial $\mathbf{h}_{\text{imp}}$ can be transformed to $\mathbf{c}'$ which possesses the matching score at the upper-limit of impostor scores distribution (refer to UB_{imp}); and hence, the adversary just need to permute the $\mathbf{h}_{\text{imp}}$ until the matching score of $\mathbf{c}'$ surpasses the secure matching threshold τ. Given the transformation function $f(\mathbf{h}_{\text{imp}}, \mathbf{e}) \rightarrow \mathbf{c}'$ which yields $(N_{\mathbf{c}})^{SIZE_{\mathbf{c}}}$ of possible $\mathbf{c}'$s where $N_{\mathbf{c}}$ is the total value of $\mathbf{c}$ and $SIZE_{\mathbf{c}}$ is the template size, the birthday attack attempt is calculated with the following formula:

$$\text{Birthday Attack Attempt} = \sqrt{2(N_{\mathrm{c}})^{SIZE_{\mathrm{c}}\times(\tau-UB_{\mathrm{imp}})} \cdot \ln(\frac{1}{1-p})} \tag{4.9}$$

where p is the probability of collisions in $\mathbf{h}$ and $SIZE_{\mathbf{c}} = 2dn$. The p is calculated as $p = FAR$ which is based on genuine/ impostor scores distributions of the input $\mathbf{h}$.

Table 4.12: Birthday attack complexity (birthday bound) under different τs

Dataset	**Proposed Scheme**				$2(N_{\mathrm{c}})^{SIZE_{\mathbf{c}}\times(\tau-UB_{\mathrm{imp}})}$	$\ln(1/(1-p))$	**Attack Complexity (Birthday Bound)**
	$2dn$	UB_{imp}	τ	p			
$\mathbf{GAR = 90\%}$							
FVC02 DB1+LFW	28160	0.555	0.594	0.0010	$\approx 2^{1099}$	≈ 0.001	$\approx 0.03 * 2^{550}$
FVC02 DB2+LFW		0.569	0.593	0.0030	$\approx 2^{677}$	≈ 0.003	$\approx 0.05 * 2^{339}$
FVC02 DB3+LFW		0.565	0.580	0.0046	$\approx 2^{423}$	≈ 0.006	$\approx 0.07 * 2^{212}$
FVC04 DB1+LFW		0.567	0.587	0.0034	$\approx 2^{564}$	≈ 0.004	$\approx 0.06 * 2^{282}$
FVC04 DB2+LFW		0.568	0.574	0.0032	$\approx 2^{170}$	≈ 0.004	$\approx 0.06 * 2^{85}$
FVC04 DB3+LFW		0.571	0.578	0.0043	$\approx 2^{198}$	≈ 0.006	$\approx 0.07 * 2^{99}$
$\mathbf{GAR = 85\%}$							
FVC02 DB1+LFW	28160	0.555	0.603	0.0010	$\approx 2^{1353}$	≈ 0.001	$\approx 0.03 * 2^{677}$
FVC02 DB2+LFW		0.569	0.599	0.0030	$\approx 2^{846}$	≈ 0.003	$\approx 0.05 * 2^{423}$
FVC02 DB3+LFW		0.565	0.589	0.0046	$\approx 2^{677}$	≈ 0.006	$\approx 0.07 * 2^{339}$
FVC04 DB1+LFW		0.567	0.595	0.0034	$\approx 2^{790}$	≈ 0.004	$\approx 0.06 * 2^{395}$
FVC04 DB2+LFW		0.568	0.582	0.0032	$\approx 2^{395}$	≈ 0.004	$\approx 0.06 * 2^{198}$
FVC04 DB3+LFW		0.571	0.587	0.0043	$\approx 2^{452}$	≈ 0.006	$\approx 0.07 * 2^{226}$

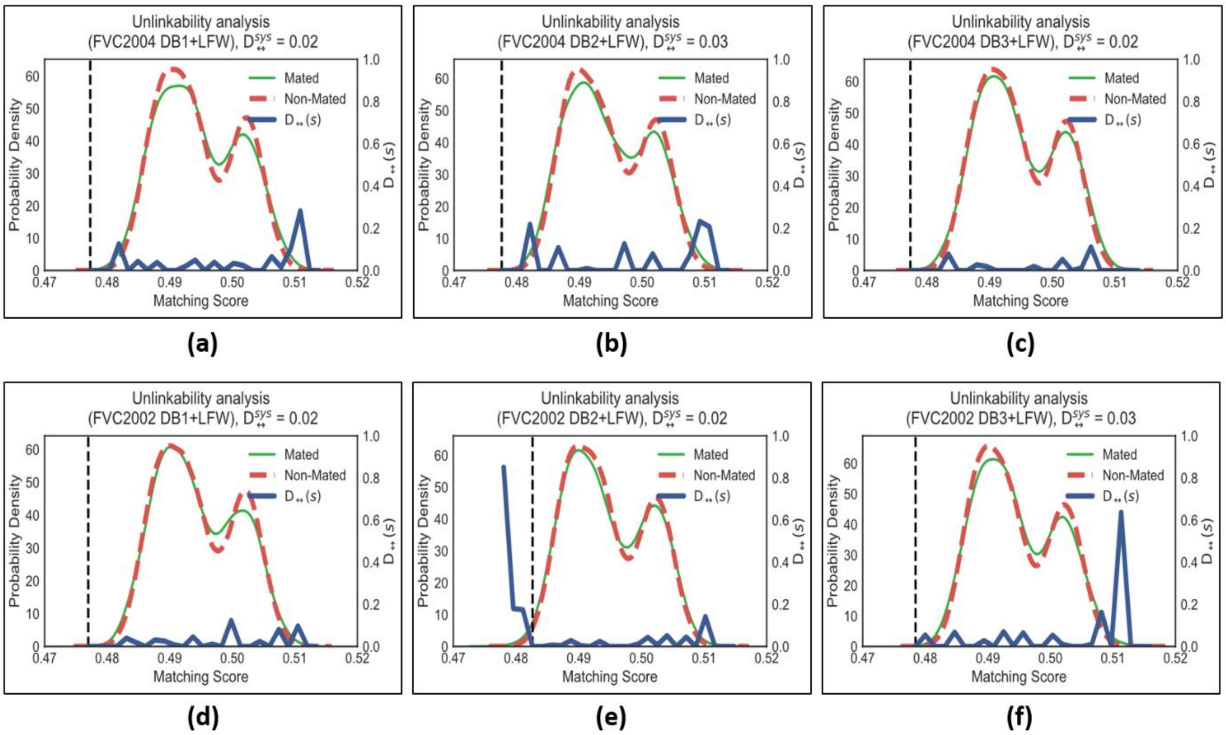
Table 4.12 tabulates the birthday attack complexity for every dataset under different GARs. As stated previously, the proposed scheme is not secure when GAR= 95% (worst-case scenario); thus, the attack complexity is not calculated. By adjusting the matching threshold τ to the case when FAR= 0% and GAR= 90%, the minimum attack complexity (birthday bound) is $0.06 * 2^{85}$. In other words, it requires at most $0.06 * 2^{85}$ attack attempts to estimate the $\mathbf{h}'$ which can gain access to the system. Yet, the estimated $\mathbf{h}'$ is not equal to the original $\mathbf{h}$. This implies the adversary has to re-estimate the $\mathbf{h}'$ when the victim renew the cancellable template, which requires another $0.09 * 2^{85}$ attack attempts. Other than that, it is expected the proposed scheme is more secure by degrading the GAR. For instance, the minimum attack complexity is increasing from $0.06 * 2^{85}$ to $0.06 * 2^{198}$ when GAR is reduced from 90% to 85%. Other than adjusting τ, the attack complexity can be increased by tuning parameter n, which increases the size of the cancellable template. As summarized from the results, the proposed scheme is considered secure when τ is set according to FAR= 0%

and GAR= 90% (in the worst-case scenario). With the minimum attack complexity of $0.06 * 2^{85}$ attempts and GAR= 90%, the verification performance is still acceptable.

4.6.3 Unlinkability analysis

Unlinkability is an important property in biometric template protection that refers to the dissimilarities between multiple cancellable templates that are generated from the same biometric input. In this thesis, the recent unlinkability analysis framework [159] is adopted to evaluate the unlinkability degree of proposed schemes statistically (see Section 3.5.3A for the detailed discussions on the evaluation framework). Briefly, the evaluation of this framework is built upon the *mated* and *non-mated* sample score distributions, which are generated from the cross-match attempts between cancellable templates generated from the *same biometric feature* (mated samples) and *different biometric features* (non-mated samples). After that, both distributions are used to calculate two linkage indicators, i.e., the local measure $D_{\leftrightarrow}(s)$ and global measure $D_{\underset{\longleftrightarrow}{sys}}$. Differ from the $D_{\leftrightarrow}(s)$ that evaluate the linkage of the score distributions based on the score-wise basis, $D_{\underset{\longleftrightarrow}{sys}}$ measure the unlinkability of the whole system [159]. Therefore, $D_{\underset{\longleftrightarrow}{sys}}$ can be used for benchmarking the unlinkability level of the biometric template protection. The value range of both $D_{\leftrightarrow}(s)$ and $D_{\underset{\longleftrightarrow}{sys}}$ is bounded from 0 to 1, where 0 shows the best unlinkable between different cancellable templates. To shows a reasonable unlinkable level of a template protection method, it is suggested the computed $D_{\underset{\longleftrightarrow}{sys}}$ to be as low as possible ($D_{\underset{\longleftrightarrow}{sys}} \leq 0.14$) [159]. In the experiment, 3 set of auxiliary data are used to generate the cancellable templates for each biometric instance.

The evaluation result for the proposed M·EFV hashing is illustrated in Fig 4.6. The blue line represents the trend of local measure $D_{\leftrightarrow}(s)$ among the score distributions. The higher the blue line, the higher the linkage level of the cancellable templates is the specific point. The green distribution describes the mated sample score distribution, while the red distribution describes the non-mated sample score distribution. According to [159], a fully unlinkable case can be identified when the red distribution and green distribution are overlapping, while a fully linkable case is observed when both score distributions do not overlap. As observed from Fig 4.6, the unlinkability of M·EFV hashing is nearly a fully unlinkable case since both score distributions are highly overlapped. As a result, the global measures $D_{\underset{\longleftrightarrow}{sys}}$ are averagely near to 0. This shows a decent privacy level of the cancellable templates (from the same biometric feature) generated via M·EFV hashing. It is important that multiple cancellable templates generated should not be distinguishable. If the cancellable templates are identical, the attacker can attempt to use a compromised cancellable template to track the users or perform a replay attack on the matcher.



(a) (b) (c)

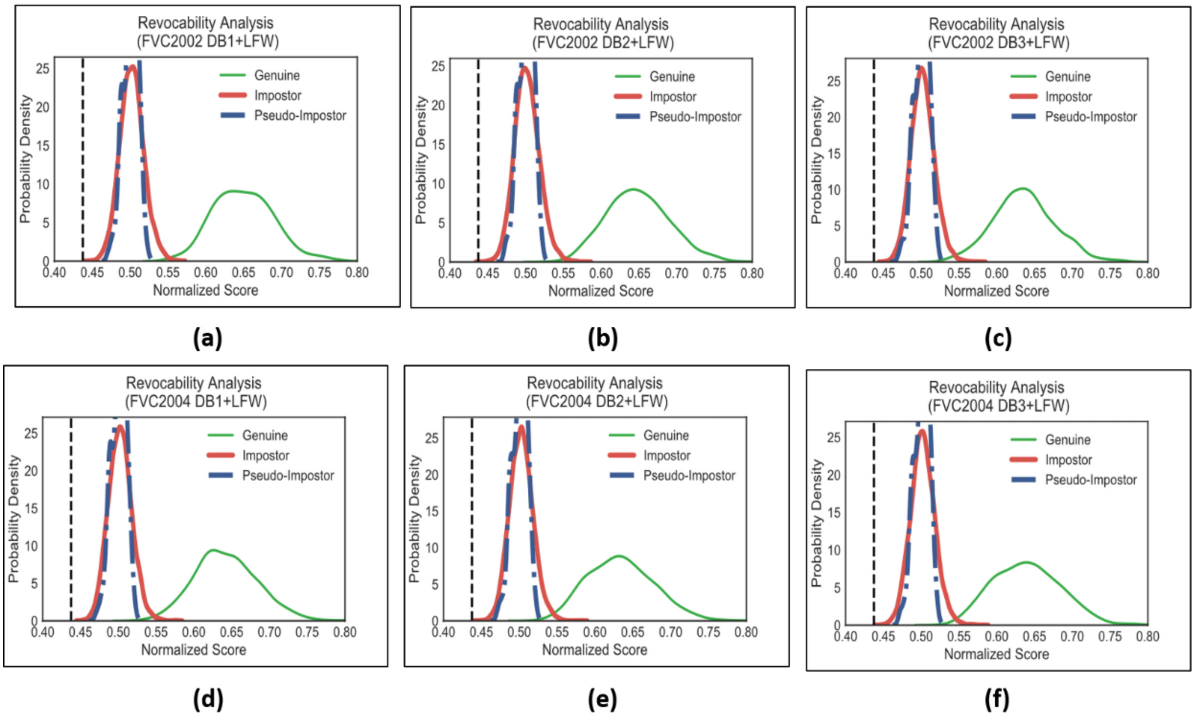
(d) (e) (f)

Fig 4.6. Unlinkability analysis result in FVC(2002, 2004)+LFW dataset

4.6.4 Renewability analysis

Renewability is one of the template protection requirements that means the user can use the same biometric feature to revoke and renew the cancellable template. In other words, multiple cancellable templates generated from the same biometric feature are independent of each other (similar to unlinkable). In this subsection, a quantitative experiment is conducted to verify the renewability of the cancellable templates, where a detailed discussion on this quantitative experiment is provided in section 3.5.3B. Briefly, the evaluation of this experiment is built upon the score distributions that are generated from the genuine, impostor and pseudo-impostor matching attempts. In the experiment, a pseudo-impostor matching attempt is assumed by matching the old cancellable template to a variety of re-new cancellable templates. Therefore, for each tested biometric sample there are up to 51 cancellable templates are generated using different transformation keys. The first cancellable templates are then be matched to the remaining 50 cancellable templates to produce the pseudo-impostor matching score. Since the renewed cancellable template should be independent of the old cancellable template, the matching score between these two entities should be similar or lower than the matching score between the genuine user and impostor user by assuming the renewed template as the impostor. Thus, the pseudo-impostor score distribution should not be overlapped with the genuine score distribution to show the renewability of the cancellable template.

The experiment result of this evaluation model is illustrated in Fig 4.7. Blue distribution describes the pseudo-impostor score distribution. Red distribution is the impostor score distribution. As observed from Fig 4.7, pseudo-impostor score distribution and impostor score distribution are mostly overlapped. This shows that up to 50 newly generated cancellable template is not even the same as the old cancellable template. In a nutshell, the result suggests that M·EFV hashing satisfies the renewability requirement.



(a) (b) (c)

(d) (e) (f)

Fig 4.7. Renewability (or revocability) analysis result in FVC(2002, 2004)+LFW dataset

4.6.5 Summary of security and privacy analysis

Throughout the analyses, several points are summarized:

- It is hard to inverse the cancellable template $\mathbf{c}$ back to the original face vector $\mathbf{x}_1$ and fingerprint vector $\mathbf{x}_2$ even multiple sets of the cancelable template and auxiliary data are known. Whenever the cancellable template is compromised, the user can always revoke and renew the cancellable template by using a different set of auxiliary data.

- The XOR encryption/ decryption is the key notion in enabling the tokenless property of the proposed method. The key idea of the tokenless is to convert the transformation key into auxiliary data that is insensitive for the original biometric feature recovery. Coupled with the prior-randomization mechanism, it is shown that the transformation key is not recoverable even if multiple databases are compromised. This prohibits the adversary from any further attack, e.g., template inversion.

- With the empirical results of the benchmarking assessment framework, multiple produced cancellable templates from the same biometric feature are independent of each other. Thus, unlinkability property is guaranteed.

4.7 Summary and contributions

This chapter focuses on the **token management** and **fusion incompatibility** problems in the face and fingerprint template protection. Two research outcomes (template protection scheme), namely the *Extended Feature Vector (EFV) Hashing* and *Multimodal Extended Feature Vector (M·EFV) Hashing* are introduced to protect the face and fingerprint templates where the latter is the enhanced version of the former scheme that can is used to fuse the face and fingerprint features into a cancellable template. This chapter demonstrates a 3-stage transformation mechanism that could efficiently embed the real-valued face and fingerprint vectors into a binarized cancellable template. In contrary to the tokenized authentication approaches, the proposed EFV hashing and M·EFV hashing incorporate the XOR encryption/ decryption machinery to enable the “one-factor” property. Comprehensive experiments are established to study and select the best-tuned parameters for generating the cancellable template. Notably, the verification accuracy of the *M·EFV* hashing could reach as low as EER= 0.24 ± 0.10 %. Furthermore, the theoretical justification and attack complexity suggest it is infeasible to recover the original face and fingerprint vector even if multiple sets of cancellable template and auxiliary data are compromised. The security property of the proposed scheme is justified by calculating the attack complexity of several security attacks which are damaging to the biometric system. In this chapter, the well-known false acceptance and birthday attacks are considered as the attack model in the analyses. It is revealed that a system is insecure when the matching threshold is set at the point where FAR=FRR. To resolve this issue, the matching threshold is suggested to be adjusted to the case when FAR $< 0\%$ in which a certain degree of GAR is traded for the security consideration. With the minimum attack complexity of $0.06 * 2^{85}$ attempts and GAR$= 90\%$, the proposed scheme can preserve verification performance while resisting the birthday attack. Lastly, unlinkability and renewability criteria are examined based on a recently developed unlinkability analysis framework [159]. The unlinkability measure (i.e., $D_{\underset{\longleftrightarrow}{sys}}$) is reported for benchmarking purposes. Lastly, it is concluded that the proposed scheme is proved to satisfy the irreversibility, unlinkability, renewability and performance preservation properties.

Chapter 5 BIOMETRIC DECISION ENVIRONMENT AND AUTHENTICATION ATTACK

This chapter focuses on the biometric decision environment and authentication attack for the cancellable biometrics-enabled system. This chapter can be divided into two parts corresponding to the contributions iii and iv in this thesis, i.e., an enhanced matching mechanism (contribution iii) and authentication attack (contribution iv). A biometric system, no matter protected or unprotected, utilizes the matching threshold to verify the identity of an individual. The trade-off between security and verification performance is inevitable towards a biometric system. To resolve this issue, an enhanced matching mechanism is introduced for the cancellable biometrics-enabled system, i.e., IoM hashing-based fingerprint system, R · HoG-based iris system, and M · EFV hashing-based multimodal system. The proposed enhanced matching mechanism is essentially a dual-phase score quantization scheme that aims to increase the intra-class similarity and reduce inter-class similarity of the cancellable template matching. Comprehensive experiments are conducted in the benchmarking fingerprint FVC, iris CASIAv3 and face LFW datasets. Experimental results suggest the proposed enhanced matching mechanism could improve the verification performance of the system. On the other hand, this chapter also studies the type-4 attack in the cancellable biometrics-enabled system and formalizes an automated authentication attack scheme, namely Whale Optimization Algorithm-based Authentication Attack (WO3A). A type-4 attack refers to the attack that aims to estimate and inject a guessed biometric template into the system for gaining illegal access. Differ from the classical false acceptance attack or birthday attack; the type-4 attack relies on the intercepted matching score to perform perturbation on the guessed biometric template. The intuition of formalizing the WO3A is to testify and quantify the security resistance of the cancellable biometric schemes and enhanced matching mechanism experimentally. Security analysis via WO3A shows the proposed enhanced matching mechanism is able to improve the security resistance of the cancellable biometric scheme towards WO3A. Under the same attack setting, the proposed enhanced matching mechanism is able to reduce the attack success rate.

5.1 Background

Cancellable biometrics (CB) [19] is important biometric template protection primitive that plays a crucial role in numerous biometric-based authentication systems to prevent the recovery of original biometric features from the enrollment information (e.g., pre-stored biometric instance and auxiliary data) for the unfavorable event, such as impersonation and privacy invasion [11]. In general, cancellable biometrics is a feature transformation-based approach that utilizes an auxiliary data-guided transformation function to transform the original biometric feature into an irreversible template (or cancellable template). Suppose $f(.)$ as the cancellable transformation function, x and x' are the biometric features belong to the same person and r represents the auxiliary data, a cancellable biometric scheme generates the cancellable templates that are highly similar in which $f(x, r) \sim f(x', r)$ even there are minor differences between x and x'. Therefore, the authentication process can be carried out in the transformed domain without revealing original biometric information, and the verification performance is comparable to the original biometric system. Due to the simplicity and decent verification performance, cancellable biometrics is popular among the community. In general, a decent cancellable biometric scheme offers the following enforcements towards a biometric system [19]:

- Irreversibility: It is hard to recover the original biometric information from the protected instance (cancellable template) even if multiple cancellable templates and auxiliary data are known to the adversary.

- Unlinkability: The user can use the same biometric feature in different cancellable biometrics-enabled systems without worrying about privacy invasion occurring. Multiple produced cancellable templates are independent of each other such that it is infeasible for the adversary to perform a cross-matching attack.

- Renewability: Since the same biometric feature can produce different cancellable templates, the user can revoke and renew once the system security (or database) is compromised.

Although cancellable biometrics prevents the original biometric information from being recovered and allows the renewal of enrollment using the same biometric feature, a cancellable biometrics-enabled system still faces a potential security threat where the adversary can attempt to gain illegal access to the system by performing the feature injection attack towards the system (refers to the type-4 attack [27], [170]). In particular, this attack is an iterative modification scheme that exploits the thresholding decision-making of the biometric system and aims to find a guessed biometric template that can produce a sufficient similarity score and bypass the authentication for one system. A general view of the attack model for this attack is given in here. In this attack, the adversary first randomly generates the biometric template. After that, the adversary injects the biometric template into the cancellable biometrics-enabled system for matching. Assuming the adversary can access the evaluation metric (i.e., similarity score S), the attack framework then updates the biometric preimage based on the S. This attack repeats until $S \geq \tau$ or the stopping threshold of the attack framework is met. Most of the existing cancellable biometric schemes are manifested as a thresholding-based system; hence this attack is feasible if the adversary could compromise the auxiliary data (or token) and attempt to inject it with a guessed biometric preimage into the system (e.g., [29], [142]). Moreover, this attack could be easily conducted since the estimated biometric preimage does not need to be the same as the original biometric input. Attributed to the renewability property, a decent cancellable biometric scheme allows the renewal of a cancellable template once the security (authentication) is compromised. In this sense, the estimated biometric preimage could not be used for the authentication attack. Therefore, cancellable biometrics is always desired to protect the system.

Although renewal of the cancellable template could prevent the attacker from using the estimated preimage for the replay attack, it is unfavorable that the adversary could gain illegal access to the system in a short time. Furthermore, this could induce privacy risk (e.g., personal information leakage) when the genuine user could not respond and renew the cancellable template in a given time. Since a cancellable biometrics-enabled system utilizes the thresholding mechanism to determine an individual's identity, a straightforward approach to improve the security resistance of the system towards the type-4 attack is to set a high matching threshold (or system threshold). However, this could lead to the increment of false rejection of the system where the matching score between the pre-stored template and query template from the genuine user is harder to surpass the threshold, which refers to a case of the trade-off between security and performance [27]. This problem is further exacerbated in a cancellable biometrics-enabled system due to the performance degradation issue where the overlap region of the *genuine* and *impostor* score distributions is larger than the unprotected counterpart [11].

This chapter deduces the performance degradation issue as the weak decision environment problem of the biometric template protection, especially a unimodal biometric template protection scheme. The concept of a weak decision environment is inspired by Daugman's work [89], where the decision environment refers to the biometric system's performance indicators that are based on the separation between the genuine and impostor score distributions. To further improve the decision environment of the cancellable biometric scheme, this chapter proposes an enhanced matching mechanism that aims to reduce the intra-class variation and increase inter-class variation for the generated cancellable biometric template. The essence of the proposed matching mechanism is that it is a dual-phase score quantization scheme that reduces the overlap region between the mean of genuine and impostor score distributions. As such, it allows the system developer to choose a higher system threshold while minimizing the sacrifice of the genuine acceptance rate (GAR) of the system. While the cancellable biometrics offers the irreversibility, unlinkability and renewability solutions, the proposal matching mechanism enhances the decision environment in terms of reducing overlap regions between *genuine* and *impostor* score distributions. As such, both solutions can be coupled to further reduce the effect of the type-4 attack.

