DESIGN OF PROTECTED IRIS RECOGNITION SYSTEMS WITH IMPROVED AUTHENTICATION PERFORMANCE

CHAI TONG YUEN

DOCTOR OF PHILOSOPHY (ENGINEERING)

LEE KONG CHIAN FACULTY OF ENGINEERING AND SCIENCE
UNIVERSITI TUNKU ABDUL RAHMAN
JANUARY 2022

DESIGN OF PROTECTED IRIS RECOGNITION SYSTEMS WITH IMPROVED AUTHENTICATION PERFORMANCE

By

CHAI TONG YUEN

A PHD thesis submitted to
Lee Kong Chian Faculty of Engineering and Science,
Universiti Tunku Abdul Rahman,
in partial fulfillment of the requirements for the degree of
Doctor of Philosophy (Engineering)
January 2022

ABSTRACT

DESIGN OF PROTECTED IRIS RECOGNITION SYSTEMS WITH IMPROVED AUTHENTICATION PERFORMANCE

Chai Tong Yuen

Iris is unique with higher confidence in matching as compared to other biometric traits. No physical contact, difficult to spoof and not easily replaceable are among the advantages of iris recognition system. However, permanent identity loss will be experienced if the raw iris code is being stolen. Biometric template protection (BTP) schemes are implemented to increase public confidence in biometric systems regarding data privacy and security. The design of BTP has naturally incurred a loss of information which leads to performance degradation at the matching stage. Despite some extended works from these iris BTP schemes, there is still lack of a generalized solution for this problem. A trainable model that requires no further modification on the protected iris templates has been proposed in this thesis to improve the authentication performance. Improvement between 14% - 82% has been reported against four publicly available iris research databases: CASIAv1, CASIAv3, CASIAv4 and ND0405. Another BTP technique, namely key binding scheme can become vulnerable due to the inherent dependency of biometric features and the capacity of error correction code (ECC). Previous literature has shown deterioration in performance without the alignment process at iris codes. In this thesis, an alignment free cancelable iris key binding scheme without ECC has been proposed. The highest genuine acceptance rate (GAR) of 96.37% at zero false acceptance rate (FAR) has been achieved on CASIA-v3-interval iris

database. The best performance can also be preserved with key length up to 200 bits. Next, focus has been put on the security concern caused by the iris code's alignment process during matching. This process can only be conducted on probe iris codes for most of the protected iris recognition systems. In addition, high correlation between adjacent iris codes has indicated dependency along vertical direction. Thus, an iris template transformation method and a matching strategy are proposed to mitigate the alignment and inherent dependency issues of iris codes in this work. The proposed model has optimized the authentication performance of iris code by achieving EER as low as 0.46% on CASIA-v3-interval iris database. Thus, vertical dependency in iris code has been mitigated while bit-shifting alignment can be applied directly onto the transformed cancelable iris template through the proposed method. In a nutshell, three methods have been proposed in this thesis to improve the authentication performance and flexibility of protected iris recognition systems.

ACKNOWLEDGMENT

Throughout the writing of this dissertation I have received a great deal of support. First of all, I feel thankful for the PhD scholarship from Universiti Tunku Abdul Rahman. I would like to thank my supervisor, Professor Dr. Goi Bok Min, whose expertise was invaluable in formulating the research questions and methodology. I appreciate also the insightful feedback from my co-supervisor, Dr. Yap Wun She who often sharpens my thinking and brought my work to a higher level.

I would like to acknowledge my colleagues Dr. Lai Yen Lung for your patient support and sharing throughout my research. In addition, I would like to thank my encouraging parents and family members for their tremendous support and sympathetic ear. You are always there for me. Finally, I could not have completed this dissertation without the moral support of my friend, Dr. Ong Chuan Fang who provided countless happy distractions to rest my mind outside of my research.

LEE KONG CHIAN FACULTY OF ENGINEERING AND SCIENCE

UNIVERSITI TUNKU ABDUL RAHMAN

Date: 24 JAN 2022

SUBMISSION OF FINAL YEAR PROJECT /DISSERTATION/THESIS

It is hereby certified that Chai Tong Yuen (ID No: ***1501021***) has completed this PhD thesis entitled "*Design of Protected Iris Recognition Systems with Improved Authentication Performance*" under the supervision of Prof. Dr. Goi Bok Min (Supervisor) from the Department of Mechatronics and Biomedical Engineering, Lee Kong Chian Faculty of Engineering and Science, and Dr. Yap Wun She (Co-Supervisor)* from the Department of Electrical and Electronic Engineering, Lee Kong Chian Faculty of Engineering and Science

I understand that University will upload softcopy of my PhD thesis in pdf format into UTAR Institutional Repository, which may be made accessible to UTAR community and public.

Yours truly,

_____

(*CHAI TONG YUEN*)

APPROVAL SHEET

This dissertation/thesis entitled "**DESIGN OF PROTECTED IRIS RECOGNITION SYSTEMS WITH IMPROVED AUTHENTICATION PERFORMANCE"** was prepared by CHAI TONG YUEN and submitted as partial fulfillment of the requirements for the degree of Doctor of Philosophy in Engineering at Universiti Tunku Abdul Rahman.

Approved by:

_____
(Prof. Ir. Dr. Goi Bok Min)

Date: 25/1/2022
Professor/Supervisor
Department of Mechatronics and Biomedical Engineering
Lee Kong Chian Faculty of Engineering and Science
Universiti Tunku Abdul Rahman

_____
(Dr. Yap Wun She)

Date: 25/1/2022
Associate Professor/Co-supervisor
Department of Electrical and Electronic Engineering
Lee Kong Chian Faculty of Engineering and Science
Universiti Tunku Abdul Rahman

DECLARATION

I hereby declare that the dissertation is based on my original work except for quotations and citations which have been duly acknowledged. I also declare that it has not been previously or concurrently submitted for any other degree at UTAR or other institutions.

Name: **CHAI TONG YUEN**

Date: **24 JAN 2022**

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

BTP	Biometric template protection
BCS	Biometric cryptosystem
CB	Cancelable biometric
CBV	Cancelable biometric vault
CNN	Convolutional neural network
ECC	Error correction code
EER	Equal Error Rate
FAR	False Acceptance Rate
FPR	False Positive Rate
FRR	False Rejection Rate
FCS	Fuzzy commitment scheme
FVS	Fuzzy vault scheme
GAR	Genuine Acceptance Rate
HD	Hamming distance
IFO	Indexing-first-one
KRR	Key retrieval rate
LSH	Local Sensitive Hashing
MAC	Message authentication code
ROI	Region of interest
ROC	Receiver Operating Characteristic
TPR	True Positive Rate

TABLE OF CONTENTS

CHAPTER 1

INTRODUCTION

1.1 Biometric System

Over the last few decades, biometric systems had been widely implemented in our daily life through biometric authentication and verification. Its applications can be ranged from smartphone unlocking system to identity authentication system at international airport. Biometrics system becomes a reliable alternative compared to traditional security systems which are mostly based on PINs, tokens and passwords. This is because the traditional approach can be easily forgotten, lost and stolen.

Biometric system serves as an advanced security system that uses biometric information of a person for the purposes of verification or authentication. There are human traits that contain measurable characteristics due to its distinctiveness, universality and permanence. These biometric identifiers can often be categorized as physiological characteristics and behavioural characteristics. Examples of physiological characteristics include but are not limited to face recognition, fingerprint, hand geometry, ear geometry, iris recognition and palm print. Behavioural characteristics are referring to the pattern of an individual's behavior which includes but is not limited to keystroke, voice, gait recognition, signature recognition and typing rhythm.

Among these biometric traits, iris recognition can be achieved without physical contact and even at a distance with the advancement of technology. Iris recognition is reliable due to its natural randomness. Iris started to form since the third month of gestation and the iris features are largely completed by the eighth month of gestation. According to Daugman (Daugman, 2004b), the inventor of the favourite iris feature representation known as iris code, every iris is unique even from the same person or identical twins. The entropy of the iris pattern is typically higher than other biometric traits based on his validation in (Daugman, 2006). This infers that the false matches between Iris codes are very unlikely to happen. Therefore, iris provides higher confidence for identification task apart from the verification. Moreover, iris is not affected much by ageing and will remain stable for many years. In this case, data update needs not to be done frequently like other biometric traits (Flom and Safir, 1987). As an internal organ, iris is safely protected by eyelid, cornea layer and aqueous humour from the outer environment. Iris as a human organ, cannot be stolen and is hard to replicate under normal circumstances.

Biometrics can be used for different purposes. When comes to biometrics-based system, there are mainly divided into either an authentication system or an identification system. Authentication systems aim to answer the questions “are you the person who you say you are?” In this system, an individual presents and claims himself or herself as a specific identity. The system will then check against an existing profile in database which is linked to the claimed identity for authentication purpose. This process can be better described as a 1-to-1 matching. Authentication process is often faster and more accurate then identification process even when the database becomes larger in

size. This is because authentication systems only compare the presented biometric with the claimed biometric reference in the database. Thus, results can be generated more quickly. On the other side, identification systems aim to ask "who are you?" or answer "who generated this biometric?" The system will check against all the registered biometric profiles in the database to identify the unknown biometric. This process can be described as a 1-to-n matching system, where n is the total number of biometric profiles in the database. This system is particularly useful when government needs to identify a latent fingerprint at a crime scene to see if it matches any of the registered fingerprints in forensic database.

For both iris authentication or identification tasks, an individual has to first enrol his/her iris data into the system. The iris data is then stored as a template (e.g., iris code) in the database. During the authentication process, only the right person can be authenticated or identified successfully by achieving a higher score when matching with the iris code of the genuine user. With the successful deployment of larger-scale iris recognition systems at the airports and hospitals (Sasse, 2007), many concerns have been raised. More people started to question the security aspects of biometric system. Biometric applications are often considered as unsecure due to the misuse of biometric data and identity management (Cimato et al., 2009). This concern is acceptable because biometric information is tied to a person inherently by using one's biometric traits as the "key". This means that the token cannot be easily replaced with a new one unlike traditional security system. Therefore, if the biometric information of a person, for instance an iris code is being compromised, such biometric trait will become

useless in all the involved biometric applications. This indicates a lifetime permanent identity loss to the user.

Other than security issue in iris authentication, non-ideal conditions have limited for the growth of biometric technology especially when users' cooperation is not required. Iris segmentation plays an essential part as well in the performance of iris recognition system. Traditional iris segmentation methods are based on specific underlying presumptions which often involve complicated algorithms with heavy calculations and parameters, sensitive to noise and time-consuming (He et al., 2008). These algorithms cannot cope with all the non-ideal constraints such as occlusion, illumination challenges, motions and user cooperation captured in different iris databases. These constraints caused the iris boundaries to show unexpected variation across their contours and intensities (Bowyer and Burge, 2016). During the iris image acquisition process, off-angle iris, motion blur, non-cooperative subjects and usage of contact lenses are among the main causes of low quality iris images. The intensity dissimilarity between iris and pupil might be reduced, thus, affecting the performance of the segmentation algorithms. Before the introduction of deep learning, the hypothesis of the non-ideal iris segmentation method is mainly based on the conditions set by the researchers. The robustness of these algorithms is indeed arguable when dealing with infinite non-ideal situations. For future work, deep learning in another way provides a generalized solution for this issue in order to develop a full-stack protected iris recognition system (Höft et al., 2014).

1.2 Biometric Template Protection (BTP)

The practicality and the risk of key management on storage and release remain challenging in cryptography. A simple password is susceptible to dictionary attacks (Klein, 1990) while lengthy passwords are difficult to remember and maintain. The security of generic cryptographic systems is weak due to practicality and nonrepudiation. This is because the password is not directly tied to a user, thus it is unable for the system to differentiate a legitimate user from an attacker. The limitations of traditional cryptographic key management incorporating passwords can be meliorated by biometric authentication. However, it is still vulnerable, as biometric data can be intercepted, stolen, altered, and replayed. This causes an invasion of identity privacy when unauthorized parties can get access through various attacks such as spoofing attacks, replay attacks, and masquerade attacks (Jain et al., 2006). These attacks affect user's confidence and lead to a lack of acceptance in biometric technology.

Apparently, encryption of the biometric templates seems to be the solution to this problem. However, cryptography does not tolerate single bit error while hashed versions of the same users can be different due to the variance in biometric samples. The idea to bind biometrics with cryptographic keys then paves an alternative in managing cryptographic keys and template protection at one go (Juels and Wattenberg, 1999). This makes biometrics security an important field of research. In this field, biometric template protection (BTP) serves as a protection step in securing biometric system by repeatedly distorting the biometric data through different transformations. The authentication of the

transformed template will be conducted in a secured domain. The transformed templates under BTP scheme are irreversible and non-decryptable to protect the privacy and security of the raw biometric information. Thus, it is more secure to store the transformed templates into the database rather than the original biometric templates (Cavoukian and Stoianov, 2011). Since the matching stage can be held in a transformed domain, raw biometric information will not be exposed to any potential threat. There are several types of BTP schemes which can be normally categorized into Biometric Cryptosystem (BCS) and Cancelable Biometric (CB). These schemes are designed to fulfill irreversibility, revocability, and unlinkability for data privacy's preservation.

The main concept of BCS is to securely bind a digital key to a biometric (key binding), or extract a key from the biometric (key generation) to ensure that it must be computationally difficult to retrieve either the key or the biometric from the stored template, which is also known as the "helper data" (Jain et al., 2008). In key binding systems, BCS is required to store helper data that is biometric trait dependent. This information is a combination of the biometric template and the cryptography key. Helper data is used to retrieve the cryptographic key from the templates. The key will be retrieved only if the query template contains sufficient similarity during authentication. BCS will store the biometric-dependent helper data instead of the cryptographic key. All of these properties of BCSs offer substantial security benefits to biometrics (Jain et al., 2004). For key generation, keys can be generated directly from the helper data and a given query biometric template. These schemes are also known as fuzzy extractors or secure sketch, as defined in (Dodis et al., 2004, Verbitskiy et al., 2010). The difficulty in realizing key generation schemes is the high intra-user

variability in biometrics that causes contradiction in achieving high key entropy and stability in authentication (Jain et al., 2008). The fact that the original design is not catered for cancelability and unlinkability also makes this scheme less popular compared to the key binding.

On the other hand, helper data is generated by binding a cryptographic key to a biometric template. Therefore, helper data is actually the fusion of the cryptographic key and biometric template. Fuzzy commitment (Juels and Wattenberg, 1999) and fuzzy vault (Juels and Sudan, 2006) are two main schemes designed for key binding. These schemes usually apply error correction code (ECC) to deal with the variance of biometric data in authentication. The independently generated cryptographic key is revocable, but re-enrollment is required whenever an update of the key is necessary. Despite the security properties and stability of this scheme, there are several drawbacks and vulnerabilities which will be discussed in the upcoming sections.

Cancelable biometrics is another scheme for biometric template protection involving repeated efforts to distort the biometric template through transformation. Authentication can then be conducted in the transformed domain (Ratha et al., 2007). The transformed templates are irreversible and computationally impossible to be decrypted. Thus, it is more secure to be stored in the database (Cavoukian and Stoianov, 2011). New templates can always be regenerated through different transformations for compromised cases. There are four important criteria to be fulfilled for the design of a good cancelable biometric scheme (Simoens et al., 2012):

1. Unlinkability (Gomez-Barrero et al., 2017): It should be computationally hard to determine whether the protected biometric templates originate from

the same biometric instance or not to avoid cross-matching across different applications.

2. Revocability: It should be computationally infeasible to derive its original data from multiple protected templates.
3. Non-Invertibility of Irreversibility (Inuma, 2014): It should be computationally infeasible to derive its original biometric data from the protected template and/or the helper data.
4. Performance: The accuracy of the cancelable template in recognition performance should be approximately preserved with respect to its original counterparts without the template protection scheme.

1.3 Problem Statements

1.3.1 Performance Degradation in Cancelable Iris BTP Schemes

Iris code contains discriminative information of a user for iris recognition. The exposure of the iris code to an adversary may lead to security breaches such as masquerade attack and replay attack (Venugopalan and Savvides, 2011, Galbally et al., 2013, Cappelli et al., 2007). The privacy concern and related challenges of iris code can be tackled by BTP technology (Natgunanathan et al., 2016, Jain et al., 2008). While the BTP schemes which fulfil the requirements above can secure a biometric system, there are still drawbacks and remaining issues in the search of optimum balance between system's performance and security. BTP schemes which emphasize more on security protection most often distort the biometric data severely via different transformations in order to achieve better entropy, irreversibility and unlinkability. These processes inevitably cause higher loss of useful information

and thus performance degradation in exchange for better security. In other words, most of the good iris BTP schemes which provide stronger security features will expect weaker performance as the drawback. Knowing the effect of this tradeoff, there are also efforts by respective iris BTP schemes (Mitzenmacher, 2002, Lai et al., 2017a) to introduce remedies such as optimizing the selection of parameters and some of the steps to mitigate the performance degradation. It is a non-trivial task to offer security guaranty to biometric template while preserving the recognition rate. This has been one of the major requirements in designing an iris BTP scheme. Some works have been done (see (Prabhakar et al., 2003, Rathgeb and Uhl, 2011d, Patel et al., 2015, Natgunanathan et al., 2016) for complete surveys) to support security of biometric template without severely deteriorate the system performance. Nevertheless, since there is a plethora of iris BTP schemes being proposed, it introduces another issue on how to determine and select the best iris BTP scheme. To address the above-mentioned issues, a method that can be generally adopted for different iris template protection schemes to improve their recognition performance is indeed required.

1.3.2 Issues in Iris Key Binding Schemes

BCS aims to protect and secure cryptographic key by binding it with the biometric information. The binding process is expected to be stable despite the intrinsic variability of biometric templates from the same user. One desired feature of key binding techniques is the generation of revocable helper data. Therefore, a new key can be generated for the same user when the previous cryptographic key is compromised.

Generally, cryptographic keys are embedded into the biometric templates to make the key recovery computationally hard or impossible during authentication (Nandakumar and Jain, 2015). Two well-known BCSs, fuzzy commitment scheme (FCS) (Juels and Wattenberg, 1999) and fuzzy vault scheme (FVS) (Juels and Sudan, 2006) have implemented error correction codes (ECC) to mitigate the effect of intra-class variability between biometric templates. Hence, the performance of these schemes particularly key length and decoding accuracy are bounded by the capability of the deployed ECC (Ouda et al., 2021). Inevitably, trade off issue exists between the key length and system accuracy for similar techniques.

Privacy leakage is another issue bothering BCSs. For example, adversary can first encodes the compromised key using the ECC deployed in FCS. Then, the biometric information can be recovered when the result is being XORed with the secure sketch. The recovery of the biometric information seems straight forward once the secure sketch and its linked cryptographic key are compromised (Natgunanathan et al., 2016). In terms of feature representation of these key binding techniques, FCS is designed for the security of binary templates, for instance iris codes while FVS suits fingerprint templates (minutiae based) better since it requires the biometric features to be represented as point sets. Additional conversion or processing steps will be needed to overcome this restriction if the biometric data of a protected template has a different representation. Thus, a more generic and flexible key binding framework is needed to address the issues regarding privacy leakage and biometric data representation. To avoid unnecessary processing efforts, a more flexible and

representation-independent key binding framework is therefore being proposed in this thesis.

1.3.3 Performance and Security Issues of Iris Code

One of the challenges in designing the cancelable transformation function for iris template is the requirement on alignment. This is particularly important for iris codes because the matching between different iris codes has to be conducted iteratively with arbitrary number of left or right bit shifts over the query iris code. The purpose of having different number of left / right bits shifting is to calculate the best match among all possible variations caused by the head tilt or cyclovergence (Daugman, 1993). Despite the fact that a lot of externals constraints can be applied for more stable and concise iris image acquisition, the inherited alignment issues due to the slight rotation cannot be completely eliminated. In designing a BTP scheme, the non-invertibility can only be achieved with additional auxiliary data (i.e., random matrices used in Bio-hashing) that introduces randomization to the input. Without pre-alignment, cancelable transformation with extra randomization would result in lower distinguishability for genuine authenticity, hence deteriorating system's recognition performance. This impact has been reported in most of the state-of-the-arts working on iris template protection schemes (Lai et al., 2016, Sadhya and Raman, 2019, Zuo et al., 2008).

A pre-alignment is necessary to account for the rotational inconsistencies which require the shifting of the probe iris code before conducting every matching in a secure domain. However, implementing a pre-alignment method increases the risk of the probe iris code being compromised since the system for

matching can potentially be hacked or hijacked by a third party. In view of this, for an Iris template protection scheme to be practically useful, the pre-alignment step which takes probe iris code as the input must be avoided. Instead, it is desirable that the system accepts only the protected iris template during matching stage without any pre-alignment steps. One notable approach of the alignment-free cancelable transformation without pre-alignment has been proposed by Rathgeb et al. (Rathgeb et al., 2013). This method has shown promising authentication performance while facing security issues due to the small key space (i.e., around 10 bits) in order to preserve the accuracy performance. Thus, designing an alignment-free cancelable transformation for iris features, for instance iris code remains a great challenge for the future implementation of protection iris recognition system.

1.4 Motivation and Contribution

1.4.1 Performance Improvement for Protected Iris Recognition System with Confidence Matrix

The proposed method contributes to tackle the performance degradation issue of iris BTP via the generation of confidence matrix. This matrix can be generally adopted for different iris protected templates of different BTP schemes. This generic solution is able to further improve the recognition performance of the protected (hashed) iris templates in iris biometric systems. Firstly, the proposed method requires no modification in order to integrate into the original algorithms of iris BTP scheme. The design of this method is kept simple and implementable onto iris protected templates of arbitrary BTP schemes. Another important feature of the proposed method is the ability to

improve the iris recognition performance further through training samples. Apart from this, the potential security threat of using confidence matrix is analyzed in terms of information leakage and security attacks through irreversibility and unlinkability studies.

Some publicly available iris research databases come with noise masks. This is another potential factor affecting recognition performance of a protected iris biometric system especially when this feature cannot be utilized by certain schemes in matching stage. This method has incorporated the information from noise masks with the proposed confidence matrix in matching stage. This allows the scheme to work on noise masks associated iris database. In this work, the proposed method has improved the recognition performance involving integer hashed values in matching stage. Probability based confidence matrix has been proposed to accelerate the authentication performance of protected iris templates from iris databases with different image quality. In a nutshell, the proposed method has shown great flexibility in dealing with the implemented iris template protection scheme, different hashed iris data types and iris databases with varying image quality. The proposed method has high adaptability on various iris databases with or without noise masks while having good potential to further improve its recognition performance via its trainable capability.

1.4.2 Cancelable Iris Key Binding Scheme

As highlighted in the previous section, there are limitations in both biometric cryptosystem and cancelable biometrics. ECC based biometric cryptosystem is often limited by its error correcting capacity and feasibility. It is susceptible to attacks such as statistical attack and trade-off between

performance and security. In addition, the performance of biometrics such as iris and fingerprint are always affected by alignment issue and the processes to reduce this effect are often tedious and time consuming.

The proposed iris key binding design is leveraging on both biometric systems to tackle this open problem. In this thesis, an alignment free cancelable iris key binding scheme is proposed without depending on ECC. The idea of this scheme is based on chaffing and winnowing besides Jin's scheme (Jin et al., 2016). This concept is often used in cryptology for data encryption when transferring through an insecure channel where direct application to biometrics is inappropriate due to the randomness and variability nature. This work has adopted Indexing-First-One (IFO) hashing to achieve non-invertible and cancelable transformation for iris templates in cryptographic key binding process. The contributions of this work are presented as follows:

1. *Key regeneration*: A new formulation to measure the success rate for key retrieval under genuine query is proposed and defined as Key Retrieval Rate (*KRR*). Thorough analysis has been conducted to prove that *KRR* is in relation to Jaccard similarity. The calculation of *KRR* has been demonstrated under certain configurations and implementations in security analysis for indistinguishability game as well as false accept attack.
2. *Cancelability and renewal*: A fast and simple method for key renewal is proposed. The proposed method requires neither re-enrollment of biometrics nor constant storage for seeds. This can be achieved by reshuffling the hashing functions randomly.

3. *Security analysis*: Adequate security analysis is performed on the indistinguishability between synthetic and genuine biometric templates under the proposed scheme. The adversary's advantages in distinguishing the genuine and synthetic templates have been evaluated through our proposed indistinguishability game. Besides that, potential brute force attack and false accept attack are also investigated in detail.
4. *Feature representation and hashed code's length*: In this non-hierarchical key binding design, biometric template size and key length will have critical effects on the storage space and computation power. Thus, the proposed format for biometric template in (Jin et al., 2016) is not directly applicable for all types of biometrics especially iris features. In view of this, flexibility in terms of tunable hashed code length has been proposed in this scheme. This is achievable via IFO hashing's controllable hash code length.
5. *Performance discrepancy*: Key binding scheme in (Jin et al., 2016) has reported FAR more than zero in their implementation on fingerprint. This implies the potential of this scheme being compromised through FAR related attacks. This can lead to significant reduction in security and severe privacy leakage. Thus, there is a need to conduct an in-depth analysis on security and privacy leakage for iris data to understand the full potential and the bottleneck of chaffing and winnowing based key binding scheme.

1.4.3 Transformation and Optimization Model for Iris Code based Cancelable Authentication System

This proposed method takes into consideration the required pre-alignment for original iris code in matching. Direct application of any cancelable transformation over the original iris code without considering the inherent vertical dependency would result in poor recognition performance (Hu et al., 2016). For a protected iris code based recognition system, only the protected iris templates are accepted for matching. Thus, we have designed a paired transformation and matching mechanism which is able to fulfil this requirement. One advantage of this proposed mechanism is that alignment can be conducted directly onto the protected template rather than reverting to original iris code during matching stage.

Specifically, the structure of the iris code, its vertical dependency and horizontal independence is also exploited. This study is aligned with the statement that the distinguishable information of an iris code is mostly displayed in the horizontal direction as mentioned in (Liu et al., 2013). On the contrary, the iris texture itself, processes inherited correlations along the radial direction. Hence, the bits in a vertically aligned iris code is expected to contain high dependency, i.e., less discriminative. The idea is to perform pre-alignment in the transformation to prevent the presence of probe iris code during matching stage. In view of the concern on vertical dependency, the proposed transformation is applied in a column-wise manner. This can mitigate the poor recognition performance caused by the vertical dependency of iris codes. In addition, a mapping function is proposed to concatenate an arbitrary number of columns within the transformed iris code as part of the proposed matching mechanism.

Results have shown that the employed mapping function could reduce the vertical dependency of iris code and improve the recognition performance of the transformed iris code. Moreover, the key space of iris codes can be increased to at least 40 bits after the proposed transformation without significantly deteriorating the original performance.

Other than this, experiment conducted using the proposed matching mechanism showed that the matching performance of the original iris code can be further improved with higher decidability score obtained. The measure of decidability (Daugman, 2004b) reflects the degree to which any improvement, for instance, in reducing the false acceptance error rate, will be paid by the increment of false rejection error rate. Apart from higher decidability score obtained using the proposed matching mechanism, it is also demonstrated empirically that the matching performance of the iris recognition system has reported lower false rejection rate (FRR), especially, under the case when only low false acceptance rate (i.e., <0.5%) is permissible. In short, the focus of this work is laid on the performance, protection and transformation for iris code in cancelable iris authentication.

1.5 Objectives

This thesis aims to improve the authentication performance, flexibility and security of iris template protection scheme.

1. Improve the authentication performance of protected iris recognition system.
2. Devise an alignment-free cancelable iris key binding scheme.
3. Mitigate the performance, pre-alignment and dependency issues in iris code based cancelable iris template protection scheme

1.6 Organization of Thesis

The thesis is organized as follows. Previous work related to iris codes, iris biometric template protection schemes and their recognition performance is described in Chapter 2. The presentation of my proposed schemes and their implementations are shown in Chapter 3. The experimental results, discussion and security analysis are provided in Chapter 4. Finally, concluding remarks and future recommendation are given in 5 followed by Appendices.

CHAPTER 2

LITERATURE REVIEW

Iris recognition was first introduced by John Daugman (Daugman, 2004b). The author encoded the iris features using quadrature 2-D Gabor wavelet demodulation. The complexity of the phase information across different persons spans about 249 degrees of freedom and discrimination entropy of about 3.2 $\boldsymbol{b/mm^2}$. It was also proven improbable that two different irises might disagree by chance in fewer than at least one third of their bits. The probability of such event was approximated to be 1 in 16 million. In this method, fractional Hamming Distance (HD) was used as the measure of dissimilarity between two irises for iris recognition. When HD of two iris codes were calculated, one of the iris code templates was shifted left and right bit-wise to compensate for rotational inconsistencies. Bit-wise shifting method corresponded to an angle of rotation at the original iris region depending on the angular resolution. This method was proposed (Daugman, 2004b) to rectify the misalignments in iris pattern due to the rotational differences during image acquisition. The best match between two iris code templates could be determined by a series of HD calculated from successive shifts.

A statistical analysis was then conducted by Kong (Kong, 2014) on the risk associated with two patented template protection schemes deployed for producing application-specific iris code is analyzed. The study showed that the application-specific iris code could be unlocked and the key could be retrieved

through statistical dependence detected. His results showed that partial statistical dependence was induced through the Gabor filters that produced iris codes. In this case, the belief where iris codes were secure as long as the key was not compromised had to be reconsidered. The security risk in these schemes as well as iris codes might endanger numerous people and organizations due to the wide deployment of iris recognition in commercial systems.

2.1 Iris Segmentation

As discussed in the previous chapter, the accuracy of iris recognition could be affected severely by iris segmentation. Conventionally, there were three essential steps in a standard iris segmentation process: localising the inner and outer iris boundaries, detecting the upper and lower eyelids based on the different formulations and lastly cornea identification and displacement of reflections (Bastys et al., 2009). Firstly, boundary fitting based methods were the most common type in the implementation of iris segmentation. The principle of this method started from locating the inner iris boundary as the baseline of the image and separate unimportant parameters outside the iris like eyelashes and eyelids (Arsalan et al., 2017). For instance, Daugman's integro-differential operator and Hough transform were both well-known methods for segmenting the iris boundary (Daugman, 2004b). However, this process required user to vary radii and centre coordinates in order to search for maximum normalised integral along circular contours. Recent work from Farmanullah Jan et al. (Jan et al., 2021) had reported an average accuracy of 97.7% on more challenging databases like CASIAv4 Iris-Distance. Viola Jones algorithm detected eye region using geometrical information of human face. Circular region of interest (ROI)

containing iris was marked after some pre-processing steps to enhance contrast, suppress reflections and smoothen gray level variations. Hough transform was used to segment iris while non-circular iris contours were extracted through a scheme that was based on Lagrange interpolating polynomial. However, noise detection was still needed to eliminate the hairs, eyebrows and eyelids within the segmented iris contour.

The second category of iris segmentation methods called pixel-based segmentation. This method differentiates the iris pixel and non-iris pixel by employing characteristics of illuminance, colour gradient and specific colour texture across the image. Khan et al. (Khan et al., 2011) proposed the method to localise the pupil using the eccentricity-based bisection. Gradients were calculated pixel-by-pixel between the sclera and iris boundary and looks for maximum changes across that region to represent the iris boundary. Colour-based clustering method had been proposed in (Parikh et al., 2014) to determine the iris boundary. The non-iris region and iris region were clustered by applying several statistical algorithms like the intersection area of two circular boundaries. Overall, most of the segmentation methods focused more on solving some constraint conditions but the noise at iris region such as eyelashes and hairs can still affect the overall iris recognition performance severely.

Active contour was another type of classical but more accurate segmentation method. This method was able to work on any arbitrary shape in an image with more accurate segmentation accuracy. Geodesic active contour (GAC) (Shah and Ross, 2009) provided a solution for the iris segmentation under non-ideal environment. An improved framework (Chang et al., 2020) that used Hough transform to segment the pupil and estimate iris circle according to the

result of GAC has yielded 79% for UBIRIS. It was mentioned that the accuracy of the algorithm could be further improved after a larger amount of data was applied. Chan-Vese active contour method was proven to be accurate on noisy and non-ideal iris images. Localised algorithm introduced by Chai et al. (Chai et al., 2016) had shown good ability in avoiding occlusions during the segmentation while demonstrating acceptable segmentation accuracy with E_1 error between 0.01-0.02 on visible wavelength iris databases, NICE.I and NICE.II. However, there were common drawbacks in the active contour-based methods. Most of the time, these methods needed to couple with pre- and post-processing methods, semi-automated, sensitive to initialization, multiresolution and multiscale transforms and limitation in handling intensity inhomogeneity especially in detecting the pupillary boundary due to low contrast.

To mitigate the drawbacks of prevailing classical segmentation methods, the proposal of deep-learning based iris segmentation method could overcome the stated challenges. Researchers started to apply convolutional neural network (CNN) in iris segmentation to enhance the robustness of their algorithms. Hierarchical convolutional neural network (HCNN) and multi-scale fully convolutional networks (MFCN) was an advanced technique for locating and segmenting the iris boundaries without any assistance from the handcrafted. The architecture of MFCN comprised 31 convolutional layers which were separated into six different layers with pooling. All the six layers were fused at the last part to formulate a multi-layer network for feature engineering and the prevention of information loss. The robust MFCN model had outperformed the conventional methods by 25.62% on the UBIRISv2 and 13.24% on CASIAv4 Iris-distance databases (Liu et al., 2016). HCNN incorporated three layers of the

convolutional neural network with different patch sizes of inputs and all these layers were fused at the last layer. It was a binary classification model like other iris deep learning models for categorising iris and non-iris pixels. The overlapping regions in three different CNNs were repeated throughout the training process before fusing them into a fully connected network indicates lower efficiency in this model.

Arsalan et al. (Arsalan et al., 2017) proposed a two-division iris segmentation method with the hybrid of convolutional neural network and the pre-processing techniques to compensate for the shortcoming of CNN. In the first stage, image pre-processing such as grayscale conversion and morphological operations were applied to the input image. Then, image's region of interest was processed and loaded into the CNN to detect the iris area precisely. The information about ratio between dilation and pupil contraction was performed to get the exact iris boundary. The CNN model came from a pre-trained VGG model. There were thirteen convolutional layers and five pooling layers in fusing with three fully connected layers to back up the learning process of the iris segmentation. Despite outstanding segmentation performance by implementing CNN for iris segmentation, this system required many handcrafted processes to determine the true boundary of the input images.

