UNIMODAL AND MULTIMODAL BIOMETRIC VERIFICATION USING CANCELABLE IRIS AND FINGERPRINT TEMPLATES

Ph.D. Thesis

By

RUDRESH DWIVEDI

DISCIPLINE OF COMPUTER SCIENCE AND ENGINEERING

INDIAN INSTITUTE OF TECHNOLOGY INDORE

FEBRUARY 2019

UNIMODAL AND MULTIMODAL BIOMETRIC VERIFICATION USING CANCELABLE IRIS AND FINGERPRINT TEMPLATES

A THESIS

submitted to the

INDIAN INSTITUTE OF TECHNOLOGY INDORE

in partial fulfillment of the requirements for
the award of the degree of

DOCTOR OF PHILOSOPHY

by

RUDRESH DWIVEDI

DISCIPLINE OF COMPUTER SCIENCE AND ENGINEERING

INDIAN INSTITUTE OF TECHNOLOGY INDORE

FEBRUARY 2019

INDIAN INSTITUTE OF TECHNOLOGY INDORE

CANDIDATE'S DECLARATION

I hereby certify that the work which is being presented in the thesis entitled **Unimodal and Multimodal Biometric Verification using Cancelable Iris and Fingerprint Templates** in the partial fulfillment of the requirements for the award of the degree of **Doctor of Philosophy** and submitted in the **Discipline of Computer Science and Engineering, Indian Institute of Technology Indore,** is an authentic record of my own work carried out during the time period from January 2014 to February 2019 under the supervision of Dr. Somnath Dey, Assistant Professor, Indian Institute of Technology Indore, Indore, India.

The matter presented in this thesis has not been submitted by me for the award of any other degree of this or any other institute.

Signature of the Student with Date

(Rudresh Dwivedi)

This is to certify that the above statement made by the candidate is correct to the best of my knowledge.

Signature of Thesis Supervisor with Date

(Dr. Somnath Dey)

Rudresh Dwivedi has successfully given his Ph.D. Oral Examination held on **12th February 2019**.

Signature of Chairperson, OEB	Signature of External Examiner	Signature of Thesis Supervisor
Date:	Date	Date:
Signature of PSPC Member #1	Signature of PSPC Member #2	Signature of Convener, DPGC
Date:	Date	Date:

Signature of Head of Discipline

Date:

ACKNOWLEDGEMENTS

I wish to seize this opportunity to acknowledge to all those who have assisted, one way or another, to the accomplishment of this dissertation, which marks another important milestone in my life.

First and foremost, my sincerest gratitude ascribes to my supervisor Dr. Somnath Dey for the immense support and unrelenting source of motivation throughout my PhD tenure. His benevolent supervision, constructive criticism, invaluable guidance, and financial support from the moment I started working at IIT Indore as a doctoral student. The consistent and unending directions steered me in the right path and transformed me into a researcher who can work independently. I confide the amicable of the work environment, created by him, which is utter different from the environments. I could not have imagined having a better, affable supervisor and mentor for my doctoral tenure.

Besides, I extend my gratitude to the rest of my research progress committee comprising experts from other domains: Dr. Kapil Ahuja and Dr. Vimal Bhatia, for their keen observation, valuable comments, insightful suggestions, encouragement, and validation of this research. I would like to express my appreciation to Dr. Surya Prakash, Head of discipline for all his extended suggestions and support. I also express my tribute to Dr. Anirban Sengupta for his efforts for encouragement and motivation. I cannot forget the continuous morale booster and stress reliever ideas provided by him.

No matter how dark the times were, I am deeply grateful to Dr. Vivek Kanhagad who has supported me during the PhD coursework in my initial days. Also, his constant invaluable insights and discussions upheld me in typical situations. I would also like to acknowledge Dr. Tanima Dutta for her valued advice in this doctoral study. I also thoroughly enjoyed working as a TA for her courses most of the time during PhD as his leadership was very cooperative such that my doctoral work wasn't affected even minimally due to the allotted TA duties.

I express sincere gratitude to Prof. Pradeep Mathur (Director, IIT Indore), who has been highly encouraging during the entire course of my doctoral work. I also convey sincere thanks to Dr. Abhishek Srivastava, Dr. Neminath Hubbali, Dr. Aruna Tiwari (DPGC Convener, Discipline of Computer Science and Engineering) for their support and motivation in all the times. A special gratitude goes out all down at Indian Institute of Technology Indore for providing me an opportunity to pursue PhD under state-of-the-art research environment and also Ministry of Human Resource Development (MHRD), Government of India for granting financial aid to carry out this doctoral study successfully.

I am also grateful to cheerful fellow doctoral students; Om Prakash Patel, Vijay Anand, Vinod Kumar Singh, Prakash Sharma, Prateek Jain, as well as the undergraduate students for their feedback, encouragement, cooperation, and of course friendship. Without their precious support, it would not be possible to reach this level. Besides, it was great sharing laboratory with Ram Prakash Sharma during last four years. Also, I would wish to thank the all lab staffs of Computer Science and Engineering discipline.

Finally, I must express my very profound gratitude to my family: my parents for providing me with unfailing support and continuous encouragement throughout my years of study and through the process of doctoral research and writing this thesis. Their belief in me and my capabilities is the prime motivation that has driven me to this stage where I can confidently take decisions to realize my dreams. This accomplishment would not have been possible without them.

Thanks for all your encouragement and help me find a whole new outlook on life.

_____

Rudresh Dwivedi
Indian Institute of Technology Indore
February 2019

Dedicated to my parents

and

my grandmother.

ABSTRACT

Biometric-based recognition systems is gaining the popularity day by day and have overcome passive issues of traditional human authentication systems. However, security theft and privacy invasion are two passive issues that still persist in the effective deployment of biometric-based authentication systems. Compromise of biometric data can potentially lead to serious security violation as the user's biometric trait cannot be changed. In order to prevent the invasion of biometric templates, it is desired to morph the original biometric template through non-invertible or irreversible transformation function. This transformed template is referred to as cancelable template and can be replaced or reissued in case of compromise. The problem still persists if a protected multi-biometric template gets compromised. Objective of this thesis is to address the mentioned concerns associated with template protection and investigate the template protection schemes for unimodal and multimodal biometric traits with large scale biometric data so that the matching can be accomplished in transformed domain without compromising the verification performance.

In this dissertation, we consider two biometric traits (iris and fingerprint). We propose an efficient template protection scheme for both biometric modalities. Next, we utilize both protected templates for cancelable multibiometric verification system. Our iris template protection scheme uses IrisCodes derived form 1-D log Gabor filter with rotation-invariant mechanism. Next, consistent bit vector is derived by aligning IrisCodes of different samples of the same subject. The consistent-bit vector is divided into equal sized words to form a decimal vector. Then, a Look-up table mapping based transformation has been applied for cancelable iris template generation.

In cancelable fingerprint template protection, we evaluate ridge features with reference to ridge co-ordinate system. The computed features are invariant to translation, scale, and rotation. These features are uniquely encoded using Cantor pairing function. Then, we apply random projection for cancelable fingerprint template generation.

Our protected multimodal verification scheme utilizes scores evaluated from the protected modalities. Corresponding to each modality, we integrate the scores from different matchers/classifiers based on the novel mean-closure weighting (MCW) mechanism. The fused scores obtained from different matchers for each trait are then combined using rectangular area weighting (RAW) mechanism. This two-level score fusion method is incorporated for cancelable multi-biometric verification.