Other than that, the security of a cancellable biometrics-enabled biometric system is studied in the case that an adversary attempts to use an automated authentication attack (type-4 attack) to gain illegal access to the system. Thus, other than the enhanced matching mechanism, this chapter also formalizes an authentication attack scheme and conducts it towards the cancellable biometrics-enabled system. To sum up, the contributions of this chapter are outlined as follows:

- An enhanced matching mechanism is proposed to further improve the verification performance of the IoM hashing-based fingerprint system [66], R·HoG-based iris system, and M·EFV hashing-based multimodal system [3]. Specifically, the proposed enhanced matching mechanism reduces the overlap region between the genuine and impostor score distribution. As such, the proposed enhanced matching mechanism allows a higher matching threshold to be chosen while maintaining the verification performance of the system.

- Comprehensive experiments are conducted on several benchmarking datasets, including FVC2002 [73], FVC2004 [74], CASIA-IrisV3-Internal [52] and LFW [84] to justify the improvement of verification performance after applying the enhanced matching mechanism. The experimental result suggests the proposed enhanced matching is effective in enhancing the decidability of the tested cancellable biometric schemes in the sense that the mean of genuine score distribution is increased and the mean of impostor score distribution is decreased.

- A new type-4 attack, namely the *whale optimization algorithm-based authentication attack* (WO3A) is formalized to testify the security resistance of the cancellable biometric schemes and proposed an enhanced matching mechanism. The formalized attack scheme is an automated authentication attack in the sense that the perturbation of the guessed biometric template is done strategically instead of the manual bit-by-bit perturbation in a brute-force or manual hill-climbing approach. Thus, the WO3A can be more efficient than the brute-force or manual hill-climbing approaches.

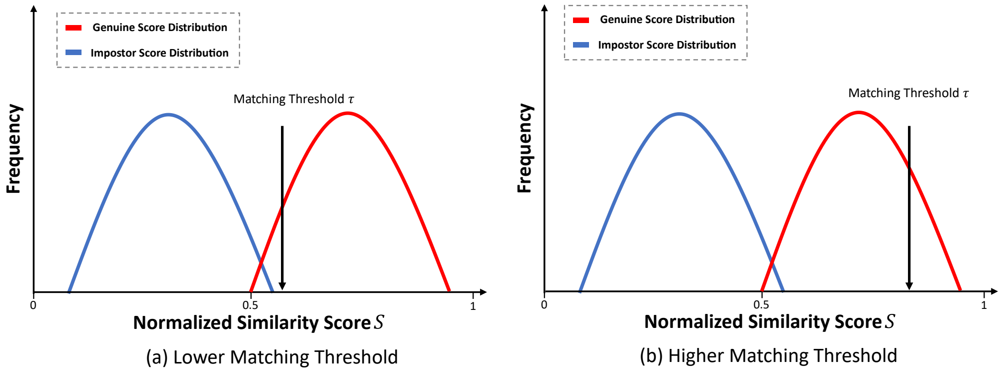
- The WO3A is conducted on the tested cancellable biometric schemes to examine the security resistance of the schemes towards the WO3A attack. The security resistance of the cancellable scheme is evaluated by calculating the success rate of the WO3A with respect to the system threshold. The experiments are conducted in the cases that (i) the cancellable biometric schemes are in the original construction and (ii) the cancellable biometric schemes are enforced with the proposed enhanced matching mechanism to show the increment of the security resistance towards the attack scheme.

This chapter is organized as follows: Section 5.2 discusses the decision environment of a biometric system and the proposal of an enhanced matching mechanism, followed by section 5.3 to examine the proposed enhanced matching mechanism in terms of parameter estimation, verification performance and computation efficiency. Section 5.4 outlines the authentication attack and formalizes a practical attack scheme. After that, section 5.5 evaluates the security resistance of the tested cancellable scheme and the proposed enhanced matching mechanism. Lastly, the findings are summarized in section 5.6.

5.2 Biometric decision environment

This chapter is divided into two parts: decision environment and authentication attack. This section focuses on the decision environment and proposes an enhanced matching mechanism that could improve the verification performance of the cancellable biometric scheme.

5.2.1 Overview



(a) Lower Matching Threshold

(b) Higher Matching Threshold

Fig 5.1. A biometric system with different settings of matching threshold (τ)

Recognition performance of a (protected or unprotected) biometric system is characterized by the decision environment that is built upon the score distributions from the *genuine* and *impostor* comparisons [89]. The genuine comparison refers to the matching between the biometric templates of the same individual, while impostor comparison refers to the comparison between the biometric templates from different individuals. Most of the existing type-4 attacks attempt to use the fake input biometric template $\mathbf{X}^*$ and get recognized as a genuine user. Typically, this attack begins by random initializing a $\mathbf{X}^*$, and then input the $\mathbf{X}^*$ to the system for matching. The attack continues until the matching score between the fake input (e.g., $\mathbf{X}^*$) and the pre-stored instance (e.g., $\mathbf{X}$) (refer to $S(\mathbf{X}, \mathbf{X}^*)$) surpass the system threshold τ, i.e., $S(\mathbf{X}, \mathbf{X}^*)) \geq \tau$. Therefore, selection of system threshold τ is crucial to provide security resistance towards potential security attacks. In most of the cases, the τ is set at the point when False Acceptance Rate (FAR) = False Rejection Rate (FRR). However, this τ is yet to be secure. For security consideration, τ should always be higher than the impostor score distribution ($\mathrm{FAR} = 0\%$). Yet, this leads to another scenario, so-called the trade-off between security and performance (genuine acceptance rate GAR). An example is shown in Fig 5.1 with two settings of the τ in the system. In Fig 5.1 (a), the τ is set slightly higher than the upper bound of impostor score distribution with minimal sacrifice of GAR to provide a certain level of security resistance. The τ could be set higher to increase the security resistance. However, this could further sacrifice the GAR and greatly reduce the usability of the system (see Fig 5.1 (b)). The limitation of selecting a suitable τ is exacerbated in a cancellable biometric-enabled system due to the performance degradation problem.

As mentioned above, the decision environment of a biometric system is characterized by the genuine and impostor score distributions, especially the overlap region between both distributions. For instance, a high Equal Error Rate (ERR) is estimated when both distributions are highly overlapped. In this case, selecting the τ at the point when $\mathrm{FAR} = 0\%$ results in high FRR. Therefore, it is desirable when the overlap region between both distributions can be reduced, or ideally, there is a separation between both distributions, which allows a higher τ without worrying about high FRR.

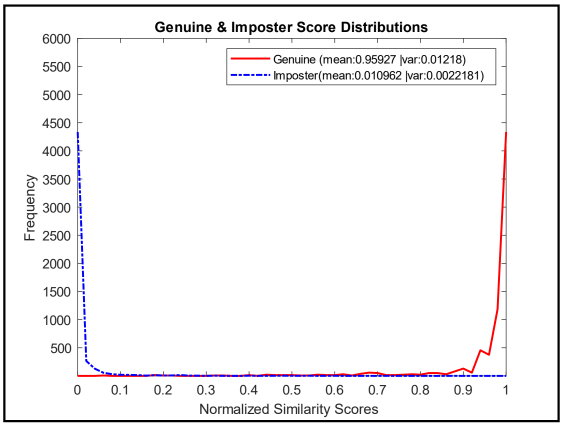


Fig 5.2: Graphical representation of an optimal case where a biometric system with high separation between the mean of genuine and impostor score distributions

Ideally, a decision environment with the mean of the genuine/ impostor score distributions highly separated (refer to Fig 5.2) enjoys the following merits:

- The verification performance of the biometric system is improved in terms of lower false acceptance rate (FAR) and false rejection rate (FRR). This is because of the decrement of the overlap region between the mean of the genuine and impostor score distributions.

- The matching threshold τ can be set to a high value to improve the security resistance towards the security attack without worrying the verification performance is degraded too much. In particular, the sacrifice degree of the GAR is reduced when eliminating the FAR of the system. The security resistance is increased in the sense that the gap between the τ and the adversary starting point (assuming it is in UB_{imp}) is large. Hence, it requires higher attack complexity to break into the system.

5.2.2 Proposed enhanced matching mechanism

This subsection presents the proposed enhanced matching mechanism. For the sake of readability, the table below lists the notations that are being used in the proposed matching mechanism.

Table 5.1: NOMENCLATURE

Notation(s)	Description
$\mathbf{X} \in \mathbb{R}^{a \times b}$	Original biometric feature
$\mathbf{R} \in \mathbb{R}^{q \times e}$	Auxiliary data of the cancellable biometrics
$\mathbf{C} \in \mathbb{R}^{k \times m}$	Cancellable biometric template
$f(.)$	Cancellable transformation function, $f(\mathbf{X}, \mathbf{R}) \rightarrow \mathbf{C}$
n	Number of local cancellable template
$\mathbf{P} = \{\mathbf{P}_1, \mathbf{P}_2, \dots, \mathbf{P}_n\}$	Permutation seed, each $\mathbf{P} \in \mathbb{R}^{l \times o}$
τ_{L}	Local quantization threshold
τ_{G}	System matching threshold
$\mathbf{s} \in \mathbb{R}^{n}$	Local score vector, each $0 \leq s_i \leq 1$
s_{G}	Global score (matching score)

The proposed enhanced matching mechanism is a simple yet effective matching mechanism that can improve the decision environment by reducing the overlap region between the *genuine* and *impostor* score distributions. The proposed *enhanced matching mechanism* is a dual-phase score quantization scheme that aims to enhance the matching process of a biometric system by separating the similarity scores that can be acquired from the *genuine comparison* and *impostor comparison.* The proposed matching mechanism consists of two phases: (i) transformation and (ii) matching. During the transformation phase, multiple randomized instances of the input biometric template are firstly generated based on the permutation seeds. To be noted, each randomized instance is a partial input biometric template in the sense that a random undersampling process is used to generate the randomized instances. After that, the cancellable transformation is employed to transform the randomized instances into n numbers of cancellable biometric templates and then store the templates into the storage.

During the matching phase, the query template set is first generated and then be matched to the pre-stored template set, which yields n numbers of similarity score (refer as local similarity score). After that, the local similarity scores are quantized into 0 or 1 based on a parameter, so-called the local quantization threshold. Lastly, the final matching score is calculated by averaging the n numbers of the local quantized score. The underlying concept of the proposed matching mechanism is to statistically count the similarity scores from the local matchings, where each local score is quantized based on a local quantization threshold that is set under at the point when FAR=FRR or higher. As such, a separation of the *genuine* and *impostor* scores is achieved where the matching score of the genuine score is increased while the impostor score is decreased. This is mainly due to the number of 0 or 1 calculated from the local matchings. In other words, the genuine comparison can obtain more '1' from the local matchings, and hence, genuine comparison matching can produce a higher matching score. The transformation and matching phases of the enhanced matching mechanism are explained as follows.

A. Transformation (or Enrollment) phase

During the transformation phase, the proposed scheme transforms the input biometric template into multiple instances of the cancellable template. Given the biometric feature $\mathbf{X} \in \mathbb{R}^{a \times b}$, cancellable transformation function $f(.)$, the auxiliary data for the transformation function $\mathbf{R} \in \mathbb{R}^{q \times e}$ and a set of random permutation seeds $\mathbf{P} = \{\mathbf{P}_1, \ldots, \mathbf{P}_n\}$, the proposed scheme first produce a set of local cancellable templates $\mathbf{C} = \{\mathbf{C}_1, \ldots, \mathbf{C}_n\}$ where each $\mathbf{C}_i \in \mathbb{R}^{k \times m}$ with the following procedures:

1) **Set random undersampling:** Generate n numbers of permuted biometric features $\mathbf{V}_i$ by using each $\mathbf{P}_i$ to permute the $\mathbf{X}$ where $i = 1 \ldots n$. To be noted, this process is a random undersampling process in the sense that each permuted biometric feature $\mathbf{V}_i$ is the partial information of the original biometric template. In particular, the parameter l and o are used to control the size of the each $\mathbf{V}_i$. Given the input biometric feature $\mathbf{X} \in \mathbb{R}^{a \times b}$, $l \leq a$ and $o \leq b$, a set of permuted biometric features $\mathbf{V} = \{\mathbf{V}_1, \ldots, \mathbf{V}_n\}$ is generated by computing $\mathbf{V}_i = \mathrm{perm}(\mathbf{X}, \mathbf{P}_i)$ where each $\mathbf{V}_i \in \mathbb{R}^{l \times o}$ and perm(.) denotes the random

undersampling function. Each $\mathbf{V}_i$ are independent of each other because of the random undersampling process, which induces another layer of randomization effect.

2) **Local cancellable template generation:** Each $\mathbf{V}_i$ is transformed to the cancellable template $\mathbf{C}_i$ by computing $\mathbf{C}_i = f(\mathbf{V}_i, \mathbf{R}\ )$ where $\mathbf{R}$ is the auxiliary data for the transformation function, $f(.)$ denotes the cancellable transformation function and $i = 1 \dots n$. To further improve the randomness of the local cancellable templates, each $\mathbf{C}_i$ is generated using different auxiliary data $\mathbf{R}$. Therefore, a set of auxiliary data $\mathbf{R} = \{\mathbf{R}_1, \dots, \mathbf{R}_n\}$ is used for the cancellable transformation.

After that, the cancellable template set $\mathbf{C} = \{\mathbf{C}_1, \dots, \mathbf{C}_n\}$ are stored in storage for authentication purposes. It is noted that the intermediate product, i.e., $\mathbf{V} = \{\mathbf{V}_1, \dots, \mathbf{V}_n\}$ is deleted after the generation of the cancellable template set. In the event that the template storage is compromised, the user can revoke and renew the enrollment by replacing the $\mathbf{P}$ and $\mathbf{R}$. Since multiple randomization processes are involved, it is unlikely that the renewed cancellable template set ($\mathbf{C}'$) can collide with the compromised cancellable template set.

Algorithm 5.1. Enhanced matching mechanism - Transformation

```
Input (From User): Biometric feature $\mathbf{X}$, Cancellable transformation $f(.)$, random permutation seeds $\mathbf{P} = \{\mathbf{P}_1, \dots, \mathbf{P}_n\}$, Transformation auxiliary data $\mathbf{R} = \{\mathbf{R}_1, \dots, \mathbf{R}_n\}$
Parameters: number of local $n$,
Output: A set of cancellable templates $\mathbf{C} = \{\mathbf{C}_1, \mathbf{C}_2, \dots, \mathbf{C}_n\}$
for $i \leftarrow 1$ to $n$
    Random undersampling $\mathbf{X}$ based on $\mathbf{P}_i$ and produce $\mathbf{V}_i$
    Compute $\mathbf{C}_i = f(\mathbf{V}_i, \mathbf{R}_i)$
end for
return $\mathbf{C} = \{\mathbf{C}_1, \dots, \mathbf{C}_n\}$
```

B. Matching (or Verification) phase

During the matching phase, the individual provides the biometric feature $\mathbf{X}'$ to the system for generating the query template set $\mathbf{C}' = \{\mathbf{C}'_1, \dots, \mathbf{C}'_n\}$, then the $\mathbf{C}'$ is matched to the pre-stored $\mathbf{C}$. In contrast to the standard matching that uses a simple matcher (e.g., Hamming similarity or Euclidean similarity), the proposed enhanced matching mechanism is a dual-phase score quantization scheme that is built upon the local matching and counting collision pair mechanisms. Given the enrolled template set $\mathbf{C} = \{\mathbf{C}_1, \dots, \mathbf{C}_n\}$ and the query template set $\mathbf{C}' = \{\mathbf{C}'_1, \dots, \mathbf{C}'_n\}$, the procedures to obtain the global similarity score s_{G} are as follow:

1) **Local similarity comparison:** Similarity comparison between $\mathbf{C}_i$ and $\mathbf{C'}_i$ is performed to obtain the local matching score s_i where $i = 1 \dots n$ and the s_i is a normalized score that is within 0 to 1. A local score vector $\mathbf{s} = \{s_1, \dots, s_n\}$ is formed after n numbers of similarity comparison.

2) **Local score quantization:** For each $s_i \in \mathbf{s}$, a uni-step function is applied to quantize the each s_i to 0 or 1. Given that each s_i is calculated from the similarity comparison between a pair of $\mathbf{C}_i$ and $\mathbf{C'}_i$, the proposed enhanced matching mechanism determine the $\mathbf{C}_i$ and $\mathbf{C'}_i$ as a collision pair when $s_i \geq \tau_\mathrm{L}$ where $i = 1 \dots n$ indicates i-th local cancellable template. As such, each $s_i \in \mathbf{s}$ is computed as

$$s_i = \begin{cases} 0, & s_i < \tau_\mathrm{L} \\ 1, & s_i \geq \tau_\mathrm{L} \end{cases} \tag{5.1}$$

where τ_l is the parameter to control the quantization process. Throughout this process, the $\mathbf{s}$ is a model with binary outcomes (each $s_i = 0$ or 1).

3) **Global score calculation:** Compute the global similarity score $s_\mathrm{G} = \frac{\sum_{i=1}^{n} s_i}{n}$ where each $s_i \in \mathbf{s}$.

In the proposed enhanced matching mechanism, the global similarity score (s_G) is the final matching score of the authentication process. Lastly, the s_G is passed to the decision module to determine the identity of the individual based on the system matching threshold τ_G, where the decision rules are as follows:

$$\text{Decision} = \begin{cases} \text{Impostor}, & s_\mathrm{G} < \tau_\mathrm{G} \\ \text{Genuine}, & s_\mathrm{G} \geq \tau_\mathrm{G} \end{cases} \tag{5.2}$$

On the whole, the value of the s_G is amplified by the local matchings. Given the similar input $\mathbf{X}$ and $\mathbf{X}'$, the proposed enhanced matching mechanism produces the $\mathbf{C} = \{\mathbf{C}_1, \dots, \mathbf{C}_n\}$ and $\mathbf{C}' = \{\mathbf{C'}_1, \dots, \mathbf{C'}_n\}$, such that majority of $\mathbf{C}_i$ and $\mathbf{C'}_i$ are highly similar. In this sense, the enhanced matching mechanism could produce a s_G that is close to 1, which maximizes the intra-class similarity.

Algorithm 5.2. Enhanced matching mechanism - Matching

```
Input (From User): Query template set $\mathbf{C}' = \{\mathbf{C}'_1, \ldots, \mathbf{C}'_n\}$
Input (From System): Enrolled template set $\mathbf{C} = \{\mathbf{C}_1, \ldots, \mathbf{C}_n\}$, Local quantization threshold $\tau_{\mathrm{L}}$
Output: Global similarity score $s_{\mathrm{G}}$
// Step 1 and 2: Local similarity comparison + score quantization
initialize $\mathbf{s} = [0]^n$
for $i \leftarrow 1$ to $n$
    $s_i = similarity(\mathbf{C}_i, \mathbf{C}_i')$
    if $s_i \geq \tau_{\mathrm{L}}$
        $s_i = 1$
    else
        $s_i = 0$
end for
// Step 3: Global score calculation
compute $s_{\mathrm{G}} = \frac{\sum_{i=1}^{n} s_i}{n}$
return $s_{\mathrm{G}}$
```

5.3 Experiments and discussions

This section is devoted to presenting the experiment results for the proposed enhanced matching mechanism in terms of verification performance and decidability. The experiments are conducted on a machine with the hardware specification of Solid-State Drive (NVMe)@480GB, Intel Core i7-7700 CPU@2.80Hz, Memory DDR4@24GB. Realization of the proposed enhanced matching mechanism and formalized attack scheme are written using MATLAB R2019a.

5.3.1 Experimental setup

This subsection presents the experimental setup in terms of matching protocol, evaluation metric, dataset and feature extraction. Other than that, this subsection outlines the targeted cancellable biometric schemes: Index-of-Max (IoM) hashing, M·EFV hashing and R·HoG.

A. Matching protocol and evaluation metric

The well-known FVC full matching protocol [163] is followed to study the recognition performance of the biometric system. Briefly, the assessment of this protocol is mainly relying on the *Equal Error Rate (EER) (%)* that is calculated from the genuine/ impostor score distributions. Given a dataset with n numbers of subject and m numbers of biometric feature, the genuine/ impostor score distributions are generated via following matching attempts:

- **Genuine (or intra-class) matching attempt:** Crossmatch all cancellable templates from the same subject. Thus, a total of $n\ ({}^{m}C_2)$ genuine matching scores are generated from genuine matching attempts.

- **Impostor (or inter-class) matching attempt:** Crossmatch all cancellable templates generated from the first biometric feature of different subjects. This yield ${}^{n}C_2$ impostor matching scores for the entire impostor matching attempt.

On the other hand, *decidability* [89] is another important metric in this research to indicate the separation between the genuine and impostor score distributions. Decidability (d') is a decision-making measurement that is determined based on the means and variances of the genuine and impostor score distributions. Given the genuine and impostor score distributions that are generated based on the FVC full matching protocol [163], the mean ($\mu_{\text{gen}},\ \mu_{\text{imp}}$) and variance ($\sigma_{\text{gen}}^2, \sigma_{\text{imp}}^2$) of the score distributions are first calculated. After that, the formula in [89] is followed to calculate the decidability d':

$$d' = \frac{|\mu_{\text{gen}} - \mu_{\text{imp}}|}{\sqrt{0.5\left(\sigma_{\text{gen}}^2 + \sigma_{\text{imp}}^2\right)}} \tag{5.3}$$

The higher d' is calculated when there is a high separation of the score distributions. Thus, it indicates a good decision environment for a biometric system when the computed d' is high [89].

Since randomly generated auxiliary information is involved in the tested cancellable biometric schemes and the proposed enhanced matching mechanism, each experiment is conducted up to 5 times with different sets of auxiliary information for a more precise reading of Equal Error Rate (EER) and decidability (d'). To be noted, each experiment is conducted under the worst-case assumption where the auxiliary information (e.g., transformation key $\mathbf{R}$ for cancellable transformation or permutation seed $\mathbf{P}$ for the proposed enhanced matching mechanism) is compromised by the adversary (stolen-token scenario). Hence, the same auxiliary information is shared among the subjects in each experiment. On the other hand, since the M·EFV hashing [Chapter 4] is a tokenless scheme, there is no stolen-token scenario. The experiments for M·EFV hashing are conducted by assuming every individual uses the pre-stored information to generate the query instance for matching, which is similar to the stolen-token scenario.

B. Dataset and feature extraction

This subsection shows the employed datasets and feature extraction methods in the experiments. For the fingerprint modality, six benchmarking datasets, i.e., *FVC2002 (DB1, DB2 and DB3)* [73] and *FVC2004 (DB1, DB2 and DB3)* [74] are employed. Each fingerprint subset consists of 100 subjects and 8 fingerprint images per subject. Fingerprint vector extraction technique originated from [62] is adopted to extract the fingerprint vector $\mathbf{x}_{\text{fingerprint}} \in \mathbb{R}^{1\times 256}$ from the fingerprint image. Given a fingerprint image, the fingerprint vector extraction processes are: (i) Extract the minutiae point set from the fingerprint image via the open-source tool, i.e., FingerJetFXOSE [166], (ii) Transform the extracted minutiae point set to Minutia Cylinder Code (MCC) descriptor [63] and (iii) KPCA-based learning is employed to convert the MCC descriptor to the fixed-length fingerprint vector $\mathbf{x}_{\text{fingerprint}} \in \mathbb{R}^{1\times 256}$. Since the adopted technique is a learning-based method, the first 3 fingerprint images per subject are employed for learning phase, while the remaining 5 fingerprint images are used to generate the fingerprint vector. Therefore, for each subset, a total of 500 (100×5) fingerprint vectors $\mathbf{x}_{\text{fingerprint}} \in \mathbb{R}^{1\times 256}$ are extracted.

For the face modality, this chapter employed the publicly available dataset, namely the *Labeled Faces in the Wild (LFW)* [84]. The LFW dataset consists of 13233 face images from 5749 subjects. To standardize the matching numbers for each subject in the matching protocol [163] as well as pairing with the FVC2004 dataset for experiments, the top 100 subjects with 5 face samples from the dataset are chosen as the testing set. The well-known face vector extraction technique, namely the FaceNet [36], is employed to extract the face vector $\mathbf{x}_{\text{face}} \in \mathbb{R}^{1\times 256}$ from the face image. Given the face image, FaceNet first employs the MTCNN [171] to crop and align the image into a 160×160 (pixel) image. After that, an end-to-end learning process is conducted to learn a real-valued vector $\mathbf{x}_{\text{face}} \in \mathbb{R}^{1\times 256}$ from the face image [36]. In this thesis, the face feature extraction is conducted using the pre-trained model that was trained based on the MS-Celeb-1M dataset [164]. The extraction and pre-trained model are adopted from David Sandberg's open-source implementation [165]. To sum up, a total of 500 face vectors $\mathbf{x}_{\text{face}} \in \mathbb{R}^{1\times 256}$ are extracted for the experiments.