Bazrafkan et al. (Bazrafkan et al., 2018) used an end-to-end semi parallel deep neural networks (SPDNN) which merged several deep networks into a single model to take the advantage of every design fully. Wang et al. (Wang et al., 2021) introduced a lightweight fully convolutional iris segmentation for mobile devices. Improved weight loss, multi-level feature dense fusion module, multi-supervised training of multi scale image and generative adversarial

network were among the initiatives to improve the segmentation performance. An average accuracy of approximately 99% had been achieved on UBIRISv2 and CASIAv4 Iris-Thousand databases. The iris segmentation time taken for an image from UBIRISv2 was only 41.56ms.

Although most of the deep learning networks showed good performance in iris segmentation, there was still a lack of research works which utilized small training samples, no pre- or post-processing steps and no data augmentation while testing with various non-ideal factors, such as illumination variations, blurring, off-angle (Jalilian et al., 2021), reflections and ghost effect in both visible light and infrared environments.

2.2 Iris Cancelable Biometrics

In this section, previous works of cancelable iris template protection scheme were revisited. The concrete idea of cancelable biometrics was proposed by Bolle et al. (Bolle et al., 2002). The work from Ratha et al. (Ratha et al., 2007) had extended the initial idea into cancelable fingerprint templates. Non-invertible geometric transformations consisting block permutation and surface folding were applied on biometric template. Fingerprint minutiae in Cartesian and polar domains were permuted to generate a cancelable template. The proposed scheme preserved the change in minutiae positions after the transformation while introducing many-to-one mapping for non-invertibility, Despite satisfactory accuracy performance was reported, the non-invertibility property was found vulnerable (Quan et al., 2008). Since then, this work had inspired more research works into the field of biometric template protection. In

general, cancelable biometrics could be categorized into biometric salting and non-invertible transformation.

Biometric salting followed the principle that independent auxiliary data such as user-specific password or random numbers were combined with biometric data to create a distorted version of the biometric template. Biohashing was first introduced by Teoh et al. (Jin et al., 2004) for fingerprint using user-specific random projection. A user-specific random matrix M with size $r \times c$ was created such that c columns of M were orthonormal. The extracted biometric feature was represented as a fixed length vector, x. Projection was carried out through inner product operation $y = M^T x$ and y was then thresholded by b_i. If $y_i > \tau, b_i = 1$, otherwise $b_i = 0$ for $i = 1,2, \dots, c$. The binary vector $b_i = \{0,1\}$ was stored as the final template. This method with its optimal setting had been tested with different biometric modalities such as iris, palm print, fingerprint and face with nearly zero error rates. However, the performance of this method degraded considerably under stolen-token scenario. The non-invertibility of biohashing was at risk when M and y were known while r, c were merely the same (Teoh et al., 2010). The stolen-token performance issue was then addressed by Lumini et al. (Lumini and Nanni, 2007) using score fusion and threshold values. Exponential increase in the size of the transformed template is solved recently by double bloom filter based transformation (Ajish and AnilKumar, 2020).

Another method of user-specific random projection was proposed by Chong et al. (Chin et al., 2006), namely S-iris code. Firstly, the vector of iris Gabor feature vector $\omega \in \mathbb{C}^n$ was generated by convoluting the 1-D log-Gabor

filter with the normalized iris image that was reshaped later into a n-dimensional feature vector. Then, the magnitude of ω, denoted as $\mathscr{w}$, was projected into a lower-dimensional feature space. The projection was achieved through the iterated inner-products of $\mathscr{w}$ with a set of user-specific orthonormal pseudo-random vectors $\{r_i \in \mathbb{R}^n | i = 1, \dots, m\}$ where $m \leq n$. Quantization process was the final step to compute the m bits S-Iris, $s_i \in 2^m$. $s_i = 0$ when $\alpha \leq \mu$; $s_i = 1$ when $\alpha > \mu$ where $\{\alpha = \mathscr{w} | r_i\}$ with $.|.$ indicated the inner-product operation and μ was a preset threshold. If a template was compromised, a new cancelable template could be regenerated by issuing a new set of pseudo-random vectors from the user-specific token. To achieve higher recognition accuracy, noise mask was proposed to act as a control bit is introduced to determine the validity of the s_i bits by eliminating the weak inner product. It was proven that noise mask can improve the performance in hamming distance matching.

Pioneering work in the field of iris biometric was proposed (Zuo et al., 2008). There were 4 non-invertible and revocable transformations. The first method, GRAY-COMBO transformed Gabor features by circular shifting followed by random rows addition. The non-invertibility criterion had been achieved through the distortion caused by data shifting. Similar transformations on iris codes were performed in the second method, BIN-COMBO but the combination was conducted through XOR operation. These methods reduced the amount of information available for recognition for better security. However, global linear transformation included outliers which could degrade the performance. The other two methods could be referred as biometric salting, namely GRAY-SALT and BIN-SALT where random patterns were added to the iris features in binary or integer representation. It was found to be difficult in

determining the relative strength of the noise patterns to be added to gain the balance between recognition performance and security. If the added patterns were weak and compromised, original iris pattern could be obtained by a simple subtraction operation. A recent cancelable iris template generation using salting approach has been proposed (Asaker et al., 2021). Iris code was mixed with a synthetic patterns, also known as cover pattern using XOR operation. The synthetic patterns were obtained from by the user specific cover images encrypted using the proposed enhanced AES algorithm. EER as low as 0.43% was reported when tested on CASIA v3-interval.

Another idea of iris template protection is based on the sectored random projections (Pillai et al., 2010). Random projections were applied to sectored iris features via a user-specific random Gaussian matrix. The random matrices were then concatenated to form a new cancelable iris template. A new template could be generated by using different random projection matrices if the existing one was compromised. This method limited the effect of outliers but reduced the size of useful information. The author pointed out that direct projection of the entire image might lead to performance degradation due to the effects of external noises such as specular reflections and eyelashes. Further research (Lacharme et al., 2013, Kong et al., 2006) found that the performance of this method was degraded when the same random matrix was being applied to different users. In addition, the protected template is likely to be inverted when the user-specific random matrices were disclosed or the adversary possesses the secret token. Thus, biometric salting is feasible for template protection if the auxiliary data is kept secret. A recent work had created iris transformed cancelable template through encryption and one-way transformation function. Double Random

Phase Encryption (DRPE) was used to generate cancelable iris code in Fractional Fourier Transform (FFT) domain (Rajasekar et al., 2021). This framework proposed to utilize both left and right iris images to form a single cancelable iris template. Low EER of 0.46% was achieved on CASIAv4 iris database.

Hamerle-Uhl et al. (Hämmerle-Uhl et al., 2009) proposed a cancelable scheme that incorporated block-remapping and image warping for non-invertible transformation. The normalized iris image was first partitioned into different image blocks. Then, random permutation was applied to each block and mapped randomly to blocks from the source texture. A key was used as a seed to represent one particular distortion on the remapped image to prevent the reconstruction of the original iris data. Jenisch et al. (Jenisch and Uhl, 2011) highlighted the vulnerability of the remapping process in the scenario of coalition attack presuming that single or multiple templates are available to an attacker. Increasing the security to the recommended level would sacrifice the performance of the system with more than 100% of EER degradation from 1.244 to 2.846. This work had demonstrated that 60 per cent of the original iris image could be reconstructed from the stolen template.

Ouda et al. (Ouda et al., 2011) proposed a tokenless cancelable biometrics scheme, BioEncoding. The consistent bits, $\boldsymbol{w} \in \{\mathbf{1}, \mathbf{0}\}^{\boldsymbol{n}}$ where $\boldsymbol{n}$ denoted the length of the bit vector with lower probability of flipping, were extracted from a series of iris codes of each user. This eliminated bits with higher probability to flip from an individual. The bits were then grouped into $\boldsymbol{n/m}$ blocks with $\boldsymbol{m}$ binary codewords in each block. Each block was mapped to a single bit of a random binary sequence with length $\boldsymbol{l = 2^m}$ where the location

was determined by the decimal value of that specific block. The mapped binary values were then arranged according to the associated positions of the blocks to form the BioCodes. The many-to-one mapping used in the generation of BioCode fulfilled the non-invertibility requirement by making the recovery of original iris code computationally infeasible. BioEncoding scheme recorded the best EER of 6.27% for CASIAv3. However, Larcharme (Lacharme, 2012) revisited bioencoding scheme and regarded that it was an application of random Boolean function on the original iris code which was indeed invertible.

An alignment-free cancelable iris template protection scheme based on adaptive Bloom filters was introduced by Rathgeb et al. (Rathgeb et al., 2013). Bloom filter-based representations of biometric templates such as iris codes enabled an efficient alignment-invariant biometric comparison at matching stages. Besides, the many-to-one mapping of biometric features to a Bloom filter was non-invertible. For cancelable template refreshment, they applied an application-specific secret key, for example, seed values to fulfill the unlinkability criterion. To resolve the alignment issues in iris code, the Bloom filter technique (Rathgeb et al., 2013) transformed original iris code $\boldsymbol{I} \in \{0,1\}^{n_1 \times n_2}$ into an alignment-free binary matrix named Bloom-filtered iris code, $\boldsymbol{B}$ through Bloom_filter $(W, L, \boldsymbol{I})$. Suppose that W and L were denoted as the number of columns and rows, respectively. The matrix of iris code was first split into $l_1 \cdot l_2$ blocks with a size $L \times W$ each, where $l_1 = \frac{n_1}{L}$ and $l_2 = \frac{n_2}{W}$. Each block constituted the formation of a Bloom filter with values within $b \in \{0,1\}^{2^L}$. All elements of b were initially zeros and element '1' was added to b according to its decimal position at the column codeword, $x_j \in \{1,0\}^L | j = 1,2,\ldots,W$ in each block. In the scenario

where the same x_j was being mapped multiple times within a Bloom filter, b thus results in a many-to-one mapping and loss of information. Hence, the reconstruction of the original iris code could be prevented with this feature of non-invertibility. The collection of every Bloom filter b_i of each block (for $i = 1,2,\dots,l_1 \cdot l_2$) in an input matrix constituted the final matrix of Bloom filtered iris code, $\boldsymbol{B} \in \{0,1\}^{l_1 \cdot l_2 \times 2^L}$. An application specific secret bit vector was XORed with each codeword prior to mapping to provide unlinkability between multiple cancelable templates of a subject. The basic operation of Bloom filter has been highlighted in Figure 6.2 in Appendix B. This representation allowed iris codes to have alignment-invariant comparison at matching stage without degrading the performance of the iris recognition system. The best EER reported was 1.49% for CASIAv3. Undesirably low attack complexities of 2^{25} for restoration of biometric template and 2^2 - 2^8 for key recovery were then reported (Hermans et al., 2014). Although it was proven that this method was susceptible to cross-matching attack, Bringer et al. (Bringer et al., 2015) successfully performed brute force attack on each block of codewords by analyzing the cancelable templates generated from two different intra-class iris codes. Unlinkability attacks pruned to happen especially when smaller key space was used to preserve the accuracy performance. However, (Gomez-Barrero et al., 2016, Gomez-Barrero et al., 2018) had demonstrated the solutions to circumvent the security limitations of the Bloom filter.

Dwivedi et al. (Dwivedi and Dey, 2015) proposed a cancelable template protection scheme based on randomized look-up table mapping. Rotation invariant iris templates were first selected based on the minimum hamming distance.

The row vector $\boldsymbol{C} \in \{\mathbf{0}, \mathbf{1}\}^{\mathbf{1}\times \boldsymbol{N}}$ was divided into $\boldsymbol{l}$ groups of $\boldsymbol{m}$ bits binary codewords. The corresponding decimal values for all these groups were encoded through a look-up table $\boldsymbol{M} \in \{\mathbf{0}, \mathbf{1}\}^{\boldsymbol{R}\times \boldsymbol{m}}$ where $\boldsymbol{R} \geq \mathbf{2}^{\boldsymbol{m}} - \mathbf{1}$ with $\boldsymbol{m}$ randomly generated bits for all possible decimal values ranging from $\mathbf{0}$ to $\mathbf{2}^{\boldsymbol{m}} - \mathbf{1}$. The newly mapped binary codewords became the final cancelable template. A degradation of 10% to 49% in EER performance was reported. The iris codes could be at risk with information about block size and $\boldsymbol{m}$ being stolen, since look-up table and cancelable templates were both stored in the database as well. The author emphasized the need to further secure the look-up table generation for stolen-token scenarios. A recent research proposed an iris protection scheme by ranking the decimal value of each group of codewords locally instead (Zhao et al., 2018). The highest degradation experienced was 5% when compared to a traditional iris recognition system with EER reported at 1.32% for CASIAv3. A recent publication (Ouda, 2021) proposed a new attack to reverse the local ranking-based cancelable biometrics (LRCB). The attack reversed the protected rank values using the distribution of order statistics for discrete random variables. The reversibility attack recovered more than 95% of the iris code bits while achieving 100% success rate for the proposed correlation attack. Umer et al. (Umer et al., 2017) demonstrated a feature learning method for a cancelable iris recognition system. Among other feature representations, a sparse representation coding technique showed better discriminability, employing a multi-class linear support vector machine (SVM) classifier. The existing Biohashing scheme was applied and extended by using two tokens, which were subject specific and subject independent,

respectively. Despite the flexibility in template renewal, no in-depth security analysis was discussed regarding the proposed scheme.

A newer non-invertible transformation, IFO hashing scheme was introduced by Lai et al. (Lai et al., 2017b) based on Min-hashing scheme from the field of similar item detection or clustering (Broder, 1997, Hollingsworth et al., 2009). First, any arbitrary binary input of iris code with a dimension $n_1 \times n_2$ was permuted with p number of random permutation sequences in a column-wise manner. All the randomly permuted iris codes were multiplied to generate a p-ordered Hadamard product code. Hadamard product imposed information loss to prevent the reconstruction of original iris code. It could exclude certain amount of fragile bits (Hollingsworth et al., 2009). Utilizing the concept of min-hashing, the first '1' was selected from the first κ elements for each row of the product code. The index value of the first occurrence of '1' was then recorded. This process invited merit such as implicit ordering of iris code rather than explicit bit information to prevent inversion attack. To strengthen further the non-invertibility of this method, a modulo-thresholding function was imposed as the final step. The imposed security threshold value τ could be used to regulate the security leakage while inducing a many-to-one mapping in strengthening the non-invertibility properties of this scheme. An $n_1 \times m$ matrix of IFO hashed codes $\boldsymbol{C} \in \mathbb{Z}_{\kappa-\tau}^{n_1 \times m}$ was obtained by repeating these steps with m independent hash functions. The basic operation of IFO hashing was illustrated in Figure 6.3 in Appendix B. This cancelable iris template protection scheme was able to achieve low EER of 0.54% with degradation around 40% in performance as compared to iris code without template protection. Despite the significant improvement in performance and

security of recent iris template protection schemes, degradation in performance was still observable when comparing against unsecured iris recognition system.

Recently, Sadhya et al. (Sadhya and Raman, 2019) proposed to generate cancelable iris code based on Locality Sensitive Hashing (LSH) with the best EER 0.105% for CASIAv3. Generally, the bit sampling strategy utilized arbitrary n number of random and independent hash functions $h_1, \dots, h_n$ to sample n independent random binary string $S_1, \dots, S_n$. First, the input iris code was being divided into b number of blocks. Independent hash functions $h_1, \dots, h_n$ could then be created under each block. For each hash function h_i, a series of bit symbols say $m > 0$ bits were being extracted according to a randomly generated indices set to form the binary string. Those were known as marked position bits. To demonstrate the non-invertibility, the sampled binary strings $S_1, \dots, S_n$ were then converted to their corresponding decimal values. Thus, a string of decimal values $C \in [0, 2^m - 1]^n$ was formed. After that, each element $\mathrm{c} \in C$ was being mapped into an output space of size at most 2^Kusing a modulo threshold function, for instance, $c' = c \; mod \; 2^K$. The hashed templates which could be denoted as $\mathrm{C}' = [c_1', \dots, c_n']$ were stored together with their corresponding hash function $H = [h_1, \dots, h_n]$ as $MAP(C', H) = [(c_1' h_1), \dots, (c_n' h_n)$. The same process was repeated for all the b blocks in order to generate the final template named as the locality sampled code (LSC). The collection of all the maps could be further summarized as $[MAP(C', H)_1, \dots, MAP(C', H)_b]$ for all the b-blocks of the input iris code. Under this framework, intra-class samples were expected to be close to each other and thus, they would be hashed to the same location. In contrary, inter-

class samples were dissimilar and consequently hashed to different locations. Low EER was reported due to the collision guarantees from bit sampling based LSH. However, EER performance at zero FAR was not available in the report. Besides issue regarding performance degradation, there was also lack of a generalized method which could improve the performance of these reputed cancelable iris template protection schemes.

2.3 Iris Biometric Cryptosystem

Besides cancelable biometrics, biometric cryptosystem was another alternative to biometric template protection aiming at generating cryptographic keys out of or with biometric traits. Generally, key generation schemes required exact recovery of the input biometric feature via error tolerance, for instance, error correction code (ECC). This was to ensure that the same key could be regenerated from the varying biometric feature for authentication. Using error correction code in biometric system introduced high tension between error correcting capability and security (Noto et al., 2011). In particular, there was an existing tradeoff between the error correcting capability of an ECC and the system security (in terms of false acceptance), duped as the granular effect, where it was crucial to know the genuine and imposter distribution before designing a biometric system with ECC. Analysis had been done in (Merkle et al., 2010, Tams, 2013) and reported that correcting large number of errors in the input feature imposed high information loss, further leads to low attack complexity. It was still an open problem on how to choose the best ECC for BCS.

The first iris biometric key generation scheme was proposed by Davida et al. (Davida et al., 1998). In their private template scheme, helper data was used for error correction check for differing bits of iris codes. This research showed the possibility of storing biometric templates directly as secret keys or in the form of hashed values. Although the empirical results of this method showed large entropy of 173 bits but there was still possibility to reconstruct raw biometric data from compromise biometric hashes (Davida et al., 1999). Juels and Wattenberg (Juels and Wattenberg, 1999) introduced fuzzy commitment scheme combining knowledge from the area of Error Correction Codes (ECC) and cryptography to protect cryptography key. Fuzzy commitment scheme had a function F, which was used to commit a codeword $c \in C$ and a witness $w \in \{0,1\}^n$. The witness was the enrolled biometric template represented by n-bits binary string while C was a set of error correcting codewords c of length n. The difference vector of w and c, $\delta \in \{0,1\}^n$ could be obtained through bit-wise XOR operation: $\delta = c \oplus w$. The δ was denoted as the helper data which would be stored together with $h(c)$ into the database where $h(.)$ was the hash function. The commitment was termed $F(c, w)$. Given a query biometric template w', a corrupted codeword c' could be reconstructed through $c' = \delta \oplus w'$using the stored helper data. At authentication stage, if the query binary string was sufficiently similar to the enrolled template within the capability of the ECC, a hash of the result tested against $h(c)$would yield a successful authentication if $h(c') = h(c)$.

The first application of fuzzy commitment scheme to iris codes was implemented by Hao et al. (Hao et al., 2006). Hadamard and Reed-Solomon

error correction codes were used in their scheme to bind 2048-bit iris codes into 140-bit cryptographic keys. The main idea was to apply Hadamard codes to eliminate bit errors caused by the natural variance such as background errors while burst errors were corrected by Reed-Solomon codes. Genuine Acceptance Rate (GAR) of 99.53% and zero False Acceptance Rate (FAR) were reported on an in-house dataset. Two-dimensional iterative min-sum decoding was then introduced (Bringer et al., 2008) for iris-based fuzzy commitment scheme with higher correction capacity and efficiency. High False Rejection Rate (FRR) was discovered on noisy channel using Reed-Solomon code. Instead, two different Reed-Muller codes were used to form a matrix for efficient decoding. This method had achieved GAR of 94.38% and zero FAR on the ICE 2005 iris database (Phillips et al., 2008) with 40 bits of bound keys. A context-based method that constructed keys based on reliable bits within the iris codes bound by BCH-code is proposed in (Rathgeb and Uhl, 2011a). User-specific masks and check bits were used to form the helper data. A variety of techniques focusing on biometric template protection, random bit-permutation, biometric feature binarization and concatenated coding scheme were then proposed to improve the performance and security of iris fuzzy commitment schemes, for e.g. (Maiorana et al., 2014, Kelkboom et al., 2011, Teoh and Kim, 2007, Zhang et al., 2009). A context-based method (Rathgeb and Uhl, 2011a) for iris biometric key generation scheme had produced revocable and reasonable system performance (70-bit, 140-bit and 280-bit). The respective GARs at these key lengths were 84.26%, 95.52% and 94.68%. A most recent enhanced iris fuzzy commitment scheme (Adamovic et al., 2017) which identified and used only certain iris regions instead of the entire iris region was proposed. The proposed scheme had

reported good recognition accuracy of FRR 3.75% when FAR was zero with high entropy of 400 bits in key length.

Ideally, fuzzy commitment was proven secure under random oracle model, hence, helper data contained no information about the secret. In other words, secret was expected to be uniformly and independently distributed where an adversary could only perform brute force attack. However, this was practically hard to achieve due to the inherent structure of the biometric data and correlation between features (Zhou et al., 2011). Privacy leakage was another concern in fuzzy commitment caused by the redundancy in an ECC which was unavoidable (Zhou et al., 2011). Cross matching could happen if large privacy leakage was discovered. Several attacks such as decodability attack (Teoh and Kim, 2007), statistical attack (Carter and Stoianov, 2008) and Attack via Record Multiplicity (ARM) (Scheirer and Boult, 2007) were indeed possible.

Kelkboom et al. (Kelkboom et al., 2011) proposed a bit-permutation process for fuzzy commitment scheme to prevent it from decodability attack that exploited the correlation of multiple helper data generated from the biometric data of a same subject. The decodability attack was first initiated by Carter and Stoinov (Carter and Stoianov, 2008) to verify the possibility of whether decoding two helper data led to a valid codeword. When there were two helper data δ_1, δ_2 being generated by two biometric data from the same subject, w_1, w_2, in decommitment process, the attacker could leverage on the helper data by performing $\delta_1 \oplus \delta_2 = (w_1 \oplus w_2) \oplus (c_1 \oplus c_2)$ which was equivalent to $\delta_1 \oplus \delta_2 = (w_1 \oplus w_2) \oplus c$. If the two helper data derived from the same subject, $w_1 \oplus w_2$ was small and the outcome would be most likely close to the correct codeword. In

short, the bit-permutation mechanism helped to improve the security through the distribution of entropy across biometric feature vectors.

Rathgeb et al. (Rathgeb and Uhl, 2011c) presented a statistical attack against iris fuzzy commitment scheme. Binary biometric feature vectors of impostor were randomly chosen and decommitment was performed successively with the stored helper data assuming that attackers were in knowledge of the applied ECC. The frequency of each possible codeword was collected and a corresponding histogram was generated for each chunk. The ECC based histograms of all the chunks could be analysed after repeating the chunk-based decommitment processes using an adequate amount of imposter templates. The most likely error correction codeword for a chunk was decided based on the bin which corresponds to the histogram maximum.

Scheirer and Boult (Scheirer and Boult, 2007) had launched an attack via record multiplicity on fuzzy vault. This referred to an imposter in possession of multiple invocations of the same secret which were combined to reconstruct secrets that led to the retrieval of biometric templates. The introduced attack on fuzzy vault, namely Surreptitious Key-Inversion (SKI) was an equivalent attack against fuzzy commitment. Under this attack, the biometric string blended with the codeword could be recovered through XOR operation using the compromised cryptographic key (secret) and the secure sketch.

Privacy and security leakages of fuzzy commitment schemes were investigated in (Ignatenko and Willems, 2010) for several biometric data statistics. The scheme was found to leak information in bound keys and non-uniform templates. For instance, keys bound of 44 bits in fuzzy commitment schemes (Hao et al., 2006) suffered from low entropy, reducing the complexity

for brute force attacks (Teoh and Kim, 2007). Zhou et al. (Zhou et al., 2011) conducted a quantitative assessment on the privacy and security leakage of fuzzy commitment scheme. Biometric data was not uniformly and independently distributed which further contributes to the security issue. Several evaluation metrics had been proposed to conclude that fuzzy commitment was highly vulnerable due to the inherent dependency of the biometric features.

Apart from that, fuzzy commitment was often bounded by the limitations introduced by ECC. The scheme was found to be affected by the tradeoff between security and performance (Kelkboom et al., 2012). Similar perspective was reported by Bringer et al. (Bringer et al., 2008) where the decoding accuracy and maximum key length were bounded by the error correction capacity of the adopted ECC. Besides, another limitation came from the design of fuzzy commitment scheme in terms of input representation and matching (Dodis et al., 2004). The input feature to fuzzy commitment was restricted to binary representation in order to conduct matching in hamming domain. This hindered the scheme from achieving better performance since many effective feature extraction and matching techniques did not comply with this requirement. Considering the discussed attacks and limitations, the security and privacy provided by iris-based fuzzy commitment still have room for improvement.

Rathgeb et al. (Rathgeb and Uhl, 2010a) had proposed an iris key generation scheme based on interval mapping for iris features in real values. The highest key generation rate reported on CASIAv3 was 95.09% for five enrollment samples. However, our proposed scheme did not require exact recovery of the input biometric. Authentication was done by computing the similarity score between two biometric templates. This avoided the usage of

ECC that lead to another code selection problem. A new post-quantum fuzzy commitment scheme (PQFC) that did not rely on ECCs like the conventional fuzzy commitment scheme was designed (Al-Saggaf, 2021). It was proven to be secured based on the hardness of Short Vector Problem (SVP) of the lattice. The authentication performance of this iris recognition was reported as 99.1% with 0% of FAR against CASIAv1 iris database. The PQFC authentication system was mentioned to be suitable for any biometric trait.

Another design provided protection and error-tolerant verification, the fuzzy vault scheme was first introduced by Juels et al. (Juels and Sudan, 2006). A secret key could be encoded as the coefficients of polynomial, F. This polynomial was evaluated with a set of points that represented the genuine biometric features $\{b_1, \dots, b_k,\}$. A set of pairs were then constructed in the form of $\{(b_1, F(b_1)), \dots, (b_k, F(b_k))\}$. To conceal the true features, large number of chaff point pairs that were not related to the polynomial, were fused together with the set of pairs from the genuine features. This combination formed a vault. If a sufficient number of genuine biometric features could successfully reconstruct the hidden polynomial, the vault could be unloacked. This process in separating the genuine points and the chaff points was indeed analogous to the chaffing and winnowing technique proposed by Rivest (Rivest, 1998).

There was an initial implementation of a fuzzy vault scheme on iris data presented in (Lee et al., 2008, Lee et al., 2007). In this method, Independent Component analysis (ICA) was employed to extract important coefficients from multiple local regions in iris image. K-mean based pattern clustering method aimed to solve the variance of the extracted iris features while ICA created

unordered sets for fuzzy vault. On a challenging CASIAv3 Iris-Interval iris database (2002a), GAR of 80% was achieved at a zero FAR employing 128 bit keys. Then, Lee et al. made another attempt to introduce iris fuzzy vault system (Lee et al., 2008) based on local iris features. Iris features were extracted from multiple regions with shift-matching applied to solve the alignment issue. Reed-Solomon (RS) coding scheme was used for error correction. The best Genuine Acceptance Rate (GAR) reported was 83.4% and 91.1% respectively for CASIAv1 and CASIAv3 iris databases under adequate system security.

Reddy et al. (Reddy and Babu, 2008) had hardened the fuzzy vault using user's password to prevent from attacks via record multiplicity. Iris features were extracted from minutiae-like coordinates obtained through image enhancement steps. At zero FAR, a degradation of 2% to 90% GAR was reported for CASIAv1 (2002b) and MMU iris database (2004) when the degree of polynomial was set to 7 or 8. More proposals on iris vaults (Mariño et al., 2012, Fouad et al., 2011) had omitted a detail explanation about iris feature encoding or protocols. Majority of the proposed schemes in biometric cryptosystem were lack of thorough security analysis, for example, larger entropy loss could be possible especially for neighbouring bits dependencies and this reduced the security all the way to 40 bits (Hao et al., 2006).

Anyhow, the implementations of fuzzy vault scheme by Juels and Sudan (Juels and Sudan, 2006) in biometrics had exposed its vulnerability to correlation attack and linkage attack (Scheirer and Boult, 2007, Kholmatov and Yanikoglu, 2008). This conflicted with the unlinkability and irreversibility requirements defined for biometric template protection. The basic idea of fuzzy vault fingerprint systems to include auxiliary data was to help in alignment issues

affected by translation, rotation and non-linear distortion. However, attacker could make use of the publicly unprotected auxiliary alignment data in performing linkage attacks. An implementation for absolute fingerprint pre-alignment that resisted any correlation between related records of the fuzzy vault scheme had been proposed as the countermeasure (Tams et al., 2015). In designing an effective fuzzy vault-based cryptosystem, practical decoding strategy was important. The error correcting capacity of Reed-Solomon decoder in the original fuzzy vault was insufficient to achieve practical implementation for biometrics especially single finger. To overcome this, Lagrange-based decoder (Nandakumar et al., 2007) had been proposed but the decoding complexity would then become infeasible for implementation.

In our proposed cancelable iris key binding scheme, the principle of chaffing and winnowing was applied. This could be regarded as a confidential way to send data without encryption over an insecure channel. The idea was to first separate the message into different blocks or packets. The process of chaffing, enclosed these raw blocks (without encryption) by fusing them with some bogus blocks of data. Next, genuine and fake message authentication codes (MAC) were generated and appended to the raw blocks and bogus blocks before sending out. The recipient filtered out the chaff and identify the genuine MACs using a secret key shared between the sender and the receiver.

The latest work from Ouda et al. (Ouda et al., 2021) had adopted chaffing and winnowing principle in their key binding biometric cryptosystem framework, known as Cancelabe Biometrics Vault (CBV). This proposed framework had cited our publication (Chai et al., 2019b) about cancelable iris key binding scheme with similar design. Both works focused in two limitations,

which were the trade-off between key length and matching accuracy, as well as potential privacy issue related to key binding scheme. Under chaffing and winnowing concept, both frameworks had utilized CB to generate protected biometric templates, in order to encode bits of a cryptography key. Extended BioEncoding was implemented to obtain the bit string. Similar to our proposed scheme, CBV framework was generic and did not rely on single or specific biometric representation. The framework had preserved the performance at FRR 6.92% with increasing key size up to 256. It was also proven through this similar framework that our proposed cancelable iris key binding framework under the principle of chaffing and winnowing had satisfied the requirements of performance preservation, non-invertibility and unlinkability.

The literature review of the related works above had highlighted a few problems. First issue, the degradation of authentication performance caused by biometric template protection scheme. Second, the trade-off issue existed between security and authentication performance of an iris key binding scheme and limitations due to the implementation of ECC. Third, iris code was widely applied in iris template protection scheme. The rotation and inherent dependency issues in iris code had affected the authentication performance and security of iris code based template protection schemes.

CHAPTER 3

METHODOLOGY

3.1 Preliminaries: Performance Degradation in BTP schemes

From the literature review, performance degradation in terms of accuracy and error rate are inevitable after the implementation of biometric template protection scheme (BTP). This is due to the fact that intentional matrix distortion, random permutation and remapping are among the techniques used to achieve irreversibility and unlinkability in most of the BTP schemes. This implies loss and distortion of biometric information in this process. In the methodology of Bloom filter (Rathgeb et al., 2013), binary to decimal value function is used along with index remapping technique. Therefore, certain degree of information loss can be expected through this mapping. For instance, using a word size of five for Bloom filter, five neighboring binary bits in a column will be converted to a decimal value. The decimal value will then be remapped into its respective index position in the Bloom filter. In this process, part of the information contained by these binary bits might lost in exchange of a decimal value as the final outcome. Referring to the recommended level of information for better security (Jenisch and Uhl, 2011) against coalition attack, an information loss of 80% can be anticipated through block remapping. If we consider this as the reference to a decimal value ‘1’ produced by ‘5’ binary values, the total information loss can be higher for longer word size. This

improves the security strength of the system but false non-match rate will increase as well. Hence, there is always a tradeoff between security and usability of a system.

In another separate example, different type of information loss can be anticipated in the process of Hadamard multiplication between permuted iris codes in BTP scheme such as IFO hashing (Lai et al., 2017b). In Figure 3.1 (right), there are 3 permuted iris codes. Hadamard multiplication process of IFO hashing can be represented by AND-operation between the permuted iris codes. The new iris code is now '01000' which has experienced information loss through AND-operation as illustrated. This is a common methodology in designing BTP scheme because the anticipated information loss is to prevent the restoration of biometric data. The scheme has experienced loss of information through the product codes generated from the permuted biometric data instead of value remapping as shown in Figure 3.1 (left) like in Bloom filter. These two methodologies are commonly introduced in BTP schemes with the purpose of strengthening the privacy or security protection through loss of information.

The purpose of stating the examples above is not to point out the degree of information loss nor the weakness of the BTP systems. In fact, information loss can happen in almost every biometric template protection scheme. It serves as a double edge sword in BTP scheme. The more information we lose in the process of template protection, the harder it is for others to reconstruct the raw biometric features. In contrary, this also means that information loss will inevitably cause performance degradation. Ideally, an optimum iris BTP scheme will need to achieve extensive information loss while maintaining minimal performance degradation. However, the requirement of stronger security

imposes a trade-off between information loss and recognition performance. Stronger security in protection scheme is likely to have more severe performance degradation (Nandakumar and Jain, 2015) while schemes which maintain recognition accuracy are often left with unattended doubts in security.