Finally, we proceed in the direction of hybrid fusion integrating both score and decision level mechanism to overcome the limitations related to unibiometric, multibiometric, and existing protected multibiometric systems. In order to perform hybrid fusion, we utilize our previous works to derive cancelable template for iris and fingerprint. Next, we apply the novel MCW to combine scores obtained from individual matchers. Then, Dempster-Shafer (DS) theory of evidence is employed to combine the decisions provided by individual matchers.

The major contributions of the thesis are cancelable template generation for iris and fingerprint biometric modalities. The proposed template protection schemes preserve the desired criteria of irreversibility, revocability, and diversity of the cancelable transformation. Also, experiments performed on different databases confirm the potential robustness of the proposed transformation.

Further, the proposed multimodal cancelable multimodal biometric verification techniques are able to attain performance improvement and provides adequate security to protect original biometric data. Thus, the proposed cancelable multibiometric verification proves to be effective for secure and accurate authentication.

PUBLICATIONS FROM THE THESIS

The following mentioned publications have evolved from this doctoral dissertation (as of February 2019):

Papers in Peer - Reviewed Journals:

Published / Accepted

1. **R. Dwivedi**, S. Dey, "A novel hybrid score level and decision level fusion scheme for cancelable multi-biometric verification", *Applied Intelligence*, Springer, Online, 2018.
   (DOI: https://doi.org/10.1007/s10489-018-1311-2)

2. **R. Dwivedi**, S. Dey, "Securing fingerprint template using non-invertible ridge feature transformation", *Journal of Electronic Imaging*, SPIE, Vol. 27, no. 5, pp. 1-17, 2018.
   (DOI: https://doi.org/10.1117/1.JEI.27.5.053031)

3. **R. Dwivedi**, S. Dey, "Score-level fusion for cancelable multi-biometric verification", *Pattern Recognition Letters*, Elsevier, Online, 2018.
   (DOI: https://doi.org/10.1016/j.patrec.2018.04.022.)

4. **R. Dwivedi**, S. Dey, R. Singh, A. Prasad, "A privacy-preserving cancelable iris template generation scheme using decimal encoding and look-up table mapping", *Computers & Security*, Elsevier, Vol. 65, pp. 373 – 386, 2017.
   (DOI: https://doi.org/10.1016/j.cose.2016.10.004)

Submitted:

1. **R. Dwivedi**, S. Dey, "Generating protected fingerprint template utilizing coprime mapping transformation", *Journal of Banking and Financial Technology*, Springer (Submitted on 21^{th} April, 2018).

2. **R. Dwivedi**, S. Dey, M. Sharma, A. Goel, "A fingerprint based crypto-biometric system for secure communication", *Journal of Ambient Intelligence and Humanized Computing*, Springer (Submitted on 28^{th} Dec, 2018).

Papers in Refereed Conferences

1. **R. Dwivedi**, S. Dey, “Coprime mapping transformation for protected and revocable fingerprint template generation", in Proc. of 5^{th} *International Conference on Mining Intelligence and Knowledge Exploration*, Hyderabad, India, Dec. 13−15, 2017, pp. 111–122. (DOI:10.1007/978-3-319-71928-3_12.)

2. **R. Dwivedi**, S. Dey, “Cancelable iris template generation using look-up table mapping", in Proc. of 2^{nd} *IEEE International Conference on Signal Processing and Integrated Networks*, Noida, India, Feb. 19−20, 2015, pp.785-790. (DOI: 10.1109/SPIN.2015.7095296)

Recognition/ prizes:

1. **R. Dwivedi**, Score-level fusion for cancelable multi-biometric verification, 7^{th} IDRBT Doctoral Colloquium, Institute for Development and Research in Banking Technology, 2017, Hyderabad. **[Special mention]**

2. **R. Dwivedi**, Consistent-bit inspired cancelable iris template generation, 5^{th} IDRBT Doctoral Colloquium, Institute for Development and Research in Banking Technology, 2015, Hyderabad. **[Won third prize]**

Contents

List of Figures

List of Tables

Nomenclature

List of Abbreviations/Acronyms

1-D	One Dimension
1VS1	One Verses One
2-D	Two Dimension
2P-MCC	Two Factor Minutiae Cylinder Code
3-D	Three Dimension
ACO	Ant Colony Optimization
ARM	Attack via Record Multiplicity
AUC	Area Under ROC Curve
BBA	Basic Belief Assignment
BC	Biometric Cryptosystem
BCH	Bose, Chaudhuri, and Hocquenghem Codes
BMI	Body Mass Index
BSIFs	Binarized Statistical Image Features
CANPASS	Canadian Passenger Accelerated Service System
CASIA	Institute of Automation, Chinese Academy of Sciences
CB	Cancelable Biometric
DFT	Discrete Fourier Transform
DS	Dempster-Shafer
EM	Expectation Maximization Algorithm
FIR	Finite-Impulse-Response
FVC	Fingerprint Verification Competition

ICE	Iris Challenge Evaluation Iris Database
IFO	Indexing-First-One Hashing
IrisCode	Iris Code
IUPUI	Indiana University - Purdue University Indianapolis
ISO	International Organization for Standardization
JL	Johnson-Lindenstrauss Lemma
KDE	Kernel Density Estimator
LBP	Local Binary Pattern
LBPH	Local Binary Patterns Histograms
LDA	Linear Discriminant Analysis
LDP	Local Direction Pattern
LR	Likelihood Ratio
MCC	Minutiae Cylinder Code
MCW	Mean Closure Weighting
MFCCs	Mel Frequency Cepstral Coefficients
MLC	Multi Line Code
MMU	Multimedia University Iris Database
MMU1	MMU Version-1 Iris Database
MOG	Mixture of Gaussians
MSU	Michigan State University Database
NIST	National Institute of Standards and Technology Database
NRC	National Register of Citizens
PCA	Principal Component Analysis
PCR	Proportional Conflict Redistribution Rule
PIN	Personal Identification Number
P-MCC	Protected Minutiae Cylinder Code
PSO	Particle Swarm Optimization
QQ	Two Quadrics
QLQ	Quadric-Line-Quadric
RAW	Rectangular Area Weighting

RLRD	Random Local Region Descriptor
ROC	Receiver Operating Characteristic Curve
SDI	Score Decidability Index
SHA-1	Secure Hash Algorithm 1
SKA-PB	Secure Key Agreement-Pure Biometrics
SKA-CB	Secure Key Agreement-Cancelable Biometrics
SURF	Speeded Up Robust Features
SVM	Support Vector Machine
TDC	Total Distance Criterion
UIDAI	Unique Identification Authority of India
VNs	Voronoi Neighbor Structure
WVU	West Virginia University Database

List of Symbols

CI	Confidence Interval
EER	Equal Error Rate
FAR	False Accept Rate
FMR	False Match Rate
FNMR	False Non-Match Rate
FRR	False Reject Rate
GAR	Genuine Accept Rate
GMR	Genuine Match Rate
HD	Hamming Distance
HTER	Half Total Error Rate
LUT	Lookup Table
NG	Number of Intra-class Comparison
NI	Number of Inter-class Comparison
NR	Number of Ridges