For the iris modality, the *CASIA-IrisV3-Internal* dataset [52] is chosen for the experiment. This dataset is heavily used by existing cancellable biometrics works (e.g., [53], [94]). Briefly, this dataset contains 249 subjects with different amounts of iris images. To standardize the matching numbers for each subject in the matching protocol [163], the dataset is a subset by choosing the subjects with 7 left iris images. Therefore, a total of 868 iris images are used for generating the irisCode. This chapter adopts the irisCode extraction methods originated from [49], [50] to extract the irisCode $\mathbf{X}_{\text{iris}} \in [0,1]^{20\times 512}$. The table below tabulates the verification performance of the face, fingerprint and iris datasets that are examined based on the FVC full matching protocol [163]. Due to the fact that the extracted irisCode possesses an alignment issue, the pre-alignment matching approach from [144] is followed to obtain the optimal verification performance.

Table 5.2: Summary of verification performance for the unprotected biometric systems

Dataset	**EER (%)**
FVC2002 DB1	0.15
FVC2002 DB2	0.49
FVC2002 DB3	2.47
FVC2004 DB1	2.11
FVC2004 DB2	5.08
FVC2004 DB3	3.62
LFW	0.60
CASIA-IrisV3-Internal (± 16 bits shifting)	0.50

C. Targeted system

In the experiment, the proposed enhanced matching mechanism and formalized attack scheme are tested on several cancellable biometric schemes for different biometric modalities, including the Index-of-Max (IoM) hashing-based fingerprint system [66] and R·HoG-based iris system Chapter 3 and the M·EFV-based multimodal system Chapter 4. This subsection discusses the transformation process of the tested cancellable biometric schemes.

IoM Hashing [66]: Index-of-Max (IoM) Hashing [66] is one of the recently developed fingerprint cancellable biometric schemes. The core concept of IoM Hashing relies on the locality sensitive hashing (LSH)-based transformation that hashes the input fingerprint vector $\mathbf{x}_{\text{fingerprint}} \in \mathbb{R}^{1\times 256}$ into a set of independent integer hash codes, which is then used to form the cancellable template. Given a set of random projection matrices $\mathbf{P} = \{\mathbf{P}_1, \dots, \mathbf{P}_q\}$ where each $\mathbf{P}_i \in \mathbb{R}^{l_{\text{iom}} \times 256}$, the procedures to transform the $\mathbf{x}_{\text{fingerprint}} \in \mathbb{R}^{1\times 256}$ to the cancellable template $\mathbf{c} \in [0, l_{\text{iom}} - 1]^q$ are as below:

3) Project $\mathbf{x}$ onto a random sub-space and form a *projected vector* $\mathbf{v}_i \in \mathbb{R}^{l_{\text{iom}}}$ by computing $\mathbf{v}_i = \mathbf{x} \cdot \mathbf{P}_i$.

4) Record the index value which corresponds to the maximum value in the $\mathbf{v}_i$ as the IoM hashed code c_i:

$$c_i \ = \text{argmax}(\mathbf{v}_i) \tag{5.4}$$

where $\text{argmax}(.)$ is the argument maximum function.

Steps 1 and 2 are repeated for $i = 1 \dots q$ times until the $\mathbf{c} \in [0, l_{\text{iom}} - 1]^q$ is formed. This chapter considers the commonly used normalized Euclidean similarity as the matcher to quantify the similarity between a pair of cancellable templates. Given a pair of IoM cancellable templates ($\mathbf{c}$ and $\mathbf{c}'$), the similarity score S is computed as follow:

$$S = 1 - \frac{||\mathbf{c} - \mathbf{c}'||_2}{||\mathbf{c}||_2 + ||\mathbf{c}'||_2} \tag{5.5}$$

where $||.||_2$ is a norm function. In the IoM hashing, there are two parameters l_{iom} and q, with l_{iom} controls the value upper-bound of the $\mathbf{c}$ and q controls the dimension of the $\mathbf{c}$. According to [66], the parameters l_{iom} doesn't affect the EER of the protected system too much; thus, l_{iom} in this research is fixed at 16. Table below tabulates the EERs of the protected fingerprint system with different settings of q.

Table 5.3: EER of the protected fingerprint system under l_{iom} = 16 and different q in FVC2002 dataset

Parameter	Equal Error Rate (EER) (%)		
q	DB1	DB2	DB3
10	25.67	24.69	30.92
20	18.26	17.79	25.95
50	9.70	9.79	18.26
100	5.05	5.33	13.19
150	3.32	3.85	10.86
250	1.69	2.55	8.39
500	**0.70**	**1.66**	**6.17**

Other than the IoM hashing, the proposed matching mechanism and formalized attack scheme are also tested on the Random Augmented Histogram of Oriented Gradient (R·HoG) and Multimodal Extended Feature Vector (M·EFV) Hashing, which are introduced in Chapter 3 and Chapter 4. The former scheme is an alignment-robust iris template protection scheme that transforms unaligned irisCode into an alignment-robust cancellable template, while the latter scheme is a tokenless (face and fingerprint)-based multimodal template protection scheme that fuses the face and fingerprint vector into a single cancellable template. Cancellable templates for both schemes are generated with the best-tuned parameters as mentioned in Sections 3.4.2C (R·HoG) and 4.5.2D (M·EFV hashing).

Table 5.4 tabulates the summary of the verification performance for the R·HoG and M·EFV hashing. Other than that, the parameter settings of the tested cancellable biometric schemes are tabulated in Table 5.6. To be noted, some parameters are different for the original and enhanced schemes. In the experiments, the undersampling size (i.e., l and o) is fixed and the settings are listed in Table 5.5. It is noted that the undersampling process for the irisCode in R·HoG is carried out on the column vector-wise basis due to the iris alignment issue (refer to Chapter 3 for the alignment issue).

Table 5.4: Verification performance of M·EFV hashing and R·HoG with best-tuned parameters

Method	Dataset	Equal Error Rate (EER) (%)
M · EFV hashing [Chapter 4]	FVC2004 DB1 + LFW	0.38
	FVC2004 DB2 + LFW	0.78
	FVC2004 DB3 + LFW	0.66
R·HoG [Chapter 3]	CASIA V3	0.62

Table 5.5: Random undersampling size for the tested cancellable biometric schemes

Method	Random Undersampling Size	
	l	o
IoM hashing	1	100
R·HoG	15	512
M·EFV hashing	1	200

Table 5.6: Summary of the parameter setting for the tested cancellable biometric schemes

Parameter	Value
IoM Hashing	
q	500 (Without enhanced matching mechanism)
	o (With enhanced matching mechanism)
l_{iom}	16
M·EFV Hashing	
α	-
m	2
q	size of the input biometric vector (Without enhanced matching mechanism)
	o (With enhanced matching mechanism)
n_{MEFV}	55
s	1
k	3
β	3
R·HoG	
d	250 (Without enhanced matching mechanism)
	75 (With enhanced matching mechanism)
a	32
b	1
h	4
β	$\frac{d}{b}$ (Without enhanced matching mechanism)
	o_{RHOG} (With enhanced matching mechanism)

5.3.2 Performance evaluation and parameter estimation

This subsection presents the experimental result of selecting the best-tuned parameters for the proposed enhanced matching mechanism, i.e., number of local cancellable template n and local quantization threshold τ_L.

A. Effect of local quantization threshold τ_L

Recall the methodology, in the matching phase, a local matching is conducted between n numbers of the pre-stored cancellable templates and query templates to produce the local similarity score vector $\mathbf{s} \in \mathbb{R}^n$ where each $0 \leq s_i \leq 1$ and $i = 1 \dots n$. After that, each $s_i \in \mathbf{s}$ is quantized to 0 or 1 according to the parameter τ_L where the $s_i \geq \tau_L$ is quantized to 1 and $s_i < \tau_L$ is quantized to 0. Lastly, the final matching score s_{G} is calculated by averaging the quantized $\mathbf{s}$, i.e., $s_{\text{G}} = \frac{\sum_{i=1}^{n} s_i}{n}$. Since the s_{G} is calculated based on the quantized $\mathbf{s}$, the local quantization process is crucial towards the verification performance of the proposed enhanced matching mechanism. Specifically, inappropriate setting of the parameter τ_L could lead to the following unfavorable scenarios:

- **Scenario-1** (high value of τ_L): When the τ_L is tuned to a high value, each $s_i \in \mathbf{s}$ in the *genuine* comparison is hard to achieve the requirement of $s_i \geq \tau_L$; and hence resulting in the majority of the $s_i \in \mathbf{s}$ are quantized into 0. Subsequently, the value of the final matching score s_{G} for the genuine comparison is highly overlap with the impostor comparison. A high false rejection rate (FRR) and low decidability (d') could be observed in this scenario.

- **Scenario-2** (low value of τ_L): In the case that the τ_L is tuned to a low value, each $s_i \in \mathbf{s}$ in the *impostor* comparison could easily surpass the τ_L and then be quantized into 1, which results in the calculated s_{G} possesses a high value (close to the upper bound of the similarity score distribution). Therefore, the impostor score distribution is “shifted” to the right-side and overlaps with the genuine score distribution. An observation in this scenario could be a high false acceptance rate (FAR) and low decidability (d').

As mentioned above, inappropriate setting of τ_L could significantly affect the verification performance of the authentication process in terms of the FAR and FRR. Therefore, several experiments are conducted to evaluate the effect of τ_L towards the proposed enhanced matching mechanism and select a suitable setting of τ_L. In the experiments, the initial value of the τ_L is varying based on the tested schemes. To testify the effect of τ_L, several experiments are conducted by setting the τ_L with the interval of ± 0.1, while the n is fixed at 30. The remaining parameters are based on Table 5.6 and Table 5.5. Since the aforementioned reasonings emphasized the FAR and FRR in the system, the experiments focus on examining the effect of τ_L towards the FAR, FRR and d' of the system.

Experimental results for the tested cancellable biometric schemes are tabulated in the tables below. From the tabulated results, it is observed that the tested systems possess high FAR and low d' when the τ_L is set to a low value. This is expected from the reasoning above, where the impostor matching scores are averagely higher and skew to the genuine matching scores, which results in high overlapping between both score distributions. With the increment of the τ_L, it is observed that the FARs are greatly reduced. In the meantime, the FRRs are slightly increasing. However, the slight increment of FRRs is still acceptable to trade with the huge decrement of FAR. For instance, in the tested IoM-based fingerprint system in FVC2002 DB1, the system performance is changed from {FAR= 83.52%;

FRR=0.00%, $d' = 0.59$} to {FAR=0.24%; FRR=0.38%, $d' = 9.36$} when τ_L increased from 0.57 to 0.67. With the increment of τ_L, it is observed that the d' continues to be increased. However, when the τ_L is set too high, the FRRs start to increase. This is as expected where the local matching scores in the genuine comparison cannot surpass the τ_L and resulting in the final matching score of genuine comparison skew to the impostor comparison. From the results, it shows the inappropriate setting of τ_L could lead to scenario-1 and scenario-2 in the system. It is observed that $\tau_L = 0.67$ (for IoM hashing), $\tau_L = 0.62$ (MEFV hashing) and $\tau_L = 0.415$ (for RHoG) serve the best effect in enhancing the verification performance (EER) and decidability (d').

Table 5.7: Effect of different τ_L in IoM Hashing-based fingerprint system (FVC2002 dataset)

Parameters		False Acceptance Rate (FAR) (%)	False Rejection Rate (FRR) (%)	Decidability (d')
n	τ_L			
FVC2002 DB1				
30	0.57	83.52	0.00	0.59
	0.67	**0.24**	**0.38**	**9.36**
	0.77	0.00	21.96	1.35
FVC2002 DB2				
30	0.57	84.86	0.00	0.57
	0.67	**0.43**	**0.58**	**7.61**
	0.77	0.00	17.10	1.54
FVC2002 DB3				
30	0.57	83.51	0.66	0.56
	0.67	**5.49**	**4.30**	**3.75**
	0.77	0.00	49.46	0.88

Table 5.8: Effect of different τ_L in M·EFV Hashing-based multimodal system (FVC 2004 + LFW dataset)

Parameters		False Acceptance Rate (FAR) (%)	False Rejection Rate (FRR) (%)	Decidability (d')
n	τ_L			
FVC2004 DB1 + LFW				
30	0.52	0.31	0.07	4.74
	0.62	**0.13**	**0.17**	**9.15**
	0.72	0.01	9.33	1.82
FVC2004 DB2 + LFW				
30	0.52	0.31	0.30	4.65
	0.62	**0.31**	**0.33**	**6.25**
	0.72	0.00	17.53	1.56
FVC2004 DB3 + LFW				
30	0.52	0.48	0.23	4.45
	0.62	**0.24**	**0.27**	**7.46**
	0.72	0.00	13.50	1.73

Table 5.9: Effect of different τ_L in R·HoG-based iris system (CASIA v3 dataset)

Parameters		False Acceptance Rate (FAR) (%)	False Rejection Rate (FRR) (%)	Decidability (d')
n	τ_L			
30	$\mathbf{0.315}$	85.36	0.00	0.53
	$\mathbf{0.415}$	$\mathbf{0.50}$	$\mathbf{0.69}$	$\mathbf{7.00}$
	$\mathbf{0.515}$	0.00	50.79	0.91

B. Effect of parameter n

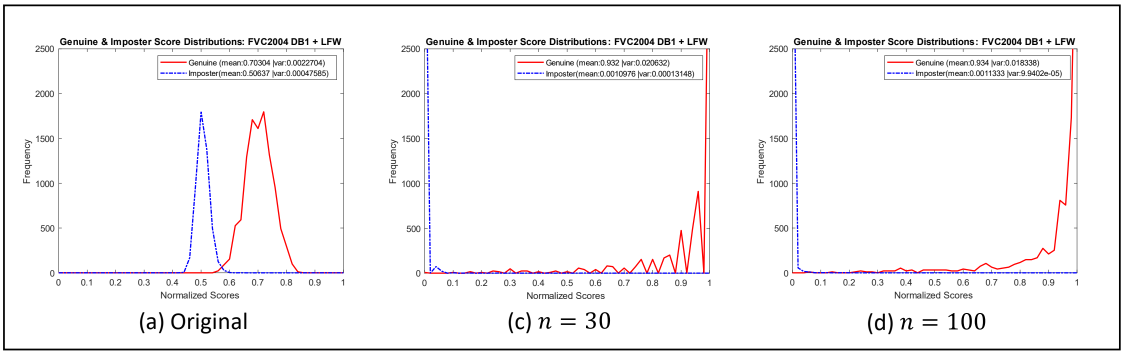
In the proposed enhanced matching mechanism, there are two phases: (i) transformation and (ii) matching. In transformation, multiple cancellable templates are generated from the input biometric feature and stored into the dataset. As such, in the matching phase, comparison between the query instances and the pre-stored cancellable template set will produce multiple local similarity scores, which are then be quantified into 0 or 1. The final matching score is calculated by averaging the quantized local scores. In the proposed matching mechanism, the parameter n is used to control the numbers of the generated cancellable templates as well as the numbers of the local similarity score produced in the matching phase. To examine the effect of n towards the decidability (d') and verification performance of the cancellable biometrics-enabled system, several experiments are conducted by setting the n from 1 until 100; while the parameter τ_{L} is fixed to the best-tuned setting acquired from the previous section. In the experiments, the cancellable templates are generated using the best-tuned parameters that are mentioned in Section 5.3.1C. It is noted that the proposed matching mechanism is merely a single-phase score quantization scheme when $n = 1$ since there is only 1 local similarity score produced. Thus, in the case that $n = 1$, the recognition performance of the system is easily affected by the local similarity score, especially the outlier in the genuine and impostor matchings (refer to the false rejection and false acceptance).

The experimental results for the targeted systems under different n are tabulated in the tables below. In addition, Fig 5.3 visualizes the genuine and impostor score distributions for the M·EFV hashing-based multimodal system under the cases of:

a) The cancellable biometric scheme is operated in its original construction.

b) The cancellable biometric scheme is enhanced by the proposed enhanced matching mechanism with parameter $n = 30$.

c) The cancellable biometric scheme is enhanced by the proposed enhanced matching mechanism with parameter $n = 100$.



(a) Original

(c) $n = 30$

(d) $n = 100$

Fig 5.3. Genuine and distribution score distributions for M·EFV Hashing-based multimodal system where (a) is the original construction, (b) is after being enhanced with $n = 30$ and (c) is after being enhanced with $n = 100$

From Fig 5.3, it is observed that the mean of genuine/ impostor score distributions are close to each other when the M·EFV hashing is not enhanced. After applying the proposed enhanced matching mechanism, the mean of genuine/ impostor score distributions is highly separated. In this sense, the proposed enhanced matching mechanism achieves the effect of improving decidability. From the tabulated results, it is observed that the EERs are starting at the highest point when $n = 1$. This is as expected where the final matching score s_G in single-phase score quantization $(n = 1)$ is directly calculated by quantizing one local matching score s_i where $i = 1$. In this case, the outlier(s) in the genuine and impostor comparisons could easily affect the verification performance of the system. It is observed that the increment of n leads to the higher separation between the genuine/ impostor score distributions (higher d') and better verification performance (lower EER) in the systems. This implies the parameter n is taking effect in enhancing the decision environment of the system in terms of EER and d'. The EERs and d's of the systems are improved significantly when n increased from 1 to 30. After that, the improvement of the decision environment is at a slower pace when $n > 30$. From the results, d' is observed to be increased alongside the increment of n. Throughout the experiments, it is observed that the $n = 100$ serves the best effect since the EER and d' are averagely desirable in every tested dataset. Therefore, $n = 100$ is concluded to be the best-tuned setting in the experiment.

Table 5.10: Effect of different n in IoM Hashing-based fingerprint system (FVC2002 dataset)

Parameters		Equal Error Rate (EER) (%)	Decidability (d')
τ_L	n		
FVC2002 DB1			
0.67	1	5.89	3.81
	5	1.73	6.96
	10	1.08	7.85
	15	0.77	8.56
	30	0.21	9.36
	50	0.17	9.65
	100	**0.13**	**10.30**
FVC2002 DB2			
0.67	1	6.48	3.56
	5	2.54	5.93
	10	1.29	6.62
	15	0.99	7.11
	30	0.50	7.61
	50	0.43	7.71
	100	**0.36**	**7.75**
FVC2002 DB3			
0.67	1	12.88	2.28
	5	6.79	3.27
	10	7.26	3.53
	15	4.94	3.61
	30	4.89	3.75
	50	4.31	3.78
	100	**2.91**	**3.84**

Table 5.11: Effect of different n in M·EFV Hashing-based multimodal system (FVC2004 + LFW dataset)

Parameters		Equal Error Rate (EER) (%)	Decidability (d')
τ_L	n		
FVC2004 DB1 + LFW			
0.62	1	3.58	5.12
	5	0.58	7.55
	10	0.29	8.80
	15	0.22	9.06
	30	0.15	9.15
	50	0.09	9.37
	100	**0.11**	**9.62**
FVC2004 DB2 + LFW			
0.62	1	5.66	3.96
	5	1.00	5.42
	10	0.82	6.01
	15	0.51	6.15
	30	0.32	6.25
	50	0.22	6.29
	100	**0.27**	**6.41**
FVC2004 DB3 + LFW			
0.62	1	4.75	4.42
	5	0.75	6.68
	10	0.81	6.82
	15	0.34	7.44
	30	0.25	7.46
	50	0.20	7.62
	100	**0.22**	**7.74**

Table 5.12: Effect of different n in R·HoG-based iris system (CASIA v3 dataset)

Parameters		**Equal Error Rate (EER) (%)**	**Decidability** (d')
τ_L	n		
0.415	1	7.37	4.41
	5	1.58	6.55
	10	0.85	7.34
	15	0.75	6.91
	30	0.59	7.00
	50	0.63	6.77
	100	**0.58**	**7.02**

C. Summary of parameter estimation

Throughout the parameter estimation process, several points are summarized:

- In the proposed enhanced matching mechanism, the parameter n is used to control the number of the local cancellable template generated as well as the number of the local scores. The proposed mechanism is merely a single-phase score quantization scheme when $n = 1$. In this case, the final matching score s_G is directly calculated by quantizing one local matching score s_i where $i = 1$. Therefore, the s_G can be highly affected by the outliner in the genuine or impostor comparison and result in low verification performance of the system where $n = 1$. The experimental results suggest the n to be tuned to a higher value to improve verification performance as well as the decidability of the system.

- τ_L is the parameter that controls the quantization process in the proposed enhanced matching. It is observed that the system possesses a high false acceptance rate (FAR) when τ_L is tuned to a lower value; while a high false rejection rate (FRR) is observed when τ_L is tuned too high. Therefore, selection of the τ_L should be very careful.

From the experiments, it is concluded that the n should be set higher to serve the best effect in improving the verification performance and decidability, while the τ_L is varied based on the tested system. The table below lists the best-tuned setting of the proposed enhanced matching mechanism for the tested cancellable biometric schemes.

Table 5.13: Best-tuned parameter setting of the proposed enhanced matching mechanism for the tested cancellable biometric schemes

Parameter	Value
IoM Hashing-based Fingerprint System	
n	100
τ_L	0.67
M·EFV Hashing-based Multimodal System	
n	100
τ_L	0.62
R·HoG-based Iris System	
n	100
τ_L	0.415

5.3.3 Verification performance and comparison

This subsection presents the verification performance and decidability of the proposed enhanced matching mechanism. A comparison of the system performance in terms of equal error rate (EER) and decidability (d') to the original counterparts (cancellable biometric schemes) is conducted for benchmarking purposes. The cancellable templates are generated using the best-tuned parameters listed in Table 5.6, and the proposed enhanced matching mechanism is operated using the best-tuned parameters (see Section 5.3.2C). In addition, the verification performance of the tested unimodal template protection schemes and the-start-of-the-art schemes are listed for benchmarking purposes. From the tabulated results, it is observed that:

- The EERs of the system after applying the proposed enhanced matching mechanism is averagely lower compared to the unenhanced system. Besides that, it is observed that the d' of the cancellable biometric schemes after applying the proposed matching mechanism is higher than the original construction of the tested schemes. This is attributed to the local quantization mechanism in the proposed scheme that enables the high separation between the mean of genuine/ impostor matching score distributions.

Table 5.14: Comparison of the EERs and d' in the system under (i) original construction and (ii) enhanced by the proposed enhanced matching mechanism

Method	**Subset**	**Similarity Metric**	**Equal Error Rate (EER) (%)**	**Decidability** (d')
(Unimodal Fingerprint) FVC2002 Dataset				
IoM Hashing [66]	DB1	Normalized Euclidean Similarity	0.70	4.34
	DB2		1.66	4.17
	DB3		6.17	2.82
IoM Hashing with proposed matching mechanism ($n = 100, \tau_{\mathrm{L}} = 0.67$)	DB1		**0.13**	**10.30**
	DB2		**0.36**	**7.75**
	DB3		**2.91**	**3.84**
(Unimodal Iris) CASIA-IrisV3 Dataset				
R·HoG [Chapter 3]	CASIA-IrisV3-Internal	Normalized Euclidean Similarity	0.62	3.47
R·HoG with proposed matching mechanism ($n = 100, \tau_{\mathrm{L}} = 0.415$)	CASIA-IrisV3-Internal		**0.58**	**7.02**
(Multimodal Fingerprint + Face) FVC2004 + LFW Dataset				
M·EFV hashing [Chapter 4]	DB1	Normalized Hamming Similarity	0.38	5.37
	DB2		0.78	4.68
	DB3		0.66	4.92
M·EFV hashing with proposed matching mechanism ($n = 100, \tau_{\mathrm{L}} = 0.62$)	DB1		**0.11**	**9.62**
	DB2		**0.27**	**6.41**
	DB3		**0.22**	**7.74**

Table 5.15: Comparison to the state-of-the-art unimodal fingerprint template protection scheme in FVC2002 dataset

Method	**Equal Error Rate (EER) (%)**		
	DB1	**DB2**	**DB3**
IoM Hashing without proposed matching mechanism [66]	0.70	1.66	6.17
IoM Hashing with proposed matching mechanism	**0.13**	**0.36**	**2.91**
Existing scheme			
$2\mathrm{P} - \mathrm{MCC}_{64,64}$ [126]	3.3	1.8	7.8
Bloom Filter [167]	2.3	1.8	6.6
Biohashing [24]	15	15	27
Yang *et al.* [168]	5.75	4.71	10.22
Wang and Hu [121]	3.5	–	–
Wang and Hu [122]	2	–	–

Table 5.16: Comparison to the state-of-the-art unimodal iris template protection scheme in CASIA v3 dataset

Method	Pre-alignment	Total Iris Images Used	EER (%) without protection	EER (%) with protection
R·HoG with proposed matching mechanism	Not required	**868** (Left eye)	**0.50**	**0.58**
IFO Hashing [53]	**Required**	868 (Left eye)	0.38	0.54
BioEncoding [103]	**Required**	740	6.02	6.27
Dwivedi *et al.* [110]	**Required**	2639	0.39	0.43
Bin-Combo [18]	Not required	1332 (Left eye)	0.81	4.41
Adaptive Bloom Filters [54]	Not required	1332 (Left eye)	1.19	1.14
Lai *et al.* [114]	Not required	868 (Left eye)	0.38	0.69

5.3.4 System threshold with respect to Genuine Acceptance Rate

This subsection reports the system threshold τ_{G} for each tested dataset with respect to the Genuine Acceptance Rate (%). The τ_{G} is used for estimating the attack success rate in Section 5.5.2C. It is noted the τ_{G} may varies due to the randomization effect (auxiliary data) of cancellable biometrics.