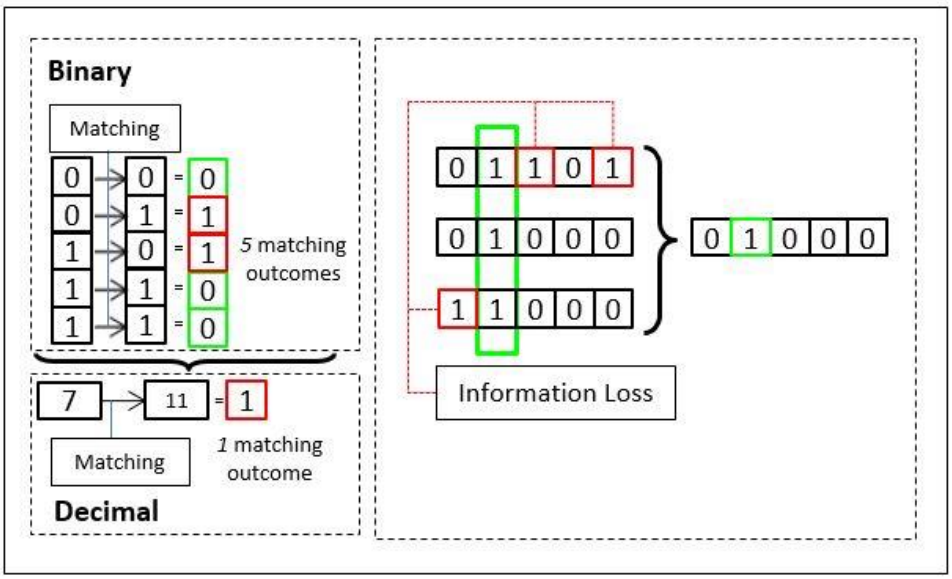


Figure 3.1: Number of Matching Outcomes Before / After Binary-To-Decimal Transformation (left) And Information Loss Through The Product Of Binary Codes (right)

3.1.1 Overview of the Proposed Method 1: Confidence Matrix for Protected Iris Recognition Systems

To mitigate the problems outlined in previous section, confidence matrix generation scheme is proposed to improve the performance of protected biometric systems. The proposed method relaxes the tradeoff suffered by most of the BTP schemes in finding a balance between security strength and recognition performance. In other words, the proposed method enables BTP

schemes to gain adequate security strength without worrying its drawback in recognition performance. Preliminary work regarding confidence bits was tested on one BTP scheme in (Chai et al., 2019a). In this thesis, confidence matrix generation scheme will be reviewed together with its experiments and analysis on various publicly available iris databases.

The proposed method, confidence matrix generation will take place after the implementation of BTP scheme. Figure 3.2 shows the basic design of a protected iris based biometric system with and without confidence matrix generation scheme. A standard system will first acquire, process and extract pertinent features given raw iris data. The extracted iris features will then undergo BTP scheme in order to conduct matching in a secured domain during authentication stage. This proposed design consists of confidence matrix generation stage and authentication stage. After BTP, confidence matrix can be generated directly with at least two protected biometric samples from each enrolled personnel. When an arbitrary iris data is being tested against another biometric sample, authentication can be carried out in a secured domain between hashed templates based on our proposed confidence scoring system.

The main concept of confidence matrix is to identify the confidence locations in the matrix, verify the results of collision between two hashed templates and authenticate based on the final confidence score computed. The proposed method is flexible in the sense that there are no limitations in terms of ways to construct the confidence matrix and its properties. In this work, two methods have been proposed to construct confidence matrix into binary and fraction forms with their corresponding computation for confidence scores.

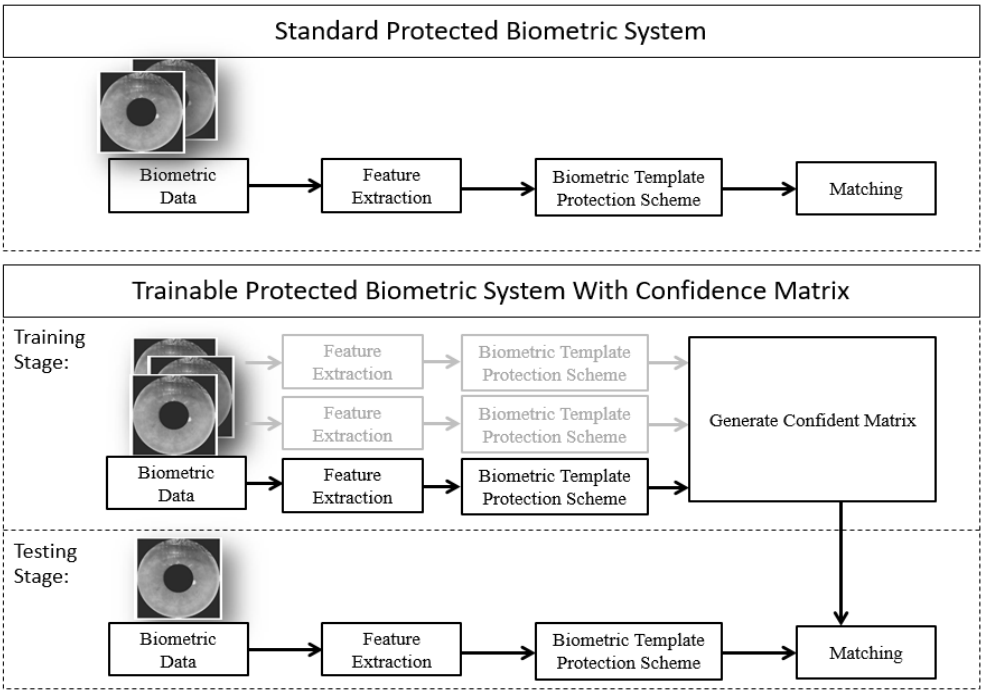


Figure 3.2: Overview of A Standard And The Proposed Protected Iris Biometrics System

3.1.2 Generation Method for Binary Confidence Matrix

In confidence matrix generation stage, multiple hashed templates can be used to generate a final confidence matrix. The process of generating confidence matrix is illustrated below (Figure 3.3).

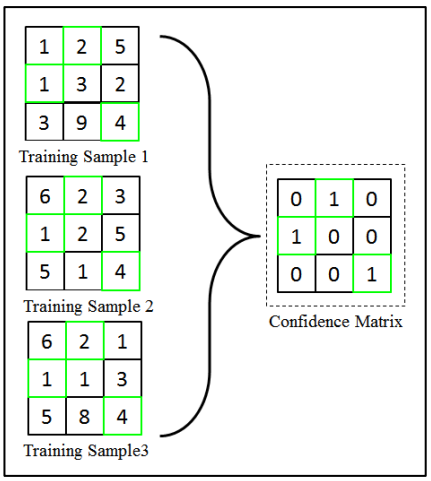


Figure 3.3: Process of Generating Binary Confidence Matrix

From this illustrated example, three samples are selected randomly. For the generation of confidence matrix, element-based collision matching can be carried out between hashed samples:

$$N = \quad {}^{n}C_{r} = \frac{n!}{r!\,(n-r)!} \tag{1}$$

Where N denotes the maximum possible combinations, n is the number of training samples to choose from and r is the number of selected samples. For this example, the number of combinations, N will equal to 3 when $r = 2$ and $n = 3$. Therefore, 3 sets of collision matching outcomes R_n will be obtained. Element-wise product rule is then used to obtain the collision matching outcomes to form the final confidence matrix, M as shown below:

$$M(x,y) = \begin{cases} 1, & if \prod_{n=1}^{N} R_n(x,y) = 1 \\ 0, & otherwise \end{cases} \tag{2}$$

The construction phase starts by creating a zero output matrix with the same size as the hashed samples. Our proposed scheme will cross-match every element within the n −selected hashed training samples. The collision formula in the equation above is mainly indicating the confidence locations across multiple hashed samples by fusing all the outcomes of collision via product rule. The main purpose of confidence matrix here is to identify hashed bits which can be categorized as confidence bits. When all the paired training samples gives the same value in particular location, a matched collision is fulfilled and this is

defined as the confidence bit location. For instance, if the same value is found at the same respective location (x, y) in all the hashed training samples, the value "1" will be assigned to that specific confidence location (x, y). If this condition is not fulfilled, the particular bit location will be labeled as "0" under "no confidence" location. Finally, a binary confidence matrix will be generated.

3.1.3 Generation Method for Probability Confidence Matrix

In this section, the flexibility of the proposed concept is demonstrated by constructing the confidence matrix alternatively. A confidence location can be determined from hashed matrix based on the frequency of matched collisions. This process generate the final matrix in fraction form instead of binary form. Note that our proposed method is different than fragile bits method (Hollingsworth et al., 2009). First, fragile bits method identifies bits which have flipped more than a preset threshold to determine inconsistent bits. In this proposed method, no threshold is being set. Mathematical fraction is being used to represent the frequency of collisions for real values instead of flipping times of binary bits in fragile bits method, as the main idea is to construct the proposed confidence matrix for authentication.

The method of generating probability confidence matrix is different compared to binary confidence matrix. Instead of using product rule to combine all the collision results, probability confidence matrix captures the frequency of matched collisions over the total number of collisions in a particular location. In binary confidence matrix, confidence location exists only if all the collisions at this particular location are matched collisions while disabling other locations

which do not fulfil this criteria. In contrary, probability confidence matrix takes every location in its matrix into account by calculating its respective frequency of matched collisions. The process of generating probability confidence matrix is shown as below (Figure 3.4).

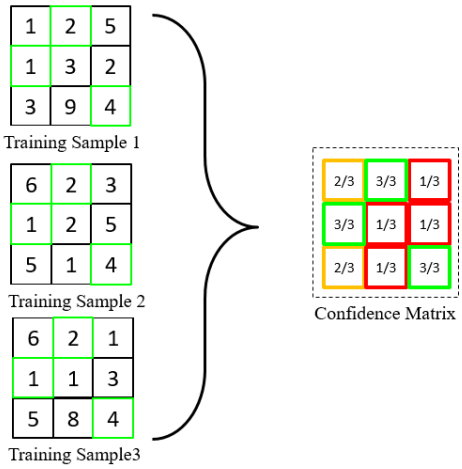


Figure 3.4: Process of Generating Probability Confidence Matrix

Referring to the visual aid above, the process of generating probability confidence matrix has been illustrated. A reference template, $R(x, y)$ can be generated for authentication later. It can be constructed in many ways, for example, taking values of all the matched locations (x, y) across the hashed samples for training. Otherwise, the default value at sample 1 will be taken. As information from multiple hashed samples are utilized in this formation, the reference template has higher reliability in representing the characteristic of a class. The probability confidence matrix tabulates the corresponding percentage of matched collisions in each location of the hashed template. This matrix is very important to determine the degree of confidence in each location. For instance,

$R(1,1)$ in Figure 3.4 indicates a confidence of 2/3 which is equivalent to 66.7%. The confidence in probability is calculated based on the matched collisions for value '6' in 2 out of 3 hashed samples. Taking $R(3,3)$ as another example, the corresponding confidence is 3/3 (100%) indicating that 3 matched collisions out of 3 hashed samples. As a result, the location at $R(3,3)$ of the reference template has higher confidence compared to the location at $R(1,1)$. Thus, the generation of a reference template and its corresponding fraction matrix will form the final probability confidence matrix.

3.1.4 Authentication Stage

Authentication stage takes place after the confidence matrix of each class is successfully constructed. The proposed strategy is different from the traditional method where two hashed templates are directly compared to produce the matching result. Instead, the confidence matrix serves as the reference in validating matching (collisions) outcomes to improve the recognition performance. The main focus of this work is to have a generalized solution to improve the performance of BTP schemes without any modification. Knowing the information from the confidence mask would imply that the attacker has succeed in performing the frequency analysis based attack on protected template. In order to address the mentioned security threat, security analysis has been conducted based on non-invertibility (irreversibility), revocability and unlinkability by referring to ISO/IEC Standard 24745 (Bassit et al., 2021).

3.1.5 Matching Strategy for Binary Confidence Matrix

In authentication, hashed template 1 as the reference template will first undergo our proposed element-wise collision matching function with another hashed template 2 (query) to produce a resulted collision matrix (Figure 3.5). After that, apply AND logic function to validate the collision result with a class specific confidence matrix. This authentication process can be carried out by determining the total number of matched collisions at the confidence locations. Finally, a proposed matching score can be formulated as follows:

$$Matching\ score = \frac{\sum_i^n (A_i \cap B_i)}{\sum_i^N (C_i)} \tag{3}$$

Where hashed template 1 and 2 are denoted as A and B respectively with $i = 1,2,\dots,n$ is the number of matched collisions. Thus, the numerator part of the Eq. (3) is representing the number of matched collisions between the two hashed templates while denominator is representing N total confidence locations in confidence matrix. Referring to the figure below, the matching score of this example is equivalent to 0.667 where there are two collided bits identified at the confidence bit locations over a total of 3 confidence bit locations as indicated in the binary confidence matrix. The matching score of Eq. (3) is also formulated mathematically in more detail at Eq. (7).

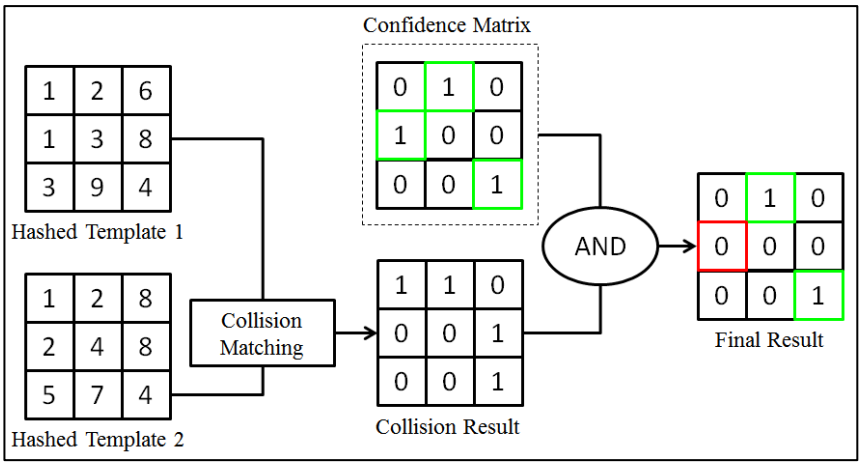


Figure 3.5: Proposed Matching Strategy for Binary Confidence Matrix

3.1.6 Matching Strategy for Probability Confidence Matrix

On the other hand, class-specific reference template generated at earlier stage will be used to authenticate any query hashed template to produce the collision result matrix. This is then followed by the dot product between the probability confidence matrix and collision result to obtain the final matrix. The proposed strategy not only determines the collided bits but also estimates the degree of confidence at the collided bit-locations. As a result, the final matching score can then be computed as follows:

$$Matching\ score = \frac{k_1\left(\frac{1}{t}\right) + k_2\left(\frac{2}{t}\right) + k_3\left(\frac{3}{t}\right)..}{n_1\left(\frac{1}{t}\right) + n_2\left(\frac{2}{t}\right) + n_3\left(\frac{3}{t}\right)..} = \frac{sum\ of\ fractions\ (Final\ Result)}{sum\ of\ fractions\ (Confidence\ matrix)} \quad (4)$$

Where $i = 1,2, \ldots t$ is the number of training samples used to construct the confidence matrix, k_i is the bit location of collisions while n_i is location of confidence bits. The matching score for the example below (Figure 3.6) is equivalent to 0.5291 (3.00/5.67).

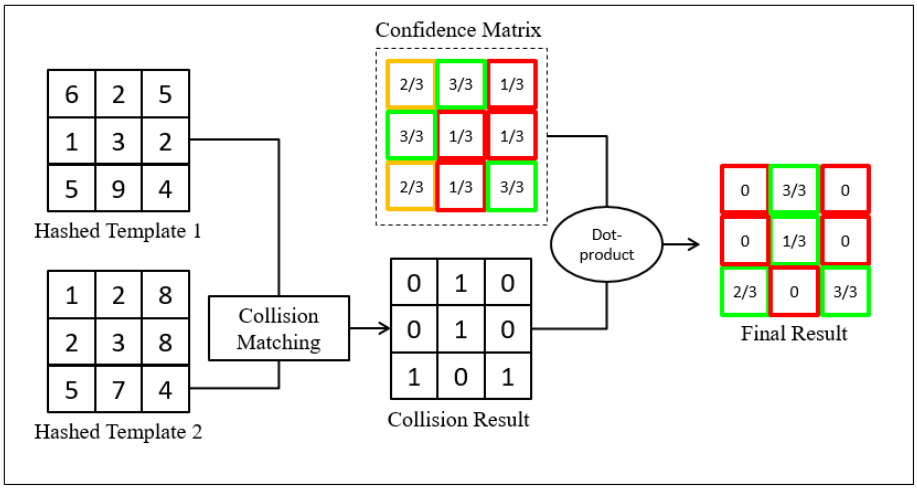


Figure 3.6: Proposed Matching Strategy for Probability Confidence Matrix

3.1.7 Iris Database with Noise Mask

In order to increase the flexibility in implementing our proposed method, the existence of noise masks in several publicly available iris databases are utilized by the proposed algorithm in the experiments to improve the recognition performance. As one of the contributions in this work, a solution is proposed to enable the integration of noise mask into popular BTP schemes, Bloom filter (Rathgeb et al., 2013) and IFO (Lai et al., 2017a) with no feature alignment process will be used in our experiments. An example of noise mask is shown below (Figure 3.7):

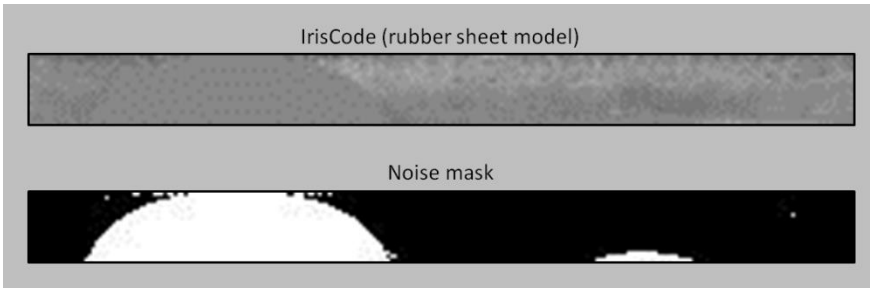


Figure 3.7: Visualization of Iris Code (top) and Noise Mask (bottom)

First, a preliminary explanation on the methodology of Bloom filter is demonstrated in Figure 3.8 below. Any arbitrary matrix of iris code will be separated into multiple iris blocks according to the word size, w and number of codeword, n. In each iris block, a column-wise binary to decimal function is used to convert binary values into decimal values. The converted decimal values are then remapped into its associated index location (column) of a row matrix, R_n. The process will be repeated for the next iris block $(w \times n)$ and the converted decimal values will be remapped again according to the indices of the next row matrix, R_{n+1}.

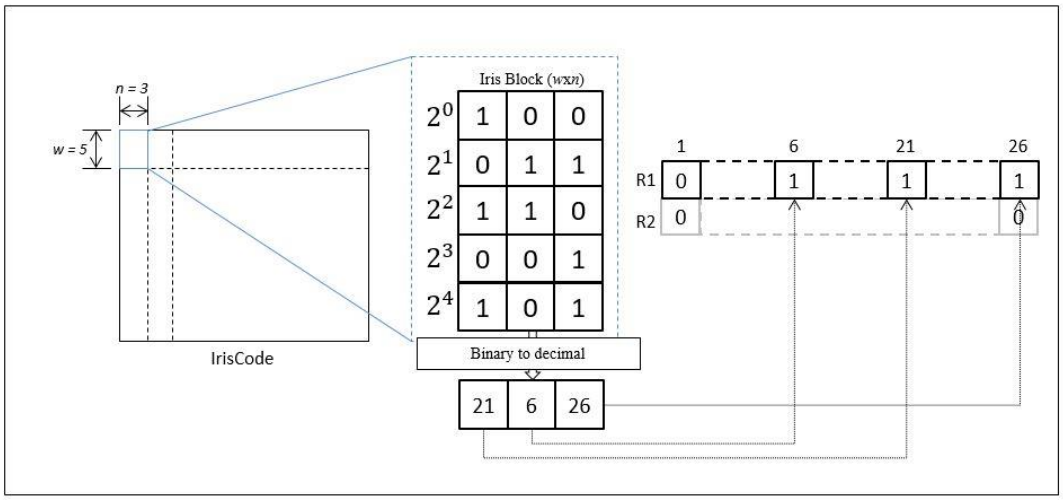


Figure 3.8: Overview of The Methodology of Bloom Filter

In order to enable the implementation of Bloom filter onto database with noise mask, a threshold based method is proposed to determine which iris block can be considered as "noisy block". By pre-setting a threshold T ($T = 0.1$ is used in our experiment), if the number of noisy bits in any iris block is more than the preset threshold, the corresponding row matrix R_n will be considered as 'null' row and excluded from the calculation of matching score as illustrated in Figure

3.9. The proposed method is also applicable for IFO hashing with Bloom filter integration to solve alignment-issue when biometric template acquisition.

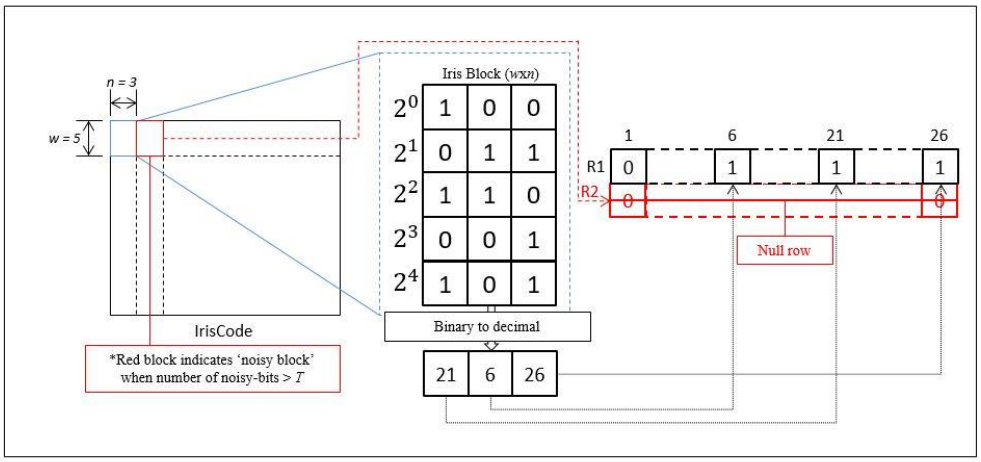


Figure 3.9: Overview of The Methodology of Bloom Filter with The Proposed Solution Utilizing Noise Mask

3.2 Overview of the Proposed Method 2: Cancelable Iris Key Binding Scheme

The proposed scheme is based on the Chaffing and Winnowing concept in cryptosystem (Rivest, 1998). The idea is to bind a random binary cryptographic key by using a set of protected iris templates named as "cancelable" iris templates. Particularly, given a random cryptographic key which is represented in binary form, i.e. [1,0,1,1], the proposed method enables the binding of different cancelable iris templates according to a randomly generated sequence of '1' and '0'. As a result, a cryptographic key can now be represented by a sequence of cancelable templates which can be stored into a database for future authentication.

For key regeneration process, the genuine cancelable template will be matched and authenticated with the formerly stored cancelable templates. For every matched instance, it enables the regeneration of partial information of the bound cryptographic key. If a binary bit '1' represents an anticipated match, this outcome will eventually allow the regeneration of the entire key (retrieval) when

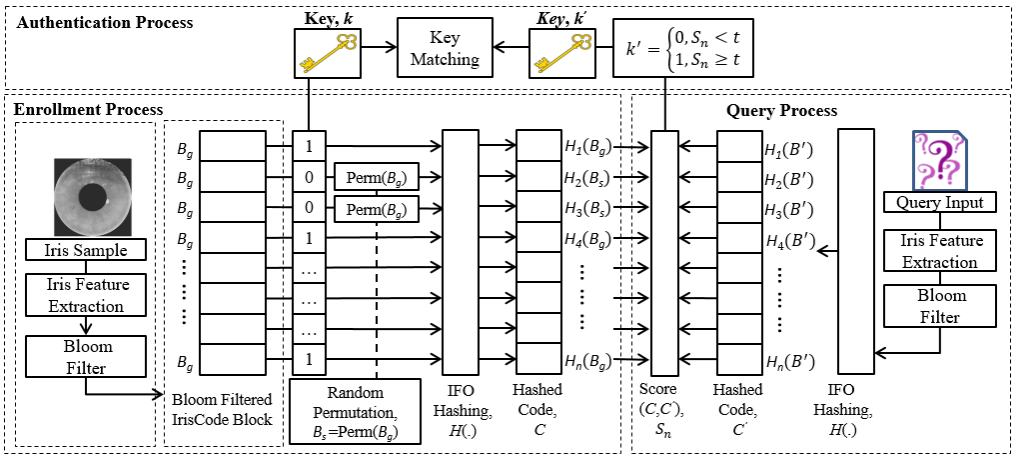


Figure 3.10: Overview of The Design for The Proposed Key Binding Scheme

3.2.1 Key Binding Process

To further explain the methodology of our proposed key binding scheme, let the input iris code denotes as $\boldsymbol{I}$, a random permutation function denotes as Perm (.) and $\boldsymbol{B}_g$ is the Bloom filtered iris code. Our proposed key binding scheme can be divided into several steps:

1. *Cryptographic key generation*: A random binary cryptographic key, $\boldsymbol{K} = \{k_j\}_{j=1}^{n}$ is generated, where $k_j \in \{0,1\}$ and n is the input parameter determining the cryptographic key length.

2. *Genuine & synthetic template generation*: iris code, $\boldsymbol{I}$ will go through feature transformation to generate genuine iris template (Bloom

filtered iris code), $\boldsymbol{B}_g$ while synthetic iris template can be generated through permutation as $\boldsymbol{B}_s \leftarrow \text{Perm}\ (\boldsymbol{B}_g)$.

3. *Key binding*: Given a key, $\boldsymbol{K} \in \{0,1\}^n$, we can define n number of IFO hash groups$\{H_1, \dots, H_n\}$. Each hash group, H_j (for $j = 1{:}\,n$) is used to generate the j-th IFO hashed code, $\boldsymbol{C}_j$ based on the input matrix of either genuine or synthetic Bloom filtered iris code. For example, if $k_j = 1$, the j-th hashed code can be described as $\boldsymbol{C}_j \leftarrow H_j(\boldsymbol{B}_g)$, where $H_j(\boldsymbol{B}_g) = \{h_{i(j)}(\boldsymbol{B}_g) | i = 1, \dots, m\ hash\ functions\}$; otherwise (if $k_j = 0$), the j-th hashed code is described as $\boldsymbol{C}_j \leftarrow H_j(\boldsymbol{B}_s)$.

4. *Hashed code generation*: n number of hashed codes shall be constructed $[\boldsymbol{C}_1, \boldsymbol{C}_2, \dots, \boldsymbol{C}_n]$ and stored in the database instead of the corresponding cryptographic key, $\boldsymbol{K}$.

5. *Storage*: The collection of output IFO hashed codes $[\boldsymbol{C}_1, \boldsymbol{C}_2, \dots, \boldsymbol{C}_n]$will then be stored together with the collection of IFO hash groups $\{H_1, \dots, H_n\}$ used in the process of key binding.

The binary key binding processes of our proposed method are defined in Figure 3.11.

3.2.2 Key Retrieval Process

Let $S(\boldsymbol{C}, \boldsymbol{C}')$ denotes a matching score between a reference (stored) IFO hashed code, $\boldsymbol{C}$ and a query hashed code, $\boldsymbol{C}'$. Given a query iris code as the input denoted as $\boldsymbol{I}'$, our proposed key retrieval scheme can be divided into several steps as follows:

1. *Genuine template generation*: $\boldsymbol{I'}$ has to go through similar transformation to first generate a query Bloom filtered iris code matrix which can then be described as$\boldsymbol{B'} \leftarrow \text{Bloom_filter}\ (W, L, \boldsymbol{I'})$.

2. *Query hashed code generation*: By using the same IFO hash groups $[H_1(\boldsymbol{B'}), \dots, H_n(\boldsymbol{B'})]$ with their respective permutations, n number of query hashed codes $[\boldsymbol{C'_1}, \boldsymbol{C'_2}, \dots, \boldsymbol{C'_n}]$ can be generated.

3. *Key retrieval*: To prepare for key retrieval, we first generate an empty array denoted as $\boldsymbol{K'} = \{k_j'\}_{j=1}^{n}$ where $k_j' \in \{0,1\}$ and n is the cryptographic key length generated via the matching between query and reference hashed codes. Given any pre-defined threshold t, matching can be carried out by calculating the similarity score $S(\boldsymbol{C_j}, \boldsymbol{C'_j})$ between the reference hashed code $\boldsymbol{C_j}$ and the query hashed code $\boldsymbol{C'_j}$. If $S(\boldsymbol{C_j}, \boldsymbol{C'_j}) \geq t$, set $k_j' = 1$, otherwise, $k_j' = 0$.

4. Eventually, a final key $\boldsymbol{K'} = \{0,1\}^n$ can be retrieved. The matching score, $S(\boldsymbol{C_j}, \boldsymbol{C'_j})$ can be measured by finding the number of agreed positions in between $\boldsymbol{C_j}$ and $\boldsymbol{C'_j}$, for example, $\frac{\text{No. of agreed positions}}{m \cdot l_1 \cdot l_2}$.

The whole process of key retrieval is being outlined in Figure 3.11.

Algorithm 1: Key binding	Algorithm 2: Key retrieval

Input: genuine Bloom filtered iris code $\boldsymbol{B}_g$ and collection of IFO hash groups $\{H_1, \dots, H_n\}$.
 	
1. Random key generation: $\boldsymbol{K} = \{k_j\}_{j=1}^{n}$
$\boldsymbol{C} \leftarrow \emptyset$
 	
2. Generate synthetic Bloom filtered iris code:
$\boldsymbol{B}_s \leftarrow \text{Perm}\left(\boldsymbol{B}_g\right)$
 	
3. Key binding:
For $j = 1$ to n
If $k_j = 1$
$\boldsymbol{C}_j \leftarrow H_j\left(\boldsymbol{B}_g\right)$
Else if $k_j = 0$
$\boldsymbol{C}_j \leftarrow H_j(\boldsymbol{B}_s)$
End if
 	
4. Hashed code generation:
Set $\boldsymbol{C} \leftarrow \boldsymbol{C} \cup \boldsymbol{C}_j$
End for
 	
5. Storage: Collection of IFO hashed codes $[\boldsymbol{C}_1, \boldsymbol{C}_2, \dots, \boldsymbol{C}_n]$ and IFO hash groups $\{H_1, \dots, H_n\}$.
	Input: query Bloom filtered iris code $\boldsymbol{B}'$, collection of the reference IFO hashed codes $[\boldsymbol{C}_1, \boldsymbol{C}_2, \dots, \boldsymbol{C}_n]$, threshold $t \in \mathbb{R}$, and collection of IFO hash groups $\{H_1, \dots, H_n\}$.
	
	1. Genuine template generation: $\boldsymbol{B}'$
	$\boldsymbol{C}' \leftarrow \emptyset$
	$\boldsymbol{K}' \leftarrow \emptyset$
	
	For $j = 1$ to n
	2. Query hashed code generation:
	$\boldsymbol{C}'_j \leftarrow H_j(\boldsymbol{B}')$
	If $\text{S}(\boldsymbol{C}_j, \boldsymbol{C}'_j) \geq t$
	$k'_j = 1$
	Else
	$k'_j = 0$
	End if
	Set $\boldsymbol{C}' \leftarrow \boldsymbol{C}' \cup \boldsymbol{C}'_j$
	
	3. Key retrieval:
	Set $\boldsymbol{K}' = \boldsymbol{K}' \cup k'_j$
	End for
	
	4. Retrieved key, $\boldsymbol{K}'$

Figure 3.11: Algorithms for Iris Key Binding (left) and Iris Key Retrieval (right)

3.2.3 The Relation of Key Retrieval Rate to Jaccard Similarity

For an efficient biometric cryptosystem, it ensures the regeneration of exact key given a similar (genuine) query Bloom filtered iris code during key retrieval. In this case, the success rate of the key retrieval attempt under genuine query can be measured through the proposed key retrieval rate (*KRR*). In this section, the relation of *KRR* to the Jaccard similarity between the enrolled and query Bloom filtered iris codes which are denoted as $\text{JA}\left(\boldsymbol{B}_g, \boldsymbol{B}'\right)$ will be briefly

discussed. For the ease of understanding, given a threshold t, suppose that we are now considering only single binary bit, $k'_j$where ($j = 1$) of a cryptographic key. Let's consider a single bit of the key as $k'_{j=1} \in \{0,1\}$ which is being retrieved by matching query hashed code $\boldsymbol{C}'_{j=1}$ against reference hashed code $\boldsymbol{C}_{j=1}$.The correctness of the regenerated key $k'_{j=1}$ can indeed be described as follows:

$$k'_{j=1} = \begin{cases} 1, & \mathrm{S}(\boldsymbol{C}, \boldsymbol{C}') \geq \mathrm{t} \\ 0, & \mathrm{S}(\boldsymbol{C}, \boldsymbol{C}') < \mathrm{t} \end{cases} \quad (5)$$

Referring to the procedures under the IFO hashing scheme, hashing of Bloom filtered iris code, $H_{j=1}(\boldsymbol{B_g})$ is conducted through independently and randomly generated permutation seeds $\{\boldsymbol{N}_1, \dots, \boldsymbol{N}_m\}_{j=1}$. Treating each bloom filter b_i as independent, the number of agreed positions (collisions) between query and reference hashed codes can be defined as $z = \sum_{i=1}^{m \cdot l_1 \cdot l_2} \chi_i$ where χ_i refers to a Bernoulli variable of $X_i = 1$ (if $\boldsymbol{C}_{j=1} = \boldsymbol{C}'_{j=1}$) or $\chi_i = 0$ (if $\boldsymbol{C}_{j=1} \neq \boldsymbol{C}'_{j=1}$). Thus, each element of $\boldsymbol{C}_{j=1}/\boldsymbol{C}'_{j=1}$ can then be treated as independent to each other. The independency of different bloom filters can be further strengthened by applying different public random permutations on the bloom filters. Therefore, $z \sim \mathrm{B}(M, P)$ follows a binomial distribution of probability of success, $P = S(\boldsymbol{B}_g, \boldsymbol{B}')$ where $M = m \cdot l_1 \cdot l_2$ denotes the total number of elements $\{c_{i=1}, \dots, c_{i=m \cdot l_1 \cdot l_2}\}_j$ in $\boldsymbol{C}_j/\boldsymbol{C}'_j$ (for $j = 1, 2, \dots, n$). This probability provides a similarity measurement between $\boldsymbol{B}_g$ and $\boldsymbol{B}'$ through $S(\boldsymbol{B}_g, \boldsymbol{B}')$.