RA	Rectangular Area
d'	d-prime Separability
V_{up}	Set of Unprotected Minutiae Points
rc	Ridge Count
ro	Mean Ridge Orientation
C^P	Cantor Paired Output
$\mathcal{L}$	Log Template
$\mathcal{R}$	Random Projection Matrix
C^T	Cancelable Template
C_b	Consistent Bit Vector
Q^T	Query Template
R_v	Output Row Vector
sim	Similarity Score
$\hat{S}$	Filtered Similarity Matrix
$\mathfrak{S}$	Global Similarity/Comparison Score
H_s	Hamming Similarity
J_s	Jaccard Similarity
Ls_dice	Dice Similarity Score
Ls_cosine	Cosine Similarity Score
Mc_i^m	Mean-closure of Matcher m for User i
w_k	Weight for Modality k
bel	Measure of Belief
pl	Plausibility

Chapter 1

Introduction

Over the last decade, biometric authentication has gained much public attention as compared to traditional knowledge (password, key) or token-based authentication systems and is widely deployed to identify/verify users firmly in several domains. However, biometric-based authentication systems suffer from security and privacy invasion challenges as their compromise may expose sensitive and ancillary information about a user. Further, if the biometric template gets compromised, it results in permanent identity theft as biometric data are intrinsically linked with the user. This introduces the research question "how do we replace the biometric data which is permanent and limited for a user without affecting the accuracy of the system?". The different attacks such as hill-climbing, correlation, inversion, and stolen-token attacks can be launched for illicit use of biometric data which reduce the reliability of the system. As a consequence, there is a demand of designing a robust biometric system with substantial template protection to deal the situation of compromise or privacy invasion across different applications.

In this dissertation, we investigate the template protection schemes for iris and fingerprint biometric modalities. We also explore the mechanism for cancelable multibiometric system by integrating these protected biometric templates. This chapter begins with a brief description of biometric-based authentication. Section 1.2 narrates the schemes for biometric template protection. The need and urgency of the biometric template protection are discussed in Section 1.3. The motivations and objectives behind the research work are presented in Section 1.4 and Section 1.5, respectively. A glimpse of contributions made from this thesis is given in Section 1.6 with research highlights. The common experimental settings utilized for

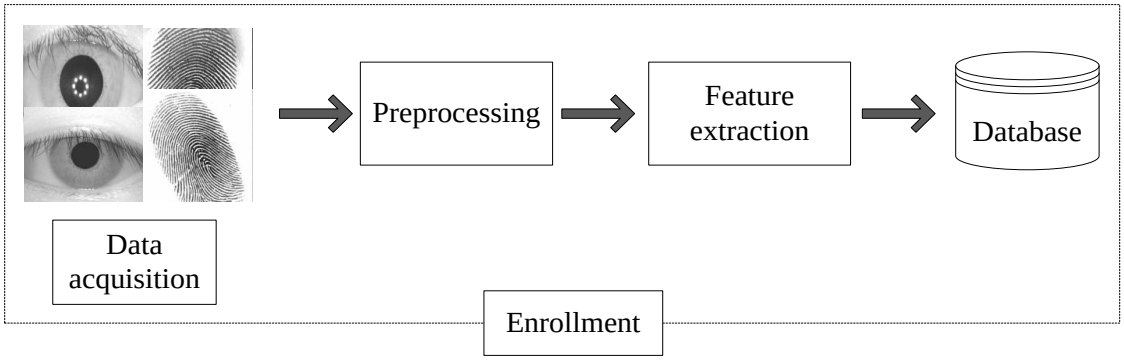
performance evaluation and experimentation are described in Section 1.7. Finally, Section 1.8 covers the coherent organization of the thesis.

1.1 Biometric-based authentication

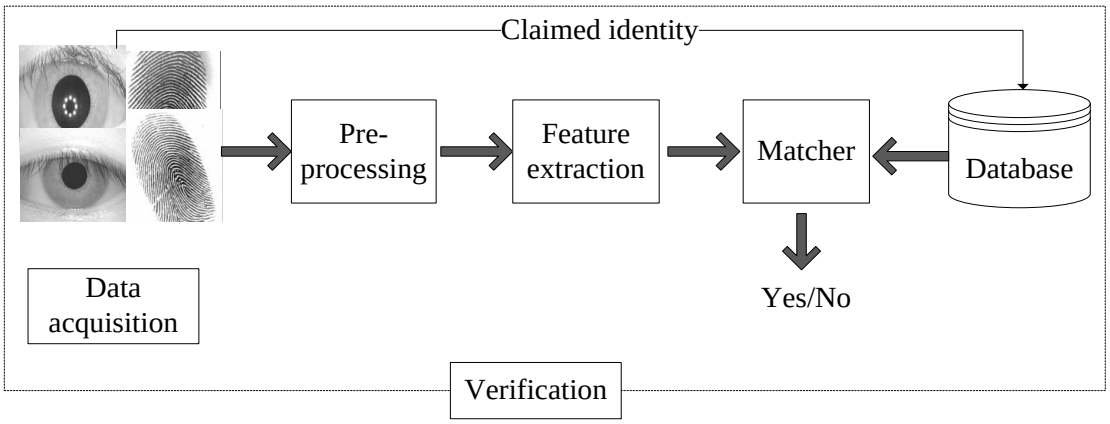
Biometrics is the unique way of verifying or identifying a user based on his/her physiological or behavioral characteristics [2]. In today's era, most of the commercial and government firms utilize biometric-based authentication in numerous security-concerned applications such as digital forensics [3, 4], airport security [5–9], cross-border management [10–14], defense and military services [15], government records [16], driving licenses [17], and financial transactions [18]. The examples of physiological traits include iris, face, fingerprint, palmprint, ear, and hand-geometry whereas gait, signature, voice, and key-stroke dynamics are categorized as behavioral biometric traits. The authentication system utilizing a single source of information i.e. only one modality is called as unimodal biometric authentication system. However, few limitations are associated with unimodal biometric systems such as erroneous data, intra-class variability, exalted error rates, constrained degrees of freedom, spoof attacks, and non-universality [19]. To mitigate these concerns, researchers have started utilizing multiple biometric modalities or other characteristics besides biometric information. Such systems are termed to be multimodal or multibiometric authentication system.

In a biometric system, a user registers himself to the system's biometric database at the time of enrollment. The enrollment phase involves pre-processing, feature extraction, and template generation from the input biometric image. At the time of verification, an individual's identity is validated by comparing the stored template with his/her biometric template. The matcher decides an individual to be genuine or imposter by one-to-one comparison. Figure 1.1(a) shows the enrollment procedure in a biometric authentication system whereas the block diagram for verification system is shown in Fig. 1.1(b).

In the block diagrams, data acquisition at user's end is performed at sensor module. The preprocessing module removes the noise and enhances the quality of the image. Feature extraction computes the features referred as original biometric template and these features are stored in the database. The matcher module performs the comparison between query and stored templates, and generates a similarity/dissimilarity score to determine whether the user is genuine or imposter.



(a) Enrollment phase



(b) Verification phase

Figure 1.1: Mode of operations in a biometric authentication system

1.2 Biometric template protection

Biometric template protection [20, 21] is a mechanism to provide security to the original biometric information as compromise may cause permanent identity disclosure. The template protection techniques are classified in two categories i.e. Cancelable biometric (CB) and Biometric cryptosystem (BC). These two categories are further divided into two distinct classes as shown in Fig 1.2.