Table 5.17: System threshold τ_{G} of IoM hashing-based fingerprint system with respect to Genuine Acceptance Rate (%) in FVC2002 dataset

	Genuine Acceptance Rate (%)	System threshold τ_{G}
FVB2002 DB1		
Without enhanced matching mechanism	95%	0.6855
	90%	0.6950
	85%	0.7034
With enhanced matching mechanism	95%	0.6900
	90%	0.8000
	85%	0.8700
FVB2002 DB2		
Without enhanced matching mechanism	95%	0.6752
	90%	0.6907
	85%	0.7021
With enhanced matching mechanism	95%	0.5400
	90%	0.7400
	85%	0.8500
FVB2002 DB3		
Without enhanced matching mechanism	95%	0.6428
	90%	0.6544
	85%	0.6639
With enhanced matching mechanism	95%	0.1600
	90%	0.3200
	85%	0.4500

Table 5.18: System threshold τ_G of R·HoG-based fingerprint system with respect to Genuine Acceptance Rate (%) in CASIAv3 dataset

	Genuine Acceptance Rate (%)	**System threshold** τ_G
Without enhanced matching mechanism	95%	0.4021
	90%	0.4151
	85%	0.4219
With enhanced matching mechanism	95%	0.4700
	90%	0.7000
	85%	0.8000

Table 5.19: System threshold τ_G of M·EFV hashing-based multimodal system with respect to Genuine Acceptance Rate (%) in FVC2004+LFW dataset

	Genuine Acceptance Rate (%)	**System threshold** τ_G
FVC2004 DB1+LFW		
Without enhanced matching mechanism	95%	0.6251
	90%	0.6472
	85%	0.6563
With enhanced matching mechanism	95%	0.6400
	90%	0.8000
	85%	0.8700
FVC2004 DB2+LFW		
Without enhanced matching mechanism	95%	0.6050
	90%	0.6214
	85%	0.6343
With enhanced matching mechanism	95%	0.4100
	90%	0.6000
	85%	0.7100
FVC2004 DB3+LFW		
Without enhanced matching mechanism	95%	0.6180
	90%	0.6355
	85%	0.6501
With enhanced matching mechanism	95%	0.5300
	90%	0.7000
	85%	0.8000

5.3.5 Computation efficiency

Recall the methodology of the proposed enhanced matching mechanism, it involves multiple rounds of local cancellable template generation and local matching in which the computation overhead is increasing. This indicates the proposed mechanism is trading a certain level of computation efficiency for enhancing the decision environment. In this subsection, the time complexity of the cancellable biometric schemes after being enhanced by the proposed enhanced matching mechanism is examined to show the practicability of adapting the enhanced matching mechanism in a real-world application. In the experiment, the time complexity is tested in terms of the processing time required for the enrollment and verification stages. The table below tabulates the processing time for each tested cancellable biometric scheme. From the tabulated results, it is observed the processing times of the enrollment stage are averagely higher than the verification stage. This is mainly due to the auxiliary data generation overhead in the enrollment stage. Nevertheless, it is a one-time process for the enrollment process. Other than that, a varying processing time is observed for different tested cancellable biometric schemes, which is mainly due to the (i) size of the input biometric template and (ii) complexity of the transformation function. Among the tested schemes, R·HoG requires the longest processing time for both stages, and this is mainly due to the high computation overhead in calculating the partitioned row and column during the transformation process (see Section 3.3.2A). Overall, the processing time for the cancellable biometric schemes after being enhanced by the proposed enhanced matching mechanism is acceptable.

Table 5.20: Time complexity of the cancellable biometric scheme after being enhanced with the proposed enhanced matching mechanism

Scheme	Time Complexity (Sec)				
	Experiment 1	Experiment 2	Experiment 3	Experiment 4	Average
Enrollment stage					
IoM Hashing	0.5016	0.5926	0.5827	0.5861	0.5658
R·HoG	1.3670	1.4535	1.3865	1.3960	1.4008
M·EFV hashing	0.5495	0.4811	0.4441	0.4605	0.4838
Verification stage					
IoM Hashing	0.1441	0.1288	0.1320	0.1324	0.1343
R·HoG	1.4423	1.3939	1.3944	1.3113	1.3855
M·EFV hashing	0.2368	0.2446	0.2271	0.2567	0.2413

5.3.6 Discussion on Attack via Record Multiplicity (ARM)

This section discusses the feasibility for the adversary to recover the original biometric input $\mathbf{X}$ from the compromised information, i.e., cancellable template set $\mathbf{C}$ and auxiliary data $\{\mathbf{P}, \mathbf{R}\}$ based on the Attack via Record Multiplicity (ARM) [168], [169]. ARM refers to the dreadful privacy attack that aims to recover the original biometric input $\mathbf{X}$ from multiple cancellable templates and the auxiliary data. The proposed enhanced matching mechanism can be referring as a Single Input Multiple Output (SIMO) model that takes one biometric template $\mathbf{X}$ as input, and then produce the cancellable template set $\mathbf{C} = \{\mathbf{C}_1, \mathbf{C}_2, \ldots . \mathbf{C}_n\}$. Therefore, one might worry about the case that the $\mathbf{C}$ from one or multiple applications are compromised for the ARM attack. A simple view of the transformation phase in the proposed enhanced matching mechanism is provided to leverage the analysis. Given an original biometric template $\mathbf{X}$, the proposed enhanced matching mechanism first random undersampling the $\mathbf{X}$ into an intermediate product, so-called the permuted biometric feature $\mathbf{V} = \{\mathbf{V}_1, \dots, \mathbf{V}_n\}$ where $\mathbf{P} = \{\mathbf{P}_1, \dots, \mathbf{P}_n\}$ is the permutation seed set. Due to the randomization effect of the random undersampling process, the $\mathbf{V}_i$ are independent of each other. After that, the cancellable transformation function is applied to each $\mathbf{V}_i$ to produce the local cancellable template $\mathbf{C}_i$ where the $\mathbf{R}_i$ refers to the auxiliary data for the cancellable biometric scheme. In short, $\mathbf{V} = \{\mathbf{V}_1, \dots, \mathbf{V}_n\}$ and the $\mathbf{R} = \{\mathbf{R}_1, \dots, \mathbf{R}_n\}$ are transformed to the cancellable template set $\mathbf{C} = \{\mathbf{C}_1, \dots, \mathbf{C}_n\}$. With the random undersampling process, each $\mathbf{V}_i$ is partial information of $\mathbf{X}$ and hence, each $\mathbf{C}_i$ is uncorrelated to each other. At the end of the enrollment phase, the intermediate product, i.e., the $\mathbf{V}$ is deleted and never stored in the system.

With the randomization effect of the cancellable biometric scheme and random undersampling process (generation of the $\mathbf{V}$), each $\mathbf{C}_i$ is unlikely to collide with each other, and hence, the feasibility of recovering the original biometric template could be deduced back to the irreversibility property of the IoM hashing, M·EFV hashing and R·HoG. The reader is encouraged to refer to Section 3.5.1B (R·HoG), Section 4.6.1B (M·EFV hashing) and [66] (IoM hashing) for the comprehensive discussion on the biometric template inversion analysis and unlinkability analysis for the respective scheme. While guaranteed by the irreversibility of the cancellable biometric scheme and the disposable intermediate product $\mathbf{V} = \{\mathbf{V}_1, \dots, \mathbf{V}_n\}$, it is infeasible for the adversary to obtain the original biometric feature $\mathbf{X}$ via ARM. It is also noted that the auxiliary date, i.e., $\mathbf{P}$ and $\mathbf{R}$ should not be re-used to prevent the collision of $\mathbf{C}$ and $\mathbf{C}'$ in different applications.

5.4 Authentication attack

Another part of this chapter is the type-4 (authentication) attack in the biometric template protection. In biometric template protection, authentication attack refers to a scenario where the adversary tries to gain illegal access to the system by means of guessed biometric input. To be noted, this is not a biometric template recovery attack where the guessed biometric input does not resemble the original biometric input. Therefore, a decent biometric template protection scheme could block the access of the adversary by renewing the cancellable template. Yet, an efficient authentication attack is still unfavorable. In this section, a practical authentication attack, namely the Whale Optimization Algorithm-based Authentication Attack (WO3A) is formalized and simulated on the tested cancellable biometric schemes.

5.4.1 Preliminary - Whale optimization algorithm (WOA)

This section discusses the preliminary work on which the formalized attack scheme is built upon. In this work, the whale optimization algorithm (WOA) [100] is selected as the modification scheme to modify the guessed biometric template due to the simplicity of implementation. On the other hand, the formalized attack scheme can employ other optimization algorithms as well. Nevertheless, the intuition of formalizing the attack scheme is to evaluate the security resistance of the biometric system towards this type of automated attack scheme. Whale optimization algorithm (WOA) is a relatively new population-based optimization algorithm introduced by Mirjalili and Lewis [100] that mimics the humpback whales' predation behavior. The underlying concept of WOA relies on the unique bubble-net foraging method to find the optimal solution within the search space. The classical WOA is built upon *exploitation* and *exploration* phases, which are briefly discussed in the following subsections.

A. Encircling prey

Suppose $\mathbf{X}$ as each search agent within the search space, the WOA aims to search for the optimal solution $\mathbf{X}^*$ within the search space through iteratively updating the $\mathbf{X}$s and $\mathbf{X}^*$. In each iteration, the WOA first determines the $\mathbf{X}^*$ and then updates each $\mathbf{X}$ based on the *exploitation* and *exploration* phases. The coefficient A is used to decide the phase to be employed in each iteration. When $||A|| < 1$, the WOA gets into the exploitation phase and updates the $\mathbf{X}$ where the A is generated by computing $A = 2vw - v$ where w is a random value fallen within $[0,1]$, $v = (2 - t \cdot \frac{2}{t_{\max}})$, t refers to the current iteration and $t_{\max}$ is the maximum iteration for the searching attempt. Exploitation can be divided into two processes: encircling prey and bubble-net attack. In the encircling prey mechanism, each $\mathbf{X}$ is updated by computing

$$\mathbf{X}(t+1) = \mathbf{X}^*(t) - A \cdot D \tag{5.6}$$

where $t = 1,2, \dots t_{\max}$ indicate the t-th iteration and $t_{\max}$ is the maximum iteration, A and C are the coefficients. C and D are calculated as follow

$$C = 2 \cdot w \tag{5.7}$$

$$D = ||C \cdot \mathbf{X}^*(t) - \mathbf{X}(t)|| \tag{5.8}$$

B. Exploitation phase – Bubble net attack

In bubble net attack, the $\mathbf{X}$ is updated by computing $\mathbf{X}(t+1) = D' \cdot e^{yl} \cdot \cos(2\pi l) + \mathbf{X}^*(t)$ where $D' = ||\mathbf{X}^*(t) - \mathbf{X}(t)||$ denote the distance between the $\mathbf{X}$ and $\mathbf{X}^*$, $y = 1$ is a constant value, and l is randomly chosen between $[-1,1]$. Since the exploitation phase consists of two different processes, WOA uses a probability variable p that is randomly chosen from $[0,1]$ to select the process to update the $\mathbf{X}$. In short, the mathematical model of the exploitation phase is described as follow:

$$\mathbf{X}(t+1) = \begin{cases} \mathbf{X}^*(t) - A \cdot D, & p \leq 0.5 \\ D' \cdot e^{yl} \cdot \cos(2\pi l) + \mathbf{X}^*(t), & \text{otherwise} \end{cases} \tag{5.9}$$

where $p \in [0,1]$ is a random number that represents the probability factor.

C. Exploration phase – Prey searching

Lastly, in the case that $||A|| \geq 1$, the exploration phase is employed to modify each $\mathbf{X}$. The motivation of the exploration phase is to diversify the search space and reduce the local optimal problem [100]. Specifically, each $\mathbf{X}$ is updated by computing

$$\mathbf{X}(t+1) = \mathbf{X}_{\text{rand}}(t) - A \cdot ||C \cdot \mathbf{X}_{\text{rand}}(t) - \mathbf{X}(t)|| \tag{5.10}$$

where $t = 1 \ldots t_{\max}$ indicate the t-th iteration and $\mathbf{X}_{\text{rand}}(t)$ is a random position vector for the agent randomly selected from the current population.

5.4.2 Formalized attack scheme – WO3A

This subsection presents the formalized authentication attack: Whale Optimization Algorithm-based Authentication Attack (WO3A).

A. Overview of attack scheme

In this section, an optimization algorithm-based authentication attack, namely the Whale Optimization Algorithm-based Authentication Attack (WO3A) is formalized to attack the cancellable biometrics-enabled system and testify the effect of the proposed enhanced matching mechanism. The main motivation of adopting the whale optimization algorithm (WOA) [100] in the WO3A is that there are fewer parameters to be tuned since most of the parameters in the WOA are randomly generated. The essence of this attack scheme is that it is an automated attack framework that is not based on the manual perturbation of the guessed biometric template during the attack. Thus, the formalized WO3A offers a certain level of efficiency in attacking the system as compared to the manual hill-climbing approach.

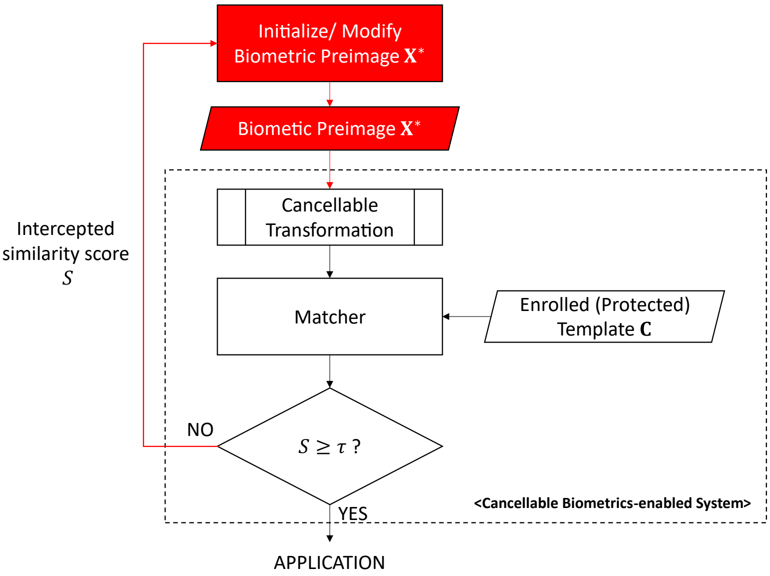

Initialize/ Modify Biometric Preimage $\mathbf{X}^*$
Biometic Preimage $\mathbf{X}^*$
Cancellable Transformation
Intercepted similarity score S
Matcher
Enrolled (Protected) Template $\mathbf{C}$
NO
$S \geq \tau$?
YES
<Cancellable Biometrics-enabled System>
APPLICATION

Fig 5.4. Overview of the formalized attack framework

The formalized attack is a type-4 attack that is cast as an authentication attack that aims to gain illegal access to the system by means of guessed biometric preimage $\mathbf{X}^*$ where the $\mathbf{X}^*$ is not the same as the original biometric input $\mathbf{X}$.

Attack scenario: Assuming a scenario where the adversary knows the auxiliary data $\mathbf{R}$ that is corresponding to the victim cancellable template $\mathbf{C}$, the adversary tries to gain illegal access to the system. The adversary attempts to use WO3A guess a suitable biometric preimage $\mathbf{X}^*$ that can be used to generate a fake cancellable template $\mathbf{C}^*$ such that the similarity between the victim's pre-stored cancellable template $\mathbf{C}$ can surpass the system threshold τ. It is noted that the estimated $\mathbf{X}^*$ is not sufficient for a replay attack where the renewal of the cancellable template $\mathbf{C}$ could block the access. This is because the estimated $\mathbf{X}^*$ is not similar to the original $\mathbf{X}$. Yet, an efficient type-4 attack could lead to serious issues, especially when the user could not renew the cancellable template in the given time.

Instead of using a manual hill-climbing approach to update the $\mathbf{X}^*$ (e.g., perturb fixed numbers of elements in $\mathbf{X}^*$ in each attack iteration), an optimization algorithm is employed. In this section, a Whale Optimization Algorithm (WOA) inspired attack scheme, namely the Optimization Algorithm Authentication Attack (WO3A) is formalized. In essence, the formalized WO3A is an iterative modification scheme that is formed by three main processes (see Fig 5.4):

1) Assuming the adversary knows the template format of the input biometric feature set (e.g., feature dimension, value type and distribution) based on his own feature, n numbers of guessed biometric template $\mathbf{X}'$s are first initialized where the value of each $\mathbf{X}'_i$ is randomly generated based on the value distribution determined and $i = 1 \dots u$. Other than that, the attack scheme is able to intercept the matching score S from the system.

2) u numbers of $\mathbf{X}'$s are iteratively inputted to the cancellable biometrics-enabled system to have the query cancellable templates $\mathbf{C}'$s to be generated. After that, the generated $\mathbf{C}'$s are matched to the pre-stored cancellable template $\boldsymbol{c}$, and n numbers of matching scores s are returned to the attack framework.

3) Update the best biometric preimage $\mathbf{X}^*$ based on the similarity score returned. To be noted, biometric preimage $\mathbf{X}^*$ is the best instance (highest similarity score) chosen from $\mathbf{X}'$s. After that, perturb each $\mathbf{X}'_i \in \mathbf{X}'$ via the modification scheme in the WO3A.

B. Detailed approach

In this subsection, the details of the formalized Whale Optimization Algorithm-based Authentication Attack (WO3A) are explained. The WO3A is a new variation of the well-known Whale Optimization Algorithm [100] that can be cast as an authentication attack towards the biometric system. Since WO3A is an optimization algorithm-driven scheme, the cancellable transformation and comparison are used to mimic the objective function evaluation. A simple view of the transformation and comparison are explained as below:

- **Cancellable transformation and comparison:** The guessed biometric template $\mathbf{X}'$ is transformed via the targeted cancellable biometric scheme and the resultant cancellable template $\mathbf{C}'$ is matched to the pre-stored cancellable template $\mathbf{C}$ from the template storage using the system matcher (e.g., canonical Cosine similarity or the proposed enhanced matching mechanism). Lastly, a normalized similarity score s is returned as the matching result.

Other than that, two new mechanisms: the uni-step binarization and adaptive mutation, are introduced in the WO3A to expand the genericity of the attack scheme and improve the attack efficiency. The mechanisms are explained as below:

- **Uni-step binarization function:** Since the classical Whale Optimization Algorithm [100] is designed for finding the optimal solution in a real-valued space, it is not suitable for the cancellable biometrics-enabled system that requires binarized input. To increase the genericity of the attack framework, the uni-step binarization function is applied to allow the WO3A to produce the binarized instance and input it into the cancellable transformation function for the attack attempt.

- **Adaptive mutation mechanism:** It is noticed from the literature that the classical Whale Optimization Algorithm suffers from slow convergence when dealing with high dimension data [172]. To accelerate the efficiency of the WO3A for obtaining a $\mathbf{X}^*$ with high s^*, an adaptive mutation mechanism is applied to further diversify guessed biometric templates $\mathbf{X}'$ after the modification process in each attack iteration. Specifically, the mutation mechanism choose a random portion from each $\mathbf{X}_i'$ and random scrambling it where $i = 1 \dots u$ indicates the i-th guessed template in $\mathbf{X}'$. To prevent the randomization effect of the mutation dominating the WO3A, the mutation occurs with the possibility that is bounded between 0.2 (or 20%) and 0.5 (or 50%).

Suppose a cancellable transformation $f(\mathbf{X}, \mathbf{R}) \rightarrow \mathbf{C}$ where $\mathbf{X} \in \mathbb{R}^{a \times b}$, $\mathbf{R} \in \mathbb{R}^{q \times e}$, $\mathbf{C} \in \mathbb{R}^{k \times m}$ respectively represent the input biometric feature, auxiliary data and the produced cancellable template, the formalized attack scheme is a population-based iterative modification scheme that aims to find a $\mathbf{X}^* \in \mathbb{R}^{a \times b}$ such that $f(\mathbf{X}^*, \mathbf{R}) \sim f(\mathbf{X}, \mathbf{R})$. Consider a worst-case scenario where the adversary compromised the auxiliary data $\mathbf{R} \in \mathbb{R}^{d \times e}$, the adversary first randomly generates a population of guessed templates $\mathbf{X}' = \{\mathbf{X}'_1, \mathbf{X}'_2, \dots, \mathbf{X}'_u\}$ where each $\mathbf{X}'_i \in \mathbb{R}^{a \times b}$ is randomly generated and $i = 1 \dots u$. Then, the procedures below are followed to obtain the $\mathbf{X}^* \in \mathbb{R}^{a \times b}$:

1) **Cancellable transformation and comparison**: Each of the $\mathbf{X'}_i$ and $\mathbf{R}$ are iteratively injected into the system for comparison and the similarity score s_i is intercepted where $i = 1 \dots u$ indicated the i-th guessed template from the population. In particular, each $\mathbf{X'}_i$ and $\mathbf{R}$ are first inputted to the cancellable transformation function $f(.)$ to have the query cancellable template $\mathbf{C'}_i$ to be generated. If the $f(.)$ requires binarized input, the uni-step binarization function is applied to generate the binarized instance $\ddot{\mathbf{X}}'_i$ of $\mathbf{X'}_i$ and use it as the input for the cancellable transformation function. The binarized instance $\ddot{\mathbf{X}}'$ is formed by computing each $\ddot{x}'_{ij} \in \ddot{\mathbf{X}}'$ as below

$$\ddot{x}'_{ij} = \begin{cases} 0, & x'_{ij} < 0 \\ 1, & x'_{ij} \geq 1 \end{cases} \tag{5.11}$$

where $i = 1 \dots a$ and $j = 1 \dots b$. After that, the $\mathbf{C'}_i$ is compared to the pre-stored cancellable template $\mathbf{C}$ using the system matcher. The similarity score s_i is intercepted by the attack scheme and stored into a score vector $\mathbf{s}$.

2) **Best template selection**: Given the population of guessed templates $\mathbf{X}' = \{\mathbf{X'}_1, \mathbf{X'}_2, \dots, \mathbf{X'}_u\}$ and the score vector $\mathbf{s} = [s_1, s_2, \dots, s_u]$, the $\mathbf{X}^* \in \mathbb{R}^{a \times b}$ is selected. If the current attack iteration is the first iteration, the $\mathbf{X'}_i$ with the best similarity score s_i is set as $\mathbf{X}^*$ where $i = \text{idxmax}(\mathbf{s})$ and $\text{idxmax}(.)$ denote the function to determine the index value of the maximum value in the input vector ($\mathbf{s}$ in this context). For the remaining attack iterations, a comparison between the similarity scores of the $\mathbf{X}^*$ and $\mathbf{X'}_i$, i.e., the s^* and s'_i. If $s'_i \geq s^*$, update the $\mathbf{X}^*$ by setting $\mathbf{X}^* = \mathbf{X'}_i$. To be noticed, the s^* is recorded for comparison purposes. If the $s^* \geq \tau$, the attack scheme immediate stops the process and returns the $\mathbf{X}^*$ and the s^* as a result.