Since the publicly known random permutations are merely applied to strengthen independency, we therefore highlight only its resultant effect on the

independency of the bloom filters here. This helps to simplify the computation of the expected value $\mathbf{E}(z) = MP$. Particularly, referring to the convention of IFO as an instance of min hash (Lai et al., 2017b), one has $P = \mathbb{P}[c_i = c_i' | i = 1,2, \dots, M] = S(\boldsymbol{B}_g, \boldsymbol{B}') = \mathrm{JA}(\boldsymbol{B}_g, \boldsymbol{B}')$, which is corresponding to Jaccard similarity of $\boldsymbol{B}_g$ and $\boldsymbol{B}'$. Thus, we can infer that $S(\boldsymbol{C}_j, \boldsymbol{C}_j') = \frac{z}{M}$ while the probability of success P is M dependence. Therefore, the *KRR* for a single binary bit cryptographic key can be described as the probability:

$$\begin{aligned} KRR &= \mathbb{P}(k_{\mathrm{j}}' = k_{\mathrm{j}}) \\ &= \mathbb{P}(S(\boldsymbol{C}_j, \boldsymbol{C}_j') \geq t) \\ &= \mathbb{P}\left(\frac{1}{M} \sum_{i=1}^{M} \chi_i \geq t\right) = \mathbb{P}(z \geq tM) \end{aligned} \tag{6}$$

The definition of the probability in Eq. (6) can be further extended for longer key length with n^* being denoted as the number of binary bit '1' (successful genuine matching) in a cryptography key. Thus, *KRR* can be redefined again as:

$$KRR = \mathbb{P}[k_j' = k_j = 1 | j = 1,2, \dots, n] = \left(\mathbb{P}(z \geq tM)\right)^{n^*} \tag{7}$$

Theoretically, $n^* \approx \frac{n}{2}$ is the approximation for maximum key entropy (Gács and Körner, 1973). Nevertheless, one can easily notice from the equation that as long as the probability $\mathbb{P}(z \geq tM)$ comes close or equal to 1, n can be further increased. This allows the flexibility to bind even longer cryptographic key in such a way that $KRR = (\approx 1)^{n^*} \approx 1$ maintains optimum success rate for key retrieval. This implies that the exact cryptographic key can be retrieved as long as $\mathbb{P}(z \geq tM) \approx 1$ for a selected threshold t. The selection of t will affect the *KRR* significantly in two folds: 1) given a fixed value of P, decreasing the value

of threshold t will increase $\mathbb{P}(z \geq tM)$ as well as KRR and vice versa. In contrary, the failure rate of a genuine query can also be computed using our proposed method through KRR. 2) Lower KRR is expected from the equation if we increase the value of n^* further and vice versa. This is another highlight of *KRR* through its amplification factor contributed by n^* which always ensures that an imposter query will have way lower KRR compared to a genuine query.

3.2.4 Example: Calculate Key Retrieval Rate (KRR)

For better illustration, hereby an example is given to calculate KRR under certain configurations. Suppose that, $M = 200$, $n = 40$ $n^* \approx 20$, and $t = 0.75$ is set given $\boldsymbol{B}_g$ and $\boldsymbol{B}'$ such that $P = S(\boldsymbol{B}_g, \boldsymbol{B}') = 0.85$ (i.e. 85% similar in terms of Jaccard similarity between the enrolled and query iris templates), we can then calculate the $KRR = \left(\mathbb{P}(z \geq 150)\right)^{20} = 0.9985$ that is close to 1 with $\mathbb{P}(z \geq 150) = 0.9999$. For higher similarity, for instance, $S(\boldsymbol{B}_g, \boldsymbol{B}') = 0.9$, we can obtain optimum $KRR = \left(\mathbb{P}(z \geq 150)\right)^{20} = 1$.

3.3 Overview of the Proposed Method 3: Cancelable Iris Template Protection Scheme

In this section, LSH technique and the implementation of our proposed transformation and matching strategy for iris codes. The optimisation in the matching and the vertical dependency are explained and analysed in this section.

3.3.1 Preliminaries – Local Sensitive Hashing (LSH)

LSH technique and its implementation in bit sampling will be briefly discussed in this section. These preliminaries would facilitate in understanding the underlying motivations of our work. Firstly, LSH technique will be discussed, followed by its implementation in randomized sampling.

LSH is based on the general idea that, if two points are close together, these two points will remain close together after going through a projection operation. LSH is a hashing technique that can be used for dimensional reduction. This can happen when similar high dimensional data is being mapped into the same bucket with high probability. However, the size of the buckets will be smaller than the input data after hashing. The main difference between LSH and conventional cryptographic hashing is that LSH aims to maximize the probability of collisions for similar data while cryptographic hashing minimizes the probability of collisions. The formal definition of LSH (Charikar, 2002) can be defined as follows:

Definition 3.1. Given that probability $P_2 > P_1$, a collection of input data M where two arbitrary inputs $\omega, \omega' \in M$ and H is the family of the hash functions h . The locality sensitive hashing scheme involves the application of i local hash functions h_i onto the input data $H = h_i . M \rightarrow U$, where output U refers to the hashed metric space that comes along with a similarity function S. To give an overview, this scheme can be viewed as a probability distribution over a family of hash functions such that $P_{h \in H}[h(\omega) = h(\omega')] = S(\omega, \omega')$.

The similarity function S particularly defined the collision probability between two hashed input data, ω and ω'. Apart from providing the local

hashing facilities, LSH also ensures that two similar inputs will render a higher probability of collision. Alternatively, dissimilar inputs will be transformed into hashes with low probability of collision. These properties can be further defined as:

$$P_{h\in H}(\big(\, h_i\,(\omega) = \, h_i\,(\omega')\big) \leq P_1, \;\; if\; S(\omega,\omega') < R_1$$

$$P_{h\in H}(\big(\, h_i\,(\omega) = \, h_i\,(\omega')\big) \geq P_2, \;\; if\; S(\omega,\omega') > R_2 \qquad (8)$$

Where $R_2 > R_1$ given that $P_2 > P_1$ is ascertained by the properties of LSH scheme.

3.3.2 Bit Sampling LSH for Hamming Distance

One of the most efficient ways of constructing a LSH family is via random bit sampling strategy (Indyk and Motwani, 1998). Precisely, given a binary string $x \in \{0,1\}^k$, one can construct LSH family $H = \{h{:}\,\{0,1\}^k \rightarrow \{0,1\}\}$ subject to the sampling function $h(x) = x_i$ where $i \in \{1, \dots, n\}$ is the index (location) chosen randomly over n indices while x_i refers to the i-th symbol of x. Thus, this generates a random binary string $v \in \{0,1\}^n$ using a LSH family of sampling functions $H = \{\, h_1,\, h_2, \dots,\, h_n\}$. Each individual sampling function is expected to generate a single symbol value of v which is equivalent to the x_i, for instance, $v = [\, h_1(x),\, h_2(x), \dots,\, h_n(x)]$. The LSH family can then be constructed using bit sampling for similarity score as follows:

$$\Pr[h(x) \neq h(y)] = 1 - (\tfrac{\|x \oplus y\|}{k}) \qquad (9)$$

Where $\|x \oplus y\|$ is the hamming distance function between x and y. For similar inputs, i.e., $x \approx y$ renders smaller $\|x \oplus y\|/k$ while dissimilar inputs, i.e., $x \neq y$ renders larger $\|x \oplus y\|/k$.

In the proposed scheme with iris code as the input biometric, the usage of the bit sampling strategy for LSH comes at two folds. Firstly, the bit sampling strategy is designed to accept a binary string as input. Therefore, it is naturally a close fit for iris code without additional needs of quantization or normalization process. Secondly, this strategy exhibits binary-wise operation, which offers simplicity and efficiency properties to our proposed scheme. Furthermore, the hashed binary string inherits LSH property. Each sampled random bit should hold as i.i.d. variable that follows the distribution of the input. This gives an insight of the relation between the original data and the hashed data when designing a non-linear cancelable transformation function.

Thus, our proposed transformation inherits the properties of LSH where each column is independent and random. This characteristic allows the application of bit-shifting straight onto the transformed template for performance optimization. Bit-shifting is indeed a powerful solution in compensating orientations that inevitably appeared in iris samples (Daugman, 2004b, Masek, 2006). Most of the transformations in BTP schemes are not able to provide this flexibility (Lai et al., 2016, Lai et al., 2017b). Meaning that, bit-shifting can only be conducted on the original iris codes and the transformation needs to be repeated each time bit-shifting is applied. This requirement makes some of the iris BTP schemes inefficient and insecure. The proposed transformation model aims to solve this problem and bit-shifting can be applied repeatedly onto our transformed iris templates straight. The following section will discuss about the steps of the proposed transformation of our iris template protection scheme.

3.3.3 Proposed Transformation for Iris Code

This section presents the details about our proposed transformation for generating cancelable iris templates. A family of LSH sampling functions is denoted as $H = \{h_1, h_2, \ldots, h_n\}$. Let $x \in \{0,1\}^{a \times b}$ be the input iris code of size $a \times b$ where a is the number or rows and b is the number of columns. Let $m > 0$ is an integer subject to $n|m$ (i.e., n is divisible by m. The proposed transformation for cancelable iris templates can be described using a function $F(x, H, m, n)$ with following steps:

Function $\boldsymbol{F(x, H, m, n)}$:

Step 1: Denote c_i as the i-th column of x. Perform bit sampling strategy with $H = \{h_1, h_2, \ldots, h_n\}$ to generate hashed outputs $v = (v_1, \ldots, v_b)$ of each column. Here, $v_i \in \{0,1\}^n$ denotes the output vector corresponds to the n sampling functions for i-th column of x, i.e., $H(c_i) = v_i$.

Step 2: For each v_i, set $r = n/m$ and divide v_i into r-tuple sub-strings (each sub-string will contain m bits). Then, convert the sub-strings into their respective decimal values. This leads to a mapping of $v_i \rightarrow T_i \in [0, 2^m - 1]^r$.

Step 3: Construct a template as $T = [T_1, \ldots, T_b] \in [0, 2^m - 1]^{r \times b}$. A random salt, R with 256 bits are generated and prepended to every element of T. Finally, perform an element-wise one-way hashing on T. For testing purpose, MD5 encryption (Rivest and Dusse, 1992) has been adopted in this experiment. Note that, this step can be replaced by a more secure one-way hashing scheme

in future for real time implementation. The steps of this transformation have been illustrated in below (Figure 3.12).

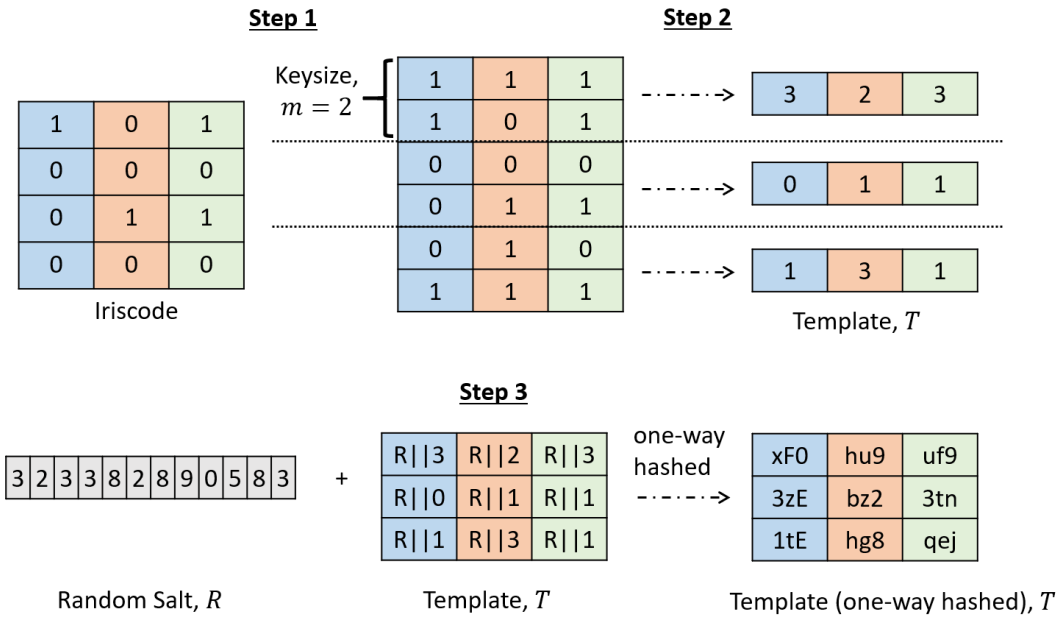


Figure 3.12: An Example of The proposed Transformation with $m = 2$ and $n = 6$. Step 1: Perform bit sampling strategy for each column independently and randomly. Step 2: Select a desired key size e.g., $m = 2$, then convert each column (m-bitwise) to its respective decimal value. Step 3: Construction of the final template T (in decimal values) with random salt R followed by one-way hashing scheme.

3.3.4 Proposed Matching Strategy for Iris Code Based Cancelable Template Protection Scheme

Given two transformed iris templates $(T, T') \in [0, 2^m - 1]^{r \times b}$, the matching between T and T' can be carried out by measuring their hamming distance, i.e., the number of symbols where T and T' are different. Similar to the conventional iris code, the matching for the transformed templates can be

conducted iteratively via several times of left and right shifting. This is to compensate the orientation variance of different iris codes. Thus, the best match for T' can be obtained by selecting the matching with the lowest error rate.

According to the studies in (Daugman, 1993, Hu et al., 2016, Liu et al., 2013), inherent correlations within an iris codes are substantially conveyed in radial direction. Therefore, iris texture made up of furrow or ciliary pattern tend to propagate in radial direction, exerting its influence on the vertically adjacent bits of iris code. The iris texture is said to have inherited correlations along the radial direction while the discriminative information is distributed along the horizontal direction. The vertically adjacent bits in an iris code are suggested to be dependent, i.e., the columns of the iris code after unwrapping the human iris to its 2D-polar equivalent space using Daugman's rubber sheet model (Masek, 2006). In view of this dependency, additional constrains have been introduced over the matching strategy between two different transformed templates (T, T'). The purpose of having this additional measure is to minimize the vertical dependency within the transformed iris template to achieve higher level of system's performance and security.

Given the stored iris template after our proposed transformation $T \in [0, 2^m - 1]^{r \times b}$ and a query iris code $x' \in \{0,1\}^{a \times b}$. The proposed matching strategy can be described using a function $F'(T, x', H, m, n, n_c, q, \tau)$ with T, x', H as the inputs and integers m, n, n_c, q, τ as the parameters where $b | n_c$.

Function $\boldsymbol{F'(T, x', H, m, n, n_c, q, \tau)}$:

Step 1: Divide the stored iris template T into b/n_c –tuples, each consists of n_c columns of T. Concatenate all n_c columns in each tuple to form one single

column of data. This step leads to a change in the dimension of the transformed template from $T \in [0, 2^m - 1]^{r \times b}$ to $T \in [0, 2^m - 1]^{(rn_c) \times (b/n_c)}$.

Step 2: Perform transformation $F'(x', H, m, n) \rightarrow T'$ onto the query iris code to obtain the transformed iris template $T' \in [0, 2^m - 1]^{r \times b}$.

Step 3: Repeat the concatenation in step 1 for T' to form a single column of data. This changes the dimension of the transformed query template to $T' \in [0, 2^m - 1]^{(rn_c) \times (b/n_c)}$.

Step 4: Initialize a score count, $z = 0$. Let T_i and T_i' are referring to the same bit location at i-th column of T and T' respectively where $T_i \in T$ and $T_i' \in T'$. Compute the hamming distance $\|T_i \oplus T_i'\|$ which means the number of different symbols between T_i and T_i'. If $\|T_i \oplus T_i'\| \leq \tau$, set $z = z + 1$. Otherwise, do nothing.

Step 5: Set T' as the bit-shifted transformed template. After applying bit-shifting technique (see (Lai et al., 2017b), Section 4.4), repeat step 3 and step 4 for q number of times (q is equivalent to the number of bit-shifting applied) to yield a set of score counts $(z_1, \dots, z_q)$. Normalize the final similarity score $s \in [0,1]$ as $s = max(z_1, \dots, z_q)/(b/n_c)$. The steps of the proposed matching strategy for iris codes are illustrated in Figure 3.13.

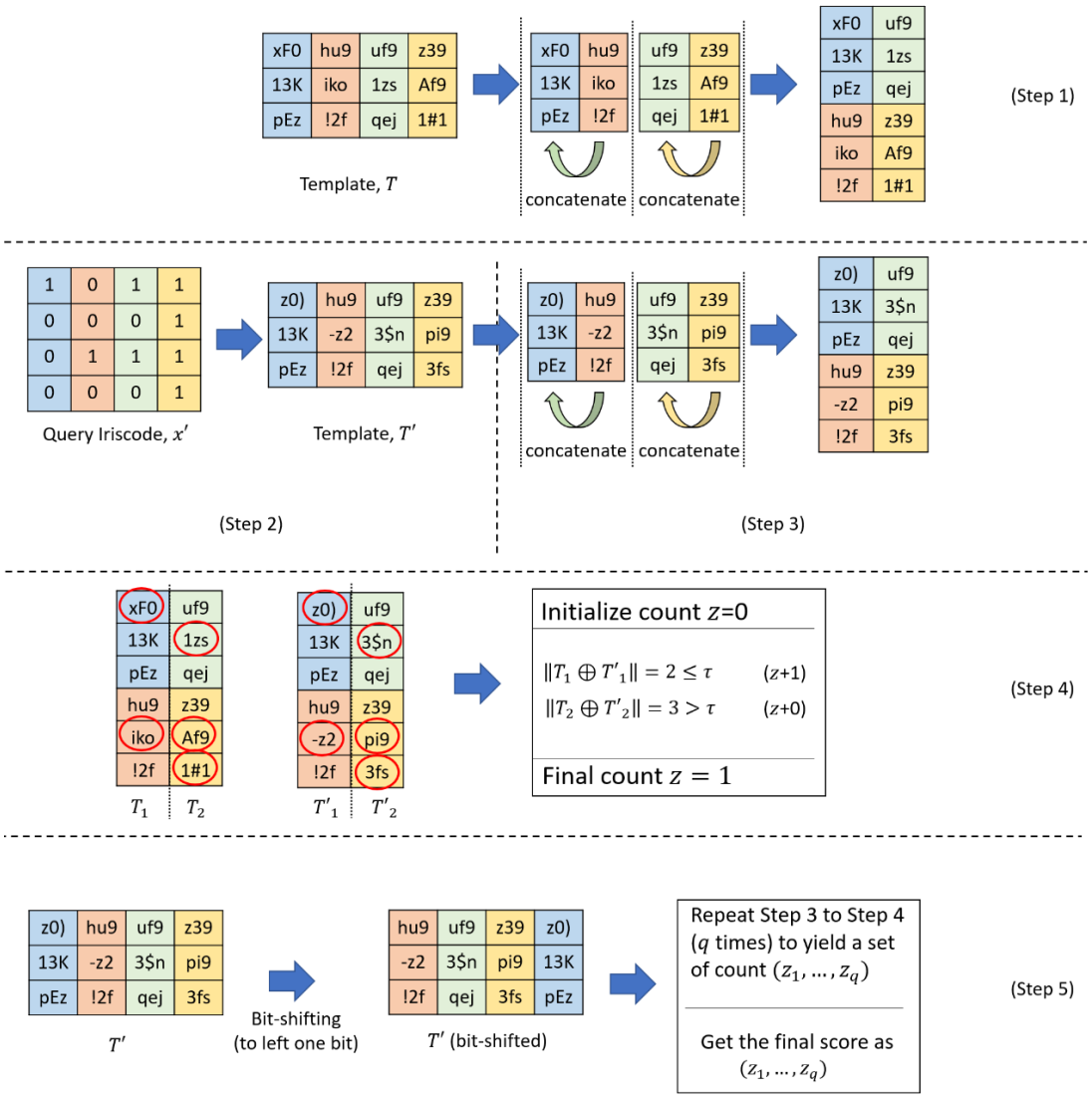


Figure 3.13: An Example of The Proposed Matching Strategy with $m = 2, \tau = 2, n = 6, n_c = 2$ and q= 1. Step 1: The transformed template is mapped from $T \in [0, 2^m - 1]^{r \times b}$ to $T \in [0, 2^m - 1]^{(rn_c) \times (b/n_c)}$. Step 2: Perform our proposed transformation for the query iris code $F'(x', H, m, n) \rightarrow T'$. Step 3: Map T' to $T' \in [0, 2^m - 1]^{(rn_c) \times (b/n_c)}$. Step 4: Compute the hamming distance of each column between T and T'. Record the score count z for i –th column with hamming distance $\|T_i \oplus T_i'\| \leq \tau$. Step 5: Perform bit-shifting on T'.

Repeat step 3 and step 4 to yield a set of score counts $(z_1, \dots, z_q)$. The final similarity score can be computed as $s = max(z_1, \dots, z_q)/(b/n_c)$.

3.3.5 Optimize the Matching of Transformed Iris Codes

Given a bit sampling function $h \in H$. The i-th column of the iris codes x and y are denoted as $c_i \in x$ and $c_i' \in y$ respectively. If x and y are two different iris codes, a dissimilarity of $\varepsilon_d = \|c_i \oplus c_i'\|/k$ will be obtained. Referring to Eq. (9), the probability for the matching between the bits sampling function can be derived as:

$$h(c_i) \neq h(c_i') = \varepsilon_d \tag{10}$$

After our proposed transformation, the stored iris template and query iris template can be represented by T and T'. Any symbol at the i-th column of the transformed templates T and T' shall consist of m bits as (Figure 3.12). Meaning that, the probability for a symbol (under the same column) between two transformed templates to be different depends upon m independent bit sampling functions $(h_1, \dots, h_m)$ can be further described as:

$$(h(c_i) \neq h(c_i'))^m = (\varepsilon_d)^m \tag{11}$$

It is arguable that different pair of columns within the iris codes x and y might result in different distances, i.e., $\|c_i \oplus c_i'\| \neq \|c_j \oplus c_j'\|$ for $(i \neq j)$ mapping the transformed template from $(T, T') \in [0, 2^m - 1]^{r \times b}$ to $(T, T') \in [0, 2^m - 1]^{(rn_c) \times (b/n_c)}$ (refer to Step 1 and Step 3 under the function $F'(x', H, m, n)$). This problem can be analyzed by deriving the minimum distance between the i-th columns of (T, T'):

$$\|T_i \oplus T_i'\| \geq \min((\|c_1 \oplus c_1'\|/k)^m, \dots, (\|c_{b/n_c} \oplus c_{b/n_c}'\|/k)^m) rn_c \tag{12}$$

On the other hand, the maximum distance between the i-th columns of (T, T') follows

$$\|T_i \oplus T_i'\| \geq \max((\|c_1 \oplus c_1'\|/k)^m, \dots, (\|c_{b/n_c} \oplus c_{b/n_c}'\|/k)^m) rn_c \tag{13}$$

Based on Eq. (12) and Eq. (13), when the computed value for $\|T_i \oplus T_i'\|$ is small, this implies a higher score count of z (refer to Step 4 in the previous section) given that the input iris codes (x, y) exhibit small pair-wise hamming distance over their columns. In the contrary, large value for $\|T_i \oplus T_i'\|$ implies a lower score count of z given that the input iris codes (x, y) exhibit large pair-wise hamming distance over their columns. This asserts our claim over the distance-preserving property of the proposed matching mechanism. This property guarantees that similar iris codes with small pair-wise distance over their columns results in high similarity score s while dissimilar iris codes with small pair-wise hamming distance over their columns will render lower similarity score as formulated in Step 5 in previous section. More formally, let $\varepsilon_{min} = \min((\|c_1 \oplus c_1'\|/k)^m, \dots, (\|c_{b/n_c} \oplus c_{b/n_c}'\|/k)^m)$ and $\varepsilon_{max} = \max((\|c_1 \oplus c_1'\|/k)^m, \dots, (\|c_{b/n_c} \oplus c_{b/n_c}'\|/k)^m)$. The parameter τ can be described in terms of any random $\varepsilon^* > 0$, n_c and r follows $\tau = rn_c\varepsilon^*$. For an arbitrary value of $\tau \in [rn_c\varepsilon_{min}, rn_c\varepsilon_{max}]$, clearly it means $\varepsilon^* \in [\varepsilon_{min}, \varepsilon_{max}]$. Taking into account that the random bit sampling for different columns of the iris code are independent, the outcome of the matching in terms of probability can be modeled by binomial distribution as shown below with mean equals to τ and variance equals to $\tau(1 - \varepsilon^*)$, thus:

$$\Pr[\|T_i \oplus T_i'\| \leq \tau] = \sum_{i=1}^{rn_c} \binom{rn_c}{i} (\varepsilon^*)^i (1 - \varepsilon^*)^{rn_c - i} \tag{14}$$

The solution for $\Pr[\|T_i \oplus T_i'\| \leq \tau]$ can be found given an appropriate value of $\varepsilon^* \in [\varepsilon_{min}, \varepsilon_{max}]$, which implies an appropriate chosen value of $\tau \in [rn_c\varepsilon_{min}, rn_c\varepsilon_{max}]$. In particular, the relation between $\Pr[\|T_i \oplus T_i'\| \leq \tau]$ versus ε^* has been illustrated (Figure 3.14). The analysis and its formulation demonstrated that a right choice of τ ensures the iris codes with small columns pair-wise hamming distance, i.e., at most τ, renders high probability and thus the expected similarity score s is overwhelmingly close to one.

The solution only exists for Eq. (14) given the value of $\tau \in [rn_c\varepsilon_{min}, rn_c\varepsilon_{max}]$. In other words, the distribution of the columns pair-wise distance of input iris codes (x, y), for instance, ε_{min} and ε_{max} must be known. Ideally, we wish that $|\varepsilon_{max} - \varepsilon_{\min}|$ can be as large as possible so that wider range of τ can be chosen to solve this problem. It is also impractical to assume that $|\varepsilon_{max} - \varepsilon_{\min}|$ can be determined precisely without precise knowledge on the distribution of the columns' pair-wise distance of the input iris codes. A naïve way to maximize the range of $|\varepsilon_{max} - \varepsilon_{\min}|$ is to increase the value of n_c which leads to the concatenation of more columns. Hence, the variance of the columns pair-wise distance's distribution will be increased with the increase of $|\varepsilon_{max} - \varepsilon_{\min}|$.

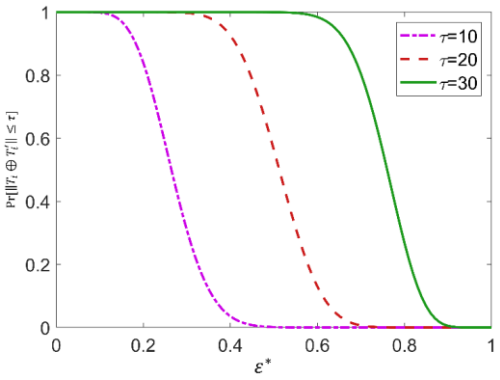
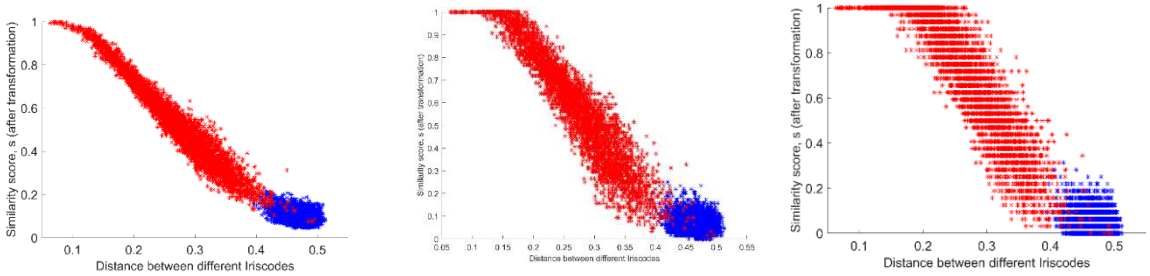


Figure 3.14: The Relation of $\Pr[\|T_i \oplus T_i'\| \leq \tau]$ vs ε^*

To support further the impact of n_c on the variance of the pair-wise distance distribution of the input iris codes, the relation of the output similarity score s versus the normalized original hamming distance [0,1] of different iris codes is plotted for analysis (Figure 3.15). Referring to the results generated, a higher value of n_c increases the separation of points over the x-axis. The spread of the distribution is greater, meaning that the variance of the columns pair-wise distance's in the input iris codes has been increased. This outcome is aligned with the proposed strategy to accept various iris codes with their columns pair-wise distances being characterized in terms of probability (refer to Eq. 14 and Figure 3.14).



(a) $n_c = 2, \tau = 8$ (b) $n_c = 8, \tau = 30$ (c) $n_c = 16, \tau = 60$

Figure 3.15: Relation Between the Similarity Score, s and The Normalized Original Hamming Distance of Different Iris Codes Under The Same Parameter Setting $m = 10$, and $n = 50$.

3.3.6 Minimizing the Vertical Dependency of Iris Code

Due to vertical dependency in iris codes (Hu et al., 2016, Liu et al., 2013), the pair-wise hamming distance of iris codes' columns are expected to be small. The similarity score $(1 - \varepsilon^*)$ between columns of the transformed templates will also be suppressed. In the matching strategy, a mapping is proposed to

concatenate n_c number of columns of $(T, T') \in [0, 2^m - 1]^{r \times b}$ to form $(T, T') \in [0, 2^m - 1]^{(rn_c) \times (b/n_c)}$. This is necessary to minimize the vertical dependency of the iris codes hence optimize our matching results.

To be more specific, the distance-preserving property ensures that the column based pair-wise hamming distance of the mapped templates as shown in Eq. (12) is proportionally related to the number of rows in the original iris code, a. For example, if the value of a is smaller, indicating lesser number of rows at the iris code, the minimum columns pair-wise hamming distance of the mapped templates (T, T') will be smaller. The pigeonhole principle can well explain such scenario. Smaller a means lesser row-wise symbols in each column could lead to higher collision of symbols over the same column between different iris codes. Hence, this scenario increases the chance of false acceptance.

In view of this, the proposed mapping imposes the concatenation of n_c columns to increase the minimum pair-wise hamming distance of the iris codes (x, y) when matching. At the same time, note that the number of columns, b in the iris codes are being reduced from b to b/n_c. The effect of n_c on the matching score in overall has been depicted in Figure 3.16. The matching of similar iris codes (genuine) is shown in red solid line while the matching of dissimilar iris codes (imposter) is shown in blue solid line. Note that the matching score here indicates the columns' minimum pair-wise hamming distance of the iris codes. As observed, the columns pair-wise hamming distance (minimum) has been increased with the increasing n_c, yielding a left-shifted matching distribution in overall. In addition, the degree of overlap between the genuine and imposter distributions has been reduced subsequently. This implies

the reduction of vertical dependency in iris codes which increases the distinguishability among genuine and imposter matching results.

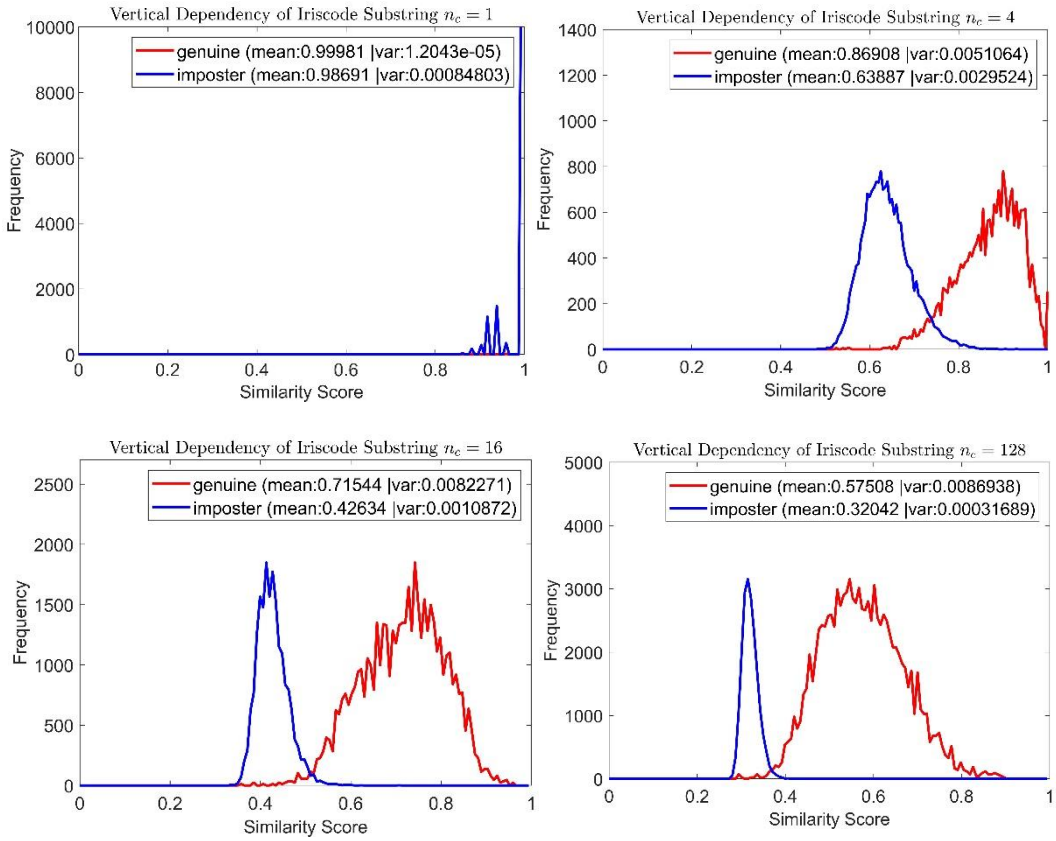


Figure 3.16: The Matching Scores of Genuine (red) and Imposter (blue) Cases with Increasing n_c

CHAPTER 4

RESULTS AND DISCUSSIONS

4.1 Performance of the Proposed Method 1 - Confidence Matrix

For experiments related to confidence matrix, four publicly available Near Infrared (NIR) iris databases, CASIAv1 (2003), CASIAv3 Iris-Interval (2002a), CASIAv4 Iris-Thousand (2014) and ND0405 (Phillips et al., 2009) databases are used. The information of these experimented databases are shown in Table 4.1:

Table 4.1: List of Iris Databases

Database	Number of Eye Images	Number of class	Resolution	Wavelength	Noise mask (Y/N)
CASIAv1	756	108	320 x 280	NIR	Yes
CASIAv3	868	124	320 x 280	NIR	No
CASIAv4	331	100	640 x 480	NIR	Yes
ND0405	784	100	720 x 100	NIR	Yes

CASIAv1 consists of iris images which are captured in two sessions by a self-developed camera with 850nm NIR illuminators. All images are stored in BMP format with resolution 320×280. The pupil region is automatically detected and specular reflections from the NIR illuminators are masked out by a circular region of constant intensity. CASIAv3 Iris-Interval (referred as CASIAv3 in this thesis) is another database constructed through two sessions by

a close-up homemade iris camera. The 320×280 iris images have very clear iris texture details due to its circular NIR LED array with optimal luminous flux for iris imaging. Left eye images from CASIAv3 are chosen to form a subset of database which contains 7 eye images for each class in this project.