Cancelable biometric (CB): The notion of cancelable biometrics refers to apply a privacy-preserving non-invertible (or hard-to-invert) feature transformation on original biometric templates before they are stored into the database. Authentication is performed in the transformed domain to maintain secrecy. Figure 1.3 illustrates this idea of feature transforma-

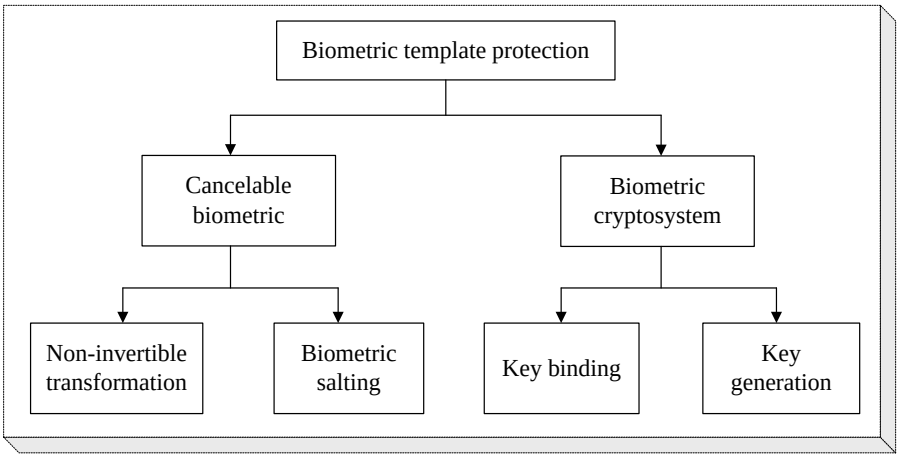


Figure 1.2: Classification of biometric template protection techniques (adopted from Jain et al. [1])

tion. Under biometric salting [22–25], the protection mechanism is based on user-specific key or randomly generated parameters [1, 20]. The nobility lies in easy revocation by altering random parameters or keys of the transformation. In biometric salting-based techniques [26–28], the transformation may become invertible if the imposter attains illegitimate access to the user-specific key and transformed template. Hence, the secrecy relies upon user-specific key or transformation parameters. In contrary, non-invertible methods are one-way function where it is very hard to invent the original template even if the adversary reveals the protected template and transformation key.

Biometric cryptosystem (BC): The mechanism of biometric cryptosystem extracts/creates a helper data from the original biometric information. This helper data does not unveil enough

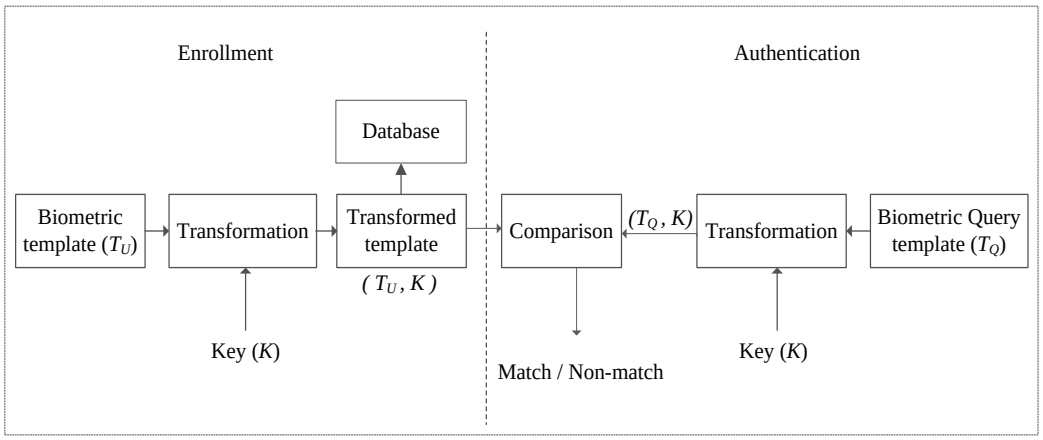


Figure 1.3: Authentication in transformed domain: cancelable biometric

information about the original biometric information or the transformation parameters i.e. it is computationally infeasible to derive the key or transformed template without original biometric data. Figure 1.4 shows the function in biometric cryptosystem transformation. Further, helper data is utilized to estimate/recover the original biometric information from a noisy or erroneous instance of it. This helper data may be in the type of a secure sketch [29, 30] or a syndrome [31].

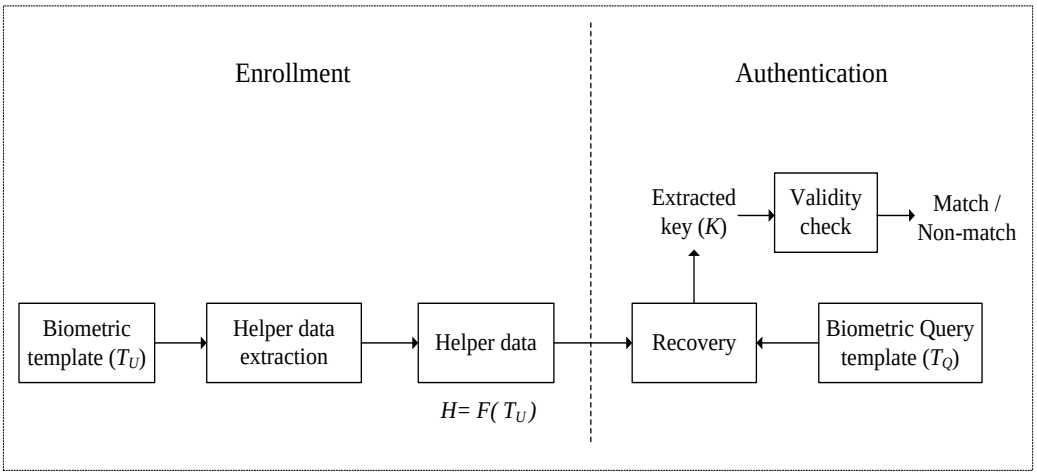


Figure 1.4: Authentication in transformed domain: biometric cryptosystem

Under key binding schemes [32, 33], the helper data is achieved by blending the original template with a key that is independent of biometric features. Note that, it is nearly infeasible to unveil the key or original template from this helper data. Comparison of protected stored and query templates requires the recovery of key using query helper data. If the transformation key is derived directly using stored helper data and query helper data, the cryptosystem is termed as key generation based biometric cryptosystem.

1.3 Need and urgency of biometric template protection

Over the last decade, the rapid growth of biometric-based authentication in government and industrial firms has disconcerted the users about privacy and security challenges. Hence, security violation and privacy invasion are two major causes behind the universal acceptance since the biometric information are intrinsically linked with the user's identity. A compromise can result into permanent identity theft. Recently, a security breach has been reported

by FireEye [34] which confirms that Android-based HTC-One smartphone is capturing biometric information in the plain text format with read permission. In Andhra Pradesh state of India, Aadhaar [16] and bank details of over 134,000 beneficiaries have been leaked from Housing Corporation's website despite the robust legislation of UIDAI's data security. In current era [18], hackers are trying to impersonate identity to steal money, illegally transfer funds, and make credit card transaction in the victim's name. Further, they may siphon the classified personal healthcare information and use those information for blackmail or commit insurance fraud.