3) **Perturbation of the guessed templates**: In this step, each of the $\mathbf{X'}_i \in \mathbf{X}$ is perturbed to diversify the search space ($\mathbf{X}$) so that the formalized WO3A able to efficiently find $\mathbf{X}^*$ with higher s^*. In the formalized attack scheme, the modification scheme from the Whale Optimization Algorithm [100] is adopted as the primary process to perturb the guess biometric templates. Briefly, there are two types of perturbation process in [100]: *exploitation* and *searching* in this step. Two coefficients, i.e., A and C are used to decide the type of perturbation in each iteration of attack. Given a w that is randomly chosen

between [0,1] and $v = (2 - t\frac{2}{t_{\max}})$ where t refer to the t-th attack iteration, A is calculated as $A = 2vw - v$, while $C = 2w$. When $||A|| \geq 1$, *searching* is carried out to perturb each $\mathbf{X'}_i \in \mathbf{X}$ where $i = 1 \dots u$. In *searching*, each $\mathbf{X'}_i$ is computed as

$$\mathbf{X'}_i = \mathbf{X}'_{\mathrm{rand}} - A \cdot ||C \cdot \mathbf{X}'_{\mathrm{rand}} - \mathbf{X'}_i|| \tag{5.12}$$

where $\mathbf{X}'_{\mathrm{rand}}$ is randomly chosen from the guessed templates $\mathbf{X}' = \{\mathbf{X'}_1, \mathbf{X'}_2, \dots, \mathbf{X'}_u\}$**.** On the other hand, *exploitation* is conducted to perturb each $\mathbf{X'}_i \in \mathbf{X}$ when $||A|| < 1$. In *exploitation*, the perturbation process is controlled by the parameter p which is randomly generated from [0,1]. Specifically, each $\mathbf{X'}_i \in \mathbf{X}$ is computed as:

$$\mathbf{X'}_i = \begin{cases} \mathbf{X}^* - A \cdot D, & p \leq 0.5 \\ D' \cdot e^{yl} \cdot \cos(2\pi l) + \mathbf{X}^*, & \text{otherwise} \end{cases} \tag{5.13}$$

where $D = ||C\mathbf{X}^* - \mathbf{X'}_i||$, $y = 1$ and l is randomly chosen from $[-1,1]$.

4) **Adaptive mutation mechanism**: To prevent the bottleneck of updating the $\mathbf{X}^*$ (or maximizing the s^*), an adaptive mutation mechanism is introduced to further diversify the $\mathbf{X}' = \{\mathbf{X'}_1, \mathbf{X'}_2, \dots, \mathbf{X'}_u\}$. Given a mutation possibility $p_m = 0.2$, a random value between $\ddot{p}_m \in [0,1]$ if first generated. If $\ddot{p}_m \geq p_m$, the random scrambling process is applied to each $\mathbf{X'}_i \in \mathbf{X}'$ where the random portion of the $\mathbf{X'}_i$ is scrambled instead of the entire $\mathbf{X'}_i$. Rather than perturbing the $\mathbf{X'}_i$ based on a fixed p_m, the mutation mechanism increase the p_m when the $\mathbf{X}^*$ is not updated for 10 attack iterations, with 0.02 per increment. The maximum p_m is 0.5. This is to prevent the modification of $\mathbf{X}'$ from being dominated by the random scrambling process.

Repeat steps $1 - 4$ until the stopping criteria are met. The criteria can be either (i) maximum attack iteration $t_{\max}$ is reached or (ii) the similarity score (s^*) of the $\mathbf{X}^*$ can surpass the system threshold τ ($s^* \geq \tau$).

5.5 Attack simulation and discussions

In this section, several experiments are conducted to testify the effect of the formalized WO3A towards the tested cancellable biometric schemes (with and without the proposed enhanced matching mechanism).

5.5.1 Attack model and matching protocol

The attack model of the WO3A is formulated to leverage the experiment in the following subsections. Suppose a cancellable biometric transformation function $f(.)$ that transform the biometric feature $\mathbf{X}$ and auxiliary data $\mathbf{R}$ (or transformation key) into the cancellable template $\mathbf{C}$, in which $f(\mathbf{X}, \mathbf{R}) \rightarrow \mathbf{C}$, the attack model of the formalized attack scheme is explained as below:

- **Attack scenario:** The adversary aims to gain illegal access to a targeted system with the victim's auxiliary data $\mathbf{R}$ and estimated biometric preimage $\mathbf{X}^*$. Consider a worst-case scenario, the system is very weak in the sense that it is not protected against malicious software, i.e., the formalized WO3A.

- **Adversary's goal**: In the attack attempt, the adversary aims to find a biometric preimage $\mathbf{X}^*$ (or guessed biometric template) that can produce a fake cancellable template $\mathbf{C}^*$, such that the similarity score between the $\mathbf{C}'$ and victim's pre-stored cancellable template $\mathbf{C}$ could surpass the system matching threshold τ. To be noted, the guessed biometric preimage is not required to be the same as the original biometric input ($\mathbf{X}^* \neq \mathbf{X}$).

- **Adversary's knowledge**: The adversary knows the template format of the input biometric feature $\mathbf{X}$, including the feature dimension, value type, value distributions. The adversary does not know about the details of the cancellable biometric scheme that is implemented in the system and the cancellable template $\mathbf{C}$. Assume it is a worst-case scenario where the auxiliary data $\mathbf{R}$ for cancellable transformation is compromised/ accessible to the adversary.

- **Adversary's capability**: The adversary can access the input interface of the cancellable biometric scheme to inject the guessed biometric template $\mathbf{X}^*$ to the system. Other than that, the adversary is able to intercept the matching score s (or s_{G} for the enhanced matching mechanism) for each comparison. Assuming the system is still secure in the sense that the transformation function and template storage is not compromised, the pre-stored cancellable templates are inaccessible to the adversary.

To simulate the attack scenario, the below attack matching attempt is followed when attacking the system:

- **Attack matching attempt:** The attack scheme repeatedly produce a biometric preimage $\mathbf{X}^*$ and input the $\mathbf{X}^*$ to the cancellable biometric scheme for authentication. Each attempt is halted when the stopping criteria of the attack scheme are met: (i) matching score S surpass the system threshold τ_{G} or (ii) the maximum attack iteration $t_{\max}$ is met.

Throughout the attack matching attempt in the tested dataset, the matching scores are used to form the attack score distribution. Since the objective of the attack is to gain illegal access to the system, the *genuine* and *attack* score distributions should be highly overlapped to show the effectiveness of the attack framework. The reader may refer to section 5.3.1A for the procedure to generate genuine and impostor score distributions.

A. Security evaluation criteria, parameter control and dataset selection

In this subsection, a definition is formulated for evaluating the security resistance of the tested cancellable biometric scheme and proposed an enhanced matching mechanism. Other than that, the WO3A attack parameters and database section for the experiment are also outlined.

Given an observation set with α number of subjects, each with β numbers of cancellable biometric templates (samples). To be noted, $M = \alpha * \beta$ denotes the total number of samples in the observation set. The security resistance is determined by the False Acceptance Rate (FAR) (or success rate) that is calculated from the attack score distribution and genuine score distribution. In each attack attempt, the adversary utilizes the WO3A and attempts to guess and inject a fake input biometric feature $\mathbf{X}^*$ to the system until the maximum attack iteration ($t_{\max}$) is met. Based on the statement above, a definition is formulated for the security assessment.

Definition 5.1: Among M targeted sample (cancellable template), we could say the scheme is $(t_{\max}, r)$-secure if the adversary can launch WO3A attack with a success rate equal to r within $t_{\max}$, where $r * M$ is equal to the numbers of succeeding attacked samples with respect to the system threshold τ_{G}.

WO3A Parameter setting: Recall the methodology of the WO3A, there are three tunable parameters, i.e., u, $t_{\max}$, τ_{G}. For a fair comparison between the tested cancellable biometric schemes and the proposed enhanced matching mechanism, the WO3A is operated with the same setting, with the $u = 5$, $t_{\max} = 500$. $t_{\max}$ and u are limited for the computation time of an authentication attack in a real-world scenario. The parameter τ_{G} is set to 1 for observing the security resistance of the tested cancellable biometric scheme and proposed enhanced matching mechanism throughout each attack attempt.

Dataset selection: To improve the comparison efficiency, a subset is created from each data set to form the observation set. This is done by randomly choosing 10 subjects, each with 3 biometric samples. Therefore, each attack experiment is conducted on the subset that is extracted from FVC2002, FVC2004, LFW and CASIAv3. A total of 30 genuine matching scores. 45 impostor matching scores and 30 attack matching scores are generated for each attack experiment.

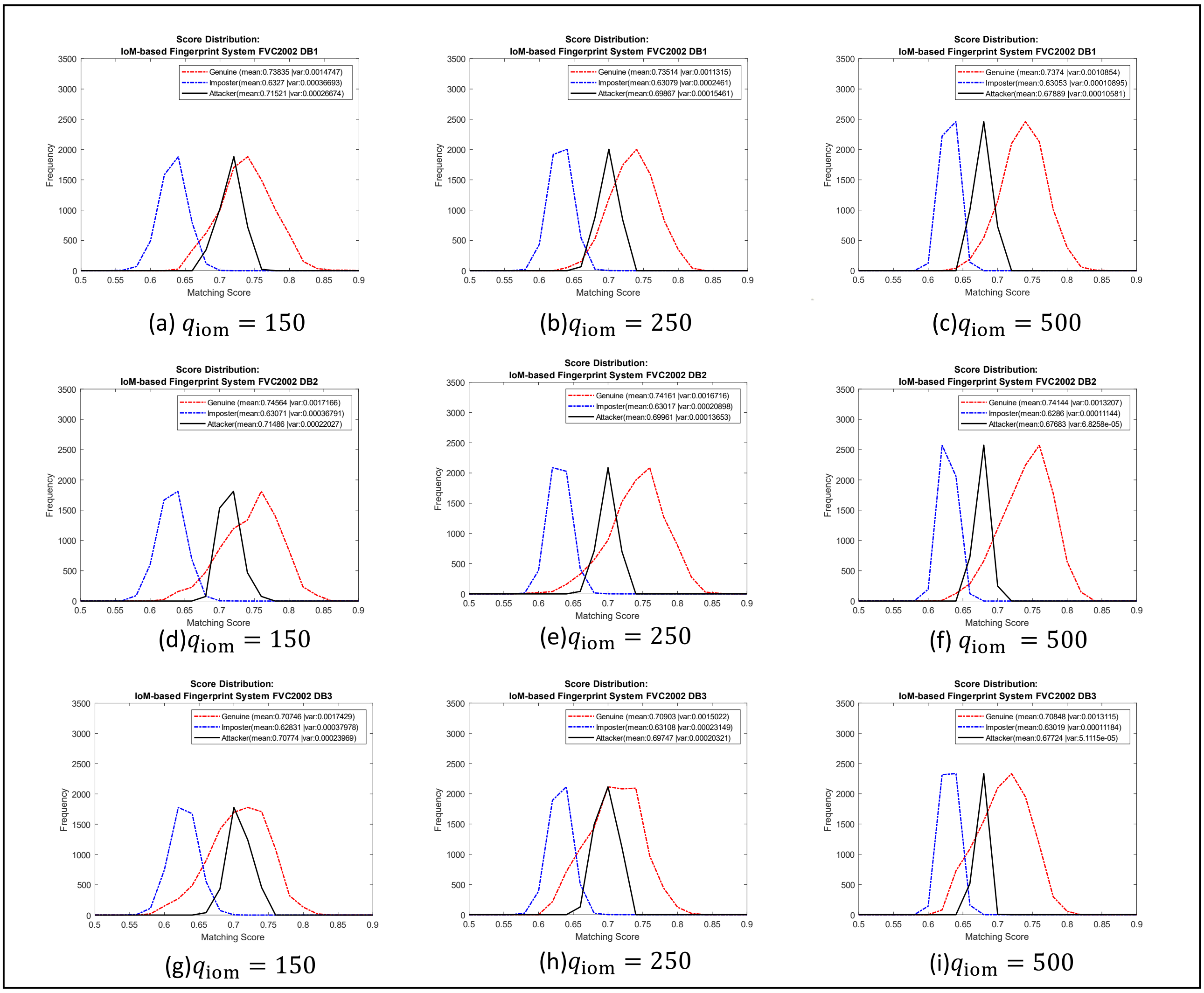
5.5.2 Attack attempt

A. Attack on the original cancellable biometric schemes

In this subsection, several experiments are conducted to evaluate the security resistance of the tested cancellable biometric schemes, i.e., IoM Hashing, M·EFV hashing and R·HoG, towards the formalized WO3A. The tested cancellable biometric schemes employ their original matcher for template comparison.

To testify the effect of the WO3A on the tested cancellable biometric schemes, several experiments are conducted on each scheme, and the cancellable templates are generated using different parameter settings. For IoM Hashing, the cancellable templates are generated with varying settings of parameter $q = 150{,}250{,}500$, while the l_{iom} is fixed to 16. For R·HoG, the cancellable templates are generated with settings of parameter $d = 175{,}200{,}225{,}250$, while the remaining parameters are following the best-tuned setting listed in Table 5.6. Recall the methodology of M·EFV hashing, one of the important parameters is the n. To prevent confusion between the parameter n for M·EFV hashing and the proposed enhanced matching mechanism, the notation, i.e., n_{MEFV} is used to represent the n for the M·EFV hashing. Thus, for M·EFV hashing, the cancellable templates are generated with different settings of $n_{\mathrm{MEFV}} = 5{,}15{,}55$; while the remaining parameters are following Table 5.6. The reader may refer to Sections 3.4.2 (R·HoG), 4.5.2 (M·EFV hashing), 5.3.1C (IoM Hashing) for the details of the parameters.

Figures below depict the attack results for the tested cancellable biometric schemes, with the red curve representing genuine score distribution, the blue curve representing impostor score distribution and the black curve representing attack score distribution. From the figures, it is observed that it is possible for the adversary to bypass the authentication within the attack attempt where the attack score distribution is largely overlapped with the genuine score distribution. For IoM hashing-based fingerprint system, it is observed that the WO3A is effective in compromising the authentication process when $q = 150$, where the attack score distribution is observed to be highly overlapped with the genuine score distribution. With the increment of parameter q, it is observed that the IoM hashing provides more security resistance towards the WO3A where the overlap region between the *attack* and *genuine* score distributions is reduced. Similar observations are found in the R·HoG-based iris system and M·EFV-based multimodal system, where the appropriate transformation parameter could improve the security resistance of the schemes. It is observed that the R·HoG and M·EFV hashing could provide more security resistance than the IoM hashing, where the overlap region between the *attack* and *genuine* score distribution is much smaller compared to IoM hashing. Nevertheless, the WO3A is still possible to bypass the authentication process since the upper bound of the attack score distribution is very close to the genuine score distribution. To improve the resistance of the schemes towards the WO3A, one may sacrifice a certain level of genuine acceptance rate (GAR) and increase security resistance by adjusting the matching threshold τ_{G} to be above the upper bound of the attack score distribution.

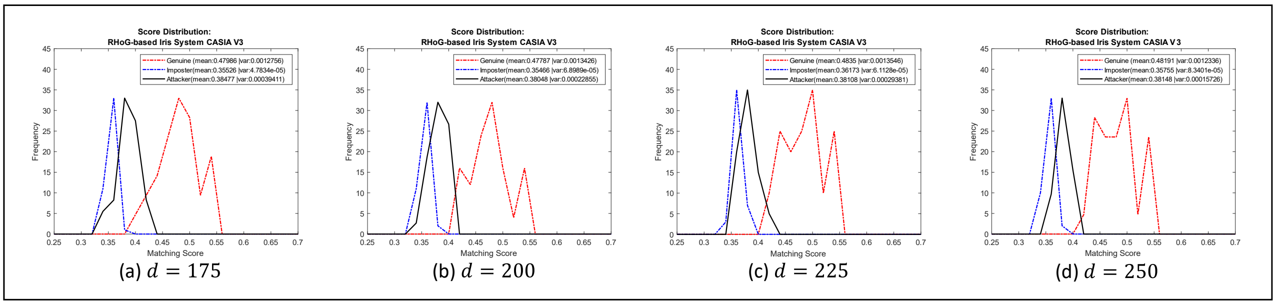


(a) $q_{\text{iom}} = 150$ (b)$q_{\text{iom}} = 250$ (c)$q_{\text{iom}} = 500$

(d)$q_{\text{iom}} = 150$ (e)$q_{\text{iom}} = 250$ (f) $q_{\text{iom}} = 500$

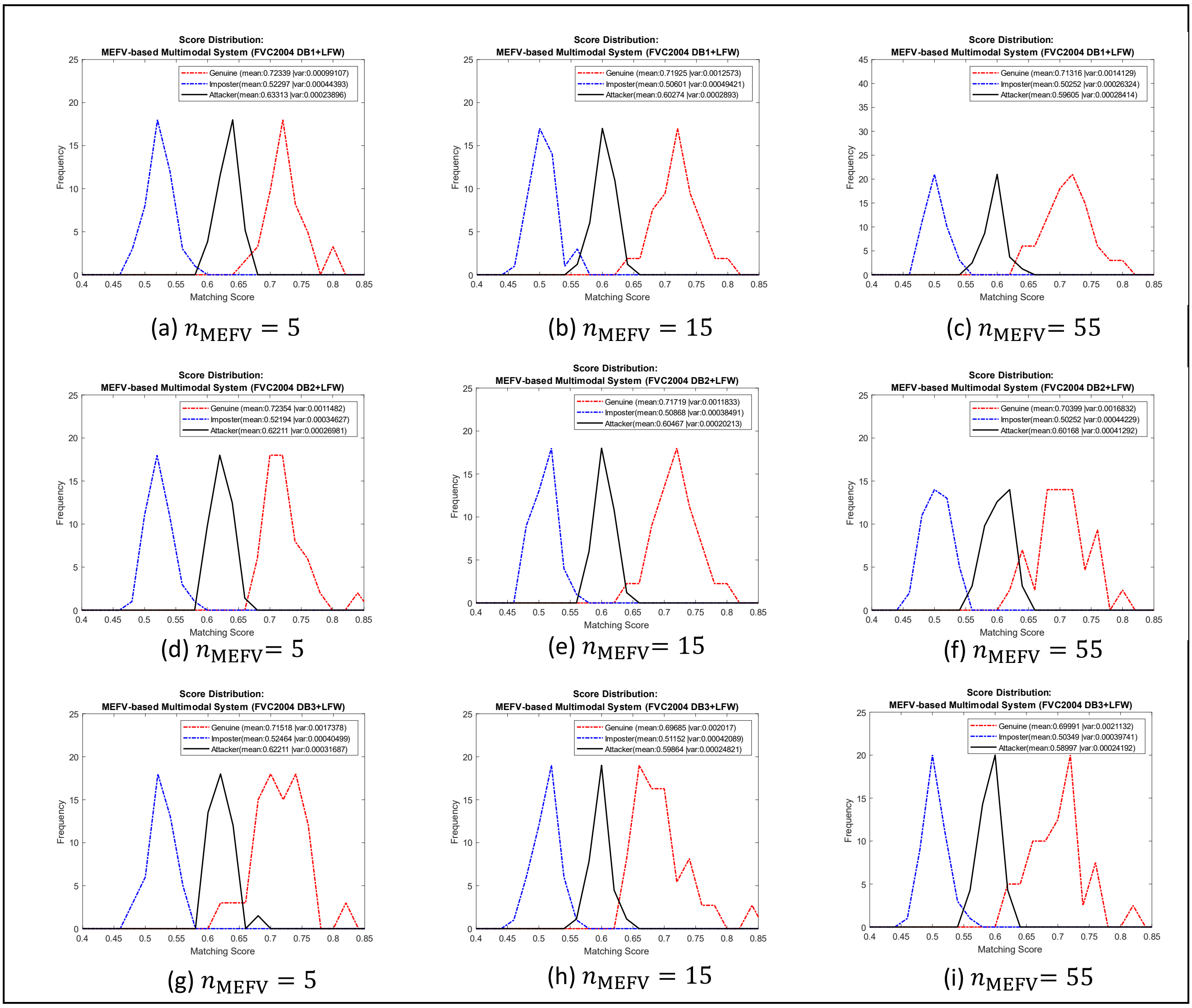
(g)$q_{\text{iom}} = 150$ (h)$q_{\text{iom}} = 250$ (i)$q_{\text{iom}} = 500$

Fig 5.5. Attack Results on IoM-based Fingerprint System FVC2002 subset where (a-c) is DB1, (d-f) is DB2 and (g-i) is DB3



(a) $d = 175$ (b) $d = 200$ (c) $d = 225$ (d) $d = 250$

Fig 5.6. Attack Results on R·HoG-based Iris System in CASIA V3 dataset



(a) $n_{\mathrm{MEFV}} = 5$ (b) $n_{\mathrm{MEFV}} = 15$ (c) $n_{\mathrm{MEFV}}= 55$

(d) $n_{\mathrm{MEFV}}= 5$ (e) $n_{\mathrm{MEFV}}= 15$ (f) $n_{\mathrm{MEFV}} = 55$

(g) $n_{\mathrm{MEFV}} = 5$ (h) $n_{\mathrm{MEFV}} = 15$ (i) $n_{\mathrm{MEFV}}= 55$

Fig 5.7. Attack Results on M·EFV-based Multimodal System in FVC2004+LFW subset where (a-c) is DB1, (d-f) is DB2 and (g-i) is DB3

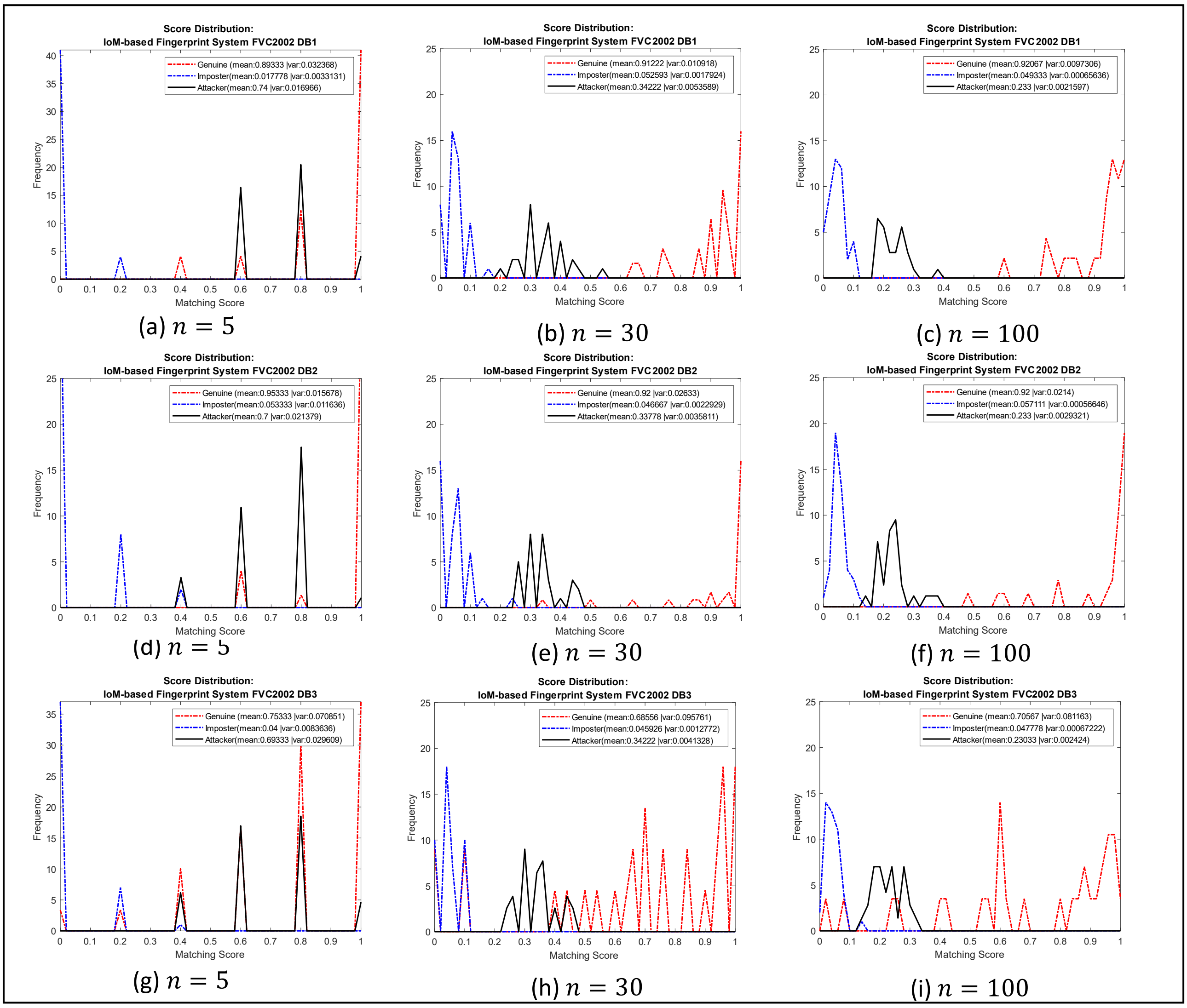
B. Attack on the enhanced cancellable biometric schemes

In this subsection, the WO3A is conducted on the cancellable biometric schemes that are enhanced by the proposed enhanced matching mechanism.