CASIAv4 Iris-Thousand (referred as CASIAv4 in this thesis) contains images collected using a dual-eye iris camera IKEMB-100. The high quality iris images with resolution 640×480 are captured with optimal pose adjustment. The intra-class variation are mainly specular reflections and eyeglasses. ND0405 is a large-scale database captured in NIR wavelength at a close distance by a LG2200 iris imaging system. Many real world conditions appear in this iris database, leading to degradations such as blurring, occlusion, specular reflection, off-angle, etc. Some subjects wore contact lenses which cause distortion on iris textures. Same as CASIAv4, both databases have uneven number of images per class. Referring to a similar work (Hu et al., 2016), CASIAv3 has the highest image quality followed by CASIAv4, CASIAv1 and ND0405. To have a compatible variability and reasonable benchmarking between the databases, the first 100 classes of CASIAv4 and ND0405 are selected for following experiments in this project. There are a few important evaluation metrics used in this work. Genuine Acceptance Rate (GAR) is the success rate after deducting False Rejection Rate (FRR): $100\% - FRR$. Basically, FAR is the percentage where the imposter will be accepted by the system whereas FRR is the percentage where the genuine users are being rejected by the system. These two metrics can be related to EER with their total sum divided by two: $(FAR + FRR)/2$. Ideally, we would like to avoid the occurrence of false acceptance and

false rejection at the same time, therefore, the EER shall be as low as possible to satisfy these conditions. On the other hands, the decidability is the normalised distance between the mean of the genuine and imposter score distributions. Higher decidability is much more desirable as it would indicate that the difference between the genuine and imposter template are huge, thus it would be much easier to be separated by a threshold as the overlapping region would be small.

The experiment below aims to examine the ability of the proposed scheme in improving the performance of iris template protection scheme when tested against iris databases with and without noise masks. The state-of-the-art BTP schemes, Bloom filter (Rathgeb et al., 2013) and enhanced IFO hashing (Lai et al., 2017a) are selected for performance evaluation as these schemes have been experimented thoroughly and widely applied in this field. Both schemes are well known with their good recognition performance and resistance against multiple attacks. Note that, enhanced IFO has incorporated Bloom filter to solve its alignment issue. In this experiment, these schemes have been tested by the selected databases with their respective recognition performance. The results are tabulated in terms of equal error rate (EER) when the false acceptance rate (FAR) is equal to the false rejection rate (FRR).

Table 4.2: Recognition Performance of the Proposed Scheme and State-of-the-arts BTP Schemes

Database	Equal Error Rate, %			
	Bloom filter	Enhanced IFO hashing	Proposed binary confidence matrix	Proposed probability confidence matrix
CASIAv1	5.91	5.81	4.80	2.01
CASIAv3	1.14	0.69	0.20	0.20
CASIAv4	8.11	6.17	1.64	1.08
ND0405	10.74	7.28	2.28	2.48

Table 4.2 above shows the best Equal Error Rate (EER) performance of the proposed confidence matrices using not more than 3 training samples for iris databases hashed by enhanced IFO. During the process of obtaining the best results of Bloom filter from different word size, minimum word size of 3 is set. Smaller word size is ignore as the security strength will reduce. Different range of parameters of enhanced IFO are tested by referring to the optimal setting published in (Lai et al., 2017a, Lai et al., 2016). In this experiment, a clear decrease in EER (%) is observed from 4 different sets of databases. For iris databases that come with noise mask (CASIAv1, CASIAv4, ND0405), performance improvement ranging from 17% to 73% is observed when using for binary confidence matrix. On the other hand, performance improvement ranging from 65.40% to 82.33% is achieved using probability confidence matrix. For CASIAv3, the database without noise-mask had achieved a reasonable

performance improvement of 70% for both binary and probability confidence matrices.

As a result, both proposed confidence matrix generation methods have successfully improved the recognition performance of the biometric template protection scheme. On top of that, the results also proved the reliability of this method when dealing with noise-masks associated databases. In upcoming experiment, the construction of confidence matrices by using different number of training samples and their performance are evaluated in Table 4.3. Probability confidence matrix is able to generate lowest EER with 3 training samples. For instance, EER as low as 1.08% is reported for CASIAv4 database. In terms of performance, the observed deviation of error rate using 2 to 4 samples is less than 2% and 3% for binary and probability confidence matrix respectively.

From Table 4.3, probability confidence matrix has outperformed binary confidence matrix in our experiments conducted on CASIAv1 and CASIAv3. The deviation in performance can range from 0.5 to 3%. Both methods have reported equally low EER for CASIAv4. Binary confidence matrix which extracts only the exact collisions has slightly better performance compared to probability confidence matrix for ND0405 which is noisier. This is expected as the former method tends to eliminate more noise where there is no collision within all the training samples used.

Table 4.3: Recognition Performance of the Proposed Scheme with Different Number of Training Samples

Iris Database	Training Sample	Equal Error Rate (%)	
		Binary Confidence Matrix	Probability Confidence Matrix
CASIAv1	2	4.80	4.40
	3	5.01	2.01
	4	4.67	2.17
	5	3.11	2.12
CASIAv4	2	3.02	3.90
	3	1.64	1.08
	4	1.41	2.82
	5	0.97	2.99
ND0405	2	3.43	4.27
	3	2.28	2.48
	4	2.34	3.12
	5	2.11	3.17
CASIAv3	2	0.51	0.49
	3	0.20	0.20
	4	0.27	0.05
	5	0.76	0.03

Figure 4.1 has shown the examples of normalized genuine-imposter matching scores for CASIAv1 (top row), CASIAv4 and CASIAv3 (bottom row) iris databases. The score distributions generated by confidence mask are shown at the right column whereas the plots without the implementation of confidence matrix are shown at the left column. It is observable that confidence matrix

enables better spread between genuine and imposter distributions visually. The mean matching scores of genuine and imposter are separated in a wider manner. This phenomena has greatly reduced the area of overlapped region between genuine and imposter while shifting the intersected matching score more to the right. Empirically, the decidability indices (Daugman, 2000) between IFO and the confidence based proposed method are recorded in Table 4.4. According to John Daugman (Daugman, 2000), "decidability" of a decision is determined by the degree of overlap between two distributions. A standard measure of decidability for genuine-imposter score distribution can be defined as follows if the means of the two distributions are μ_1 and μ_2 and their standard deviations are σ_1 and σ_2:

$$d = \frac{|\mu_1 - \mu_2|}{\sqrt{\frac{1}{2}(\sigma_1^2 + \sigma_2^2)}} \tag{14}$$

Better decidability indices for genuine-imposter distributions are proven achievable through the implementation of our proposed scheme as shown in Table 4.4. As an additional reference, Receiver Operating Characteristic curves (ROCs) are also plotted with True Positive Rate (TPR) against the False Positive Rate (FPR) to measure the separability of classes. The ROCs of binary confidence matrix in Figure 4.2 (a) and probability confidence matrix in Figure 4.2 (b) are plotted against enhanced IFO for iris databases CASIAV1, CASIAV4 and ND0405 (arranged in rows). Improvement in recognition performance have been observed in all ROC graphs. In overall, all the statistical and empirical studies conducted on the proposed method have indicated an increase in recognition performance and decidability.

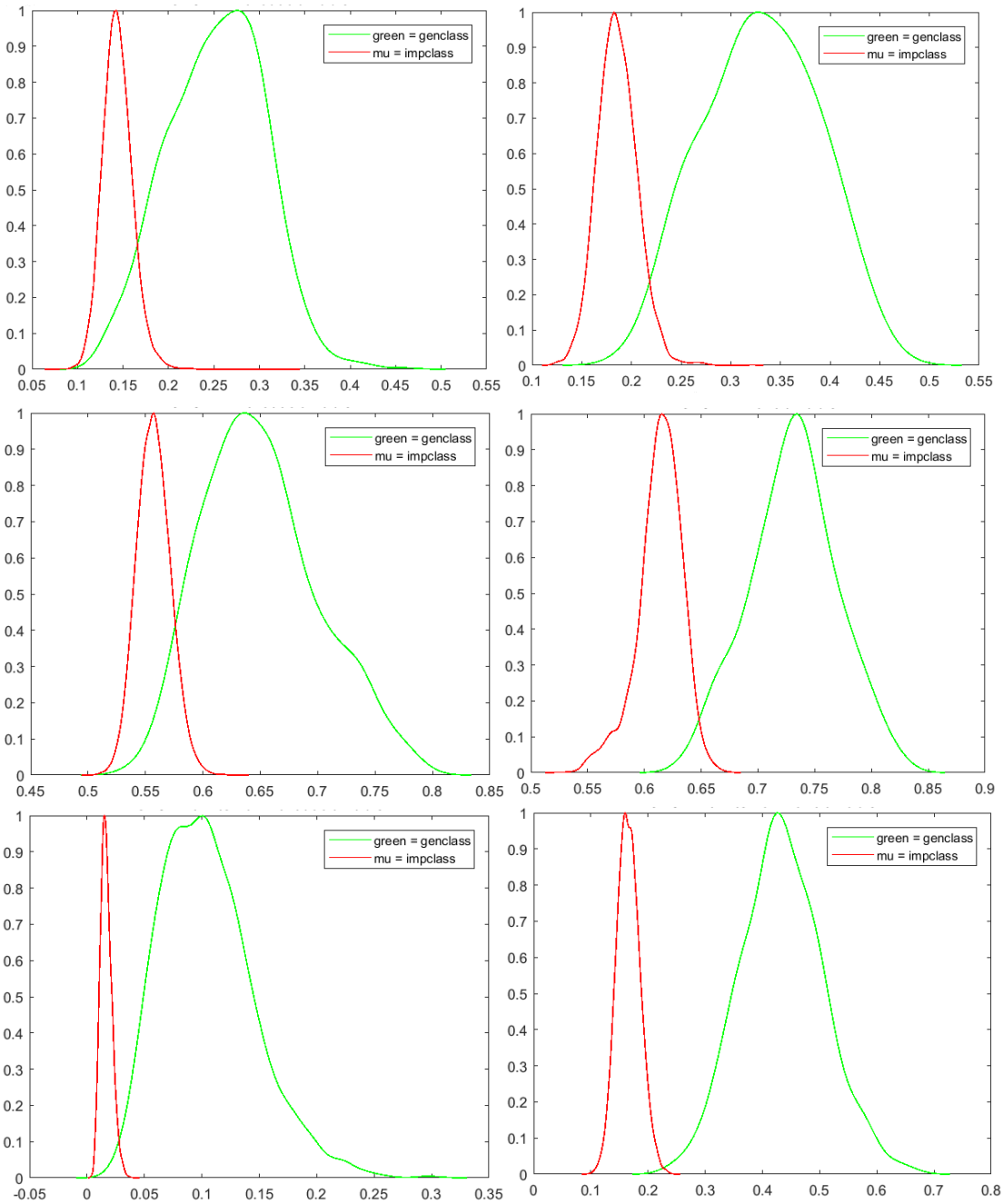


Figure 4.1: Genuine-Imposter Score Distributions for a) CASIAv1 b) CASIAv4 c) CASIAv3

Table 4.4 Decidability Measure for IFO and Confidence matrix

Methods	Iris Databases			
	CASIAv1	**CASIAv4**	**ND0405**	**CASIAV3**
Enhanced IFO	2.772	2.521	2.641	4.94
Confidence Matrix (binary/probability)	3.624 / 3.404	4.567 / 3.859	4.12 / 3.7064	5.92 / 4.91

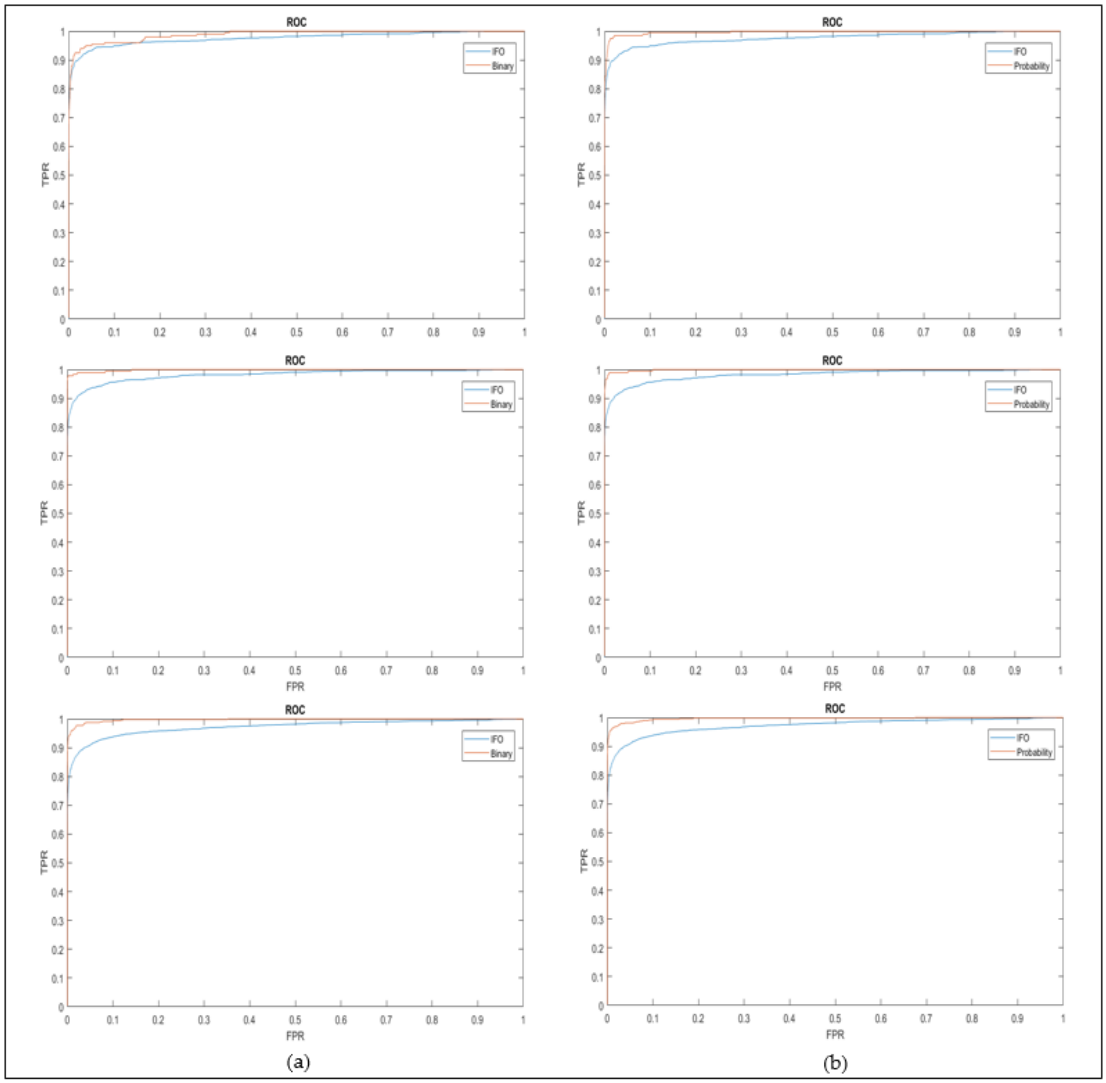


Figure 4.2: Example of ROC plots for the Implementation of a) Binary and b) Probability Confidence against Enhanced IFO

4.1.1 Security Model

Security model will be focused on the case when attacker is trying to attack the reference template to get the confidence information. If confidence information leaks, it leads to permanent identity loss as biometric is individually associated. In view of this, frequency analysis based attacks like Attack via Record Multiplicity (ARM) is the common threat for this method.

For binary confidence matrix, reference template contains the locations of confidence bits. Compromising the reference template indeed enables the construction of binary mask. Thus, we would like to calculate the complexity in getting all ones in the mask. Randomly taking a hashed reference template of size $\mathbf{5940 \times 50}$ from the databases, which is equivalent to $\mathbf{297,000}$ elements with 143038 confident bits. The complexity of this attack to be successful can be estimated as ${}^{297000}C_{143038} \gg \mathbf{6.39 \times 10^{89315}}$ combinations.

For probability confidence matrix, non-binary values in each reference template are non-zero. The confidence values are calculated as probability instead of binary. It is difficult for attacker to know the exact confidence location where the perfect matched collision happens (i.e. confidence score of 3/3 if the same number occurs at the same position across 3 hashed samples). Given a more relaxing security situation by assuming that the system can be compromised with a success probability of 0.33 instead of 1, the complexity of this probability can be assessed. In another words, his scenario is equivalent to the probability of guessing the positions in the reference template with probability of 1/3 (1 occurrence out of 3) correctly. The probability of the

attacker in getting $\boldsymbol{k}$ positions among $\boldsymbol{n}$ tries given unlimited computation power can be estimated through:

$$\boldsymbol{p_X(k) = \Pr(X = k) = \frac{\binom{K}{k}\binom{N-K}{n-k}}{\binom{N}{n}}} \quad (15)$$

Where $\boldsymbol{N}$ is the population size, $\boldsymbol{K}$ is the number of success states in the population, $\boldsymbol{n}$ is the number of draws, $\boldsymbol{k}$ is the number of observed successes and $\binom{a}{b}$ is a binomial coefficient.

The success probability of attacker $\boldsymbol{p_X(k)}$ in this case is equivalent to the matching score of our probability confidence matrix since $\frac{(\#\mathbf{1/3})}{\boldsymbol{sum\ of\ probabilities\ from\ all\ positions}}$. In another words, the attacker can only achieve the matching score if he can get $\boldsymbol{k}$ positions with probability 1/3. Same scenario is applicable to obtain positions for other probabilities such 2/3 or 3/3. If an attacker is able to get most of the positions of a probability, other probabilities can be revealed. Using the same random protected template, the number of positions with probability 1/3 are found to be $\boldsymbol{K = 25543}$ from a template size of $\boldsymbol{N = 297000}$. Referring to Rathgeb et al. (Rathgeb and Uhl, 2010b), it is acceptable that $\mathbf{2^{200}}$ can be considered as computationally infeasible for an attack on arbitrary secure iris template. Thus, this is approximately $^{297000}C_{13}$ for our case where the number of trials allowed are only as low as $\boldsymbol{n = 13}$. Using the determined parameter, the success probability for an attack can then be estimated at:

$$\boldsymbol{p_X(k) = \Pr(X = k) = \frac{\binom{25543}{k}\binom{297000-25543}{13-k}}{\binom{297000}{13}} = \frac{\binom{25543}{k}\binom{271457}{13-k}}{\binom{297000}{13}}} \quad (16)$$

The success probability in Eq. 16 is positive when $\mathbf{0} \leq \boldsymbol{k} \leq \mathbf{13}$. Theoretically, $\boldsymbol{k} \approx \frac{\boldsymbol{n}}{\mathbf{2}}$ can be the approximation for the lower bound of the observed success while the highest observed success can be 12 out of 13 draws. As a result, the success probability of an attack is estimated to be within the range of $\mathbf{1.92} \times \mathbf{10^{-12}} \leq \mathbf{Pr}(\boldsymbol{X} = \boldsymbol{k}) \leq \mathbf{3.48} \times \mathbf{10^{-5}}$. An attacker needs to go through a computation complexity of $\mathbf{2^{200}}$ steps before he can achieve a low success probability of $\mathbf{1.92} \times \mathbf{10^{-12}}$. In view of this, the attack becomes highly complicated. This is because more $\boldsymbol{n}$ positions are needed to increase the matching score in real case scenario and this will extensively increase the computation complexity of ${}^{N}C_{n}$ before obtaining the low success probability. In addition, note that the increase of template size, $\boldsymbol{N}$ will increase the complexity exponentially. Using the example above, the matching score of the confidence matrix can be further expressed as:

$$\boldsymbol{Matching\ score} = \frac{\boldsymbol{k_1}\left(\frac{\mathbf{1}}{\boldsymbol{t}}\right)+\boldsymbol{k_2}\left(\frac{\mathbf{2}}{\boldsymbol{t}}\right)+\boldsymbol{k_3}\left(\frac{\mathbf{3}}{\boldsymbol{t}}\right)}{\boldsymbol{n_1}\left(\frac{\mathbf{1}}{\boldsymbol{t}}\right)+\boldsymbol{n_2}\left(\frac{\mathbf{2}}{\boldsymbol{t}}\right)+\boldsymbol{n_3}\left(\frac{\mathbf{3}}{\boldsymbol{t}}\right)} = \left(\frac{\boldsymbol{k_i}}{\sum_{\boldsymbol{i}=\mathbf{1}}^{\boldsymbol{t}} \boldsymbol{n_i}}\right) \tag{17}$$

Where $\boldsymbol{i} = \mathbf{1}, \mathbf{2}, \ldots,\ \boldsymbol{t}$ is the $\boldsymbol{i} - \boldsymbol{th}$ number of training samples used for the construction of confidence matrix ($\boldsymbol{t} = \mathbf{3}$ is used for the example above). Theoretically, the higher the expected number of collisions $\boldsymbol{k_i}$, the higher is the matching score. However, the increase of $\boldsymbol{k_1}$ will inevitably reduce the success probability of an attacker as shown in Eq. 16. Hence, we can fairly say that it is computationally infeasible by looking at the large amount of steps incurred even before achieving the success probability which can be negligible. This is because the computation will also become infeasible if a larger template size is used due

to the asymptotic behaviour caused by the increase of $\boldsymbol{N}$ or $\boldsymbol{k}$. Thus, the requirement of irreversibility for our proposed scheme has been fulfilled.

The ARM analysis has revealed that it is computationally infeasible to guess the positions in the reference template even for the probability of 1/3 under a more relaxing security situation. Non-invertibility of confidence matrix has been achieved. Besides, a detail non-invertibility analysis based on various attacks such as single hash attack (SHA) and ARM has been conducted on IFO hash code (Lai et al., 2017b). Therefore, it is computationally infeasible to derive the original iris code from IFO hashed code. The confirmation on irreversibility property of IFO hashing assures the achievement of revocability since multiple IFO hashed codes can be generated from a single iris code. In addition, new confidence matrix can also be generated from the new IFO hashed codes once it is compromised. A quantitative experiment was conducted to evaluate the revocability of IFO hashed codes (Lai et al., 2017b). The large degree of overlapping between imposter and pseudo-imposter distribution indicated that the refreshed IFO hashed codes were distinctive although they were generated from the same iris code. This verifies that IFO hashing is able to fulfil the revocability requirement. Old hashed code can be replaced by new hashed code with different permutation tokens. Thus, the revocability property of confidence matrix has been achieved.

Unlinkability emphasizes that multiple protected templates generated from the same iris code should be indistinguishable from each other. To evaluate the unlinkability of our proposed scheme, the method proposed by Gomez et al. (Gomez-Barrero et al., 2017) is adopted. The unlinkability can be evaluated by

the mated and non-mated score distributions using this method. The mated scores are generated by matching between protected templates of the same subject using different sets of hashing functions, h while non-mated scores refer to the matching of protected templates belonged to different subjects using different sets of h. The unlinkability property of a biometric system is fulfilled if there is an overlap between the score distributions of mated and non-mated distributions (Gomez-Barrero et al., 2017).

Let $P(s|M_s)$ be the conditional probability of a similarity score $s \in [0,1]$ that belongs to the mated matching group M_s and $P(s|M_s')$ denotes the conditional probability of a similarity score s that belongs to the non-mated group M_s'. Two protected templates are said to have linkage if it is more likely that both templates are mated samples (M_s) rather than non-mated samples (M_s') given a score s: $P(M_s|s) > P(M_s'|s)$. The unlinkability property can be characterized by the local linkability:

$$D(s) = 2\frac{\omega LR(s)}{1+\omega LR(s)} - 1 \tag{18}$$

Given that $\omega LR(s) = \frac{P(s|M_s)}{P(s|M_s')} > 1$ where $LR(s)$ is the likelihood ratio between the known probabilities $P(s|M_s)/P(s|M_s')$ and $\omega = P(M_s)/P(M_s')$ denotes the ratio between the unknown probabilities of the *mated samples* and *non-mated samples* distributions. We can assume that $P(M_s) = P(M_s')$, thus set $\omega = 1$. The system's overall linkability can be further defined as:

$$D_{sys} = \int D(s).P(s|M_s)ds \tag{19}$$

This measure is within the range of $D_{sys} \in [0,1]$ with zero represents full unlinkability and unity for system which is completely linkable. Therefore, to attain the unlinkability of a BTP scheme, it is desirable to show that D_{sys} is negligibly small.

Figure 4.3 depicted three different graphs of CASIAv1, CASIAv4 and ND0405 generated using our proposed binary (first row) and probability (second row) confidence matrices using the same parameter settings with 3 training samples. All the mated and non-mated score distributions showed significant overlapping and negligibly small value of $D_{sys\,(binary)} = 0.09,0.07,0.05$; $D_{sys\,(probability)} = 0.04,0.06,0.05$ respectively. Therefore, we assert that the proposed scheme fulfils the criteria on unlinkability.

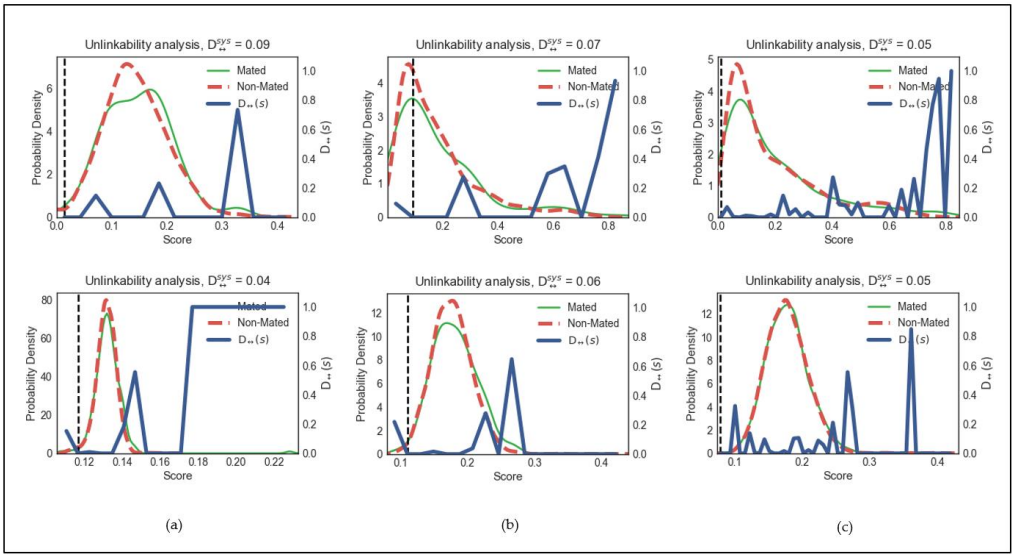


Figure 4.3: Unlinkability Analysis of the Proposed Binary (first row) and Probability (second row) Confidence Matrices for Databases a) CASIAv1 b) CASIAv4 c) ND0405

4.1.2 Discussion

From the result obtained in the previous section, improvement in performance has been proven on all the four different publicly available iris databases using our proposed methods. The proposed scheme is able to mitigate the performance degradation caused by BTP scheme in existing biometrics recognition system. However, there are still several key points which are worth to be discussed. First, a solution has to be formulated to overcome the implementation problem since most of the publicly available databases come with noise masks. The conventional Bloom filter and Indexing-first-one hashing scheme did not attempt to solve this problem which can potentially be a roadblock in mitigating performance degradation.

Noise mask serves as an aid to determine the noisy pixels within the biometric template. These pixels will be excluded at the matching stage of protected biometric templates. The enhanced IFO hashing scheme, which does not require alignment, will first divide the iris data into different blocks of Bloom filters. Our proposed solution is to first determine the acceptable noise level of protected iris recognition system through a noise threshold. When a Bloom filter block has exceeded the acceptable noise level, the corresponding row of hashed data will be considered as null and thus excluded during matching stage in the secure domain. This enables our proposed method to work with any iris database with associated noise masks. However, note that higher requirement on the noise level of your protected iris recognition system might cause larger amount of null rows. This can lead to unnecessary information loss and greatly reduce the amount of information available for confidence matrix generation. Therefore,

our proposed probability confidence matrix is useful in optimizing the matching accuracy though probabilities of collision in this situation.

On the other hand, experiments between the two proposed methods have been carried out in this research. Firstly, we studied the relationship between the number of training samples and the performance of our proposed methods. The generated results have indicated that, three training samples have the optimum performance in most of the tested databases. Our proposed binary confidence matrix has shown better performance when it is tested with noisier iris images while probability confidence matrix performs better when dealing with better quality iris images. In a nutshell, the proposed binary confidence matrix has higher tolerance to noise because of its nature in eliminating noise via the implementation of AND logic operation. Thus, this is more suitable to improve the performance of protected biometric templates which are captured under challenging and non-cooperative environment.

4.2 Performance of the Proposed Method 2 - Cancelable Iris Key Binding Scheme

A thorough analysis about the performance and security of our proposed key binding scheme has been conducted on a public iris database CASIA v3-interval (2002a). This dataset contains 2639 iris images from 396 different classes (eyes). In our experiments, left eye images are chosen since the patterns of genetically identical eyes appear to be uncorrelated as they are among imposters' eyes statistically (Daugman, 2004a). To standardize the matching from all the left eye images, we have selected any subset that contained at least

7 iris samples per class. This results to a total of 124 classes with 868 iris images (Lai et al., 2017b). Each iris image has gone through iris code generation (Daugman, 2004a) to generate iris code $I \in \{0,1\}^{n_1 \times n_2}$ of dimension $n_1 = 20, n_2 = 512$ with a total of 10240 bits.

The experiments have been designed with the purpose to emphasize more on the implementation and security analysis. The proposed key binding scheme here has not been addressed or analyzed thoroughly to provide insights regarding its potential, limitation and tradeoff in iris biometric. Firstly, the performance tradeoff upon introducing an alignment-free cancelable iris code is being presented. Besides, IFO hashing has shown its ability in preserving the system's performance in the following section. Next, an overview on the performance of the proposed key binding scheme is presented through standard metrics evaluation. The inter-relation of the main parameters: similarity threshold (t), cryptographic key length (n) and IFO hashed code length (m) have been tested and examined in this studies. In addition, the proposed scheme has demonstrated flexibility in managing various hashed code sizes due to the integration of IFO into the key binding's design without sacrificing security strength with reducing key length. All the experiments are conducted under a PC with processor core i7- 2.60 GHz, 8GB RAM and with MATLAB R2013b.

4.2.1 Performance of Original Iris Code and Bloom Filtered Iris Code

The first experimental testing is conducted on the original iris code $I \in \{0,1\}^{20 \times 512}$ and Bloom filtered iris code respectively. The parameters used for Bloom filter generation (Rathgeb et al., 2013) are fixed as $W = 7$ and $L = 20$, yielding $l_1 \cdot l_2 = 50$ blocks and Bloom filtered iris code $B_g \in \{0,1\}^{50 \times 128}$ as the

outputs. This testing has covered different matching protocols such as genuine matching and imposter matching. For genuine matching, all iris images are used to generate iris codes. The matching is done by calculating the hamming distance between different iris codes of the same user which then yields $\frac{7\times6\times124}{2} = 2604$ genuine matching scores in total. Same genuine matching protocol has been implemented all the respective Bloom filtered iris codes. For imposter matching, the matching is done by calculating the hamming distance between iris codes of different users, interclass matching in this case. Each user comes with 7 iris codes, this yields a total of $\frac{7\times123\times7\times124}{2} = 373674$ imposter matching scores. Same imposter matching protocol has been implemented as well for Bloom filtered iris codes. Besides, we have also tested the performance of Bloom filtered iris codes after applying IFO hashing in (Lai et al., 2017b) ($m = 200, p = 3, \kappa = 64, \tau = 30$) by using the same genuine and imposter protocols.

In biometric systems, Equal Error Rate (EER) has been widely used for performance evaluation by calculating the False Acceptant Rate (FAR) and False Rejection Rate (FRR) between the collected genuine and imposter scores, where lower EER implies higher performance. In our context, EER is approximated as $\text{EER} \approx (\text{FAR} + \text{FRR})/2$. The result is tabulated in Table 4.5 as shown below.