According to Ratha et al. [35], eight level of attacks can be launched against a biometric system. Figure 1.5 demonstrates these underlying attacks. Thereafter, Jain et al. [1] highlighted three possible vulnerabilities for biometric-based authentication: 1) Illegitimate access by exchanging genuine template with imposter's template, 2) Spoof may be derived by unauthorized access of genuine template and, 3) Cross-matching could be performed to invade user's privacy in other applications.

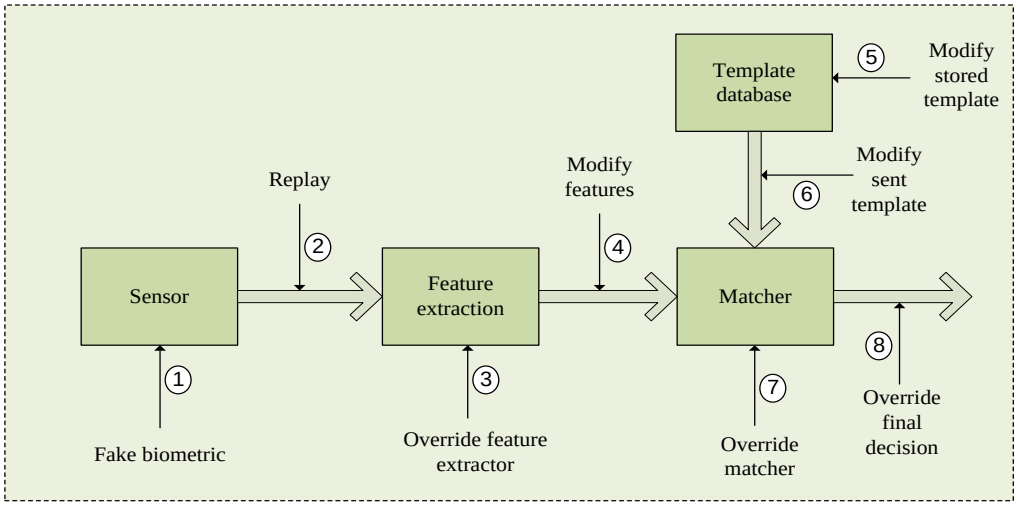


Figure 1.5: Level of attacks in a biometric system [1]

For these underlying concerns, there is a necessity to design a biometric system with substantial template protection scheme [20]. Generally, the following axioms are followed to ensure adequate secrecy and privacy [20, 36]:

1. Non-invertibility/irreversibility: It should be sufficiently infeasible to retrieve original template from the protected template or the helper data.

2. Revocability: In the situation of compromise, a new template should be reissued to replace the compromised one.

3. Diversity: The transformation should be able to derive numerous secure template, and those secure templates should be uncorrelated/unlinkable to each other.

4. Performance: The performance with respect to unprotected biometric system should be preserved i.e. there should not be larger performance degradation compared to unprotected biometric system.

This thesis focuses on the privacy and security assessment of these vulnerabilities and proposes novel template protection schemes to alleviate the security challenges. The research accomplished is motivated by these three underlying observations from the literature:

- There is an invariable requirement to access these vulnerabilities in privacy-concerned applications to redress the need of public and private infrastructures. This is the sole mean to provide sufficient privacy-protection to meet the demand of enrolled users.

- Though, there exist numerous unlinkable and non-invertible solution which are introduced in recent years, still there is a need of template protection scheme that abides by the ISO standards [37, 38] and adequate verification performance under reference security architecture [39].

- There are scarcity of techniques [40, 41] that can be implemented to other biometric modalities and cannot be extended in a point-blank manner as the primitive transformations are applicable to only single biometric modality. Hence, there is a demand to design a new transformation suited to multiple biometric modalities.

Last but not the least, the existing experimental evaluations are carried out and presented without abiding any reference architecture [39] or generic protocol. Also, rigorous security and privacy analysis are not performed in the existing state-of-the-art. As a result, the evaluated performance measures cannot be compared and veritable. Therefore, there is a necessity of a theoretical assessment of security and privacy concerning different scenarios of information leakage.

1.4 Motivations of the thesis

Ensuring the template protection for enrolled subjects is the pivotal concern for biometric-based authentication. This thesis is oriented upon the proposal of new protection schemes to mitigate different privacy threats and possible attacks on biometric systems. The research carried out has been primarily motivated by the following observations from the literature:

- The transformational inconsistencies such as alignment, scale, and translational deformations caused at the time of acquisition may degrade the performance. It is quite challenging to match iris image with rotational inconsistencies caused by tilt head while capturing the image. In case of a fingerprint image, selection of invariant features from the minutiae points results in significant performance improvement over the original minutiae information. Also, the limitation of existing methods [42–44] lies with the accurate detection of the singular point (core or reference point) which is not possible for all type of fingerprint images. These will lead to more performance degradation in the protected domain. Hence, there is a need to propose new cancelable template generation methods with alignment-free and rotation-invariant features for iris and fingerprint biometric.

- It has also been observed from the literature that a number of approaches [45, 46] utilize user-specific key/token for cancelable template generation. These approaches perform well if tokens used for verification are different for each user. However, the performance degrades in case of stolen-token scenario. Therefore, a robust cancelable transformation is required to mitigate the underlying attacks and privacy threats.

- In multibiometric systems, an incorrect decision may occur in scenarios where sufficient training samples are absent. Further, the cost of false acceptance may differ from the cost of false rejection, and the selection of an optimal classifier for a given data set is a challenging task [47,48]. In density fusion methods [49], the assumption of incorrect models for genuine and impostor scores may lead to deficient fusion rules besides complex density estimation. Therefore, there is a need to design a transformation-based technique which should compute appropriate weights to combine different biometric traits.

- The traditional fusion methodologies have not considered the scores from cancelable biometric templates yet. As a multimodal biometric system is able to attain performance improvement and overcome spoofing attacks, template security schemes aim to protect original biometric data. The compositions of these two schemes achieve a win-win scenario for the template protection and performance enhancement. As a result, the integration of multiple protected modalities is desired to improve the performance and enhance the security of the authentication system.

1.5 Objectives of the thesis

The performance and security are the two main parameters for wide deployment of biometric authentication system. For secure authentication, an attack-resilient template protection mechanism needs to be designed which must provide non-invertibility, diversity, and revocability preserving the recognition accuracy with respect to their baseline recognition simultaneously. However, authentication may be performed by integrating different biometric modalities to facilitate utmost security and to compensate performance degradation caused due to transformation. Based on the context described above, the distinctive objectives pursued are stated in the following:

- Reviewing and proposing the template protection scheme for iris biometric to alleviate the security and privacy concerns present in the literature with different scenarios of template compromise.

- Assessing literature findings and introducing the template security mechanism for fingerprint biometric to prevent the security theft and privacy invasion with different situations of template leakage.

- Introducing multibiometirc template verification techniques using the protected template designed for iris and fingerprint biometric modality.

- Proposing a hybrid fusion scheme to overcome the limitations of the individual fusion schemes using protected iris and protected fingerprint templates.

1.6 Contributions of the thesis

In this section, we present the major contributions of the research work carried out for template protection and fusion schemes with respect to a unified framework. The unified framework for cancelable iris and fingerprint template generation, and fusion of these two protected modalities for secure authentication is illustrated in Fig. 1.6. There are four main modules in the framework where each module denotes either unimodal or multimodal biometric verification. Our contributions in each module are described in the following.