The cancellable templates are generated using the best-tuned setting listed in Table 5.6 and Table 5.5. Since the main purpose of this subsection is to testify the security resistance of the cancellable biometric schemes after being enhanced, several experiments are conducted using different settings for the parameter n in the proposed enhanced matching mechanism. In particular, n is testified for $n = 5{,}30{,}100$ in each experiment, while the parameter τ_{L} is fixed to the best-tuned setting that is determined in Section 5.3.2A.

Figures below depict the attack results for the proposed enhanced matching mechanism in terms of the score distributions, with the red curve representing genuine score distribution, the blue curve representing impostor score distribution and the black curve representing attack score distribution. From the figures, it is observed the mean of the *genuine* and *impostor* score distributions are highly separated. This is as expected where the proposed enhanced matching mechanism achieves the effect of separating the matching score that can be obtained by the genuine or impostor matching attempt. From the depicted result, it is observed that the security resistance of the cancellable biometric schemes is enhanced since the mean of the attack score distributions is not getting close to the mean of the genuine score distribution.

Overall, it is observed the proposed enhanced matching mechanism improves the security resistance of the cancellable biometric scheme towards the WO3A. It is observed under the same attack parameter, the R·HoG-based iris system and M·EFV-based multimodal systems (after enhanced) could provide more security resistance as compared to the IoM hashing-based fingerprint system, where the gap between the attack score distribution and the mean of genuine score distribution is larger than the unenhanced counterpart. This is mainly due to the guessed biometric template generated by the adversary could not surpass the τ_{L} that is set for the R·HoG-based iris system and M·EFV hashing-based multimodal system; and hence, it is hard for the WO3A to obtain a higher global matching score S_{G} throughout the attack attempt. On the other hand, it is observed in the IoM-based fingerprint, it is still possible for the attacker to obtain high matching score when n is tuned to a lower value ($\tau_{\mathrm{G}} = 5$). By incrementing the n, it is observed the proposed enhanced matching mechanism is taking effect where the gap between the upper bound of attack score distribution and mean of genuine score distribution is enlarged. Therefore, it is suggested that the parameter n be tuned higher to provide more security resistance for the cancellable biometric scheme. In short, the proposed enhanced matching mechanism could improve the security resistance of the tested systems against the WO3A, where the attack success rate is reduced.

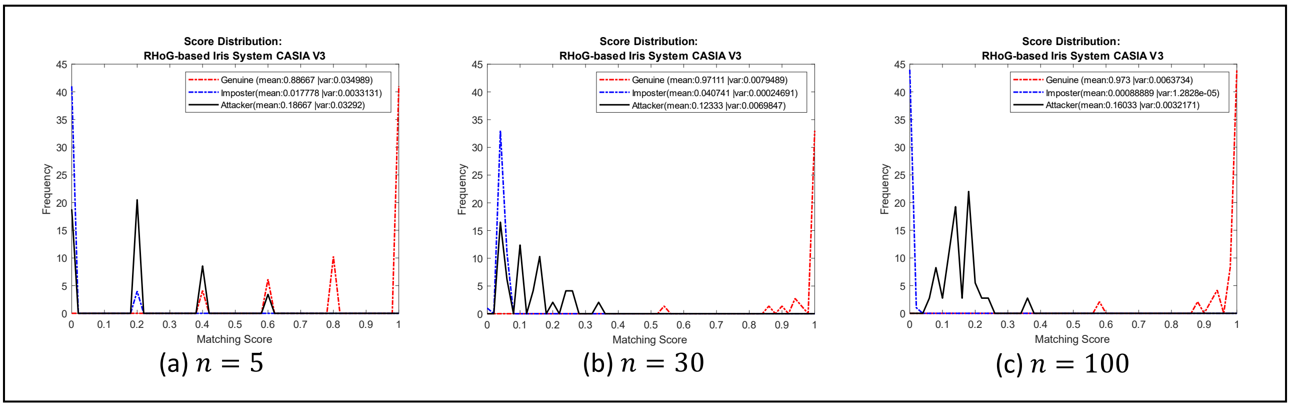


(a) $n = 5$ (b) $n = 30$ (c) $n = 100$

(d) $n = 5$ (e) $n = 30$ (f) $n = 100$

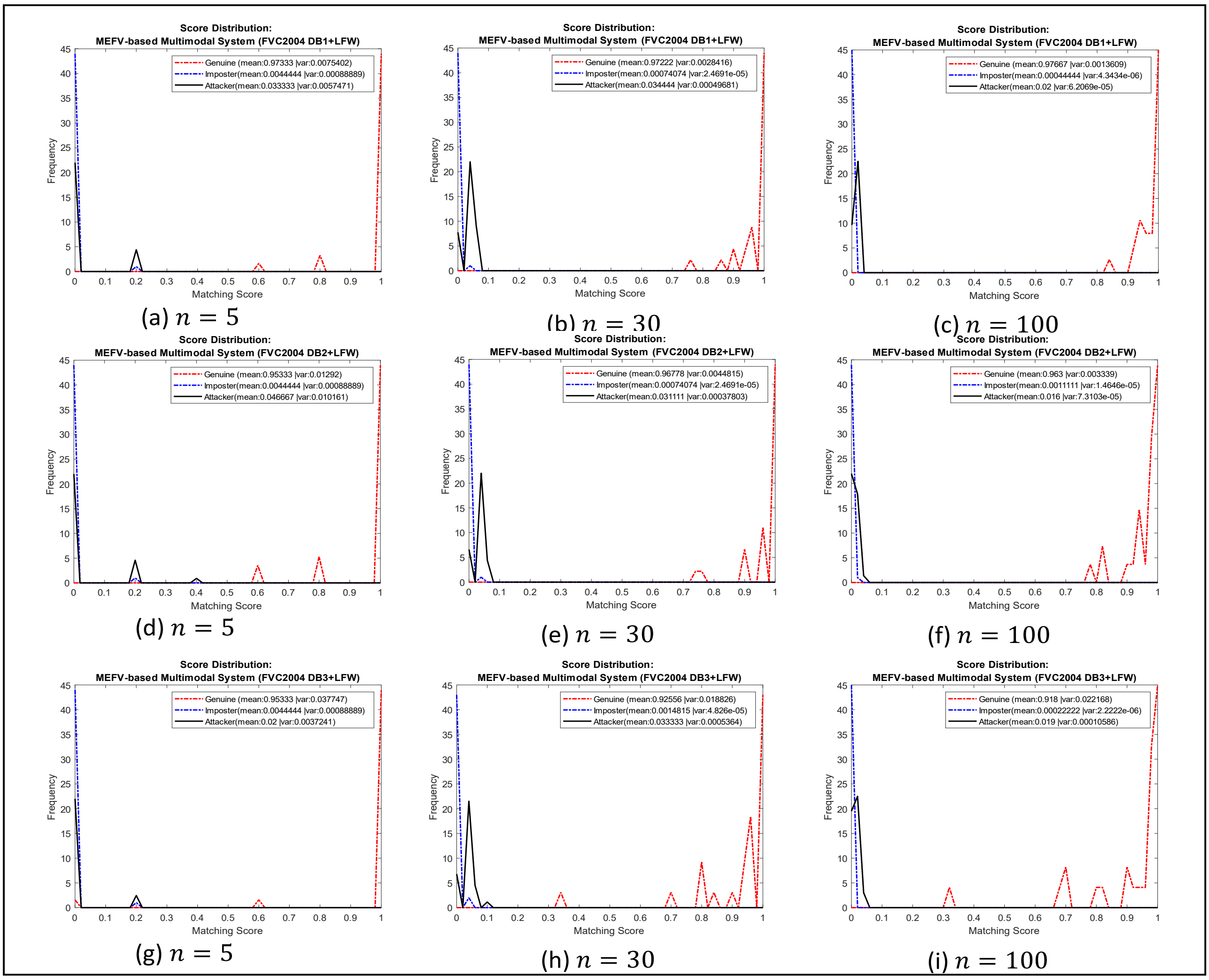
(g) $n = 5$ (h) $n = 30$ (i) $n = 100$

Fig 5.8. Attack Results on Enhanced IoM-based Fingerprint System in FVC2002 subset where (a-c) is DB1, (d-f) is DB2 and (g-i) is DB3



(a) $n = 5$ (b) $n = 30$ (c) $n = 100$

Fig 5.9. Attack Results on Enhanced R·HoG-based Fingerprint System in CASIA v3



(a) $n = 5$ (b) $n = 30$ (c) $n = 100$

(d) $n = 5$ (e) $n = 30$ (f) $n = 100$

(g) $n = 5$ (h) $n = 30$ (i) $n = 100$

Fig 5.10. Attack Results on enhanced M·EFV-based Multimodal System in FVC2004+LFW subset where (a-c) is DB1, (d-f) is DB2 and (g-i) is DB3

C. Comparison of the attack results

This subsection further studies the WO3A attack results and performs a comparison between the tested cancellable biometric schemes and the proposed enhanced matching mechanism. Recall the definition 5.1 in section 5.5.1A, the scheme is $(t_{\max}, r)$-secure if the r% of targeted samples are compromised in the sense that the adversary is able to surpass the threshold τ_{G}. Therefore, the r should be as lower as possible to reflect the security resistance towards the WO3A.

As mentioned earlier, the security of a biometric system can be enhanced by tuning the τ_{G}. However, this could lead to the trade-off between security and performance [27], which is unavoidable for a biometric system. Specifically, the sacrifice of the Genuine Acceptance Rate (GAR) is required for the higher τ_{G} that could help to lower attack success rate r. In this subsection, an analysis is conducted to evaluate the attack success rate, r of the WO3A with respect to the threshold τ_{G} under different GARs. For a more precise reading of r, the τ_{G} for each dataset is acquired from Section 5.3.4. The WO3A is operated with the same parameter setting ($t_{\max}$) for a fair comparison between the cancellable biometric scheme and the proposed enhanced matching mechanism. To be noted, the cancellable biometric schemes are operated using the same best-tuned setting as discussed in previous sections (see Table 5.6 and Table 5.13). The security resistance ($t_{\max}, r$) with respect to the GAR are tabulated in the table below, where the red font points out the potential security risk. To be noted, for the security consideration, GAR= 100% is not included in the evaluation. From the tabulated results, several observations are made:

- The formalized WO3A is effective in maximizing the attack score when the cancellable biometric schemes are not being enhanced by the proposed enhanced matching mechanism. For instance, in IoM hashing-based fingerprint system, the attack success rate r is very high even the system threshold is tuned to a higher value (with lowest GAR= 85%). This also shows that the IoM hashing is highly vulnerable to the WO3A attack.

- The proposed enhanced matching mechanism could improve the security resistance of the cancellable biometric schemes in the sense that the attack success rate r is averagely reduced. Furthermore, the gap between the upper bound of the attack score distribution (refer to UB_{attacker}) and the system threshold is larger compared to the unenhanced counterpart.

- The proposed enhanced matching mechanism is very effective in strengthening the security resistance of the M·EFV hashing and R·HoG in the sense that the attack success rate r is reduced to 0% after applying the enhanced matching mechanism. After applying the enhanced matching mechanism, both M·EFV hashing and R·HoG could resist the WO3A attack with (500, 0)-secure and maintain decent verification performance with GAR= 95%. It is observed the attack score distribution is not even close to the genuine score distribution.

- For the IoM hashing (after enhanced), it is observed that the attack success rate $r = 97\%$ in the FVC2002 DB3 subset when $\mathrm{GAR} = 95\%$. This is mainly due to the outliner in the genuine score distributions that limits the selection of system threshold. By sacrificing the GAR from 95% to 85%, the success rate is reduced from 97% to 0%. As compared to the original counterpart, where the success rate r is equal to $93-100\%$ under different GAR, the improvement is significant after applying the enhanced matching mechanism. With the GAR$=85\%$ and the reduced attack success rate, the verification performance of the system is still reasonable. These results also show that the parameter n for IoM hashing should be tuned higher to further improve the security resistance.

From the observations above, it is concluded that the proposed enhanced matching mechanism is able to increase the security resistance of the system under the same attack parameter. The proposed enhanced matching mechanism also reduces the scarification degree of the genuine acceptance rate (GAR) for the higher security resistance. With the GAR$=90-85\%$, the verification performance is still reasonable, and the system can provide more resistance towards the WO3A compared to the unenhanced system. It is noted that the WO3A is an authentication attack such that the estimated biometric preimage could not be re-used after the user renews the cancellable template. It is observed that under the same attack parameter settings, the attack required much more computation resources to conduct the attack attempt. Yet, the attack success rate is minimal as compared to the unenhanced system. The increase of security resistance allows the user to respond to an attack event and renew the cancellable template before the attack can succeed.

One may argue that the attacker could increase the WO3A attack iteration $t_{\max}$ for a higher attack success rate towards the proposed enhanced matching mechanism. However, it is infeasible for the attacker to do so due to the time complexity of attacking each sample. Under the same attack parameter, it is observed that the WO3A requires much more time to perform an attack on the enhanced scheme and yet, the increment of the attack success rate r is minimal as compared to the attack on the unenhanced scheme. For instance, the attack time (per sample) for IoM hashing (in FVC2002) is increased from an average of 36.2325 seconds to an average of 559.5348 seconds after the proposed enhanced matching mechanism is applied, while the attack success rate is decreased from an average of 53% to 32% when the GAR of the system is equal to 95%. In addition, with the slight decrease of GAR, the system (after enhanced) could provide more security resistance. As compared to the unenhanced systems, the sacrifice of GAR is minimal. Furthermore, it is shown in Fig 5.8, incrementing the parameter n could help to increase the security resistance of the proposed enhanced matching mechanism as well as the decidability of the system. Therefore, it is also suggested to tune the parameter n for a higher value to counter the WO3A attack. It is also noted the increment of parameter n could increase the attack time complexity. In short, the experiment result shows that the proposed enhanced matching mechanism is able to enhance the security resistance of the cancellable biometric scheme towards the WO3A and allow a higher matching threshold (with minimal reduction of GAR) to be set in the system.

Table 5.21: Attack analysis on IoM Hashing-based fingerprint system with respect to the Genuine Acceptance Rate (FVC2002)

Method	**Subset**	UB_{attacker}	**System threshold** τ_{G}	Attack Iteration $t_{\max}$	**Attack success rate** r (%)	**Security resistance** $(t_{\max}, r)$	**Average time taken for each sample (sec)**
GAR=95%							
IoM Hashing (original)	DB1	**0.6999**	**0.6855**	500	**10**	**(500, 10)**	32.8473
	DB2	**0.6807**	**0.6752**	500	**50**	**(500, 50)**	36.7436
	DB3	**0.6972**	**0.6428**	500	**100**	**(500, 100)**	39.1066
IoM Hashing with proposed matching mechanism ($n = 100, \tau_{\mathrm{L}} =$ 0.67)	DB1	0.3800	0.6900	500	0	(500,0)	585.3941
	DB2	0.3800	0.5400	500	0	(500,0)	547.3615
	DB3	**0.3200**	**0.1600**	500	**97**	**(500, 97)**	545.8487
GAR=90%							
IoM Hashing (original)	DB1	**0.6999**	**0.6950**	500	**3**	**(500, 3)**	32.8473
	DB2	**0.6807**	**0.6907**	500	**3**	**(500, 3)**	36.7436
	DB3	**0.6972**	**0.6544**	500	**100**	**(500, 100)**	39.1066
IoM Hashing with proposed matching mechanism ($n = 100, \tau$_L = 0.67)	DB1	0.3800	0.8000	500	0	(500,0)	585.3941
	DB2	0.3800	0.7400	500	0	(500,0)	547.3615
	DB3	**0.3200**	**0.3200**	500	**3**	**(500, 3)**	545.8487
GAR=85%							
IoM Hashing (original)	DB1	**0.6999**	**0.7034**	500	0	(500,0)	32.8473
	DB2	**0.6807**	**0.7021**	500	0	(500,0)	36.7436
	DB3	**0.6972**	**0.6639**	500	**93**	**(500, 93)**	39.1066
IoM Hashing with proposed matching mechanism ($n = 100, \tau$_L = 0.67)	DB1	0.3800	0.8700	500	0	(500,0)	585.3941
	DB2	0.3800	0.8500	500	0	(500,0)	547.3615
	DB3	0.3200	0.4500	500	0	(500,0)	545.8487

Table 5.22: Attack analysis on M·EFV hashing-based multimodal system with respect to the Genuine Acceptance Rate (FVC2004 + LFW)

Method	**Subset**	UB_{attacker}	**System threshold** τ_{G}	Attack Iteration $t_{\max}$	**Attack success rate** r (%)	**Security resistance** $(t_{\max}, r)$	**Average time taken for each sample (sec)**
GAR=95%							
M·EFV hashing (original)	DB1	**0.6360**	**0.6251**	500	**10**	**(500, 10)**	44.9462
	DB2	**0.6325**	**0.6050**	500	**47**	**(500, 47)**	44.1383
	DB3	**0.6245**	**0.6180**	500	**3**	**(500, 3)**	43.3733
M·EFV hashing with proposed matching mechanism ($n = 100, \tau_{\text{L}} =$ 0.62)	DB1	0.0300	0.6400	500	0	(500,0)	817.7611
	DB2	0.0400	0.4100	500	0	(500,0)	808.1642
	DB3	0.0400	0.5300	500	0	(500,0)	805.6682
GAR=90%							
M·EFV hashing (original)	DB1	**0.6360**	**0.6472**	500	0	(500,0)	44.9462
	DB2	**0.6325**	**0.6214**	500	**23**	**(500, 23)**	44.1383
	DB3	**0.6245**	**0.6355**	500	0	(500,0)	43.3733
M·EFV hashing with proposed matching mechanism $n = 100, \tau_{\text{L}} =$ 0.62)	DB1	0.0300	0.8000	500	0	(500,0)	817.7611
	DB2	0.0400	0.6000	500	0	(500,0)	808.1642
	DB3	0.0400	0.7000	500	0	(500,0)	805.6682
GAR=85%							
M·EFV hashing (original)	DB1	**0.6360**	**0.6563**	500	0	(500,0)	44.9462
	DB2	**0.6325**	**0.6343**	500	0	(500,0)	44.1383
	DB3	**0.6245**	**0.6501**	500	0	(500,0)	43.3733
M·EFV hashing with proposed matching mechanism $n = 100, \tau_{\text{L}} =$ 0.62)	DB1	0.0300	0.8700	500	0	(500,0)	817.7611
	DB2	0.0400	0.7100	500	0	(500,0)	808.1642
	DB3	0.0400	0.8000	500	0	(500,0)	805.6682

Table 5.23: Attack analysis on R·HoG-based iris system with respect to the Genuine Acceptance Rate (CASIA V3)

Method	UB_{attacker}	**System threshold** τ_{G}	Attack Iteration $t_{\max}$	**Attack success rate** r (%)	**Security resistance** $(t_{\max}, r)$	**Average time taken for each sample (sec)**
GAR=95%						
R·HoG (original)	$\mathbf{0.4044}$	$\mathbf{0.4021}$	500	$\mathbf{13}$	$\mathbf{(500, 13)}$	274.1536
R·HoG with proposed matching mechanism $(n = 100, \tau_{\mathrm{L}} = 0.415)$	0.3700	0.4700		0	(500,0)	2867.8720
GAR=90%						
R·HoG (original)	$\mathbf{0.4044}$	$\mathbf{0.4151}$	500	0	(500,0)	274.1536
R·HoG with proposed matching mechanism $(n = 100, \tau_{\mathrm{L}} = 0.415)$	0.3700	0.7000		0	(500,0)	2867.8720
GAR=85%						
R·HoG (original)	$\mathbf{0.4044}$	$\mathbf{0.4219}$	500	0	(500,0)	274.1536
R·HoG with proposed matching mechanism $(n = 100, \tau_{\mathrm{L}} = 0.415)$	0.3700	0.8000		0	(500,0)	2867.8720

5.6 Summary and contributions

This chapter focuses on the decision environment and authentication attack in a cancellable biometrics-enabled system. The two research outcomes are enhanced matching mechanism and whale optimization algorithm-based authentication attack (WO3A). The enhanced matching mechanism is a dual-phase score quantization scheme that is able to improve the verification performance and decidability of the cancellable biometric schemes. Comprehensive experiments are conducted to examine the verification performance on several benchmarking datasets. The proposed enhanced matching mechanism is shown to improve the verification performance for IoM hashing, R·HoG and M·EFV hashing. The high separation between the mean of genuine/ impostor score distributions allows the high matching threshold for higher security resistance. Apart from that, this chapter studies the authentication attack and formalizes a practical attack scheme, namely the WO3A. The WO3A is conducted on the IoM hashing, R·HoG and M·EFV hashing. The attack result shows the IoM hashing is highly vulnerable towards the WO3A in the sense that a high attack success rate is observed. Although a high matching threshold could help IoM hashing to reduce the attack success rate, it requires a high reduction of the Genuine Acceptance Rate (GAR). Other than that, the WO3A is also conducted to the schemes that are enhanced by the proposed enhanced matching mechanism under the same attack scenario. The attack result shows that the enhanced matching mechanism could improve the security resistance where the attack success rate is greatly reduced. It is also observed that the proposed enhanced matching mechanism allows the lower sacrifice of GAR to improve the security resistance as compared to the unenhanced counterpart. Furthermore, the proposed enhanced matching mechanism could be further tuned to increase the security resistance of the cancellable biometric scheme. It is noted that the main purpose of formalizing WO3A is to simulate an authentication attack where the guessed biometric template does not resemble the original biometric template (or even the biometric feature). Therefore, the extension of the WO3A to template recovery attack or other extensive scenarios could be interesting future work.

Chapter 6 Conclusions

This chapter concludes the thesis by discussing the summary of thesis chapters and plausible future directions of the proposal work in this thesis. Security and privacy of biometric identity management (IdM) is an open problem until now. Among various aspects, biometric template protection requires attention as the compromise of the original biometric templates usually implies permanent identity loss. Specifically, the victim is prohibited from using the same biometric feature due to the irrevocable nature of biometrics. As one of the consequences, tremendous monetary loss is required to recover from the damage. For instance, in 2015, roughly $\$133$ million dollars was costed to the U.S federal Office of Personnel Management for covering up the loss when $1.1 - 5.6$ million of biometric data were compromised [15]. In this thesis, a study on biometric template protection for face, fingerprint, and iris modalities was carried out. There are 5 outcomes throughout the venture: (i) 3 template protection schemes, (ii) 1 enhanced matching mechanism and (iii) 1 automated type-4 attack. Among the works, 3 template protection methods, i.e., R·HoG, EFV hashing and M·EFV hashing, are dedicated to alignment-robust cancellable transformation and tokenless cancellable transformation, respectively. The enhanced matching mechanism is devoted to enhancing the decision environment of the biometric authentication, while the type-4 attack, i.e., WO3A, is formulated for testifying security and privacy aspects of the biometric system. The proposals are presented, and the experimental results are evidenced chapter-by-chapter throughout the thesis.