The result from Table 4.5 indicates that the system performance does not experience significant deterioration after applying Bloom filter to resolve the alignment issues originated from iris code's generation process (rotational inconsistency due to head tilt during eye image acquisition). Moreover, IFO hashing which has inherited properties such as distance and similarity

preservation from Jaccard similarity and min hashing shows compatible performance after the its application to form Bloom filtered iris code.

Table 4.5: System Performance for The Original, Alignment-free and Hashed Iris Codes

CASIAv3 Database (Lai et al., 2017b)	Equal Error Rate (EER %)
Iris code	0.38
Bloom filtered Iris code	0.50
Bloom filtered Iris code (IFO applied)	0.58

4.2.2 Performance of the Proposed Key Binding Method

This section provides the evaluation and overview on the performance of our proposed key binding method. For performance evaluation, intensive experiments have been carried out under different parameters configurations. The metrics used for performance evaluation are FAR and FRR as discussed in earlier session. Lower FAR and FRR implies higher system performance.

In order to measure the system's performance, similar protocols have been applied in the following experiments. The first one refers to the genuine matching protocol where the first Bloom filtered iris code is used for key binding (enrollment) purpose and the remaining Bloom filtered iris codes from the same class will be used for key retrieval (query). Hence, this protocol yields a total of 2604 testing results. The genuine matching protocol is then used to calculate the system's FRR $= \frac{\text{No. of wrongly retrieved key}}{2604}$ x100%. The second protocol refers to the imposter matching protocol where the first Bloom filtered iris code of each class is used for key binding (enrollment). The key retrieval (query) is then

conducted over the second Bloom filtered iris codes of all the classes excluding the samples from the enrolled class, hence, yields a total of $(124 \times 123)/2 = 7626$ testing results. The imposter matching protocol is then used to calculate the FAR $= \frac{\text{No.correctly retrieved key}}{7626}$ x100%.

4.2.3 Evaluation on Similarity Score Threshold, t

As mentioned earlier, there are three main parameters (t, n, m) in our proposed cancelable iris key binding scheme . Several tests have been carried out to study the relation of these important parameters to the system performance. By using the same parameter setting for IFO in previous section, the evaluation for similarity score threshold, t have been carried out by fixing parameters $m = 100$ and $n = 10$. The genuine matching and imposter matching protocols are performed under a range of values, $t = [0.16, 0.17, \dots, 0.25]$. The results of FAR and FRR for every t, given the parameter set $(t, 10{,}100)$ are recorded. Meanwhile, we have also calculated their corresponding EERs as tabulated in Table 4.6.

From the result showed in Table 4.6, the best EER (0.62%) obtained is close to the original Bloom Filtered iris code's performance (0.58%) in Table 4.5 under a slightly different setting. This is mainly attributed to the Jaccard similarity's preserving property which allows us to measure the similarity between different Bloom filtered iris codes under IFO's hashed domain. The best performance at optimum security where FAR is zero percent is 1.33% of EER. This can be achieved by setting the similarity score threshold, t at 0.20. Although FAR remains zero if the threshold is being increased but EER has increased accordingly.

Table 4.6: System Performance for Parameter Set $(t, 10, 100)$

t	FRR (%)	FAR (%)	EER (%)
0.16	0.15	12.14	6.97
0.17	0.31	3.23	1.77
0.18	0.62	0.62	0.62
0.19	1.65	0.05	0.85
0.20	2.65	0.00	1.33
0.21	3.80	0.00	1.90
0.22	5.61	0.00	2.81
0.23	8.26	0.00	4.13
0.24	11.56	0.00	5.78
0.25	15.40	0.00	7.70

Besides, the matching scores between each IFO hashed code $j = 1,2, \dots, n$ under genuine matching and imposter matching have been plotted and depicted in Figure 4.4. It shows an overlapped region between genuine and imposter matching scores. This scenario is mainly due to the imposed synthetic Bloom filtered iris codes. The matching between a hashed synthetic Bloom filtered iris code and the query hashed code always results in a smaller matching score. This observation has further supported the claim where synthetic template is indeed acting like an imposter template in chaffing and winnowing process to conceal and protect the genuine IFO hashed code in our proposed method. Moreover, the best threshold value, $t = 0.2$ has been highlighted in the zoomed region in Figure 4.4 to avoid any imposter from potentially getting access into the system with FAR equals to zero. In fact, this has been justified by our results in Table 4.6 where the system has reported EER of 1.33% when FAR is 0 at $t =$

0.2. The table summarizes an observable trend that an increase in t will result in higher FRR but lower FAR and vice versa.

For a cryptosystem to be useful, it is normally suggested that the FAR should be 0, hence any imposter or adversary can certainly be rejected by our proposed system for higher level of system security. Therefore, our analysis suggests that the optimal value of t for this iris database lies under the range such that $t \geq 0.2$.

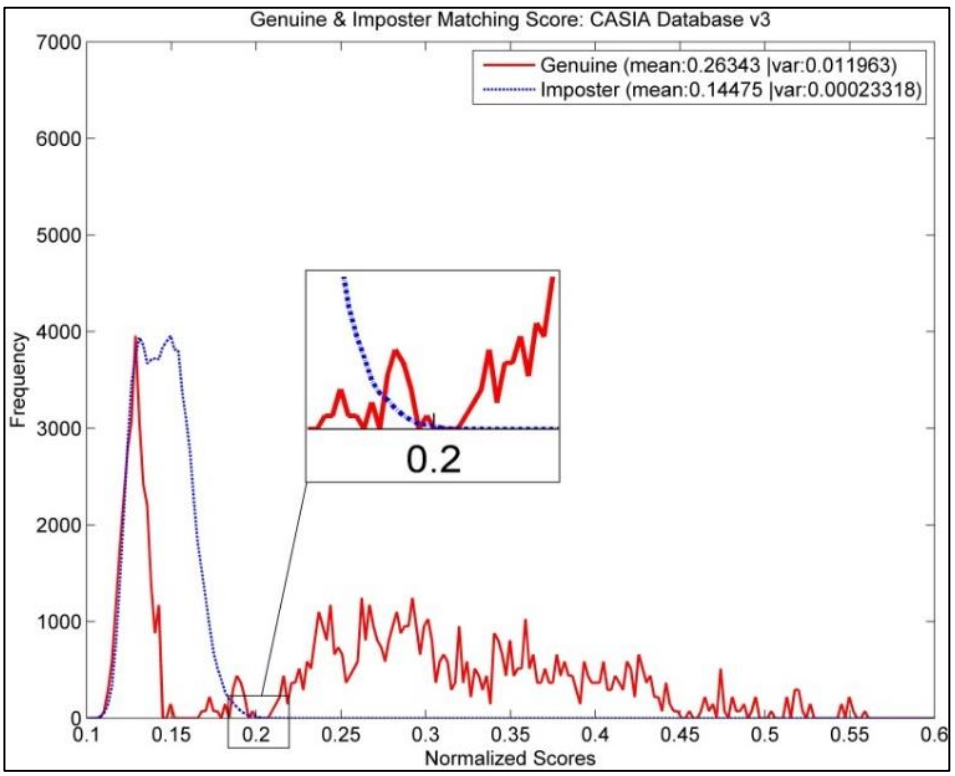


Figure 4.4: Graph for the Genuine and Imposter Matching Score

4.2.4 Evaluation on Cryptographic Key Length, n

The evaluation on the effect of cryptographic key length, n on system performance have been carried out by fixing the values for parameters t and m. The genuine and imposter matching protocols are performed by setting different

key lengths where $n = [10, 20, 40, 60, 80, 100, 150, 200]$. As a result, FAR and FRR for every n given $t = 0.2$ and $m = 100$ are recorded. Meanwhile, their corresponding Genuine Acceptance Rate, $GAR = 100 - FRR$ and EER are also calculated and tabulated in Table 4.7.

Table 4.7: System Performance for Parameter Set (0.2, *n*,100)

n	GAR (%)	FAR (%)	EER (%)
10	97.35	0.00	1.33
20	96.67	0.00	1.67
40	96.67	0.00	1.67
60	96.37	0.00	1.82
80	96.37	0.00	1.82
100	96.37	0.00	1.82
150	96.37	0.00	1.82
200	96.37	0.00	1.82

From Figure 4.5, EER as low as 1.33% can be observed when shorter key length ($n = 10$) is being used. The EER has gradually increased when the key length becomes longer and remains stagnant at 1.82% even though the key length has been increased further from 60 to 200. In contrary, GAR has shown a slight reduction of 0.98% when the key length is being increased from 10 to 200. Besides that, the result in Table 4.7 shows that the increase in key length n will reduce the FAR as emphasized and explained in our proposed KRR. Given $t = 0.2$, the system performance is preserved even though the key length n is being increased up to 200. This implies that the binding of long cryptographic key with

bit length as long as 200 bits is feasible while maintaining the same KRR and system performance as captured by GAR.

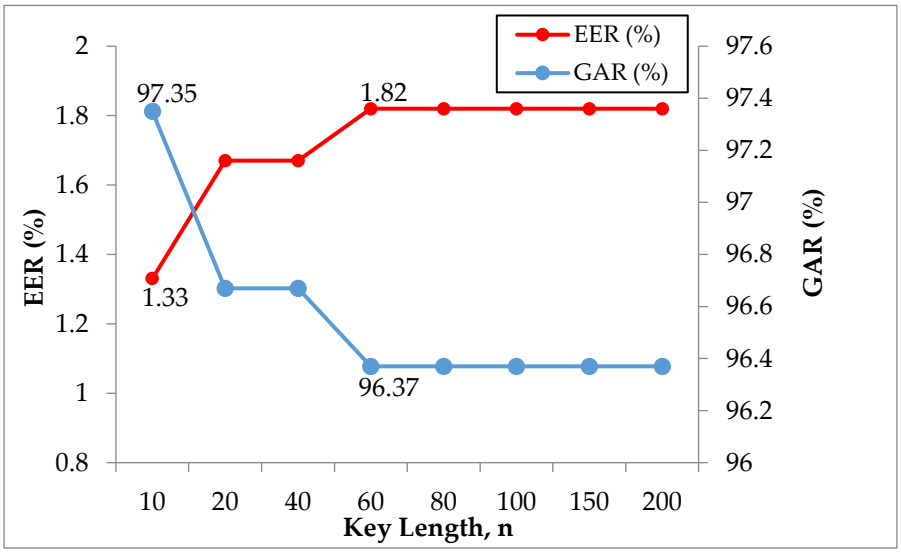


Figure 4.5: Graph for the Evaluation on Cryptographic Key Length

4.2.5 Evaluation on Hashed Code Length, *m*

The evaluation on the effect of IFO hashed code length, m on system performance have been conducted by fixing the parameters t and n which can be obtained from the experiments earlier. The genuine and imposter matching protocols are performed through different $m = [10, 50, 100, 150, 200, 250, 300]$ for this study. The tested results of FAR and FRR for every value of m given $t = 0.2$ and $n = 10$ in the parameter set $(0.2, 10, m)$ are recorded. Meanwhile, their corresponding GAR, EER and storage per bit kB$/n$ are computed and tabulated in Table 4.8. The unit of storage per bit is also measured in kilo bytes (kB) to serve as reference for the space required (for single bit of key binding, $n = 1$) for different hashed code length, m used in IFO hashed code generation.

The IFO hashed code length plays a critical role in terms of system storage as the proposed method binds the key by using IFO hashed code. In order to serve as an efficient biometric cryptosystem, the storage requirement especially for storing the helper data must be kept within an acceptable limit apart from high system security and performance. A system can become infeasible in actual implementation if it requires infinite storage for helper data to facilitate the key retrieval process despite high performance and security.

Table 4.8: System Performance for Parameter Set (0.2,10,m)

m	GAR (%)	FAR (%)	EER (%)	Storage/bit (kB/n)
10	89.51	0	5.25	0.19
50	95.97	0	2.02	0.94
100	96.37	0	1.82	1.90
150	96.37	0	1.82	2.81
200	96.37	0	1.82	3.75
250	96.37	0	1.82	4.69
300	96.37	0	1.82	5.63

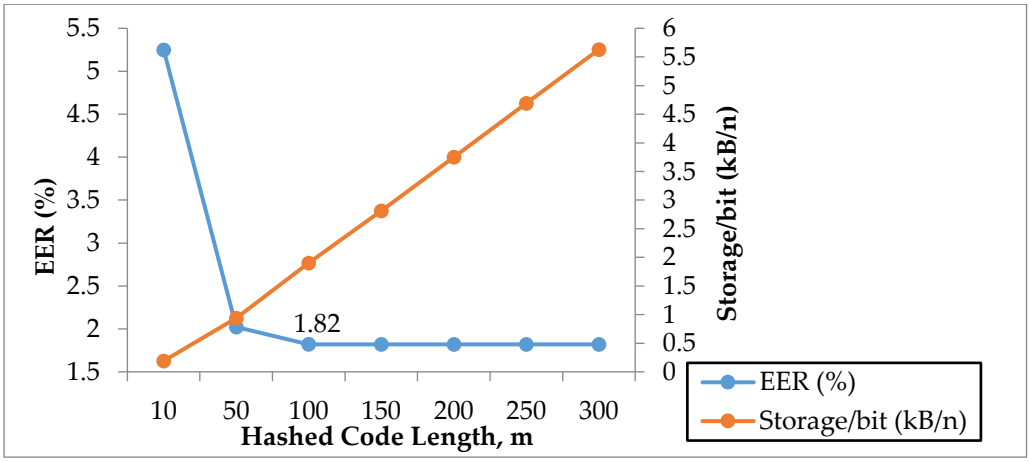


Figure 4.6: Graph for the Evaluation on Hashed Code Length

On the other hand, the proposed key binding method offers flexibility in terms of variable hashed code length. In our scheme, the IFO hashing provides flexible and controllable code length (regulated by parameter m). This feature allows us to tune our storage space while maintaining acceptable system performance. As shown in Table 4.8, the proposed method achieves high GAR around 95-96% with storage consumption from 0.94 to 1.90kB. The form of storage consumption offered by this proposed scheme is more compact than the records generated by other schemes such as (Li et al., 2010). It is also demonstrated that the system's storage requirement can be decreased further with shorter hashed code length (for e.g. decreasing from $m = 300$ to 100) while maintaining the same system performance as shown in Figure 4.6. Therefore, the system storage factor in this scheme is indeed controllable with respect to m. Figure 4.6 shows that EER is being reduced sharply from 5.25% ($m = 10$) to 1.82% ($m = 100$) and remains stable even with the further increment of hashed code length until $m = 300$. Thus, the proposed key binding method has achieved its optimum performance (GAR of 96.37%) at $m = 100$ which requires a storage space of 1.90kB for each hashed instance through thorough evaluation of the three main parameters in our scheme which are similarity score threshold (t), key length (n) and hashed code length (m).

4.2.6 Security analysis: Cancelable Iris Key Binding Scheme

As this proposed method utilizes synthetic templates to conceal the genuine templates (with IFO hashing applied), it is important to examine the indistinguishability property in such a way that any attacker cannot gain advantages in distinguishing whether the stored IFO hashed code is generated

from genuine or synthetic Bloom filtered iris code. The security of this proposed method focuses in the aspect of indistinguishability between genuine and synthetic templates. Besides, analysis has also been extended to potential security attacks on the proposed system such as brute force attack and false accept attack.

4.2.7 Indistinguishability Between Genuine and Synthetic Templates

The indistinguishability property is examined in such a way that an attacker is allowed to accumulate certain information during matching process and gain advantages that may be useful to retrieve the secret key. In this case, the indistinguishability between genuine and synthetic templates is measured in an indistinguishability game between a challenger and an adversary to achieve the objective. The proposed indistinguishability game has been designed as follows:

1. To start the game, given a group of IFO hash function H, challenger allows adversary to choose any class/individual from the database.
2. After a class is being chosen by the adversary, the challenger will select a random Bloom filtered iris code of that individual and generate $\boldsymbol{B}_g \leftarrow \text{Bloom\_filter}(W = 7, L = 20, \boldsymbol{I})$.
3. The challenger can then produce IFO hashed code $\boldsymbol{C}_g \leftarrow H(\boldsymbol{B}_g)$ and give $\boldsymbol{C}_g$ to the adversary.
4. After that, the challenger flips a fair coin $b \in \{0,1\}$. If $b = 1$, the challenger selects another Bloom filtered iris code of the selected person $\boldsymbol{B}_g{}'$ with a threshold $t' \in [0,1]$, such that $\text{JA}(\boldsymbol{B}_g, \boldsymbol{B}_g{}') \leq t'$ and generate

$\boldsymbol{C} \leftarrow H(\boldsymbol{B}_g{}')$. In addition, hashed code, $\boldsymbol{B}_g{}'$ can also be generated by adding random noise to the filtered iris code as long as JA($\boldsymbol{B}_g, \boldsymbol{B}_g{}'$) $\leq t'$. If $b = 0$, the challenger permutes the Bloom filtered iris code $\boldsymbol{B}_s \leftarrow$ Perm ($\boldsymbol{B}_g$) and generates $\boldsymbol{C} \leftarrow H(\boldsymbol{B}_s)$. Then challenger gives $\boldsymbol{C}$ to the adversary.

5. The adversary outputs a word $\hat{k} \in \{0,1\}$ and wins if $\hat{k} = k$.

Based on the game above, it is valid to say that if $\hat{k} = k$, then the adversary has successfully retrieved a single bit of the cryptography key. It is important to note that the adversary does not know whether $\boldsymbol{C}$ is generated from genuine, $\boldsymbol{B}_g$ or synthetic $\boldsymbol{B}_s$ Bloom filtered iris templates. Therefore, the adversary is required to find out the answer by matching the hashed codes and get $S(\boldsymbol{C}, \boldsymbol{C}_g)$. We hereby describe the adversary in this game as $\mathrm{Adv}_{\mathrm{Gen-Syn}}$ for advantages gained in retrieving a single bit of the cryptographic key successfully. When $\mathrm{Adv}_{\mathrm{Gen-Syn}} = 0$, we say that the scheme is perfectly indistinguishable between genuine and synthetic templates. The advantages gained by $\mathrm{Adv}_{\mathrm{Gen-Syn}}$ can be described as follows:

$$\mathrm{Adv}_{\mathrm{Gen-Syn}} = \left| \mathbb{P}[\hat{k} = k] - \frac{1}{2} \right| \tag{20}$$

Given that:

$$\mathbb{P}[\hat{\boldsymbol{k}} = \boldsymbol{k}] == \frac{\mathbf{1}}{\mathbf{2}} \mathbb{P}[\boldsymbol{S}(\boldsymbol{C}, \boldsymbol{C_g}) \geq \boldsymbol{t} | \boldsymbol{k} = \mathbf{0}] + \frac{\mathbf{1}}{\mathbf{2}} \mathbb{P}[\boldsymbol{S}(\boldsymbol{C}, \boldsymbol{C_g}) \geq \boldsymbol{t} | \boldsymbol{k} = \mathbf{1}]$$

Assuming that for the case where $S(\boldsymbol{C}, \boldsymbol{C}_g) \geq t$, the adversary can surely differentiate $\boldsymbol{C}$ is generated by $\boldsymbol{B}_g$, we can therefore define $\mathbb{P}\left[S(\boldsymbol{C}, \boldsymbol{C}_g) \geq t \middle| k = 1\right] = 1$ and yield the final formulation:

$$\begin{aligned} \mathrm{Adv}_{\mathrm{Gen-Syn}} &= \frac{1}{2}\left|\mathbb{P}\left[S(\boldsymbol{C}, \boldsymbol{C_g}) \geq t \middle| k = 0\right]\right| \\ &= \frac{1}{2}\left|\mathbb{P}[\mathrm{z} \geq tM | k = 0]\right| \end{aligned} \tag{21}$$

As aforementioned, $\mathbb{P}[\mathrm{z} \geq tM | k = 0]$ is highly depending on $P = S(\boldsymbol{B}_g, \boldsymbol{B}')$. From our matching result depicted in Figure 4.4, we are expected to gain zero FAR with threshold $t = 0.2$ while $S(\boldsymbol{C}, \boldsymbol{C}_g) < 0.2$ indicates imposter matching score (showed in red-blue overlapped imposter distribution region). Thus, we let $t = 0.2$ and calculate $\mathbb{P}[\mathrm{z} \geq tM | k = 0]$ to estimate the adversary advantages various $S(\boldsymbol{B}_g, \boldsymbol{B}')$ in this analysis. For further estimation, let $\mathrm{Adv}^n_{\mathrm{Gen-Syn}} = n\mathrm{Adv}_{\mathrm{Gen-Syn}}$ which describes the total adversary advantages gained from n bits cryptographic key. The total advantages are estimated by running the indistinguishability game n times independently (repeating Step 4 and 5 of the indistinguishability game). Table 4.9 shows the results with $S(\boldsymbol{B}_g, \boldsymbol{B}') = [0.16, 0.17, 0.18, 0.19]$ for $n = [1, 50, 100, 200]$ and $M = 10000$.

From this table, the adversary's advantages in distinguishing the genuine and synthetic iris templates can be quantitatively estimated through our proposed indistinguishability game. It is important to take into consideration the level of similarity between synthetic and genuine templates for chaffed key binding scheme to evaluate fairly the indistinguishability property in terms of security. For instance, the computed adversary's advantage is $\mathrm{Adv}_{\mathrm{Gen-Syn}} = 0.58$ with

$S(\boldsymbol{B}_g, \boldsymbol{B}') = 0.19$ when $n = 100$. The total advantages will go up to more than 1 when n is being increased to 200. This is because more iris templates are needed in order to bind longer key length, thus, greater information leakage. Particularly, with $\text{Adv}^{n}_{\text{Gen-Syn}} \geq 1$ one can expect weaker security due to excessive information leakage. Nevertheless, our result shows that with $S(\boldsymbol{B}_g, \boldsymbol{B}') = 0.16, 0.17$ and 0.18, the total adversary advantages to learn single bit of information at the key length of 200 bits are estimated to be $2^{-78}, 2^{-41}$ and 2^{-15} bits respectively (lower bounded at 2^{-11}). The security of this scheme is based upon the selected threshold value and the similarity score which determine the amount of information leakage (i.e. mutual information) due to the linkability between B_g and B'. To the best of our knowledge, there is still no known algorithm to extract this information for the purpose of full iris code reconstruction practically in relation to similarity score.

Table 4.9: Indistinguishability Between Genuine and Synthetic Iris Templates

$S(\boldsymbol{B}_g, \boldsymbol{B}')$	$\textbf{Adv}_{\textbf{Gen-Syn}}$ $(\boldsymbol{n = 1})$	$\textbf{Adv}^{\boldsymbol{n}}_{\textbf{Gen-Syn}}$ $(\boldsymbol{n = 50})$	$\textbf{Adv}^{\boldsymbol{n}}_{\textbf{Gen-Syn}}$ $(\boldsymbol{n = 100})$	$\textbf{Adv}^{\boldsymbol{n}}_{\textbf{Gen-Syn}}$ $(\boldsymbol{n = 200})$
0.16	2.0561×10^{-26}	1.0281×10^{-24}	2.0561×10^{-24}	4.1122×10^{-24}
0.17	3.0075×10^{-15}	1.5038×10^{-13}	3.0075×10^{-13}	6.015×10^{-13}
0.18	1.4936×10^{-7}	7.6480×10^{-6}	1.4936×10^{-5}	2.9872×10^{-5}
0.19	0.0058	0.29	0.58	1.16

4.2.8 Cancelability and Renewal

For renewal process, a new key needs to be reissued when the current cryptographic key is compromised. Our proposed key binding method requires no re-enrollment in this scenario. Key update can be achieved by interchanging the positions of the genuine and synthetic iris templates randomly together with their corresponding hashing groups. Thus, a new binary key string can be updated automatically. Our proposed design aims to provide a simple and fast key renewal process. The proposed algorithm has achieved GAR of more than 96% at zero FAR with hashed code length, m and key length, n up to 300 and 200 respectively.

In terms of cancelability, the regeneration of cancelable template has been guaranteed by the revocability and unlinkability of IFO hashing scheme. It has been verified through security analysis (Lai et al., 2017b) that it is computationally infeasible to derive the original biometric information from the IFO hashed code. The revocability has been evaluated thoroughly by analyzing the pseudo-imposter score distribution of the randomly generated hashed codes of multiple subjects. The refreshed hashed codes are distinctive and uncorrelated to the old hashed code albeit they are generated from the same iris code. With rigorous analysis backed by empirical data, IFO hashing scheme has satisfied the revocability and unlinkability requirements while users are not required to keep their permutation token in secret.

4.2.9 Potential Attacks

Besides the indistinguishability between genuine and synthetic template, we extended our analysis into potential security attacks. In this section, the proposed method is being evaluated against potential security attacks.

4.2.10 Brute Force Attack

For brute force attack, it relies on randomly guessing of the n bit cryptographic key without the needs of actual interception between the adversaries and the cancelable templates' storage. Therefore, the complexity of this attack is merely depending on the cryptographic key length which is controlled by the parameter n in our proposed method. Straightforwardly, the brute force attack complexity can be described as follows:

$$Bf_n = 2^n \tag{22}$$

Higher n indicates higher attack complexity which also requires more cancelable templates for key binding process. For instance, key length of $n = 100$, the brute force attack complexity is measured as $\mathrm{Bf}_n = 2^{100}$. Our best performance is preserved even up to a cryptographic key length of 200 as shown in Table 4.8. This is equal to an upper bound brute force attack's complexity of 2^{200} which is already sufficient in cryptography applications. The proposed method has demonstrated the flexibility to allow potentially key length longer than 200 while preserving acceptable performance when there is a need for higher attack complexity.

4.2.11 False Accept Attack

Apart from brute force attack, another security attack that needs to be taken into consideration is the false accept attack. In conjunction to brute force attack, this kind of attack requires the interception of the adversary with the cancelable storage. Instead of randomly guessing, the false accept attack relies on the continuous trials of an attacker through conventional matching between the stored cancelable templates and the imposter templates. In our context, unlimited number of trials are allowed. Therefore, the false accept attack is not constrained only to the usage of several imposter templates but also infinite number of artificial/synthetic templates instead.

Since the false accept attack relies on the conventional matching mechanism, the false accept attack complexity can be calculated based on our proposed key retrieval rate, KRR. To avoid confusion, we denote the key retrieval rate for false accept attack by arbitrary attacker as KRR_{imp}. Thus, false accept attack's complexity, $\mathbf{fa}_{KRR_{\text{imp}}}$ can be described directly as:

$$\mathbf{fa}_{KRR_{\text{imp}}} = \mathbb{P}\left[k_j' = k_j | j = 1,2,\dots,n\right] = \left(\mathbb{P}(z \geq tM)\right)^{n^*} \qquad (23)$$

We can estimate the $\mathbf{fa}_{KRR_{\text{imp}}}$ by assuming that the adversary is able to generate a cancelable template, $\boldsymbol{C}_j'$ with $S(\boldsymbol{B}_g, \boldsymbol{B}') < 0.2$. In this experiment, the $\mathbf{fa}_{KRR_{\text{imp}}}$ is estimated using synthetic templates which showed high similarity score when compared with genuine template. Thus, $S(\boldsymbol{B}_g, \boldsymbol{B}') = [0.195, 0.196, 0.197, 0.198, 0.199, 0.20]$ are being tested in Table 6 with following parameters: $n^* = \frac{n}{2}$ for maximum key entropy, $m = 200$ and $t = 0.20$.

Table 4.10: Estimation of Complexity for Brute Force and False Accept Attacks

$S(\boldsymbol{B}_g, \boldsymbol{B}')$	$\mathbf{Bf}_{n=100}$	$\mathbf{fa}_{KRR_{\text{imp}}}$
0.195	2^{100}	2^{162}
0.196	2^{100}	2^{133}
0.197	2^{100}	2^{107}
0.198	2^{100}	2^{85}
0.199	2^{100}	2^{66}

The calculated result shows that the false accept attack's complexity is lower compared to brute force attack given $S(\boldsymbol{B}_g, \boldsymbol{B}') > 0.198$. This indicates that if any attacker is able to generate hashed code with similarity $S(\boldsymbol{B}_g, \boldsymbol{B}') > 0.198$, he/she can potentially get access into the system due to lower attack complexity. Referring to Figure 4.4, the region where an imposter can launch a false accept attack is typically within the range of $0.1 - 0.2$ with the mean of the imposter matching distribution around 0.14. It is expected that any false accept attack at similarity score around $S(\boldsymbol{B}_g, \boldsymbol{B}') = 0.14$ or < 0.195 will likely be infeasible ($\mathbf{fa}_{KRR_{\text{imp}}} \gg 2^{162}$) due to much higher false accept attack's complexity.

In fact, the worst case scenario has been taken into consideration by calculating the $\mathbf{fa}_{KRR_{\text{imp}}}$ according to a list of high similarity scores $S(\boldsymbol{B}_g, \boldsymbol{B}')$ ranging from 0.195 to 0.199 according to the threshold set. The proposed method shows false accept complexity of 2^{66} bits. It is important to note that the overlapped region from 0.1 to 0.15 in Figure 4.4 is mainly contributed by the

synthetic iris templates which act like imposter iris templates as an extra layer of protection to chaff the genuine iris templates.

4.2.12 Comparison

In reviewing the performance of the state-of-the-art, Rathgeb and Uhl (Rathgeb and Uhl, 2011b) conducted a compact survey compiling the key binding schemes in iris biometric cryptosystems. Representing one of the simplest key binding schemes, fuzzy commitment scheme has been successfully applied to iris. More significant performance evaluation on iris based fuzzy commitment scheme (Rathgeb and Uhl, 2011b) has been applied after analyzing the error distribution of iris codes of different iris recognition algorithms. The method reported a GAR of 95.08% at zero FAR. In another extended work (Rathgeb and Uhl, 2009), the authors apply a context-based reliable component selection in order to extract cryptographic keys from iris codes which are then bound to Hadamard codewords achieving a lower GAR of around 93%. Emphasizing on the security, a cryptosystem based on iris key generation is proposed (Wu et al., 2008). The Reed-Solomon ECC and Hash function are employed to transform iris features to cipher key through encryption and decryption. The FRR of this system is nearly 6%. This means that 6% of the genuine users have to present their iris more than one time for decryption. A most recent work aiming to improve the security and performance of fuzzy vault scheme using multi-biometrics (Rathgeb et al., 2016), the best GAR of approximately 95% has been achieved with security level around 50 bits. As for fuzzy vault using single iris, lower GAR around 90% are reported with similar security levels.

The proposed iris key binding scheme is competitive by generating approximately 96% of GAR with security level of 66 bits at zero FAR as shown in Table 4.6 and Table 4.10. Our proposed algorithm has better security assurance compared to another chaffing and winnowing based approach for fingerprint (Jin et al., 2016) of having zero FAR and able to increase the key length from 40 to 200 bits while maintaining optimum performance for GAR. A more precise estimation on the success/failure rate for key retrieval by genuine query has been covered through our proposed KRR. At brute force security of 2^{100}, GAR of above 96% can be achieved while the scheme in (Jin et al., 2016) do not have any accompanying analysis that shows its resistance against this attack.

One advantage of the proposed scheme is ECC free and alignment free without scarifying the performance. In our exposition, the ARM attacks are indeed possible when information can be collected from genuine and synthetic iris templates to retrieve the biometric template. In this case, information leakage from helper data can still be possible even though the adversary has no prior knowledge about the key to distinguish between genuine and synthetic iris templates. In conjunction to this, we have further estimated the possible information leakage by calculating the adversary's advantages gained via our proposed indistinguishability game. Referring to the mean of the imposter distribution at 0.14, the effort for the adversary to learn a single bit is expected to be lower than 2^{-78}. Thus, ARM attacks (Scheirer and Boult, 2007) and correlation related attacks can be prevented through the proposed key binding scheme. ECC-based key binding scheme (Rathgeb and Uhl, 2011c) are often bounded to separate parts of a binary template among which biometric entropy is dispersed. Chunks of

helper data are prone to statistical significant false acceptance caused by the variation in binomial distributions. This forms the basis of statistical attacks as key retrieval attempts are more likely to succeed when binomial distributions of the matching are flattened (Rathgeb and Uhl, 2011c). In our proposed method, the hashed codes can be viewed as the chunks of helper data in the security analysis while false accept attacks complexity can be used as the measure against statistical attacks. False acceptance attacks are prone to happen below the set threshold 0.20 as shown in Figure 4.4. The false acceptance complexity is found to be within the range from 2^{66} to 2^{162}. The complexity is deemed acceptable and sufficient when compared to the best false acceptance security of a multi-biometric iris based fuzzy fault (Rathgeb et al., 2016) which is around 52 bits at zero FAR with GAR approximately 95%. A summarized results of state-of-the-arts iris key binding methods are shown in Table 4.11 below.

Another advantage of our implementation is the flexibility and compactness of the stored helper data. As discussed in previous researches, the records from an alignment free minutiae-based fuzzy vault implementation which consume typically from 896 bytes to 1780 bytes (Tams et al., 2015) can be used as a benchmark. Our experimental results in Table 4.8 has showed a flexible range within $190 - 1900$ bytes with higher GAR. This shows significant storage management of the helper data given that iris features are commonly larger in size.

Table 4.11: Summarized Results of State-of-the-arts

Methods	Databases	GAR (%)	FAR (%)
Iris-based fuzzy commitment schemes (Rathgeb and Uhl, 2011b)	CASIAv3	95.08	0
Iris-biometric key generation (Rathgeb and Uhl, 2009)	CASIAv3	93.47	0
Iris fuzzy vault (Rathgeb et al., 2016)	CASIAv3	93.93	0
Iris key generation (Wu et al., 2008)	CASIAv1	94.45	0
Proposed method	CASIAv3	97.35	0

4.3 Performance of The Proposed Method 3: Tranformation and Matching Strategy for Iris Code

In this section, the performance of the proposed transformation and matching strategy for iris template protection scheme are evaluated. In our experiment, the CASIA v3-interval iris database is adopted. This dataset contains 2639 iris images from 396 different subjects (eyes). For intra-class comparison, each template is matched against the templates from different iris samples of the same subject, leading to a total of 4406 genuine comparisons. As for inter-class comparisons, every template is matched with the first template generated from the first iris samples of different subjects. This yields a total of 199110 imposter comparison. The false acceptance rate (FAR) and false rejection rate (FRR) are used for the evaluation of recognition performance.