1.6.1 Cancelable iris template generation

A cancelable iris template generation technique is proposed based on randomized look-up table mapping. First, the iris image is pre-processed using existing techniques [50]. Next, we extract the IrisCodes in the form of 0–1 matrix using 1-D Log-Gabor filter [50] with phase quantization from the preprocessed iris images. Thereafter, rotation-invariant IrisCode is generated from the original IrisCodes and transformed into a row vector. In the next step, we find the consistent bits by aligning the row vectors and generate the consistent bit vector. This consistent bit vector is exploited to decimal encoding. Finally, we create a look-up table and map the decimal-encoded vector to generate the cancelable iris template.

We have performed experimentation on three widely used benchmark iris databases (CASIA-V 1.0 [51], CASIA IrisV3-Interval [51], and ICE 2005 [52]). We achieve EER of 0.37, 0.43, and 0.79 for CASIA-V 1.0, CASIA IrisV3-Interval, and ICE 2005 databases, respectively. It is evident from reported results that our approach performs optimally on these databases. Moreover, the security analysis with respect to revocability, irreversibility, and diversity confirms that our approach fulfills the criteria for template protection.

1.6.2 Cancelable fingerprint template generation

In this technique, a non-invertible random projection based technique is proposed using ridge features to protect the original fingerprint template information. First, we preprocess the input fingerprint image and detect minutiae points along with the thinned noise-free preprocessed image. We partition the fingerprint region into a number of sectors with reference

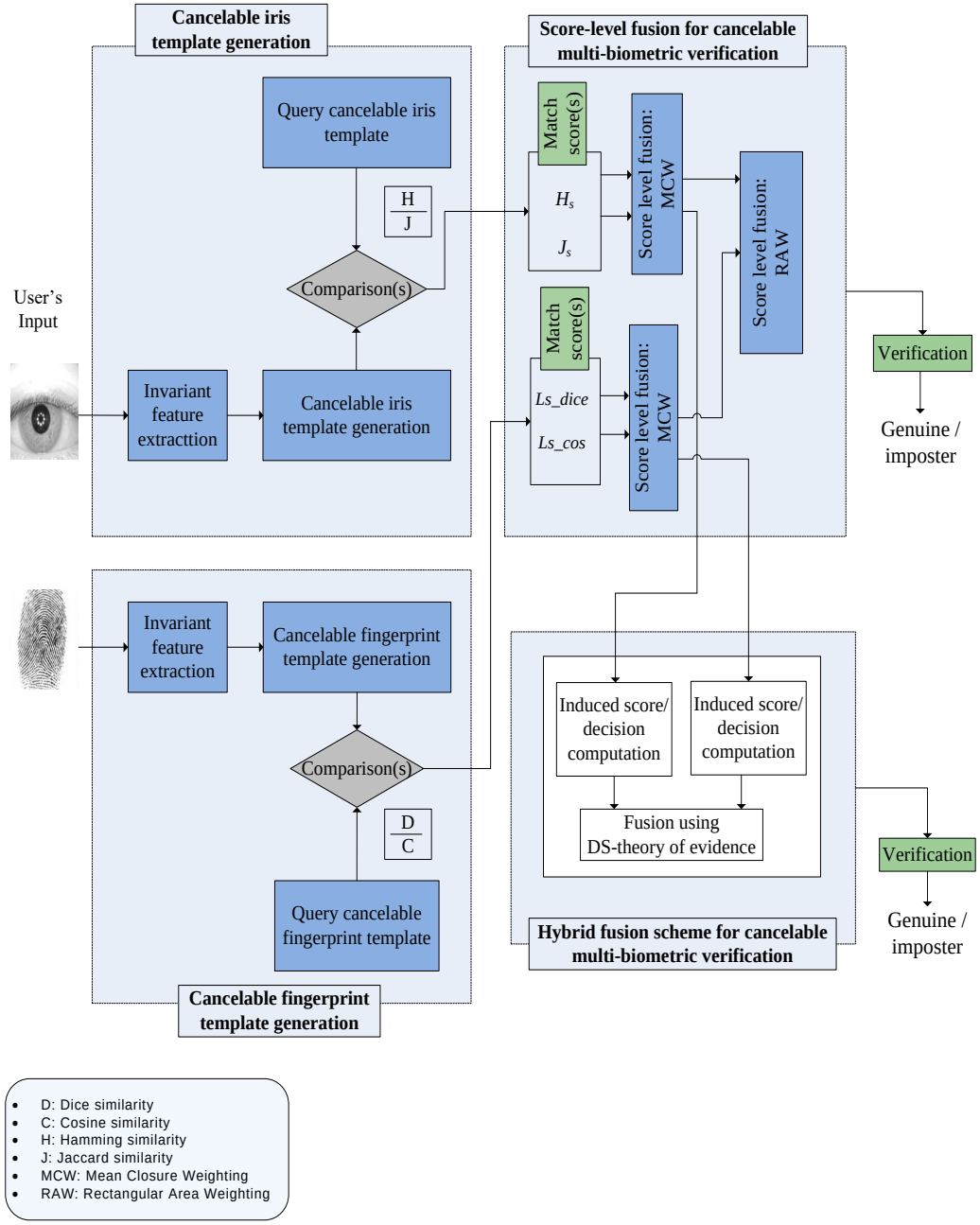


Figure 1.6: Unified framework of the proposed workflow

to each minutiae point employing the ridge-based co-ordinate system. The nearest neighbor minutiae in each sector are identified, and ridge-based features are computed. We employ Cantor pairing function to encode ridge features uniquely. Next, we apply the point-wise logarithm operation on the paired output to obtain a uniform distribution of paired output which is utilized to minimize EER. Finally, we apply random projection onto the paired output to derive the protected template.

We have conducted our experiment on publicly available FVC2002, FVC2004, and FVC2006 fingerprint databases, and each database contains four datasets namely, DB1, DB2, DB3, and DB4 [53]. The standard FVC protocol and 1VS1 protocol are considered to compute the performance of our method. We achieve EER of 1.75, 0.98, 4.02, and 3.74 for DB1, DB2, DB3, and DB4 of FVC2002, EER of 4.38, 6.59, 3.97, and 3.16 for DB1, DB2, DB3, and DB4 of FVC2004, and EER of 5.14, 0.14, 1.63, and 0.49 for DB1, DB2, DB3, and DB4 of FVC2006, respectively under FVC protocol. Under 1VS1 protocol, we obtain an EER of 0, 0.13, 3.39, and 3.02 for DB1, DB2, DB3, and DB4 of FVC2002, EER of 4.02, 5.77, 3.88, and 3.04 for DB1, DB2, DB3, and DB4 of FVC2004, and EER of 0.38, 0.09, 2.02, and 1.03 for DB1, DB2, DB3, and DB4 of FVC2006, respectively. Evaluation performed over four datasets of FVC2002, FVC2004, and FVC2006 databases depicts that the significant performance is achieved from the experiments. The proposed method fulfills the necessary requirements of template protection mechanism. Moreover, the proposed method is resilient against different attacks such as Attacks via Record Multiplicity (ARM), pre-image, cross-matching, distinguishing, and annealing attacks.