6.1 Summary of thesis chapters

This section revisits each thesis chapter and briefly discusses the research outcomes and contributions. In Chapter 2, an extensive literature review is conducted based on the three research contexts of this thesis: (i) alignment problem in iris template protection, (ii) token management in unimodal and multimodal template protection and (iii) security and privacy in thresholding-based matching. Throughout the literature searching process, various numbers of works that are associated with the face, fingerprint and iris modalities are revisited and have been discussed section-by-section. The chapter first revisits the existing iris template protection works in the categories of alignment-based and alignment-robust approaches. The former approach refers to the template protection method that requires a pre-alignment process to deal with the unaligned iris feature, while the latter approach could directly derive a protected iris template from the unaligned iris feature. In the process of revisiting the existing works, it is observed that the alignment-robust approach is preferable compared to the alignment-based approach. Although the alignment-based approach gains a slight advantage in terms of verification performance, the necessity of having pre-alignment could drastically slow down the authentication process. For instance, the recently developed IFO hashing [53] employs the shifting-based pre-alignment to compensate for the inability to transform the unaligned irisCode. Subsequently, the time complexity of the IFO hashing is highly affected by the repeating shifting and transformation process. To reduce the time complexity, a number of alignment-robust approaches are introduced in the literature. It is still observed that some concerns, e.g., performance degradation, security vulnerabilities, are yet to be fully resolved. This drove the author to propose the alignment-robust iris template protection scheme, i.e., R·HoG. The next section in Chapter 2 puts the focus on token management in unimodal and multimodal biometric template protection. In this section, the works are reviewed in the classification of tokenized unimodal/ multimodal template protection and tokenless multimodal template protection. In addition, due to the hybrid nature of the author’s proposal, this section also revisits hybrid template protection works. Due to the increment of the needs of biometric template protection, the tokenless approach that does not require the user to handle the transformation key gains more attention since this approach could reduce the burden of managing the token, especially the user enrolled into multiple cancellable biometrics-enabled systems. Moreover, due to the lack of an efficient template protection scheme that can handle the biometric feature fusion and tokenless approach, the author is motivated to propose the face and fingerprint-based template protection schemes, i.e., EFV hashing and M·EFV hashing. Lastly, Chapter 2 explores the type-4 attack that targeted the security and privacy of the thresholding-based matching. From the reviewed work, it is observed that the type-4 attack could recover the original biometric feature when the system is unprotected; hence the importance of biometric template protection is demonstrated. Despite biometric template protection offering a privacy solution by replacing the protected template once the authentication of the system is compromised, it is unfavorable that the adversary could compromise the authentication process in a short time. More deadly, the type-4 attack does not require the guessed input biometric feature to be similar to the original biometric feature. To provide sufficient security resistance towards the type-4 attack, one has to trade the Genuine Acceptance Rate (GAR) for a higher system threshold. However, due to the performance degradation in biometric template protection, the sacrifice of GAR is usually large. This motivated the author to explore a solution that can further improve the performance preservation of the cancellable biometric scheme.

Chapter 3 studies the alignment problem in iris template protection and introduces an alignment-robust iris template protection scheme coined as Random Augmented Histogram of Oriented Gradient (R·HoG). In iris recognition, irisCode is the most employed iris feature despite a various number of alternatives being introduced. The most challenging task in protecting the irisCode feature is to overcome the alignment issue when transforming the irisCode into the protected template (cancellable template). To address this problem, the Random Augmented Histogram of Oriented Gradient (R·HoG) is proposed. R·HoG is an alignment-robust cancellable biometric scheme that transforms the unaligned irisCode into a cancellable template without the necessity of having a pre-alignment process. The matching process can be completed rapidly since the resultant cancellable templates can be directly compared to the query template. Differ from the existing studies that employ the well-known Histogram of Oriented Gradient (HoG) for feature extraction, the author demonstrated an unconventional usage of HoG in biometric template protection by coupling it with two mechanisms, i.e., (i) column vector-wise random augmentation and (ii) gradient orientation grouping. The mechanism (i) enables the cancellability property and compensates for the performance degradation that is led by the alignment-robust transformation, while the mechanism (ii) induces security property and enables the R·HoG to produce a compact cancellable template. Experimental results showed the R · HoG achieving a decent verification performance with the EER= 0.62% in CASIA-IrisV3-Internal dataset. Since the main functionality of R·HoG is to protect the irisCode template, several analyses and experiments were carried out to examine the R·HoG in terms of irreversibility, unlinkability and renewability properties. With the employment of disposable parameters during the transformation process, it is hard for the adversary to recover the original irisCode input if even multiple cancellable templates and transformation keys are generated. An interesting finding is that in the proposed R·HoG, the z-score normalization process can be operated as an irreversible transformation. Specifically, R·HoG utilizes the many-to-one mapping trait of the normalization process and the disposable transformation parameter to increase the difficulty of reverse transforming the cancellable template. The security aspect of the R·HoG is examined by conducting three main security attacks that aim to generate a guessed template for matching. The security analysis showed that the sacrifice of GAR=5% provides decent security strength to combat the birthday attack. On the other hand, the unlinkability and renewability properties of the R·HoG are well examined via a benchmarking evaluation framework [112]. More remarkably, R·HoG enables the fast similarity comparison in iris verification system in which the produce cancellable template can be directly compared, and the pre-alignment process is not required.

Chapter 4 focuses on the token management problem in the face and fingerprint-based template protection. In the existing studies, most of the existing face and fingerprint-based template protection schemes are manifested as a tokenized authentication scheme that requires two input factors, i.e., biometric feature and a token for cancellable template generation and matching. The tokenized approach requires the user to keep the token securely; otherwise, there could be a security and privacy risk when the token is exposed to the adversary. For instance, a zero-effort false acceptance attack could be launched to gain illegal access to the system [27]. As compared to tokenized schemes, tokenless schemes abandon the external token; hence, the security and privacy threats that are related to the exposure of tokens could be mitigated. Furthermore, the removal of tokens improves the convenience of the cancellable biometric scheme where there is no need for the user to manage the token. On the other hand, biometric fusion is getting the public's interest because it improves the verification performance of a biometric system. However, the security and privacy issue of the multimodal biometric system could be more severe than a unimodal biometric system since the templates of multiple biometric modalities are stored. Based on these issues, two tokenless template protection schemes: (i) Extended Feature Vector (EFV) hashing and (ii) Multimodal Extended Feature Vector (M·EFV) hashing are proposed for fingerprint and face-based biometric systems. In particular, the former scheme focuses on exploring the tokenless template protection in a unimodal fingerprint system, while the latter scheme extends and enhances the methodology of the former scheme. Differ from the existing cancellable biometric schemes that store the transformation key as an external token, the proposed EFV and M·EFV hashing employ the XOR encryption/ decryption to transform the transformation key into an encrypted string. Since another ingredient for generating the encrypted string is biometric-dependent information that can be regenerated by the genuine user, all the ingredients for the encrypted string are discarded from the system once the encrypted string is generated. Hence, the original transformation key can never be recovered. On top of the EFV hashing, M·EFV hashing introduces the prior-randomization mechanism to improve the capability to combat the Attack via Record Multiplicity (ARM) [168], [169]. Other than that, M·EFV hashing conducted an in-depth study of fusing the real-valued biometric vectors and pointed out an ineffective biometric fusion could highly affect the verification performance of the generated cancellable template. The proposed EFV and M·EFV hashing are examined and proved to satisfy the irreversibility, unlinkability, renewability and performance preservation properties.

Chapter 5 studies the security threat and the weak decision environment problem for a cancellable biometrics-enabled system. The tradeoff between security and performance is inevitable in a biometric system [23], where the sacrifice of Genuine Acceptance Rate (GAR) for security consideration is required. The scarification degree of a cancellable biometric scheme is larger due to the performance degradation issue. Therefore, it requires a solution that can further reduce the performance degradation issue of a cancellable biometric scheme. Motivated by the aforementioned problem, an enhanced matching mechanism is proposed for the IoM hashing [66], R·HoG and M·EFV hashing-based biometric system. The enhanced matching mechanism is a dual-phase score quantization scheme that could enhance the decidability of the cancellable biometric in the sense that the gap between the mean of genuine/ impostor matching score distributions is increased. The high separation of the genuine/impostor scores allows the system developer to choose a higher matching threshold with minimal sacrifice of genuine acceptance rate (GAR). Comprehensive experiments were carried out to assess the verification performance and decidability of the cancellable biometric schemes after applying the proposed enhanced matching mechanism. The experiment results suggest the proposed enhanced matching mechanism could improve the decidability and verification performance of the system.

Besides that, chapter 5 also studies the type-4 attack and has formalized an automated type-4 attack, namely Whale Optimization Algorithm-based Authentication Attack (WO3A) that aims to bypass the authentication process of a cancellable biometrics-enabled system. By considering the WO3A as the attack model, security assessments are conducted on the cancellable biometric scheme and the proposed enhanced matching mechanism. The security assessment suggests the proposed enhanced matching mechanism could improve the security resistance of the cancellable biometric scheme. It is also showing the potential of further improving the security resistance by tuning the parameter of the enhanced matching mechanism.

6.2 Future recommendations

This section outlines the plausible extensions that are based on the research outcomes and findings in this thesis.

- **Expansion of scheme design:** There are several directions to expand the methodology of the proposed works. For instance, parallel processing techniques (e.g., multi-threading or SSE programming [173]) could be integrated into the proposed enhanced matching mechanism to realize parallel local template generation and matching; hence, optimizing the efficiency of the authentication process. On the other hand, since M·EFV hashing and R·HoG were designed for different biometric features, the design concept of both schemes could be combined to produce a new variation of the biometric template protection that can handle a wider range of input biometric features (e.g., fingerprint + iris).

- **Propagation of the schemes to other biometric modalities:** This thesis focuses on the face, fingerprint and iris modalities and designed three biometric template protection schemes. Since the proposed template protection schemes accept the matrix or vector-based biometric feature as the input, it is possible to propagate the proposed schemes to other biometric modalities, e.g., fingervein and speech. It would involve the modification of the scheme since the structure of the extracted feature would not be exactly the same as the adopted biometric feature in this thesis. Hence, it would be an exciting venture to explore the usage of the proposed works on other biometric modalities.

- **Hybrid biometric template protection:** Biometric key binding is the sub-class of biometrics cryptosystem that focuses on using the biometric feature to bind or release the cryptographic key. Recent studies have pointed out the direct employment of the original biometric feature for key binding could lead to the recovery of the biometric feature when the auxiliary data is compromised. As such, many existing studies combine the key binding system with cancellable biometrics to prevent the direct involvement of the original biometric feature in the key binding process. Such an approach is recognized as hybrid template protection. Most of the existing hybrid schemes are tokenized authentication approaches that suffer from token management issues. Therefore, future research could explore tokenless authentication in the biometric key binding.

6.3 Concluding remarks

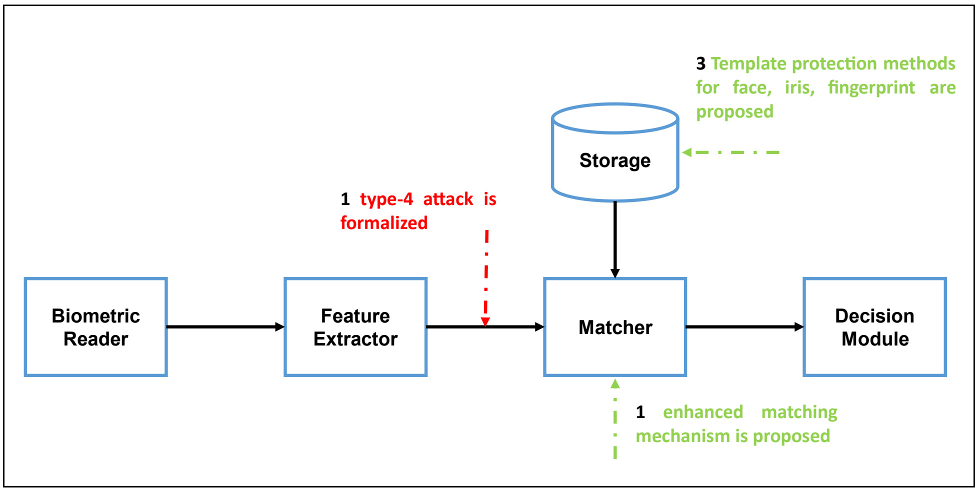

3 Template protection methods for face, iris, fingerprint are proposed
Storage
1 type-4 attack is formalized
Biometric Reader
Feature Extractor
Matcher
Decision Module
1 enhanced matching mechanism is proposed

Fig 6.1. Graphical illustration of basic biometric system infrastructure and the research outcomes

Biometric template protection (BTP) is one of the essential aspects of the biometric system in the sense that the original biometric information is never revealed. As such, the security and privacy threats that are associated with the biometric template storage compromisation could be mitigated. Until now, biometric template protection is still an open issue with the various numbers of unsolved security and privacy shortcomings. This thesis was established to address the unsolved problems in face, fingerprint and iris template protection. In short, this thesis designed 3 cancellable biometrics schemes, 1 enhanced matching mechanism and 1 automated type-4 attack (Fig 6.1).

One of the outcomes is the tokenless multimodal template protection scheme (i.e., M·EFV hashing). The M·EFV hashing shows the possibility of a tokenless template protection scheme that overcomes the feature incompatibility issue in the real-valued face and fingerprint vector and produces the fused cancellable template. The existence of M·EFV hashing points out the potential expansion of tokenless biometric template protection. A new alignment-robust iris template protection scheme (i.e., R·HoG) is proposed to resolve the alignment issue in irisCode template protection. With the alignment-robust and decent performance preservation properties, it is concluded that the proposed R·HoG can be employed in the existing iris verification system. Apart from that, an interesting finding is that the verification performance and decidability of a cancellable biometrics-enabled system could be further improved by replacing the canonical matching mechanism with an enhanced matching mechanism. The proposed template protection schemes and enhanced matching mechanism were tested on the benchmarking fingerprint FVC [73], [74], face LFW [84] and iris CASIA [52] databases. Various experiments and analyses were conducted, and the results are presented in the respective chapter.

Apart from that, it is worthwhile to draw attention to an article by Jain *et al.* [23], where the biometric community has made a massive progression on the automated biometric system over the past $50 - 60$ years. The advancement of technological tools has increased the applications of biometric identity management, e.g., biometric authentication in smart devices [23]. While the intuition of deploying a biometric system is to secure identity management from illegal access, there is no guarantee that the biometric system itself can be completely secure [23]. Hence, the security and privacy problems of the biometric system should be studied to address the potential threats, so that the biometric recognition could be brought to the next level.

BIBLIOGRAPHY

[1] M. J. Lee, Z. Jin, and A. B. J. Teoh, “One-factor Cancellable Scheme for Fingerprint Template Protection: Extended Feature Vector (EFV) Hashing,” in *2018 IEEE International Workshop on Information Forensics and Security (WIFS)*, 2018, pp. 1–7.

[2] M. J. Lee, Z. Jin, M. Li, and D. B.-W. Chen, “Mixing Binary Face and Fingerprint based on Extended Feature Vector (EFV) Hashing,” in *2019 International Symposium on Intelligent Signal Processing and Communication Systems (ISPACS)*, 2019, pp. 1–2.

[3] M. J. Lee, A. B. J. Teoh, A. Uhl, S.-N. Liang, and Z. Jin, “A Tokenless Cancellable Scheme for Multimodal Biometric Systems,” *Computers & Security*, vol. 108, p. 102350, 2021.

[4] A. K. Jain, A. A. Ross, and K. Nandakumar, “Introduction,” in *Introduction to Biometrics*, Boston, MA: Springer US, 2011, pp. 1–49.

[5] R. Crozier, “Monash Uni deploys MFA after Iran attacks targeting universities,” *itnews*, 11-Jul-2019.

[6] “Yubico - Protect your digital world with YubiKey.” [Online]. Available: https://www.yubico.com/. [Accessed: 29-Apr-2020].

[7] R. F. Nogueira, R. de Alencar Lotufo, and R. C. Machado, “Fingerprint Liveness Detection Using Convolutional Neural Networks,” *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 6, pp. 1206–1213, Jun. 2016.

[8] A. K. Jain and A. Ross, “Introduction to Biometrics,” in *Handbook of Biometrics*, A. K. Jain, P. Flynn, and A. A. Ross, Eds. Boston, MA: Springer US, 2008, pp. 1–22.

[9] A. K. Jain, A. A. Ross, and K. Nandakumar, “Multibiometrics,” in *Introduction to Biometrics*, Boston, MA: Springer US, 2011, pp. 209–258.

[10] A. K. Jain, A. A. Ross, and K. Nandakumar, “Fingerprint Recognition,” in *Introduction to Biometrics*, Boston, MA: Springer US, 2011, pp. 51–96.

[11] A. K. Jain, K. Nandakumar, and A. Nagar, “Biometric Template Security,” *EURASIP J. Adv. Signal Process*, vol. 2008, pp. 113:1--113:17, Jan. 2008.

[12] “Biometrics: Secure Authentication in the Modern Age.” [Online]. Available: https://www.okta.com/identity-101/biometrics-secure-authentication/. [Accessed: 29-Apr-2020].

[13] “Use Touch ID on iPhone and iPad - Apple Support.” [Online]. Available:

https://support.apple.com/en-my/HT201371. [Accessed: 30-Oct-2018].

[14] “Windows Hello: Discover facial recognition on Windows 10.” [Online]. Available: https://www.microsoft.com/en-my/windows/windows-hello. [Accessed: 04-Jun-2019].

[15] “OPM Now Admits 5.6m Feds’ Fingerprints Were Stolen By Hackers.” [Online]. Available: https://www.wired.com/2015/09/opm-now-admits-5-6m-feds-fingerprints-stolen-hackers/. [Accessed: 29-Apr-2019].

[16] S. Al-Kuwari, J. H. Davenport, and R. J. Bradford, “Cryptographic Hash Functions: Recent Design Trends and Security Notions.” 2011.

[17] C. Rathgeb and A. Uhl, “A survey on biometric cryptosystems and cancelable biometrics,” *EURASIP Journal on Information Security*, vol. 2011, no. 1, p. 3, Sep. 2011.

[18] J. Zuo, N. K. Ratha, and J. H. Connell, “Cancelable iris biometric,” in *2008 19th International Conference on Pattern Recognition*, 2008, pp. 1–4.

[19] V. M. Patel, N. K. Ratha, and R. Chellappa, “Cancelable Biometrics: A review,” *IEEE Signal Processing Magazine*, vol. 32, no. 5, pp. 54–65, Sep. 2015.

[20] A. K. Jain, A. A. Ross, and K. Nandakumar, “Security Of Biometric Systems,” in *Introduction to Biometrics*, Boston, MA: Springer US, 2011, pp. 259–306.

[21] “ISO/IEC 24745:2011 information technology security techniques biometric information protection, 2011,” 2011.

[22] “ISO/IEC 30136:2018 information technology performance testing of biometric template protection schemes, 2018,” 2018.

[23] A. K. Jain, K. Nandakumar, and A. Ross, “50 years of biometric research: Accomplishments, challenges, and opportunities,” *Pattern Recognition Letters*, vol. 79, pp. 80–105, 2016.

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

[25] A. Kong, K.-H. Cheung, D. Zhang, M. Kamel, and J. You, “An analysis of BioHashing and its variants,” *Pattern Recognition*, vol. 39, no. 7, pp. 1359–1368, 2006.

[26] U. Uludag and A. K. Jain, “Attacks on biometric systems: a case study in fingerprints,” *Security, Steganography, and Watermarking of Multimedia Contents VI*, vol. 5306, p. 622, 2004.

[27] K. Nandakumar and A. K. Jain, “Biometric Template Protection: Bridging the performance gap between theory and practice,” *IEEE Signal Processing Magazine*,

vol. 32, no. 5, pp. 88–100, Sep. 2015.

[28] J. Galbally, C. McCool, J. Fierrez, S. Marcel, and J. Ortega-Garcia, “On the vulnerability of face verification systems to hill-climbing attacks,” *Pattern Recognition*, vol. 43, no. 3, pp. 1027–1038, 2010.

[29] A. Rozsa, A. E. Glock, and T. E. Boult, “Genetic algorithm attack on minutiae-based fingerprint authentication and protected template fingerprint systems,” in *2015 IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW)*, 2015, pp. 100–108.

[30] M. Martinez-Diaz, J. Fierrez, J. Galbally, and J. Ortega-Garcia, “An evaluation of indirect attacks and countermeasures in fingerprint verification systems,” *Pattern Recognition Letters*, vol. 32, no. 12, pp. 1643–1651, 2011.

[31] J. Galbally, A. Ross, M. Gomez-Barrero, J. Fierrez, and J. Ortega-Garcia, “Iris image reconstruction from binary templates: An efficient probabilistic approach based on genetic algorithms,” *Computer Vision and Image Understanding*, vol. 117, no. 10, pp. 1512–1525, 2013.

[32] M. Gomez-Barrero, J. Galbally, and J. Fierrez, “Efficient software attack to multimodal biometric systems and its application to face and iris fusion,” *Pattern Recognition Letters*, vol. 36, pp. 243–253, 2014.

[33] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, *Handbook of Fingerprint Recognition*. Springer London, 2009.

[34] J. Wayman, A. Jain, D. Maltoni, and D. Maio, “An Introduction to Biometric Authentication Systems,” in *Biometric Systems: Technology, Design and Performance Evaluation*, J. Wayman, A. Jain, D. Maltoni, and D. Maio, Eds. London: Springer London, 2005, pp. 1–20.

[35] K. W. Bowyer and M. J. Burge, *Handbook of Iris Recognition*. London: Springer London, 2016.

[36] F. Schroff, D. Kalenichenko, and J. Philbin, “FaceNet: {A} Unified Embedding for Face Recognition and Clustering,” *CoRR*, vol. abs/1503.0, 2015.

[37] Y. Wang, F. Agrafioti, D. Hatzinakos, and K. N. Plataniotis, “Analysis of Human Electrocardiogram for Biometric Recognition,” *EURASIP Journal on Advances in Signal Processing*, vol. 2008, no. 1, p. 148658, 2007.

[38] J. Daugman, “Information Theory and the IrisCode,” *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 2, pp. 400–409, Feb. 2016.

[39] J. Daugman, “The importance of being random: statistical principles of iris

recognition," *Pattern Recognition*, vol. 36, no. 2, pp. 279–291, 2003.

[40] J. Daugman and C. Downing, "Broken Symmetries, Random Morphogenesis, and Biometric Distance," *IEEE Transactions on Biometrics, Behavior, and Identity Science*, vol. 2, no. 3, pp. 271–278, 2020.

[41] A. K. Jain, A. A. Ross, and K. Nandakumar, "Iris Recognition," in *Introduction to Biometrics*, Boston, MA: Springer US, 2011, pp. 141–174.

[42] P. Hugo, "Towards Non-Cooperative Biometric Iris Recognition," University of Beira Interior, 2006.

[43] E. Wolff, "The Anatomy of the Eye and Orbit: including the Central Connections, Development and Comparative Anatomy of the Visual Apparatus," *Nature*, vol. 132, no. 3342, p. 767, 1933.

[44] J. Daugman, "How iris recognition works," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 14, no. 1, pp. 21–30, Jan. 2004.

[45] J. G. Daugman, "High confidence visual recognition of persons by a test of statistical independence," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 15, no. 11, pp. 1148–1161, 1993.

[46] A. W. K. Kong, D. Zhang, and M. S. Kamel, "An Analysis of IrisCode," *IEEE Transactions on Image Processing*, vol. 19, no. 2, pp. 522–532, 2010.

[47] J. Daugman, "Collision Avoidance on National and Global Scales: Understanding and Using Big Biometric Entropy," 2021.

[48] J. G. Daugman and C. Downing, "Radial correlations in iris patterns, and mutual information within IrisCodes," *IET Biom.*, vol. 8, pp. 185–189, 2019.

[49] C. Rathgeb, A. Uhl, and P. Wild, *Iris Recognition: From Segmentation to Template Security*. Springer, 2012.

[50] C. Rathgeb, A. Uhl, P. Wild, and H. Hofbauer, "Design Decisions for an Iris Recognition SDK," in *Handbook of Iris Recognition*, K. W. Bowyer and M. J. Burge, Eds. London: Springer London, 2016, pp. 359–396.

[51] "Center for Biometrics and Security Research." [Online]. Available: http://www.cbsr.ia.ac.cn/english/IrisDatabase.asp. [Accessed: 07-Jul-2021].

[52] "CASIA Iris Image Database." [Online]. Available: http://biometrics.idealtest.org/. [Accessed: 13-Jan-2022].

[53] Y.-L. Lai *et al.*, "Cancellable iris template generation based on Indexing-First-One hashing," *Pattern Recognition*, vol. 64, pp. 105–117, 2017.

[54] C. Rathgeb, F. Breitinger, and C. Busch, "Alignment-free cancelable iris biometric

templates based on adaptive bloom filters," in *2013 International Conference on Biometrics (ICB)*, 2013, pp. 1–8.