Specifically FAR refers to the rate of imposter samples being recognized as a genuine user (falsely accepted) whereas FRR refers to the rate of genuine samples being recognized as an imposter (falsely rejected). The equal error rate (EER) is also being used in the evaluation, which refers to the error rate when FAR = FRR.

4.3.1 Appropriate Selection of the Parameter $\boldsymbol{\tau}$

In this section, experiments are conducted based on different values of $\boldsymbol{\tau}$ with increasing key size, $\boldsymbol{m = 5, 10, 15, 20}$ and constant $\boldsymbol{r = 50}$ for the setting of $\boldsymbol{n = r \times m}$ using $\boldsymbol{20 \times 512}$ iris codes as the input. $\boldsymbol{n_c = 2}$ and $\boldsymbol{q = 9}$ are set while considering the left $(-)$ and right (+) shifting of bits from $\boldsymbol{-4, -3, -2, -1, 0, 1, 2, 3, 4}$ during matching. The result is tabulated in Table 4.12, showing that an appropriate selection of the parameter $\boldsymbol{\tau}$ is necessary to show promising recognition performance of the proposed scheme with low FAR and FRR.

4.3.2 Performance

The achievable EER (lowest) with different parameter settings are tested and tabulated in Table 4.13. It is noticeable that the performance shows slight degradation when m increases. This is due to the trade-off between security and recognition where larger m is necessary to show higher security in terms of non-invertibility.

Table 4.12: Performance of the Proposed Scheme with Varying τ and m

τ		99	95	90	80	60	40	20
$m = 5$	FRR,%	12.4	6.50	2.33	0.65	0.61	1.15	3.54
	FAR,%	33.4	6.27	2.00	0.78	0.56	1.00	1.85
$m = 10$	FRR,%	3.08	3.08	0.68	0.65	0.86	2.33	4.26
	FAR,%	3.04	0.74	0.79	0.93	2.76	7.04	3.97
$m = 15$	FRR,%	0.93	0.83	1.27	2.65	7.73	8.55	24.5
	FAR,%	1.05	0.86	1.59	2.64	3.73	7.91	0.97
$m = 20$	FRR,%	0.70	1.18	2.22	3.42	7.12	14.5	37.0
	FAR,%	0.74	1.30	1.70	4.10	8.57	4.46	0.52

Table 4.13: Performance of the Proposed Scheme with Different Parameter Settings

n_c	r	Performance EER,%				
		$m = 5$	$m = 10$	$m = 15$	$m = 20$	$m = 40$
4	50	**0.46 (τ = 125)**	0.69 (τ = 180)	0.76 (τ = 190)	0.79 (τ = 199)	1.97 (τ =199)
	100	0.49 (τ = 250)	0.69 (τ = 380)	0.75 (τ = 385)	0.84 (τ = 390)	1.67 (τ =399)
	200	0.48 (τ = 500)	0.71 (τ = 780)	**0.71 (τ = 790)**	**0.79 (τ = 790)**	1.36 (τ =799)
	800	0.70 (τ = 3120)	0.88 (τ = 3140	0.78 (τ = 3160)	0.81 (τ = 3180)	**0.92 (τ =3199)**
8	50	0.58 (τ = 250)	0.71 (τ = 360)	0.81 (τ = 385)	1.08 (τ = 396)	2.32 (τ =199)
	100	0.56 (τ = 650)	0.81 (τ = 760)	0.91 (τ = 770)	1.13 (τ = 785)	1.62 (τ =399)
	200	0.56 (τ = 1000)	**0.66 (τ = 1480**)	0.85 (τ = 1540)	1.00 (τ = 1580)	1.32 (τ =799)
	800	0.60 (τ = 3120)	0.70 (τ = 3140)	0.88 (τ = 3160)	1.11 (τ = 3180)	1.36 (τ =3199)
16	50	0.55 (τ = 500)	0.84 (τ = 720)	0.98 (τ = 780)	1.18 (τ = 790)	2.50 (τ = 3299)
	100	0.58 (τ = 1000)	0.96 (τ = 1520)	1.01 (τ = 1555)	1.24 (τ = 1575)	2.55 (τ = 3299)
	200	0.58 (τ = 2000)	0.67 (τ = 2960)	1.05 (τ = 3130)	1.24 (τ = 3160)	2.36 (τ = 3299
	800	0.74 (τ = 3120)	0.70 (τ = 3140)	1.18 (τ = 3160)	1.31 (τ = 3180)	2.70 (τ = 3299

4.3.3 Security Analysis: Non-Invertibility

The non-invertibility of the proposed scheme can be achieved by the one-way hashed of the transformed template (T, T'). The usage of cryptographic one-way hashing in this scheme is an unorthodox manner instead. Specifically, the matching between the transformed templates is done by counting the number of non-collided entries in between the pair-wise (columns) transformed template (after one-way hashed). Only the column of the enrolled and query templates that show at most τ non-collided entries, i.e., $\|T_i \oplus T_i'\| \leq \tau$, will contribute to the count (z) for the final similarity matching score. This is to assert a strong prerequisite for the attacker in reverting the original iris code, where the attacker is required to look for the pre-image of the hashed entry that consists of m bits in order to revert the original iris code. For instance, given an original entry of the transform template $\mathrm{x} = 7$ (where $m = 3$), its corresponding binary value would be 111, which indicates different bit locations of the original iris code. Since x is one-way hashed, i.e., $\mathrm{hash(x)}$, the attacker would have to look for a pre-image x' s.t. $\mathrm{hash(x')} = \mathrm{hash(x)}$. Given x', reverting $m = 3$ bits information of the original iris code thus can be done trivially by 'reverse permutation' using the published bit-sampling functions.

In view of above, for an arbitrary key length m, the non-invertibility of our proposed scheme reduced to the computational hardness in looking for a preimage of the one-way hash function. Nevertheless, due to the dimensional compatibility requirement, i.e., the key length must same for each transformed templates, which is necessary for template matching; The number of trials in looking for a preimages of the one-way hashed function must be bounded by

$O(2^m)$. Therefore, large m is necessary to show strong non-invertibility claim of this proposed scheme.

Besides from this, consider that the attacker is capable of pre-computing a hash table for all possible 2^m entries of the transformed template, we proposed to use a random salt that is used as an additional input to a one-way function such as md5 or AES encryption. Using additional random salt can defend against attacks that use precomputed tables for e.g. rainbow tables (Hellman, 1980) as they can make the size of table needed for a successful attack prohibitively large without burdening users. Since salts differ from one another, they also protect redundant (e.g. commonly-used, re-used) passwords as different salted hashes are created for different instances of the same transformed entries(Anderson, 2020).

For different system/application, a new salt can be randomly generated for each transformed template, and fed together with the template entries to a one-way cryptographic hash function. Noting that the salt don't need to be encrypted or stored separately from the hashed password itself, because even if an attacker has access to the database with the hash values and the salts, a pre-image x' is still necessary to obtain any bit information of the original iris code. This has been assured by the non-invertibility of our proposed transformation.

Correlation in between iris codes: Because the distribution of a biometric source is random and not necessary to be uniformly distributed. Two Iris codes generated from different users may show some degree of similarity by correlation. One example as shown in Figure 3.16 (a) demonstrated that when

$n_c = 1$, it is hard to distinguish whether the query iris code (column) is belonged to the genuine user or imposter. This result implies that the attacker is capable of making use of the vertical dependency property in iris codes and try to revert the original iris code while intercept with the transformed template. A straightforward way of doing this is by sampling a random iris code and follows the proposed transformation and matching mechanism. Since hashing leaks information, the attacker can look for any collided entries in between the stored and query template. Then, perform a reverse engineering process to recovery the original iris code. In such a case, the non-invertibility of the proposed scheme can be examined upon the capability of the attacker to sample an iris code that shows at least one collided entries with the stored template when taking into consideration the correlation in between iris codes. To show the resistance of a scheme against this kind of attack, one needs to ensure that, in average-case, the attacker cannot obtain a single or more than one collided entries by random sampling on an iris code. In view of this, reducing the number of hash entries (reduce information loss) of the stored template would be necessary to achieve strong non-invertibility property against different correlated iris codes.

In the favour of reducing the number of hash entries, the parameters r is meant to be minimized. Table 4.14 below tabulates the performance (EER, %) of the proposed scheme with different parameter settings for r ranging from 10 to 40 with constant $\tau = r - 1$ and $n_c = 1$. This result shows that minimizing r will lead to performance degradation (while τ and n_c are fixed), resulting a trade-off in between non-invertibility and system performance.

Table 4.14: Trade-off between non-invertibility and system performance

Performance EER,%	r = 10	r = 15	r = 20	r = 25	r = 30	r = 35	r = 40
Proposed Method	0.92	0.87	0.83	0.66	055	0.53	0.48

Besides, Figures 4.7 depicts the average number of collided entries for individual columns of the transformed templates (1 to 512). It is clearly observable that the transformed templates show several peaks due to the number of the collided entries under different columns. Such peaks indicate the columns of the iris codes that exhibit strong correlation. Such correlation can be minimized using smaller value of r which render, in average, less than single collided entries over the one-way hashed template to resist against the abovementioned attack.

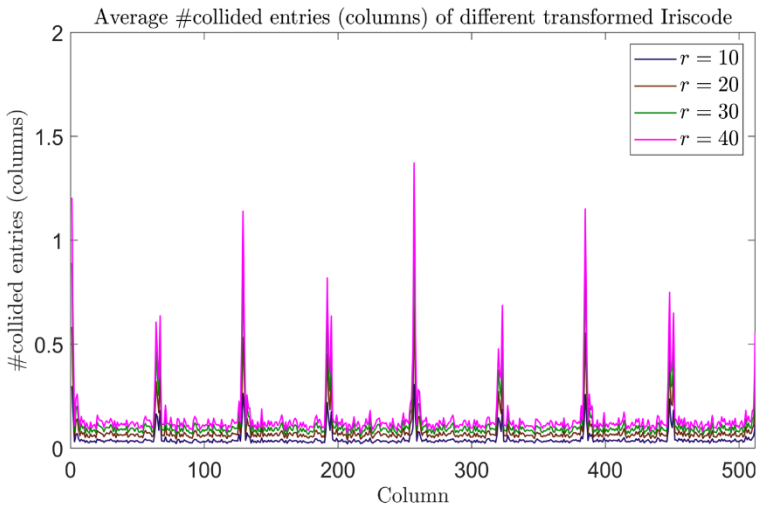
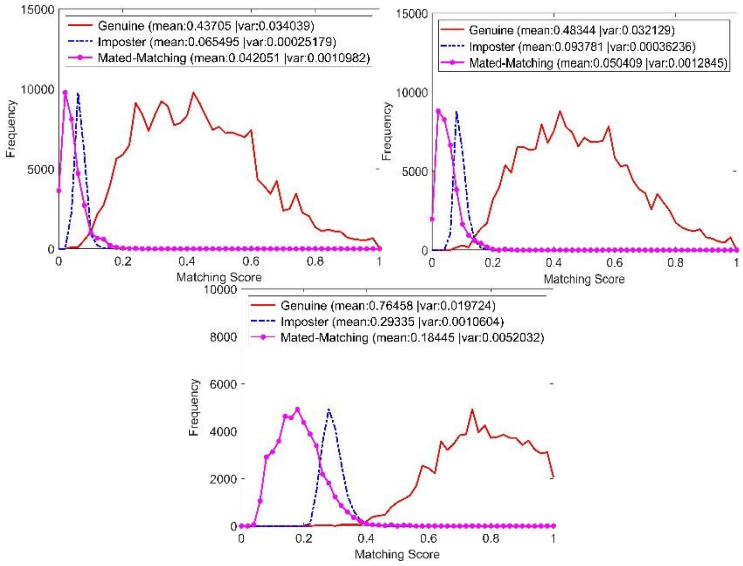


Figure 4.7: Correlation Between Different One-way Hashed Templates

4.3.4 Security Analysis: Revocability

To evaluate the revocability of the algorithm pair, the same experimental setup has been adopted to generate 4406 mated-matching scores. These scores are obtained by performing intra-class comparison among the transformed templates where each transformed template is generated by using a LSH family of sampling function H. The revocability of the proposed scheme is evaluated under different values of $m = 10; 20; 30$. The genuine and imposter similarity score distributions using a single set of sampling function H are plotted together with the mated-scores distribution (4406 different sets of H) in a single graph. Figure 4.8 depicts three different graphs generated by using different parameter settings and constants $n_c = 2; r = 50; q = 9$. In this experiment, a large degree of overlapping in between the mated-matching scores' distribution and the imposter's similarity score distributions are observed. This result implies that the refreshed templates are sufficiently distinctive, albeit they are generated from the same subject. Indeed, the new transformed samples generated with different sets of H act as the 'imposter' as opposed to the distribution of genuine similarity score. The outcome has verified the revocability of the proposed scheme in generating new transformed templates to replace the old one if it is compromised.



(a) $m = 10, \tau = 20$ (b) $m = 20, \tau = 1$

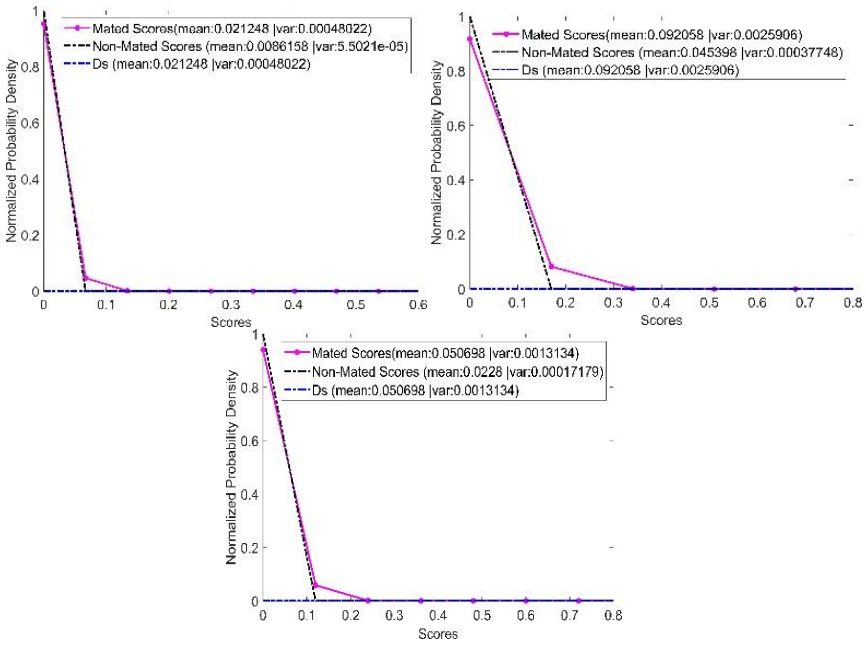
(b) (c) $m = 30, \tau = 1$

Figure 4.8: Evaluate the Revocability of the Proposed Scheme

4.3.5 Security Analysis: Unlinkability

Unlinkability highlights that multiple transformed templates generated from the same iris code should be indistinguishable from each other. To evaluate the unlinkability of the proposed scheme, the method proposed by Gomez et al. (Gomez-Barrero et al., 2017) is adopted as explained in section 4.1.1 Security Model.

In figure 4.9 four different graphs are depicted. Each graph contains 4406 mated-matching scores and 199110 non-mated matching scores generated under different parameter settings with constant $n_c = 2; r = 50; q = 9$ and different (a) $\tau = 20$, (b) $\tau = 1$, (c) $\tau = 1$ respectively. All the mated and non-mated score distributions show significant overlapping and negligibly small value of $D_{sys} =$ 0.01,0.03,0.01 respectively. Therefore, the proposed scheme fulfils the criteria on unlinkability.



(a) $m = 10, \tau = 20$ (b) $m = 20, \tau = 1$

(c) $m = 30, \tau = 1$

Figure 4.9: Evaluate the Unlinkability of the Proposed Scheme

4.3.6 Comparison

In this section, the proposed scheme has been benchmarked with respect to the performance of the original iris code and the state-of-the-art BTP schemes for iris code. To maintain the consistency, the comparison is carried out by using the iris code generated from the public available CASIA v3-interval iris database.

Table 4.15 tabulates the outcome of this benchmarking. All the methods in this table have adopted the subsets or full version of CASIAv3 iris database for their experiments. Thus, the comparison is fair and compatible based on the best authentication performance of these methods. The results show that the proposed scheme is able to preserve the performance of the original iris code by achieving

the lowest EER (0.47%) before the transformation and no degradation is observed after the proposed transformation.

Table 4.15: Performance of The State-of-the-arts in Iris Template Protection

BTP scheme	No. iris images used	EER (%)	
		Before BTP scheme apply	After BTP scheme apply
IFO hashing (Lai et al., 2017b)	868(left eye)	0.38	0.54
Block Remapping (Hämmerle-Uhl et al., 2009)	2653	1.10	1.30
Bio-Encoding (Ouda et al., 2011)	740	6.02	6.27
Bloom filter (Rathgeb et al., 2013)	1332(left eye)	1.18	1.14
Bin-Combo (Zuo et al., 2008)	1332(left eye)	0.81	4.41
LSC (Sadhya and Raman, 2019)	1332(left eye)	0.57	0.11
Proposed Method	1332(left eye)	0.46	0.46

CHAPTER 5

CONCLUSION

For this PhD work, the conclusion has been summarized into 3 parts according to the 3 objectives set in the beginning of this thesis; proposed method 1: confidence matrix, proposed method 2: cancelable iris key binding scheme and proposed method 3: improvements on iris code through cancelable transformation and matching strategy.

5.1 Proposed Confidence Matrix to Mitigate Performance Degradation

To summarize this work, two methods have been proposed to mitigate the performance degradation in protected iris recognition system due to the implementation of biometric template protection scheme. The reported EER with three training samples is within the range from 0.20% to 2.48% for four different publicly available iris databases with varying image quality. As shown in the section 4.1, the proposed methods have successfully improved the performance of state-of-the-art enhanced IFO scheme through experiments from 17% to 90% under the best scenario by using not more than 3 training samples. Thus, objective 1 to improve the performance of cancelable iris template protection scheme has been achieved. In overall, the proposed probability-based method seems to outperform binary-based confidence matrix in mitigating the performance degradation.

5.2 Proposed Cancelable Iris Based Key Binding Scheme

In this work, a cancelable iris based key binding scheme which is freed from the limitation of error correcting capacity and tedious alignment process has been proposed. This proposed scheme has achieved objective 2 of this thesis. The reason of introducing IFO hashing as part of the proposed method is to enable tunable hashed code length besides fulfilling the non-invertibility and unlinkability requirements. Storage (kB) per bit has been adopted as the metric to vindicate the significant effect of controllable hashed code length in managing the storage space and preserving the accuracy performance. As a result, highest GAR of 96.37% at zero FAR has been achieved by our proposed scheme. A precise and useful key retrieval metric, *KRR* is proposed and implemented for security analysis such as false accept attack and indistinguishability game.

In addition, the complexity and security level of the proposed method are also justified against potential attacks. For example, this proposed method shows brute force attack complexity of 2^{100} and sufficient false accept complexity of 2^{66} bits under worst case scenario for key length of 100 bits. The proposed method embraces the flexibility while maintaining significant accuracy performance and security level. The security-performance tradeoff has been attended through experiments where the optimum GAR ranges from 96.37% to 97.35% and zero FAR remains stagnant regardless of the increasing key length all the way from 10 to 200 bits. This implies that quality preservation of accuracy performance at higher security level is achievable through the proposed key binding scheme. Finally, the proposed method requires no re-enrollment in case of compromise.

5.3 Proposed Improvements on Iris Code Based Biometric Template Protection Scheme

The demand for protected Iris recognition has raised to make it more trustable and secure in identity verification nowadays. A cancelable iris template protection scheme has been introduced for protected iris recognition system to achieve objective 3 of this thesis. The work has considered the existence of pre-alignment and vertical dependency issues in iris codes when designing the proposed cancelable transformation and matching mechanism for iris BTP scheme. Therefore, this model allows bits-shifting to be conducted directly onto the transformed iris template without the need to present or revert to the original iris code during matching stage. It is important to highlight that the proposed method does not face performance degradation due to the strong collision probability guaranteed by the underlying bit-sampling based Locality Sensitive Hashing (LSH) technique. This theoretical claim is further justified by our satisfactory equal error rates (EERs) for the CASIA v3-interval iris database under multiple parameter settings. EER as low as 0.48% is preserved with key space of iris code being increased to at least 40 bits. The proposed model has been verified according to the security requirements for BTP scheme: non-invertibility, revocability and unlinkability. In a nutshell, the proposed iris BTP transformation and matching strategy provides strong theoretical security while preserving satisfactory authentication accuracy. This model can be extended and improved further for its implementation in multi-modal biometrics in future.

5.4 Future Recommendation

Non-cooperative iris recognition system is indeed referring to recognize individuals automatically by utilizing the captured iris patterns without requiring any cooperative actions from them. This encourages the needs to strengthen system security and extend the robustness of iris segmentation algorithms in a user friendly manner. However, under uncontrolled conditions, obtained iris images are often deformed, defocused, off-angle, low contrast, blurred, occluded and disturbed by background noise. To cater for this issue, related databases such as UBIRISv2 (Proença et al., 2009), MICHE (Hu et al., 2015) and WVU (Crihalmeanu et al., 2007) have been created and shared openly for this purpose. Accurate classification depends on the accuracy of the segmentation algorithms. Poor quality images especially those captured under unconstrained environment or without the cooperation of the subjects will affect the efficiency of the iris segmentation. It is reported that most failures in iris recognition systems are resulted from inaccurate segmentation (Proença and Neves, 2017).

In view of the issues in segmentation inaccuracy, a learning based network, U-Net has been devised for the purpose of end-to-end iris segmentation (Chai et al., 2020). The proposed CNN-based segmentation model has proven to be very successful in segmenting the iris and outperformed most of the state-of-the-arts. The proposed model does not require a great amount of training data like other deep learning networks while performing well without the use of data augmentation during training. The proposed method provides an automated end-to-end solution for iris segmentation with insignificant segmentation error reported in our preliminary testing on non-cooperative iris datasets (refer to Appendix A for more details). Note that, this generic solution avoids the needs

to go through complex and expensive hand-crafted image processing steps for iris detection, localization and segmentation. As future work, the proposed framework can be extended to test with more challenging non-cooperative iris databases. By replacing inefficient iris detection, localization and segmentation methods for non-cooperative system with the proposed automated end-to-end segmentation framework, iris codes with lesser noise can then be generated. Better authentication accuracy for non-cooperative protected iris recognition systems is thus feasible.

In conjunction with this, the proposed transformation and matching strategy for iris template protection scheme can be integrated for the construction of protected non-cooperative iris recognition system. In addition, the effects of non-cooperative factors such as occlusions, incomplete data and noise on the improved iris template protection scheme can be further investigated. Alternatively, the proposed iris protected template can be used as the input to the proposed cancelable iris key binding scheme for future work.

The devised key binding scheme can be extended into the area of multimodal biometrics, particularly fingerprint and iris. A couple of modifications can be made. For instance, the synthetic hashed code $C_j \leftarrow H_j(B_s)$ is replaceable with the existence of other biometric modalities such as fingerprint. There are a lot of uncertainties with non-cooperative factors being considered. There is no single biometric feature that can perform well all the time in different environments. A protected multimodal biometric system that adopts iris and fingerprint in its authentication can improve its resistance against these challenges. However, different biometric features perform differently due

to many reasons such as uniqueness of such feature, quality of the acquisition devices, environmental factors and user behaviours. For an efficient protected multimodal biometric system, the contribution of each biometric feature should be weighted to get the optimum performance based on this hypothesis. Therefore, a weighted protected multimodal biometric system should be developed for future work.

To shed more lights on the future work of weighted protected multimodal biometric system, a feature level fusion scheme is necessary to create the protected multimodal templates. The scheme needs to be flexible in terms of variance in template sizes of different biometrics and contribution in the matching. IFO hashing scheme is preferable as adaptive Bloom filters hash templates of different biometric modalities into different matrix sizes according to the respective parameters set. Although a flexible weighted system can still be applied but larger hashed template tends to influence the performance at the higher degree if this is not adjustable. For further explanation about this future idea, iris and fingerprint will be used as the multimodal biometric modalities. IFO hashing scheme will be first applied onto the extracted iris and fingerprint features respectively. A flexible weighted feature level fusion scheme can be achieved by tuning the number of hash functions, m of different biometric modalities. This proposed idea represents the desired weightage as the number of hashing functions set for different biometric modalities. For example, if higher weightage on fingerprint samples is desired, higher number of hash functions should be applied on fingerprint features when generating protected templates. In this case, if the desired weightage for fingerprint features and iris features is 2:1, the hash code length of fingerprint protected templates can be set as $m =$

$2a$ while the hash code length of iris protected templates will become $m = a$. This indicates that the number of columns in the protected template of fingerprint will double the amount of columns in the protected template of iris.

Adaptive Bloom filters can then be generated based on the hashed codes of iris and fingerprint features. For instance, if a single hashed value of iris IFO template is 8, then the initial value '0' at 8-th location of the Bloom filter of iris will be updated to '1'. Many to one mapping will happen when multiple identical hashed values are mapped to the same location in the Bloom filter. The Bloom filters of iris and fingerprint can have a feature level fusion through a logical OR function. This is to combine the Bloom filters of different modalities into a fused protected multimodal biometric template. Using the example above, protected template of fingerprint is expected to contribute approximately twice during the integer to binary mapping process during the fusion stage. Under the proposed future work, any weighted, cancelable and protected template can then be generated for different biometric modalities using different weightage for performance optimization. In a nutshell, a weighted and protected multimodal biometric system can be achieved in future by integrating the proposed cancelable key binding scheme in this thesis with the newly proposed feature level fusion scheme.

REFERENCES

2002a. Chinese Academy of Sciences. [Online]. CASIA Iris Image Database V3.0 - Interval. Available: http://biometrics.idealtest.org.

2002b. Chinese Academy of Sciences' Institute of Automation: CASIA Iris Image Database V1.0. http://biometrics.idealtest.org

2003. Chinese Academy of Sciences. [Online]. CASIA Iris Image Database V1.0.

2004. Multimedia University: MMU Iris Image Database. http://pesona.mmu.edu.my/ccteo

2014. Biometrics Ideal Test. [Online]. CASIA Iris Thousand Database V4.0.

ADAMOVIC, S., MILOSAVLJEVIC, M., VEINOVIC, M., SARAC, M. & JEVREMOVIC, A. 2017. Fuzzy commitment scheme for generation of cryptographic keys based on iris biometrics. *IET Biometrics,* 6**,** 89-96.

AJISH, S. & ANILKUMAR, K. 2020. Iris template protection using double bloom filter based feature transformation. *Computers & Security,* 97**,** 101985.

AL-SAGGAF, A. A. 2021. A Post-Quantum Fuzzy Commitment Scheme for Biometric Template Protection: An Experimental Study. *IEEE Access,* 9**,** 110952-110961.

ANDERSON, R. 2020. Security engineering: a guide to building dependable distributed systems. *John Wiley & Sons.*

ARSALAN, M., HONG, H. G., NAQVI, R. A., LEE, M. B., KIM, M. C., KIM, D. S., KIM, C. S. & PARK, K. R. 2017. Deep learning-based iris segmentation for iris recognition in visible light environment. *Symmetry,* 9**,** 263.

ARSALAN, M., NAQVI, R. A., KIM, D. S., NGUYEN, P. H., OWAIS, M. & PARK, K. R. 2018. IrisDenseNet: Robust iris segmentation using densely connected fully convolutional networks in the images by visible light and near-infrared light camera sensors. *Sensors,* 18**,** 1501.

ASAKER, A. A., ELSHARKAWY, Z. F., NASSAR, S., AYAD, N., ZAHRAN, O. & ABD EL-SAMIE, F. E. 2021. A novel cancellable Iris template generation based on salting approach. *Multimedia Tools and Applications,* 80**,** 3703-3727.

BASSIT, A., HAHN, F., ZEINSTRA, C., VELDHUIS, R. & PETER, A. Bloom Filter vs Homomorphic Encryption: Which approach protects the biometric data and satisfies ISO/IEC 24745? 2021 International Conference of the Biometrics Special Interest Group (BIOSIG), 2021. IEEE, 1-6.

BASTYS, A., KRANAUSKAS, J. & MASIULIS, R. 2009. Iris recognition by local extremum points of multiscale Taylor expansion. *Pattern recognition,* 42**,** 1869-1877.

BAZRAFKAN, S., THAVALENGAL, S. & CORCORAN, P. 2018. An end to end deep neural network for iris segmentation in unconstrained scenarios. *Neural Networks,* 106**,** 79-95.

BOLLE, R. M., CONNELL, J. H. & RATHA, N. K. 2002. Biometric perils and patches. *Pattern recognition,* 35**,** 2727-2738.

BOWYER, K. W. & BURGE, M. J. 2016. *Handbook of iris recognition,* Springer.

BRINGER, J., CHABANNE, H., COHEN, G., KINDARJI, B. & ZEMOR, G. 2008. Theoretical and practical boundaries of binary secure sketches. *IEEE Transactions on Information Forensics and Security,* 3**,** 673-683.

BRINGER, J., MOREL, C. & RATHGEB, C. Security analysis of bloom filter-based iris biometric template protection. Biometrics (ICB), 2015 International Conference on, 2015. IEEE, 527-534.

BRODER, A. Z. On the resemblance and containment of documents. Proceedings. Compression and Complexity of SEQUENCES 1997 (Cat. No. 97TB100171), 1997. IEEE, 21-29.

CAPPELLI, R., MAIO, D., LUMINI, A. & MALTONI, D. 2007. Fingerprint image reconstruction from standard templates. *IEEE transactions on pattern analysis and machine intelligence,* 29**,** 1489-1503.

CARTER, F. & STOIANOV, A. Implications of biometric encryption on wide spread use of biometrics. EBF Biometric Encryption Seminar (June, 2008), 2008.

CAVOUKIAN, A. & STOIANOV, A. 2011. Biometric encryption. *Encyclopedia of Cryptography and Security.* Springer.

CHAI, T.-Y., GOI, B.-M. & HONG, Y.-Y. 2020. End-to-End Automated Iris Segmentation Framework Using U-Net Convolutional Neural Network. *Information Science and Applications.* Springer.

CHAI, T.-Y., GOI, B.-M. & TAY, Y.-H. 2019a. The Construction of Confidence Bits to Improve Protected Iris Recognition System. *Int. J. Advance Soft Compu. Appl,* 11.

CHAI, T.-Y., GOI, B.-M., TAY, Y.-H. & JIN, Z. 2019b. A new design for alignment-free chaffed cancelable iris key binding scheme. *Symmetry,* 11**,** 164.

CHAI, T.-Y., GOI, B.-M., TAY, Y. H., TENG, K. & YEO, I. 2016. Bi-local region based iris segmentation framework for less-constrained visible wavelength images.

CHANG, Y.-T., SHIH, T. K., LI, Y.-H. & KUMARA, W. 2020. Effectiveness evaluation of iris segmentation by using geodesic active contour (GAC). *The Journal of Supercomputing,* 76**,** 1628-1641.

CHARIKAR, M. S. Similarity estimation techniques from rounding algorithms. Proceedings of the thiry-fourth annual ACM symposium on Theory of computing, 2002. 380-388.

CHIN, C. S., JIN, A. T. B. & LING, D. N. C. 2006. High security iris verification system based on random secret integration. *Computer Vision and Image Understanding,* 102**,** 169-177.

CIMATO, S., GAMASSI, M., PIURI, V., SASSI, R. & SCOTTI, F. 2009. Privacy in biometrics. *Biometrics: theory, methods, and applications***,** 633-654.

CRIHALMEANU, S., ROSS, A., SCHUCKERS, S. & HORNAK, L. 2007. A protocol for multibiometric data acquisition, storage and dissemination. *Technical Report, WVU, Lane Department of Computer Science and Electrical Engineering.*

DAUGMAN, J. 2000. Biometric decision landscapes. University of Cambridge, Computer Laboratory.

DAUGMAN, J. 2004a. How iris recognition works. *IEEE Trans. Cir. and Sys. for Video Technol.,* 14**,** 21-30.

DAUGMAN, J. 2004b. How iris recognition works. *IEEE Transactions on circuits and systems for video technology,* 14**,** 21-30.

DAUGMAN, J. 2006. Probing the uniqueness and randomness of iriscodes: Results from 200 billion iris pair comparisons. *Proceedings of the IEEE,* 94**,** 1927-1935.

DAUGMAN, J. G. 1993. High confidence visual recognition of persons by a test of statistical independence. *IEEE transactions on pattern analysis and machine intelligence,* 15**,** 1148-1161.

DAVIDA, G. I., FRANKEL, Y., MATT, B. & PERALTA, R. On the relation of error correction and cryptography to an online biometric based identification scheme. Workshop on coding and cryptography, 1999. Citeseer.

DAVIDA, G. I., FRANKEL, Y. & MATT, B. J. On enabling secure applications through off-line biometric identification. Proceedings. 1998 IEEE Symposium on Security and Privacy (Cat. No. 98CB36186), 1998. IEEE, 148-157.

DODIS, Y., REYZIN, L. & SMITH, A. Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. International conference on the theory and applications of cryptographic techniques, 2004. Springer, 523-540.

DWIVEDI, R. & DEY, S. Cancelable iris template generation using look-up table mapping. Signal Processing and Integrated Networks (SPIN), 2015 2nd International Conference on, 2015. IEEE, 785-790.

FLOM, L. & SAFIR, A. 1987. Iris recognition system. Google Patents.

FOUAD, M., EL SADDIK, A., ZHAO, J. & PETRIU, E. A fuzzy vault implementation for securing revocable iris templates. Systems Conference (SysCon), 2011 IEEE International, 2011. IEEE, 491-494.