1.6.3 Score-level fusion for cancelable multi-biometric verification

In the multimodal cancelable biometric verification approach, the cancelable iris and cancelable fingerprint templates are utilized from the previous contributions. In this work, we propose a two-level score fusion approach for integrating the scores obtained from cancelable templates of different biometric modalities. At the first level, scores from multiple matchers are combined using a novel Mean-Closure Weighting (MCW) technique to achieve the desired score for a particular biometric modality. We measure the separation of scores to mean of the genuine distribution and to the mean of imposter distribution. The ratio of these two decides the weight for different matchers utilized to compute score. Further, we integrate the derived scores from different modalities using a novel Rectangular Area Weighting (RAW) technique at the second level to obtain the overall fused score. The rectangular area measures the overlap region covered between the region of uncertainty.

The performance of the fusion mechanism is evaluated on three virtual databases i.e., Virtual_A, Virtual_B, and Virtual_C. We achieve an EER of 0.69, 0.17, and 0.61 for Virtual_A, Virtual_B, and Virtual_C databases, respectively. The experimental results signify

that the proposed multibiometric system outperforms over the unimodal system for scores obtained through original and cancelable biometric systems. Also, the method claims the requisite criteria of non-invertibility, diversity, and revocability preserving the performance with respect to original templates.

1.6.4 Hybrid fusion scheme for cancelable multi-biometric verification

In this scheme, we propose a generic hybrid fusion framework where the protected modalities are combined to fulfill the requirement of secrecy and performance improvement. This work presents a method to integrate cancelable modalities utilizing a novel MCW-based score level and Dempster-Shafer (DS) theory-based decision level fusion for iris and fingerprint to mitigate the limitations in the individual score or decision fusion mechanisms. First, we integrate the individual scores obtained from different matchers for each modality using MCW score fusion method. For cancelable iris templates, we evaluate Hamming and Jaccard similarities whereas Dice and Cosine similarities are evaluated for cancelable fingerprint templates. Further, we apply DS theory of evidence to the induced scores to obtain the final decision. Finally, verification is performed using a pre-defined threshold to classify user either a genuine or an imposter.

The performance of the hybrid fusion technique is evaluated on three virtual databases i.e., Virtual_A, Virtual_B, and Virtual_C. We obtain an EER of 0.55, 0.13, and 0.50 for Virtual_A, Virtual_B, and Virtual_C databases, respectively. From the experimental evaluations, it has been observed that the proposed multibiometric system outperform both the unimodal unprotected and unimodal protected biometric system for decisions obtained through original and cancelable biometric systems. Further, the security analysis of our work ensures that our approach fulfills the desired characteristics of non-invertibility, revocability, and diversity preserving the recognition accuracy.

In summary, we present chapter-wise research highlights of our thesis in the following.

Research highlights in cancelable iris template generation (Chapter 3):

- In cancelable iris biometric system, rotation-invariant IrisCodes have been utilized as feature computed using 1-D log Gabor filter.

- Consistent bit vector is used to generate decimal vector instead of original row vector to attain performance improvement over the original IrisCodes.
- The entries in the decimal vector are mapped uniquely to a random look-up table. Cancelable iris template is generated by selecting check bits from mapped entries in the look-up table.
- Comprehensive experimental evaluation on CASIA V-3.0 Interval [51], CASIA V 1.0, and ICE2005 [52] has been performed to test the efficacy of the method.
- The necessary criteria of template protection i.e. non-invertibility, revocability, and diversity are achieved for cancelable iris transformation.

Research highlights in cancelable fingerprint template generation (Chapter 4):

- To generate cancelable fingerprint template, the ridge features are evaluated with reference to ridge-based co-ordinate system to cope with rotation, translation and scale deformations in the input fingerprint image which ensures that the proposed transformation would not lean upon prior alignment with the singularities.
- The Cantor pairing function followed by random projection is utilized to generate non-invertible cancelable fingerprint template.
- Rigorous experimental evaluations are performed over public benchmark FVC 2002, FVC 2004, and FVC2006 databases to validate the robustness of the method.
- The required constrains of template security i.e. non-invertibility, revocability, and diversity are achieved for cancelable fingerprint generation scheme.

Research highlights in score-level fusion for cancelable multi-biometric verification (Chapter 5):

- A two-level fusion mechanism has been proposed to integrate cancelable (protected) scores utilizing mean-closure and rectangular area based weighting methods.
- The exhaustive experimentations on three virtual databases has been performed to evaluate the performance.

Research highlights in hybrid fusion scheme for cancelable multi-biometric verification (Chapter 6):

- A hybrid fusion framework has been developed for combining multiple protected biometric traits (iris and fingerprint) to aid security and performance improvement.
- Extensive experiments on three virtual databases have been performed to evaluate the performance of the hybrid fusion mechanism.

1.7 Common experimental environment

The proposed work is implemented using MATLAB 7.8.0 (R2010b) of MathWorks, Inc, USA. The machine specification includes DELL Precision Tower 5810, RAM 64 GB, Intel E5-1600 processor with Windows10 operating system.

The efficiency of the proposed method is evaluated by different performance measures such as False Accept Rate (FAR), False Reject Rate (FRR) and Equal Error Rate (EER). As we evaluate our method on publicly available benchmark databases, failure-to-enroll rate (FTE) and failure-to-acquire rate (FTA) are not considered. Hence, FAR, FRR, and GAR terms can also be used as False Match Rate (FMR), False Non-match Rate (FNMR), and Genuine Match Rate (GMR) interchangeably in our work. These terms are defined in the following:

$$\text{FAR/FMR} = \frac{\text{Comparison decision of 'match' for imposters}}{\text{Total comparisons from different subjects}} \tag{1.1}$$

$$\text{FRR/FNMR} = \frac{\text{Comparison decision of 'non-match' for genuine users}}{\text{Total comparisons from same biometric subjects}} \tag{1.2}$$

$$\text{EER} = \text{Point}|_{\text{FAR=FRR}} \tag{1.3}$$

$$\text{GAR/GMR} = 1 - \text{FRR} \tag{1.4}$$

1.8 Organization of the thesis

This dissertation is structured based on a traditional background with coherent literature review on iris and fingerprint modalities, proposed methods with independent experimental

studies, and to conclude our investigation in the domain of template protection and verification on the basis of unimodal and multimodal biometric modalities.