[55] W. J. Wong, M. L. D. Wong, Y. H. Kho, A. Beng, and J. Teoh, "Minutiae set to bit-string conversion using multi-scale bag-of-words paradigm," in *2014 IEEE International Workshop on Information Forensics and Security (WIFS)*, 2014, pp. 1–6.

[56] "Products – zwipe." [Online]. Available: http://zwipe.com/products/. [Accessed: 02-Nov-2018].

[57] "Fingerprint Analysis and Representation," in *Handbook of Fingerprint Recognition*, London: Springer London, 2009, pp. 97–166.

[58] "Introduction," in *Handbook of Fingerprint Recognition*, London: Springer London, 2009, pp. 1–56.

[59] D. Maltoni and R. Cappelli, "Fingerprint Recognition," in *Handbook of Biometrics*, A. K. Jain, P. Flynn, and A. A. Ross, Eds. Boston, MA: Springer US, 2008, pp. 23–42.

[60] W. J. Wong, A. B. J. Teoh, Y. H. Kho, and M. L. D. Wong, "Kernel PCA enabled bit-string representation for minutiae-based cancellable fingerprint template," *Pattern Recognition*, vol. 51, pp. 197–208, 2016.

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

[62] Z. Jin, M. H. Lim, A. B. J. Teoh, B. M. Goi, and Y. H. Tay, "Generating Fixed-Length Representation From Minutiae Using Kernel Methods for Fingerprint Authentication," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 46, no. 10, pp. 1415–1428, Oct. 2016.

[63] R. Cappelli, M. Ferrara, and D. Maltoni, "Minutia Cylinder-Code: A New Representation and Matching Technique for Fingerprint Recognition," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 32, no. 12, pp. 2128–2141, Dec. 2010.

[64] A. Juels and M. Wattenberg, "A Fuzzy Commitment Scheme," in *Proceedings of the 6th ACM Conference on Computer and Communications Security*, 1999, pp. 28–36.

[65] Y.-L. Lai, J. Y. Hwang, Z. Jin, S. Kim, S. Cho, and A. B. J. Teoh, "Symmetric keyring encryption scheme for biometric cryptosystem," *Information Sciences*, vol. 502, pp. 492–509, 2019.

[66] Z. Jin, J. Y. Hwang, Y. L. Lai, S. Kim, and A. B. J. Teoh, "Ranking-Based Locality Sensitive Hashing-Enabled Cancelable Biometrics: Index-of-Max Hashing," *IEEE*

Transactions on Information Forensics and Security, vol. 13, no. 2, pp. 393–407, Feb. 2018.

[67] N. Abe, S. Yamada, and T. Shinzaki, “Irreversible fingerprint template using Minutiae Relation Code with Bloom Filter,” in *2015 IEEE 7th International Conference on Biometrics Theory, Applications and Systems (BTAS)*, 2015, pp. 1–7.

[68] H. Xu, R. N. J. Veldhuis, T. A. M. Kevenaar, A. H. M. Akkermans, and A. M. Bazen, “Spectral minutiae: A fixed-length representation of a minutiae set,” in *2008 IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops*, 2008, pp. 1–6.

[69] H. Xu and R. N. J. Veldhuis, “Complex spectral minutiae representation for fingerprint recognition,” in *2010 IEEE Computer Society Conference on Computer Vision and Pattern Recognition - Workshops*, 2010, pp. 1–8.

[70] N. Abe and T. Shinzaki, “Vectorized fingerprint representation using Minutiae Relation Code,” in *2015 International Conference on Biometrics (ICB)*, 2015, pp. 408–415.

[71] W. J. Wong, M. L. D. Wong, and Y. H. Kho, “Multi-line code: A low complexity revocable fingerprint template for cancelable biometrics,” *Journal of Central South University*, vol. 20, no. 5, pp. 1292–1297, May 2013.

[72] “FVC-onGoing.” [Online]. Available: https://biolab.csr.unibo.it/FVCOnGoing/UI/Form/Home.aspx. [Accessed: 14-Jul-2021].

[73] D. Maio, D. Maltoni, R. Cappelli, J. L. Wayman, and A. K. Jain, “FVC2002: Second Fingerprint Verification Competition,” in *Object recognition supported by user interaction for service robots*, 2002, vol. 3, pp. 811–814 vol.3.

[74] D. Maio, D. Maltoni, R. Cappelli, J. L. Wayman, and A. K. Jain, “FVC2004: Third Fingerprint Verification Competition,” in *Biometric Authentication*, 2004, pp. 1–7.

[75] R. Cappelli, M. Ferrara, A. Franco, and D. Maltoni, “Fingerprint verification competition 2006,” *Biometric Technology Today*, vol. 15, no. 7, pp. 7–9, 2007.

[76] S. Z. Li and A. K. Jain, *Handbook of Face Recognition*. Springer London, 2011.

[77] M. Wang and W. Deng, “Deep face recognition: A survey,” *Neurocomputing*, vol. 429, pp. 215–244, 2021.

[78] A. Krizhevsky, I. Sutskever, and G. E. Hinton, “ImageNet Classification with Deep Convolutional Neural Networks,” *Commun. ACM*, vol. 60, no. 6, pp. 84–90, May 2017.

[79] B. Maze *et al.*, “IARPA Janus Benchmark - C: Face Dataset and Protocol,” in *2018 International Conference on Biometrics (ICB)*, 2018, pp. 158–165.

[80] Y. Sun, D. Liang, X. Wang, and X. Tang, “DeepID3: Face Recognition with Very Deep Neural Networks,” *CoRR*, vol. abs/1502.0, 2015.

[81] Y. Taigman, M. Yang, M. Ranzato, and L. Wolf, “DeepFace: Closing the Gap to Human-Level Performance in Face Verification,” in *2014 IEEE Conference on Computer Vision and Pattern Recognition*, 2014, pp. 1701–1708.

[82] C. Lu and X. Tang, “Surpassing Human-Level Face Verification Performance on LFW with GaussianFace,” *Proceedings of the AAAI Conference on Artificial Intelligence*, vol. 29, no. 1, 2015.

[83] Y. Sun, Y. Chen, X. Wang, and X. Tang, “Deep Learning Face Representation by Joint Identification-Verification,” in *Proceedings of the 27th International Conference on Neural Information Processing Systems - Volume 2*, 2014, pp. 1988–1996.

[84] G. B. Huang, M. Ramesh, T. Berg, and E. Learned-Miller, “Labeled Faces in the Wild: A Database for Studying Face Recognition in Unconstrained Environments,” Oct. 2007.

[85] E. Learned-Miller, G. B. Huang, A. RoyChowdhury, H. Li, and G. Hua, “Labeled Faces in the Wild: A Survey,” in *Advances in Face Detection and Facial Image Analysis*, M. Kawulok, M. E. Celebi, and B. Smolka, Eds. Cham: Springer International Publishing, 2016, pp. 189–248.

[86] S. Chauhan, A. S. Arora, and A. Kaul, “A survey of emerging biometric modalities,” *Procedia Computer Science*, vol. 2, pp. 213–218, 2010.

[87] D. Gafurov, “Emerging Biometric Modalities: Challenges and Opportunities,” in *Security Technology, Disaster Recovery and Business Continuity*, 2010, pp. 29–38.

[88] “ISO/IEC 19795-1:2021(en), Information technology — Biometric performance testing and reporting — Part 1: Principles and framework.” [Online]. Available: https://www.iso.org/obp/ui/#iso:std:iso-iec:19795:-1:ed-2:v1:en. [Accessed: 06-Jul-2021].

[89] J. Daugman, “Biometric decision landscapes,” 2000.

[90] A. K. Jain, A. A. Ross, and K. Nandakumar, *Introduction to Biometrics*. Springer US, 2011.

[91] “Major breach found in biometrics system used by banks, UK police and defence firms,” *The Guardian*. [Online]. Available: https://www.theguardian.com/technology/2019/aug/14/major-breach-found-in-biometrics-system-used-by-banks-uk-police-and-defence-firms. [Accessed: 09-Jan-2022].

[92] M. Grasdal, L. E. Hunter, M. Cross, L. Hunter, D. L. Shinder, and T. W. Shinder, “Chapter 11 - MCSE 70-293: Planning, Implementing, and Maintaining a Security Framework,” in *MCSE (Exam 70-293) Study Guide*, M. Grasdal, L. E. Hunter, M. Cross, L. Hunter, D. L. Shinder, and T. W. Shinder, Eds. Rockland: Syngress, 2003, pp. 781–859.

[93] M. Burnett and J. C. Foster, Eds., “Chapter 2 - Authenticating and Authorizing Users,” in *Hacking the Code*, Burlington: Syngress, 2004, pp. 53–108.

[94] C. Rathgeb, F. Breitinger, C. Busch, and H. Baier, “On application of bloom filters to iris biometrics,” *IET Biometrics*, vol. 3, no. 4, pp. 207–218, 2014.

[95] J. Hermans, B. Mennink, and R. 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)*, 2014, pp. 1–6.

[96] P. Lacharme, “Analysis of the Iriscodes Bioencoding Scheme,” no. 6, pp. 315–321, 2012.

[97] Y. Lee, Y. Chung, and K. Moon, “Inverse operation and preimage attack on BioHashing,” in *2009 IEEE Workshop on Computational Intelligence in Biometrics: Theory, Algorithms, and Applications*, 2009, pp. 92–97.

[98] M. Singh, R. Singh, and A. Ross, “A comprehensive overview of biometric fusion,” *Information Fusion*, vol. 52, pp. 187–205, 2019.

[99] M. Gomez-Barrero, C. Rathgeb, G. Li, R. Ramachandra, J. Galbally, and C. Busch, “Multi-biometric template protection based on bloom filters,” *Information Fusion*, vol. 42, pp. 37–50, 2018.

[100] S. Mirjalili and A. Lewis, “The Whale Optimization Algorithm,” *Advances in Engineering Software*, vol. 95, pp. 51–67, 2016.

[101] J. K. Pillai, V. M. Patel, R. Chellappa, and N. K. Ratha, “Sectored Random Projections for Cancelable Iris Biometrics,” in *2010 IEEE International Conference on Acoustics, Speech and Signal Processing*, 2010, pp. 1838–1841.

[102] J. K. Pillai, V. M. Patel, R. Chellappa, and N. K. Ratha, “Secure and Robust Iris Recognition Using Random Projections and Sparse Representations,” *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 33, no. 9, pp. 1877–1893, 2011.

[103] O. Ouda, N. Tsumura, and T. Nakaguchi, “Tokenless Cancelable Biometrics Scheme for Protecting Iris Codes,” in *2010 20th International Conference on Pattern*

Recognition, 2010, pp. 882–885.

[104] O. Ouda, N. Tusmura, and T. Nakaguchi, “Securing BioEncoded IrisCodes against Correlation Attacks,” in *2011 IEEE International Conference on Communications (ICC)*, 2011, pp. 1–5.

[105] O. OUDA, N. TSUMURA, and T. NAKAGUCHI, “On the Security of BioEncoding Based Cancelable Biometrics,” *IEICE Transactions on Information and Systems*, vol. E94.D, no. 9, pp. 1768–1777, 2011.

[106] J. Hämmerle-Uhl, E. Pschernig, and A. Uhl, “Cancelable iris-templates using key-dependent wavelet transforms,” in *2013 International Conference on Biometrics (ICB)*, 2013, pp. 1–8.

[107] Li Ma, Tieniu Tan, Yunhong Wang, and Dexin Zhang, “Efficient iris recognition by characterizing key local variations,” *IEEE Transactions on Image Processing*, vol. 13, no. 6, pp. 739–750, Jun. 2004.

[108] J. Hämmerle-Uhl, E. Pschernig, and A. Uhl, “Cancelable Iris Biometrics Using Block Re-mapping and Image Warping,” in *Information Security*, 2009, pp. 135–142.

[109] R. Dwivedi and S. Dey, “Cancelable iris template generation using look-up table mapping,” in *2015 2nd International Conference on Signal Processing and Integrated Networks (SPIN)*, 2015, pp. 785–790.

[110] R. Dwivedi, S. Dey, R. Singh, and A. Prasad, “A privacy-preserving cancelable iris template generation scheme using decimal encoding and look-up table mapping,” *Computers & Security*, vol. 65, pp. 373–386, 2017.

[111] Manisha and N. Kumar, “Cancelable Biometrics: a comprehensive survey,” *Artificial Intelligence Review*, vol. 53, no. 5, pp. 3403–3446, 2020.

[112] M. Gomez-Barrero, C. Rathgeb, J. Galbally, C. Busch, and J. Fierrez, “Unlinkable and irreversible biometric template protection based on bloom filters,” *Information Sciences*, vol. 370–371, pp. 18–32, 2016.

[113] J. Bringer, C. Morel, and C. Rathgeb, “Security analysis of Bloom filter-based iris biometric template protection,” in *2015 International Conference on Biometrics (ICB)*, 2015, pp. 527–534.

[114] Y. Lai, B. Goi, and T. Chai, “Alignment-free indexing-first-one hashing with bloom filter integration,” in *2017 IEEE International Conference on Intelligence and Security Informatics (ISI)*, 2017, pp. 78–82.

[115] A. S and K. S. AnilKumar, “Iris template protection using double bloom filter based feature transformation,” *Computers & Security*, vol. 97, p. 101985, 2020.

[116] T. Connie, A. Teoh, M. Goh, and D. Ngo, "PalmHashing: a novel approach for cancelable biometrics," *Information Processing Letters*, vol. 93, no. 1, pp. 1–5, 2005.

[117] A. B. J. Teoh, A. Goh, and D. C. L. Ngo, "Random Multispace Quantization as an Analytic Mechanism for BioHashing of Biometric and Random Identity Inputs," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 28, no. 12, pp. 1892–1901, Dec. 2006.

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

[119] C. S. Chin, A. T. B. Jin, and D. N. C. Ling, "High security Iris verification system based on random secret integration," *Computer Vision and Image Understanding*, vol. 102, no. 2, pp. 169–177, 2006.

[120] A. B. J. Teoh and C. T. Yuang, "Cancelable Biometrics Realization With Multispace Random Projections," *IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics)*, vol. 37, no. 5, pp. 1096–1106, Oct. 2007.

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

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

[123] M. Savvides, B. V. K. V. Kumar, and P. K. Khosla, "Cancelable biometric filters for face recognition," in *Proceedings of the 17th International Conference on Pattern Recognition, 2004. ICPR 2004.*, 2004, vol. 3, pp. 922-925 Vol.3.

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

[125] M. Ferrara, D. Maltoni, and R. Cappelli, "Noninvertible Minutia Cylinder-Code Representation," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 6, pp. 1727–1737, Dec. 2012.

[126] M. Ferrara, D. Maltoni, and R. Cappelli, "A two-factor protection scheme for MCC fingerprint templates," in *2014 International Conference of the Biometrics Special Interest Group (BIOSIG)*, 2014, vol. P-230, pp. 1–8.

[127] M. S. Charikar, “Similarity Estimation Techniques from Rounding Algorithms,” in *Proceedings of the Thiry-fourth Annual ACM Symposium on Theory of Computing*, 2002, pp. 380–388.

[128] J. Kim and A. B. J. Teoh, “One-factor Cancellable Biometrics based on Indexing-First-Order Hashing for Fingerprint Authentication,” in *2018 24th International Conference on Pattern Recognition (ICPR)*, 2018, pp. 3108–3113.

[129] L. Nanni and A. Lumini, “Empirical tests on BioHashing,” *Neurocomputing*, vol. 69, no. 16, pp. 2390–2395, 2006.

[130] E. Maiorana, P. Campisi, and A. Neri, “Bioconvolving: Cancelable templates for a multi-biometrics signature recognition system,” in *2011 IEEE International Systems Conference*, 2011, pp. 495–500.

[131] P. P. Paul and M. Gavrilova, “Multimodal Cancelable Biometrics,” in *2012 IEEE 11th International Conference on Cognitive Informatics and Cognitive Computing*, 2012, pp. 43–49.

[132] Y. J. Chin, T. S. Ong, A. B. J. Teoh, and K. O. M. Goh, “Integrated biometrics template protection technique based on fingerprint and palmprint feature-level fusion,” *Information Fusion*, vol. 18, pp. 161–174, 2014.

[133] C. Rathgeb, M. Gomez-Barrero, C. Busch, J. Galbally, and J. Fierrez, “Towards cancelable multi-biometrics based on bloom filters: a case study on feature level fusion of face and iris,” in *3rd International Workshop on Biometrics and Forensics (IWBF 2015)*, 2015, pp. 1–6.

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

[135] M. Ao and S. Z. Li, “Near Infrared Face Based Biometric Key Binding,” in *Advances in Biometrics*, 2009, pp. 376–385.

[136] Y. C. Feng, P. C. Yuen, and A. K. Jain, “A Hybrid Approach for Generating Secure and Discriminating Face Template,” *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 1, pp. 103–117, Mar. 2010.

[137] Z. Jin, A. B. J. Teoh, B.-M. Goi, and Y.-H. Tay, “Biometric cryptosystems: A new biometric key binding and its implementation for fingerprint minutiae-based representation,” *Pattern Recognition*, vol. 56, pp. 50–62, 2016.

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

[139] M. Gomez-Barrero, J. Galbally, J. Fierrez, and J. Ortega-Garcia, “Hill-Climbing Attack Based on the Uphill Simplex Algorithm and Its Application to Signature Verification,” in *Biometrics and ID Management*, 2011, pp. 83–94.

[140] M. Gomez-Barrero, J. Galbally, J. Fierrez, and J. Ortega-Garcia, “Face verification put to test: A hill-climbing attack based on the uphill-simplex algorithm,” in *2012 5th IAPR International Conference on Biometrics (ICB)*, 2012, pp. 40–45.

[141] J. A. Nelder and R. Mead, “A Simplex Method for Function Minimization,” *The Computer Journal*, vol. 7, no. 4, pp. 308–313, Jan. 1965.

[142] A. Pashalidis, “Simulated annealing attack on certain fingerprint authentication systems,” in *2013 International Conference of the BIOSIG Special Interest Group (BIOSIG)*, 2013, pp. 1–11.

[143] D. E. Goldberg, *Genetic Algorithms in Search, Optimization and Machine Learning*, 1st ed. USA: Addison-Wesley Longman Publishing Co., Inc., 1989.

[144] C. Rathgeb, A. Uhl, and P. Wild, “Shifting score fusion: on exploiting shifting variation in iris recognition,” in *SAC ’11*, 2011.

[145] A. W. K. Kong, D. Zhang, and M. Kamel, “Introduction to the IrisCode Theory,” in *Handbook of Iris Recognition*, K. W. Bowyer and M. J. Burge, Eds. London: Springer London, 2016, pp. 229–245.

[146] J. R. Matey, R. Broussard, and L. Kennell, “Iris image segmentation and sub-optimal images,” *Image and Vision Computing*, vol. 28, no. 2, pp. 215–222, 2010.

[147] C. Rathgeb, H. Hofbauer, A. Uhl, and C. Busch, “TripleA: Accelerated accuracy-preserving alignment for iris-codes,” *2016 International Conference on Biometrics (ICB)*, pp. 1–8, 2016.

[148] H. Ma, N. Hu, and C. Fang, “The biometric recognition system based on near-infrared finger vein image,” *Infrared Physics & Technology*, p. 103734, 2021.

[149] R. Anusha and C. D. Jaidhar, “Human gait recognition based on histogram of oriented gradients and Haralick texture descriptor,” *Multimedia Tools and Applications*, vol. 79, no. 11, pp. 8213–8234, 2020.

[150] M. Sharifnejad, A. Shahbahrami, A. Akoushideh, and R. Z. Hassanpour, “Facial expression recognition using a combination of enhanced local binary pattern and pyramid histogram of oriented gradients features extraction,” *IET Image Processing*, vol. 15, no. 2, pp. 468–478, 2021.

[151] W. T. Freeman, K. Tanaka, J. Ohta, and K. Kyuma, “Computer vision for computer games,” in *Proceedings of the Second International Conference on Automatic Face*

and Gesture Recognition, 1996, pp. 100–105.

[152] R. K. McConnell, “Method of and apparatus for pattern recognition.”

[153] N. Dalal and B. Triggs, “Histograms of oriented gradients for human detection,” in *2005 IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR’05)*, 2005, vol. 1, pp. 886–893 vol. 1.

[154] A. Uhl and P. Wild, “Weighted adaptive Hough and ellipsopolar transforms for real-time iris segmentation,” in *2012 5th IAPR International Conference on Biometrics (ICB)*, 2012, pp. 283–290.

[155] L. Masek, “Recognition of Human Iris Patterns for Biometric Identification,” 2003.

[156] W. J. Scheirer and T. E. Boult, “Cracking Fuzzy Vaults and Biometric Encryption,” in *2007 Biometrics Symposium*, 2007, pp. 1–6.

[157] B. Tams, P. Mihailescu, and A. Munk, “Security Considerations in Minutiae-Based Fuzzy Vaults,” *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 5, pp. 985–998, May 2015.

[158] E. H. Mckinney, “Generalized Birthday Problem,” *The American Mathematical Monthly*, vol. 73, no. 4, pp. 385–387, 1966.

[159] M. Gomez-Barrero, J. Galbally, C. Rathgeb, and C. Busch, “General Framework to Evaluate Unlinkability in Biometric Template Protection Systems,” *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 6, pp. 1406–1420, Jun. 2018.

[160] C. Rathgeb and C. Busch, “Cancelable multi-biometrics: Mixing iris-codes based on adaptive bloom filters,” *Computers & Security*, vol. 42, pp. 1–12, 2014.

[161] W. Yang, J. Hu, and S. Wang, “A Finger-Vein Based Cancellable Bio-cryptosystem,” in *Network and System Security*, 2013, pp. 784–790.

[162] W. Yang *et al.*, “Securing Mobile Healthcare Data: A Smart Card Based Cancelable Finger-Vein Bio-Cryptosystem,” *IEEE Access*, vol. 6, pp. 36939–36947, 2018.

[163] R. Cappelli, D. Maio, D. Maltoni, J. L. Wayman, and A. K. Jain, “Performance evaluation of fingerprint verification systems,” *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 28, no. 1, pp. 3–18, Jan. 2006.

[164] Y. Guo, L. Zhang, Y. Hu, X. He, and J. Gao, “MS-Celeb-1M: {A} Dataset and Benchmark for Large-Scale Face Recognition,” *CoRR*, vol. abs/1607.0, 2016.

[165] “GitHub - davidsandberg/facenet: Face recognition using Tensorflow.” [Online]. Available: https://github.com/davidsandberg/facenet. [Accessed: 05-Dec-2021].

[166] “GitHub - FingerJetFXOSE/FingerJetFXOSE: Fingerprint Feature Extractor; the initial contribution by DigitalPersona is MINEX Compliant (SDK 3F).” [Online]. Available:

https://github.com/FingerJetFXOSE/FingerJetFXOSE. [Accessed: 05-Dec-2021].

[167] G. Li, B. Yang, C. Rathgeb, and C. Busch, “Towards generating protected fingerprint templates based on bloom filters,” in *3rd International Workshop on Biometrics and Forensics (IWBF 2015)*, 2015, pp. 1–6.

[168] W. Yang, J. Hu, S. Wang, and Q. Wu, “Biometrics Based Privacy-Preserving Authentication and Mobile Template Protection,” *Wireless Communications and Mobile Computing*, vol. 2018, p. 17, 2018.

[169] C. Li and J. Hu, “Attacks via Record Multiplicity on Cancelable Biometrics Templates,” *Concurr. Comput. : Pract. Exper.*, vol. 26, no. 8, pp. 1593–1605, Jun. 2014.

[170] A. K. Jain, K. Nandakumar, and A. Nagar, “Fingerprint Template Protection: From Theory to Practice,” in *Security and Privacy in Biometrics*, P. Campisi, Ed. London: Springer London, 2013, pp. 187–214.

[171] K. Zhang, Z. Zhang, Z. Li, and Y. Qiao, “Joint Face Detection and Alignment Using Multitask Cascaded Convolutional Networks,” *IEEE Signal Processing Letters*, vol. 23, no. 10, pp. 1499–1503, Oct. 2016.

[172] X. Yuan, Z. Miao, Z. Liu, Z. Yan, and F. Zhou, “Multi-Strategy Ensemble Whale Optimization Algorithm and Its Application to Analog Circuits Intelligent Fault Diagnosis,” *Applied Sciences*, vol. 10, no. 11, 2020.

[173] “Intel® Instruction Set Extensions Technology.” [Online]. Available: https://www.intel.com/content/www/us/en/support/articles/000005779/processors.html. [Accessed: 24-Oct-2021].

END OF DOCUMENT