GÁCS, P. & KÖRNER, J. 1973. Common information is far less than mutual information. *Problems of Control and Information Theory,* 2**,** 149-162.

GALBALLY, J., ROSS, A., GOMEZ-BARRERO, M., FIERREZ, J. & ORTEGA-GARCIA, J. 2013. Iris image reconstruction from binary templates: An efficient probabilistic approach based on genetic algorithms. *Computer Vision and Image Understanding,* 117**,** 1512-1525.

GOMEZ-BARRERO, M., GALBALLY, J., RATHGEB, C. & BUSCH, C. 2017. General framework to evaluate unlinkability in biometric template protection systems. *IEEE Transactions on Information Forensics and Security,* 13**,** 1406-1420.

GOMEZ-BARRERO, M., RATHGEB, C., GALBALLY, J., BUSCH, C. & FIERREZ, J. 2016. Unlinkable and irreversible biometric template protection based on bloom filters. *Information Sciences,* 370**,** 18-32.

GOMEZ-BARRERO, M., RATHGEB, C., LI, G., RAMACHANDRA, R., GALBALLY, J. & BUSCH, C. 2018. Multi-biometric template protection based on bloom filters. *Information Fusion,* 42**,** 37-50.

HÄMMERLE-UHL, J., PSCHERNIG, E. & UHL, A. Cancelable Iris Biometrics Using Block Re-mapping and Image Warping. ISC, 2009. Springer, 135-142.

HAO, F., ANDERSON, R. & DAUGMAN, J. 2006. Combining crypto with biometrics effectively. *IEEE transactions on computers,* 55**,** 1081-1088.

HE, Z., TAN, T., SUN, Z. & QIU, X. 2008. Toward accurate and fast iris segmentation for iris biometrics. *IEEE transactions on pattern analysis and machine intelligence,* 31**,** 1670-1684.

HELLMAN, M. 1980. A cryptanalytic time-memory trade-off. *IEEE transactions on Information Theory,* 26**,** 401-406.

HERMANS, J., MENNINK, B. & PEETERS, R. When a bloom filter is a doom filter: security assessment of a novel iris biometric template protection system. Biometrics Special Interest Group (BIOSIG), 2014 International Conference of the, 2014. IEEE, 1-6.

HÖFT, N., SCHULZ, H. & BEHNKE, S. Fast semantic segmentation of RGB-D scenes with GPU-accelerated deep neural networks. Joint German/Austrian Conference on Artificial Intelligence (Künstliche Intelligenz), 2014. Springer, 80-85.

HOLLINGSWORTH, K. P., BOWYER, K. W. & FLYNN, P. J. 2009. The best bits in an iris code. *IEEE Transactions on Pattern Analysis and Machine Intelligence,* 31**,** 964-973.

HU, Y., SIRLANTZIS, K. & HOWELLS, G. 2015. Improving colour iris segmentation using a model selection technique. *Pattern Recognition Letters,* 57**,** 24-32.

HU, Y., SIRLANTZIS, K. & HOWELLS, G. 2016. Optimal generation of iris codes for iris recognition. *IEEE Transactions on Information Forensics and Security,* 12**,** 157-171.

IGNATENKO, T. & WILLEMS, F. M. 2010. Information leakage in fuzzy commitment schemes. *IEEE Transactions on Information Forensics and Security,* 5**,** 337-348.

INDYK, P. & MOTWANI, R. Approximate nearest neighbors: towards removing the curse of dimensionality. Proceedings of the thirtieth annual ACM symposium on Theory of computing, 1998. 604-613.

INUMA, M. 2014. A relation between irreversibility and unlinkability for biometric template protection algorithms. *Josai Mathematical Monographs,* 7**,** 55-65.

JAIN, A. K., NANDAKUMAR, K. & NAGAR, A. 2008. Biometric template security. *EURASIP Journal on Advances in Signal Processing,* 2008**,** 113.

JAIN, A. K., ROSS, A. & PANKANTI, S. 2006. Biometrics: a tool for information security. *IEEE transactions on information forensics and security,* 1**,** 125-143.

JAIN, A. K., ROSS, A. & PRABHAKAR, S. 2004. An introduction to biometric recognition. *IEEE Transactions on circuits and systems for video technology,* 14**,** 4-20.

JALILIAN, E., KARAKAYA, M. & UHL, A. 2021. CNN-based off-angle iris segmentation and recognition. *IET Biometrics***,** 1-18.

JAN, F., ALRASHED, S. & MIN-ALLAH, N. 2021. Iris segmentation for non-ideal Iris biometric systems. *Multimedia Tools and Applications***,** 1-29.

JENISCH, S. & UHL, A. Security analysis of a cancelable iris recognition system based on block remapping. Image Processing (ICIP), 2011 18th IEEE International Conference on, 2011. IEEE, 3213-3216.

JIN, A. T. B., LING, D. N. C. & GOH, A. 2004. Biohashing: two factor authentication featuring fingerprint data and tokenised random number. *Pattern recognition,* 37**,** 2245-2255.

JIN, Z., TEOH, A. B. J., GOI, B.-M. & TAY, Y.-H. 2016. Biometric cryptosystems: A new biometric key binding and its implementation for fingerprint minutiae-based representation. *Pattern Recognition,* 56**,** 50-62.

JUELS, A. & SUDAN, M. 2006. A fuzzy vault scheme. *Designs, Codes and Cryptography,* 38**,** 237-257.

JUELS, A. & WATTENBERG, M. A fuzzy commitment scheme. Proceedings of the 6th ACM conference on Computer and communications security, 1999. ACM, 28-36.

KELKBOOM, E. J., BREEBAART, J., BUHAN, I. & VELDHUIS, R. N. 2012. Maximum key size and classification performance of fuzzy commitment for gaussian modeled biometric sources. *IEEE Transactions on information forensics and security,* 7**,** 1225-1241.

KELKBOOM, E. J., BREEBAART, J., KEVENAAR, T. A., BUHAN, I. & VELDHUIS, R. N. 2011. Preventing the decodability attack based cross-matching in a fuzzy commitment scheme. *IEEE Transactions on Information Forensics and Security,* 6**,** 107-121.

KHAN, T. M., KHAN, M. A., MALIK, S. A., KHAN, S. A., BASHIR, T. & DAR, A. H. 2011. Automatic localization of pupil using eccentricity and iris using gradient based method. *Optics and Lasers in Engineering,* 49**,** 177-187.

KHOLMATOV, A. & YANIKOGLU, B. Realization of correlation attack against the fuzzy vault scheme. Security, Forensics, Steganography, and Watermarking of Multimedia Contents X, 2008. International Society for Optics and Photonics, 68190O.

KLEIN, D. V. Foiling the cracker: A survey of, and improvements to, password security. Proceedings of the 2nd USENIX Security Workshop, 1990. 5-14.

KONG, A., CHEUNG, K.-H., ZHANG, D., KAMEL, M. & YOU, J. 2006. An analysis of BioHashing and its variants. *Pattern Recognition,* 39**,** 1359-1368.

KONG, A. W.-K. 2014. A statistical analysis of IrisCode and its security implications. *IEEE transactions on pattern analysis and machine intelligence,* 37**,** 513-528.

LACHARME, P. 2012. Analysis of the iriscodes bioencoding scheme. *Int. J. Comput. Sci. Softw. Eng.(IJCSSE 2012),* 6**,** 315-321.

LACHARME, P., CHERRIER, E. & ROSENBERGER, C. Preimage attack on biohashing. Security and Cryptography (SECRYPT), 2013 International Conference on, 2013. IEEE, 1-8.

LAI, Y.-L., GOI, B.-M. & CHAI, T.-Y. Alignment-free indexing-first-one hashing with bloom filter integration. Intelligence and Security Informatics (ISI), 2017 IEEE International Conference on, 2017a. IEEE, 78-82.

LAI, Y.-L., JIN, Z., GOI, B.-M., CHAI, T.-Y. & YAP, W.-S. Iris Cancellable Template Generation Based on Indexing-First-One Hashing. International Conference on Network and System Security, 2016. Springer, 450-463.

LAI, Y.-L., JIN, Z., TEOH, A. B. J., GOI, B.-M., YAP, W.-S., CHAI, T.-Y. & RATHGEB, C. 2017b. Cancellable iris template generation based on Indexing-First-One hashing. *Pattern Recognition,* 64**,** 105-117.

LEE, Y. J., BAE, K., LEE, S. J., PARK, K. R. & KIM, J. Biometric key binding: Fuzzy vault based on iris images. International Conference on Biometrics, 2007. Springer, 800-808.

LEE, Y. J., PARK, K. R., LEE, S. J., BAE, K. & KIM, J. 2008. A new method for generating an invariant iris private key based on the fuzzy vault system. *IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics),* 38**,** 1302-1313.

LI, P., YANG, X., CAO, K., TAO, X., WANG, R. & TIAN, J. 2010. An alignment-free fingerprint cryptosystem based on fuzzy vault scheme. *Journal of Network and Computer Applications,* 33**,** 207-220.

LIU, J., SUN, Z. & TAN, T. Code-level information fusion of low-resolution iris image sequences for personal identification at a distance. 2013 IEEE Sixth International Conference on

Biometrics: Theory, Applications and Systems (BTAS), 2013. IEEE, 1-6.
LIU, N., LI, H., ZHANG, M., LIU, J., SUN, Z. & TAN, T. Accurate iris segmentation in non-cooperative environments using fully convolutional networks. 2016 International Conference on Biometrics (ICB), 2016. IEEE, 1-8.
LUMINI, A. & NANNI, L. 2007. An improved biohashing for human authentication. *Pattern recognition,* 40**,** 1057-1065.
MAIORANA, E., CAMPISI, P. & NERI, A. IRIS template protection using a digital modulation paradigm. Acoustics, Speech and Signal Processing (ICASSP), 2014 IEEE International Conference on, 2014. IEEE, 3759-3763.
MARIÑO, R. Á., ALVAREZ, F. H. & ENCINAS, L. H. 2012. A crypto-biometric scheme based on iris-templates with fuzzy extractors. *Information Sciences,* 195**,** 91-102.
MASEK, L. 2006. Recognition of human iris patterns for biometric identification. 2003. *University of Western Australia*.
MERKLE, J., NIESING, M., SCHWAIGER, M., IHMOR, H. & KORTE, U. 2010. Security capacity of the fuzzy fingerprint vault. *International Journal on Advances in Security,* 3.
MITZENMACHER, M. 2002. Compressed bloom filters. *IEEE/ACM transactions on networking,* 10**,** 604-612.
NANDAKUMAR, K. & JAIN, A. K. 2015. Biometric template protection: Bridging the performance gap between theory and practice. *IEEE Signal Processing Magazine,* 32**,** 88-100.
NANDAKUMAR, K., JAIN, A. K. & PANKANTI, S. 2007. Fingerprint-based fuzzy vault: Implementation and performance. *IEEE transactions on information forensics and security,* 2**,** 744-757.
NATGUNANATHAN, I., MEHMOOD, A., XIANG, Y., BELIAKOV, G. & YEARWOOD, J. 2016. Protection of privacy in biometric data. *IEEE access,* 4**,** 880-892.
NOTO, S., CORREIA, P. L. & SOARES, L. D. Analysis of error correcting codes for the secure storage of biometric templates. 2011 IEEE EUROCON-International Conference on Computer as a Tool, 2011. IEEE, 1-4.
OUDA, O. 2021. On the Practicality of Local Ranking-Based Cancelable Iris Recognition. *IEEE Access*.
OUDA, O., NANDAKUMAR, K. & ROSS, A. Cancelable Biometrics Vault: A Secure Key-Binding Biometric Cryptosystem based on Chaffing and Winnowing. 2020 25th

International Conference on Pattern Recognition (ICPR), 2021. IEEE, 8735-8742.

OUDA, O., TSUMURA, N. & NAKAGUCHI, T. 2011. On the security of bioencoding based cancelable biometrics. *IEICE TRANSACTIONS on Information and Systems,* 94**,** 1768-1777.

PARIKH, Y., CHASKAR, U. & KHAKOLE, H. Effective approach for iris localization in nonideal imaging conditions. Proceedings of the 2014 IEEE Students' Technology Symposium, 2014. IEEE, 239-246.

PATEL, V. M., RATHA, N. K. & CHELLAPPA, R. 2015. Cancelable biometrics: A review. *IEEE Signal Processing Magazine,* 32**,** 54-65.

PHILLIPS, P. J., BOWYER, K. W., FLYNN, P. J., LIU, X. & SCRUGGS, W. T. The iris challenge evaluation 2005. Biometrics: Theory, Applications and Systems, 2008. BTAS 2008. 2nd IEEE International Conference on, 2008. IEEE, 1-8.

PHILLIPS, P. J., SCRUGGS, W. T., O'TOOLE, A. J., FLYNN, P. J., BOWYER, K. W., SCHOTT, C. L. & SHARPE, M. 2009. FRVT 2006 and ICE 2006 large-scale experimental results. *IEEE transactions on pattern analysis and machine intelligence,* 32**,** 831-846.

PILLAI, J. K., PATEL, V. M., CHELLAPPA, R. & RATHA, N. K. Sectored random projections for cancelable iris biometrics. Acoustics Speech and Signal Processing (ICASSP), 2010 IEEE International Conference on, 2010. IEEE, 1838-1841.

PRABHAKAR, S., PANKANTI, S. & JAIN, A. K. 2003. Biometric recognition: Security and privacy concerns. *IEEE security & privacy,* 1**,** 33-42.

PROENCA, H. & ALEXANDRE, L. A. 2011. Toward covert iris biometric recognition: Experimental results from the NICE contests. *IEEE Transactions on Information Forensics and Security,* 7**,** 798-808.

PROENÇA, H., FILIPE, S., SANTOS, R., OLIVEIRA, J. & ALEXANDRE, L. A. 2009. The UBIRIS. v2: A database of visible wavelength iris images captured on-the-move and at-a-distance. *IEEE Transactions on Pattern Analysis and Machine Intelligence,* 32**,** 1529-1535.

PROENÇA, H. & NEVES, J. C. IRINA: Iris recognition (even) in inaccurately segmented data. Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, 2017. 538-547.

QUAN, F., FEI, S., ANNI, C. & FEIFEI, Z. Cracking cancelable fingerprint template of Ratha. Computer Science and Computational Technology, 2008. ISCSCT'08. International Symposium on, 2008. IEEE, 572-575.

RAJASEKAR, V., PREMALATHA, J. & SATHYA, K. 2021. Cancelable Iris template for secure authentication based on random projection and double random phase encoding. *Peer-to-Peer Networking and Applications*, 14**,** 747-762.

RATHA, N. K., CHIKKERUR, S., CONNELL, J. H. & BOLLE, R. M. 2007. Generating cancelable fingerprint templates. *IEEE Transactions on pattern analysis and machine intelligence,* 29**,** 561-572.

RATHGEB, C., BREITINGER, F. & BUSCH, C. Alignment-free cancelable iris biometric templates based on adaptive bloom filters. Biometrics (ICB), 2013 International Conference on, 2013. IEEE, 1-8.

RATHGEB, C., TAMS, B., WAGNER, J. & BUSCH, C. 2016. Unlinkable improved multi-biometric iris fuzzy vault. *EURASIP Journal on Information Security,* 2016**,** 26.

RATHGEB, C. & UHL, A. 2009. Context-based texture analysis for secure revocable iris-biometric key generation.

RATHGEB, C. & UHL, A. Privacy preserving key generation for iris biometrics. IFIP International Conference on Communications and Multimedia Security, 2010a. Springer, 191-200.

RATHGEB, C. & UHL, A. Secure iris recognition based on local intensity variations. International Conference Image Analysis and Recognition, 2010b. Springer, 266-275.

RATHGEB, C. & UHL, A. 2011a. Context-based biometric key generation for Iris. *IET computer vision,* 5**,** 389-397.

RATHGEB, C. & UHL, A. 2011b. The state-of-the-art in iris biometric cryptosystems. *State of the art in Biometrics***,** 179-202.

RATHGEB, C. & UHL, A. Statistical attack against iris-biometric fuzzy commitment schemes. Computer Vision and Pattern Recognition Workshops (CVPRW), 2011 IEEE Computer Society Conference on, 2011c. IEEE, 23-30.

RATHGEB, C. & UHL, A. 2011d. A survey on biometric cryptosystems and cancelable biometrics. *EURASIP Journal on Information Security,* 2011**,** 1-25.

REDDY, E. S. & BABU, I. R. Performance of iris based hard fuzzy vault. Computer and Information Technology Workshops,

2008. CIT Workshops 2008. IEEE 8th International Conference on, 2008. IEEE, 248-253.
RIVEST, R. & DUSSE, S. 1992. The MD5 message-digest algorithm. MIT Laboratory for Computer Science Cambridge.
RIVEST, R. L. 1998. Chaffing and winnowing: Confidentiality without encryption. *CryptoBytes (RSA laboratories),* 4**,** 12-17.
RONNEBERGER, O., FISCHER, P. & BROX, T. U-net: Convolutional networks for biomedical image segmentation. International Conference on Medical image computing and computer-assisted intervention, 2015. Springer, 234-241.
SADHYA, D. & RAMAN, B. 2019. Generation of cancelable iris templates via randomized bit sampling. *IEEE Transactions on Information Forensics and Security,* 14**,** 2972-2986.
SASSE, M. A. 2007. Red-eye blink, bendy shuffle, and the yuck factor: A user experience of biometric airport systems. *IEEE Security & Privacy,* 5.
SCHEIRER, W. J. & BOULT, T. E. Cracking fuzzy vaults and biometric encryption. Biometrics Symposium, 2007, 2007. IEEE, 1-6.
SHAH, S. & ROSS, A. 2009. Iris segmentation using geodesic active contours. *IEEE Transactions on Information Forensics and Security,* 4**,** 824-836.
SIMOENS, K., YANG, B., ZHOU, X., BEATO, F., BUSCH, C., NEWTON, E. M. & PRENEEL, B. Criteria towards metrics for benchmarking template protection algorithms. 2012 5th IAPR International Conference on Biometrics (ICB), 2012. IEEE, 498-505.
TAMS, B. 2013. Attacks and countermeasures in fingerprint based biometric cryptosystems. *arXiv preprint arXiv:1304.7386*.
TAMS, B., MIHĂILESCU, P. & MUNK, A. 2015. Security considerations in minutiae-based fuzzy vaults. *IEEE Transactions on Information Forensics and Security,* 10**,** 985-998.
TEOH, A. B. J. & KIM, J. 2007. Secure biometric template protection in fuzzy commitment scheme. *IEICE Electronics Express,* 4**,** 724-730.
TEOH, A. B. J., YIP, W. K. & TOH, K.-A. 2010. Cancellable biometrics and user-dependent multi-state discretization in BioHash. *Pattern Analysis and Applications,* 13**,** 301-307.
UMER, S., DHARA, B. C. & CHANDA, B. 2017. A novel cancelable iris recognition system based on feature learning techniques. *Information Sciences,* 406**,** 102-118.

VENUGOPALAN, S. & SAVVIDES, M. 2011. How to generate spoofed irises from an iris code template. *IEEE Transactions on Information Forensics and Security,* 6**,** 385-395.

VERBITSKIY, E. A., TUYLS, P., OBI, C., SCHOENMAKERS, B. & SKORIC, B. 2010. Key extraction from general nondiscrete signals. *IEEE Transactions on Information Forensics and Security,* 5**,** 269-279.

WANG, Q., MENG, X., SUN, T. & ZHANG, X. 2021. A light iris segmentation network. *The Visual Computer***,** 1-11.

WU, X., QI, N., WANG, K. & ZHANG, D. A novel cryptosystem based on iris key generation. 2008 Fourth International Conference on Natural Computation, 2008. IEEE, 53-56.

ZHANG, L., SUN, Z., TAN, T. & HU, S. 2009. Robust biometric key extraction based on iris cryptosystem. *Advances in Biometrics***,** 1060-1069.

ZHAO, D., FANG, S., XIANG, J., TIAN, J. & XIONG, S. 2018. Iris template protection based on local ranking. *Security and Communication Networks,* 2018.

ZHOU, X., KUIJPER, A., VELDHUIS, R. & BUSCH, C. Quantifying privacy and security of biometric fuzzy commitment. Biometrics (IJCB), 2011 International Joint Conference on, 2011. IEEE, 1-8.

ZUO, J., RATHA, N. K. & CONNELL, J. H. Cancelable iris biometric. Pattern Recognition, 2008. ICPR 2008. 19th International Conference on, 2008. IEEE, 1-4.

APPENDIX A

End-to-End Segmentation Framework for protected iris recognition system

The U-Net (Ronneberger et al., 2015) model represents a popular CNN architecture for solving biomedical problems, for instance, segmenting different kinds of cells and detecting boundaries between very dense cell structures and other image translation tasks. The main advantage of this model is its ability to learn relatively accurate models from very small datasets, which is a common problem for data-scarce computer-vision tasks, including iris segmentation.

6.1 Model Architecture

U-Net is a fully convolutional network that consists of the contracting path (down-sampling path) and an expansive path (up-sampling path), which form a U-shaped design at last. The contracting path is the basis of the typical convolutional network that undergoes repeated application of convolutions in each layer where the max pooling operation and the activation function – rectified linear unit (ReLu) take place. The purpose of the max pooling operation and activation function is to reduce the spatial information and increase the feature information for substituting this input to the expansive path. A sequence of concatenating great solution features from the contracting path with the respective layer and deconvolution methods to upsample the feature is going through the expansive path to combine the feature and spatial information for

greater segmentation outcome. When the process is finished, the model outputs a segmentation map at the last stage of this architecture and will compare with the ground truth. In overall, the modification of this U-net architecture is the pooling operator in the fully convolutional network (FCN) are substituted by upsampling operators with a large number of feature channels to preserve the feature information to high-resolution layers. This modification makes the symmetric structure with the contracting path which looks like alphabet U.

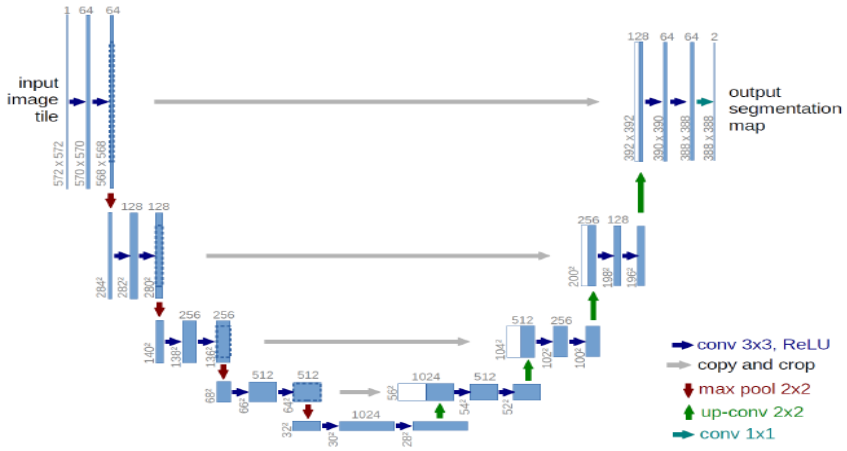


Figure 6.1: U-Net Architecture Design

Table 6.1: Setting and architecture of U-Net model

Name	Filters size	Filters number	Output shape
Input Layer	-	0	(400,400,1)
conv2d_1	(3,3)	64	(400,400,64)
conv2d_2	(3,3)	64	(400,400,64)
max_pooling_2d_1	(2,2)	-	(200,200,64)
conv2d_3	(3,3)	128	(200,200,128)
conv2d_4	(3,3)	128	(200,200,128)
max_pooling_2d_2	(2,2)	-	(100,100,128)
conv2d_5	(3,3)	256	(100,100,256)
conv2d_6	(3,3)	256	(100,100,256)
max_pooling_2d_3	(2,2)	-	(50,50,256)

conv2d_7	(3,3)	512	(50,50,512)
conv2d_8	(3,3)	512	(50,50,512)
max_pooling_2d_4	(2,2)	-	(25,25,512)
conv2d_9	(3,3)	1024	(25,25,1024)
conv2d_10	(3,3)	1024	(25,25,1024)
conv2d_transpose_1	(2,2)	-	(50,50,512)
concatenate_1	-	-	(50,50,1024)
conv2d_11	(3,3)	256	(50,50,256)
conv2d_12	(3,3)	256	(50,50,256)
conv2d_transpose_2	(2,2)	-	(100,100,256)
concatenate_2	-	-	(100,100,512)
conv2d_13	(3,3)	128	(100,100,128)
conv2d_14	(3,3)	128	(100,100,128)
conv2d_transpose_3	(2,2)	-	(200,200,128)
concatenate_3	-	-	(200,200,256)
conv2d_15	(3,3)	64	(200,200,64)
conv2d_16	(3,3)	64	(200,200,64)
conv2d_transpose_4	(2,2)	-	(400,400,64)
concatenate_4	-	-	(400,400,128)
conv2d_17	(3,3)	32	(400,400,32)
conv2d_18	(3,3)	32	(400,400,32)

6.2 Datasets and Experiment Protocol

For this research, several publicly available iris datasets are adopted: NICE.I, NICE.II and MICHE as in (Hu et al., 2015). All the images have been resized to 400 x 400 pixels for standardization to provide square inputs to U-Net. The validation split of 0.1 is used to form the validation set within the training set. Hence, In U-Net training process, the training set and test set are split into 80:20, 70:30 and 60:40 to study the overall performance of the proposed method. A well accepted evaluation metric, E_1 is used to assess the performance of our proposed algorithm. The result is shown in Table 6.2.

NICE.I: This is the NICE.I contest subset that selected by (Hu et al., 2015)

NICE.II: Combining two 1000 images subsets that retained by the NICE.II committee during the NICE.II contest as the test set. The images in this dataset are captured at a distance and suffer from realistic noise such as illumination variance, motion blur and occlusion of glasses and eyelids.

MICHE: MICHE-I is a challenging dataset captured with mobile devices to ensure the developing algorithms in non-ideal difficult situations. This database is collected using three smartphones: iPhone5 with 8 MP (72 dpi) back camera and 1.2 MP (72 dpi) frontal camera, Samsung Galaxy S4 with 13 MP (72 dpi) back camera and 2 MP (72 dpi) frontal camera. This dataset is also based on the selection by (Hu et al., 2015).

All the images including ground truth are first divided by 255 for data normalization. All datasets are trained to operate Adam optimiser with a learning rate of $10^{-4,}$ and no decay is set. Kernel initialiser is added into the model to improve the segmentation results. There are no image augmentations applied to the datasets. The model is trained from 10 epochs to 20 epochs on the original U-net model and choose the best E_1 values and tabulate the metrics in Table 6.2, Table 6.3 and Table 6.4. This model is implemented in Python using Keras deep learning libraries with the backend of Tensorflow to support the training process in this project. The experiment is carried out using an online platform with 16GB of RAM and NVIDIA Tesla P100 12GB GPU.

6.3 Performance Metric

The performance of the proposed method is evaluated by using the NICE.I evaluation protocol. This evaluation method is well accepted by the researchers of the field of iris segmentation to evaluate segmentation

performance. E_i, the evaluation protocol that takes account of seeking out the differences between the resultant image $I_i(m', n')$and ground truth image $G_i(m', n')$ by XOR function, given as:

$$E_i = \frac{1}{m*n} \sum_{(m',n')} I_i(m', n') \otimes G_i(m', n') \quad (24)$$

Where m' and n' are the respective width and height of the image. E_i is computed as the pixel classification accuracy which is only valid for a single image. The segmentation error rate, E_1 is given by the average of errors on the input images, E_i:

$$E_1 = \frac{1}{t} \sum_i E_i \quad (25)$$

Where t is the total number of images to be evaluated. The value of E_1 is within the range of [0,1] interval. In this context, "1" and 0 will be respectively the worst and optimal matching between ground truth and resultant images.

Table 6.2: Segmentation Error of Proposed Method for Different Ratio of Training Set / Test Set

Training set / Test set	NICE.I	NICE.II	MICHE IP5	MICHE GS4
80:20	0.01084	0.01467	0.01282	0.01737
70:30	0.01192	0.01197	0.01261	0.01705
60:40	0.01330	0.01117	0.01324	0.01637

The proposed U-net method has achieved the lowest segmentation error (E_1) with 0.01084, 0.01117, 0.01261 and 0.01637 on the NICE.I, NICE.II, MICHE GS4 subset and MICHE IP4 subset databases respectively. Although there is difficulty to compare the results against different model of architectures

and settings, it is still meaningful to benchmark the proposed method with the state-of-the-art deep learning based iris segmentation methods which use the same evaluation protocol. From Table 6.3 and Table 6.4, the proposed U-Net model is among the top 3 methods with segmentation error as low as 0.01084 and 0.01117 even though the training sets are limited on NICE.I and NICE.II. Most of the methods in the table trained their model using more than 1000 images and conducted data augmentation. This might gradually improve the effectiveness of the model but we use lesser images in the training as the iris data is defined as protected personal data and it is reasonable to predict that only limited samples per individual will be collected for identification purpose. Besides that, no data augmentation is performed in our experiment to avoid the regularization effect which sometimes causes the net to be under fit.

Table 6.3: Performance of the Proposed Method and State-of-the-arts in Iris Segmentation using NICE.I Iris Dataset

State-of the-art Methods (Proenca and Alexandre, 2011)	E_1
Luengo-Oroz et al.	0.0305
Scotti and Labbati	0.0301
Chen et al.	0.0297
Jeong et al.	0.0282
Li et al.	0.0224
P. Almeida	0.0180
Sankowski et al.	0.0162
Tan et al.	0.0131
Proposed Method	0.01084

Table 6.4: Performance of the Proposed Method and State-of-the-arts in Iris Segmentation using NICE.II Iris Dataset

State-of the-art Methods	E_1
Proenca et al. (Arsalan et al., 2018)	0.0187
Tan et al. (Arsalan et al., 2018)	0.0172
Hu et al. (Hu et al., 2015)	0.0143
Haindl et al. (Arsalan et al., 2018)	0.0124
Zhao et al. (Arsalan et al., 2018)	0.0121
Arsalan et al. (Arsalan et al., 2017)	0.0082
IrisDenseNet (Arsalan et al., 2018)	0.00695
Proposed Method	0.01117

APPENDIX B

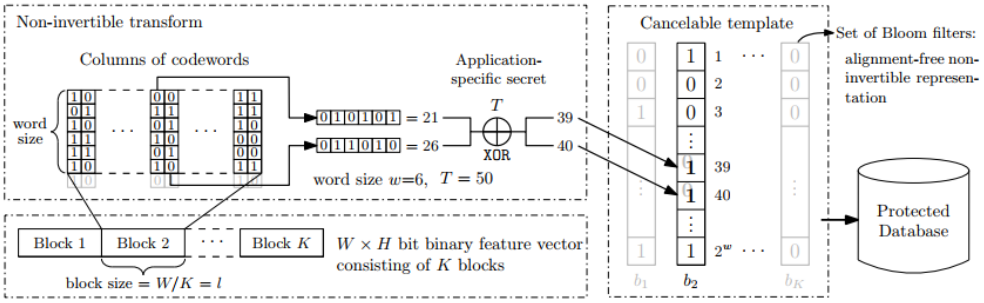


Figure 6.2: Basic Operation of Adaptive Bloom Filter

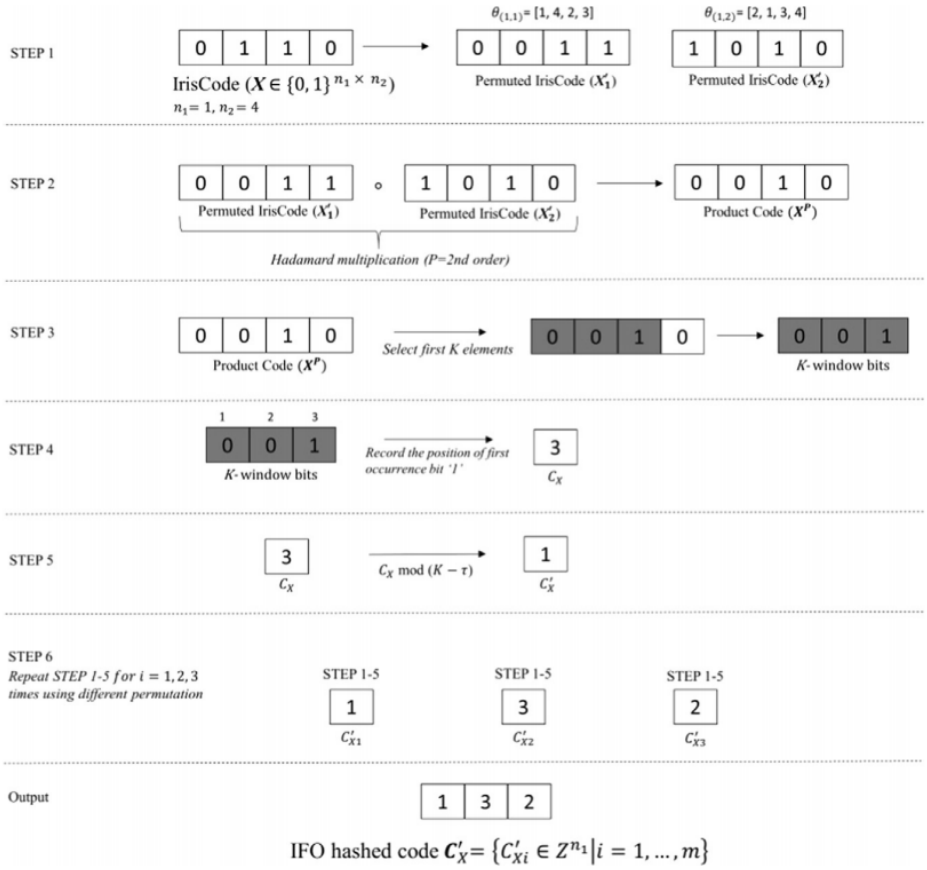


Figure 6.3: Basic Operation of IFO Hashing