The dependency among the thesis chapters is illustrated in Fig. 1.7. For example, reading Chapter 5 is required before reading Chapters 6. Following the guidelines given in Fig. 1.7

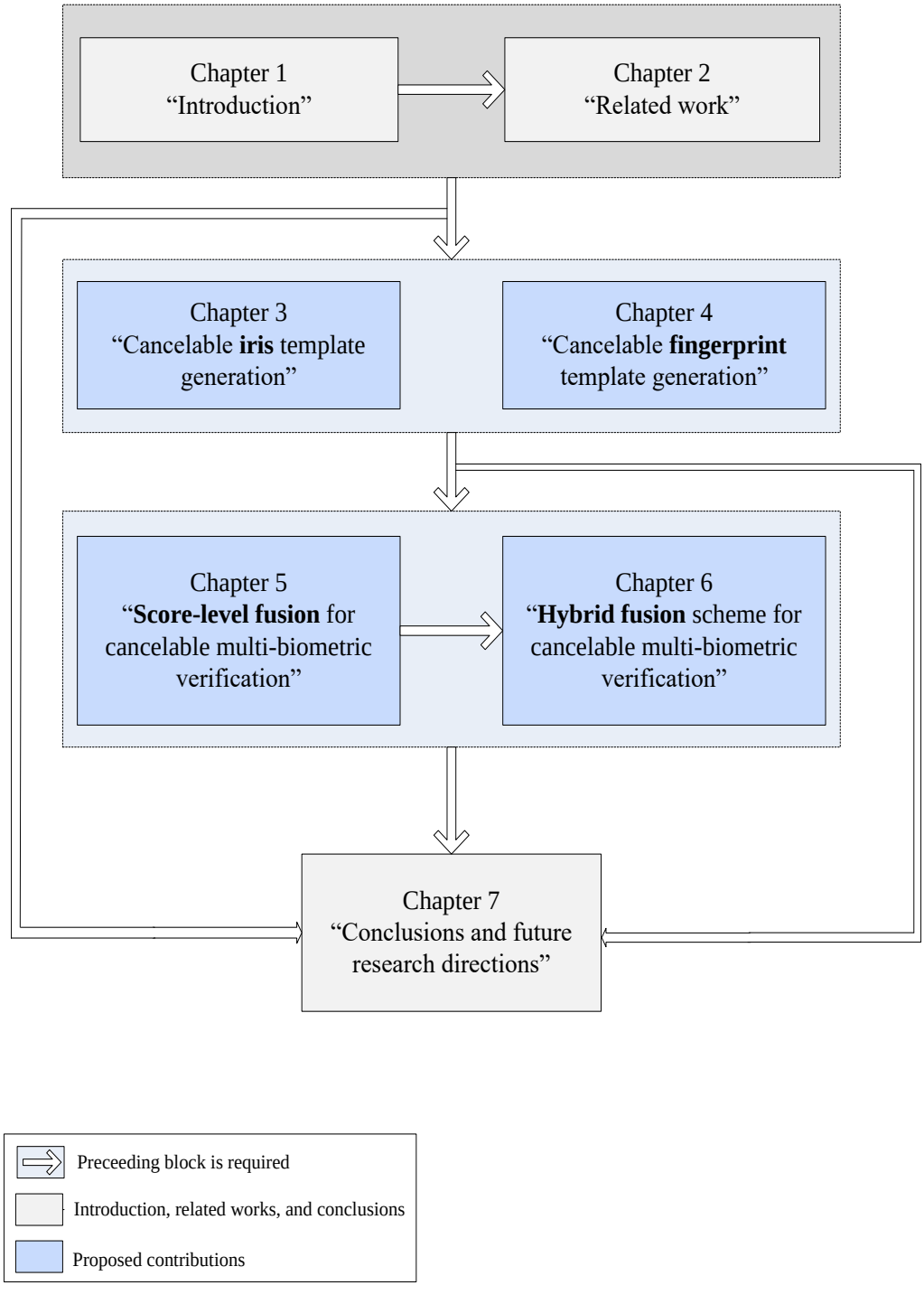


Figure 1.7: Dependency among thesis chapters

and assuming a background elaborated in chapter 1, one can optionally read the chapter 3, 4, 5, and 6 independently. This thesis comprises seven chapters including this introductory chapter. The rest of the thesis is organized as follows.

Chapter 2 : Related work

This chapter describes the existing methods for different template protection schemes for iris and fingerprint biometric modalities. We also discuss about different fusion mechanism for cancelable multibiometric systems.

Chapter 3 : Cancelable iris template generation

We describe the proposed canclable iris biometric template generation scheme based on 1-D log Gabor features and look-up table mapping based transformation. Experimental evaluations are also provided on different iris databases in this chapter.

Chapter 4 : Cancelable fingerprint template generation

The proposed cancelable fingerprint template generation scheme based on Cantor pairing and random projection is described in this chapter. The experimental results achieved from different fingerprint databases are also reported in this chapter.

Chapter 5 : Score-level fusion for cancelable multi-biometric verification

This chapter describes the proposed score-level fusion performed on cancelable iris and cancelable fingerprint biometric modalities. Alongwith, we provide the experimental results of secure multi-biometric verification method.

Chapter 6 : Hybrid fusion scheme for cancelable multi-biometric verification

In this chapter, we describe the proposed hybrid (score and decision) level fusion technique applied over cancelable iris and cancelable fingerprint biometric modalities. We also present experimental evaluations performed onto three virtual databases to validate the potential robustness of the method.

Chapter 7 : Conclusions and future research directions

This chapter concludes our study in the domain of biometric template protection for unimodal and multibiometric systems and discusses few potential future research directions.

Chapter 2

Related work

Several security breaches have been reported in last two decades against the common use of biometric-based authentication for different applications. As a consequence, biometric template protection has gained a great interest among the research communities, and several works have been done for iris and fingerprint modalities. The researchers started working on fingerprint template protection in 90's. Initially, the protected template had been derived from key binding or key generation schemes using fuzzy schemes (e.g. fuzzy commitment, fuzzy vault, and secure sketches). Thereafter, approaches on iris template protection were proposed by different research communities in late 90's. Multibiometric recognition methods alongwith the protected multibiometric approaches were also introduced for more secure and optimal performance extensively thereafter.

This chapter surveys existing work related to contributions made in this thesis. It covers cancelable iris template generation, cancelable fingerprint template generation, and cancelable multimodal verification methods. The organization of this chapter is as follows. First, a literature review on cancelable iris biometric verification is presented in Section 2.1. Section 2.2 reviews various approaches on cancelable fingerprint template generation. Section 2.3 encompasses the detailed description of different techniques for multimodal cancelable biometric based verification. Finally, a summary of existing work is provided in Section 2.4.

2.1 Cancelable iris biometric template generation

In the last few years, several approaches have been proposed to address various underlying concerns in protecting biometric templates by the biometric research community. The

approaches related to biometric template security presented in the literature can be classified into two categories namely, cancelable biometric [26, 54–62] and biometric cryptosystem [30, 32, 33, 63, 64]. In the following, we discuss the existing techniques for both of these two categories for iris biometric.

In literature, Zuo et al. [54] proposed four different non-invertible transforms namely GRAY-COMBO, BIN-COMBO, GRAY-SALT, and BIN-SALT. GRAY-COMBO method performs circular shift operation on Gabor features and random addition of rows. BIN-COMBO utilizes similar transformation on the iris codes with random shifting and XOR operations. Random patterns are added to the Gabor features in GRAY-SALT method and XORed with original iris code in BIN-SALT method.

Du et al. [55] applied a key on the original iris template which rearranges the bit positions to achieve irreversibility. The feature point map is created from the arranged bit positions. The average euclidean distance between the overlapping positions are evaluated to compute match scores.

A well-known approach for cancelable biometric is biohashing which derives a uniformly distributed random sequence using a hash key [26, 56, 57]. In biohashing, biometric input is mixed with token and discretized into a binary string. In non-invertible transform based approach, instead of storing the original biometric, the biometric data is modified using a one-way function and stored into the database to ensure security and privacy of the actual biometric trait.

Ouda et al. [58] derived BioCode by mapping randomly generated seed with biometric features evaluated using biohashing algorithm [26]. First, iriscodes are generated based on the widely used Daugman's method [65]. Next, position of significant bits are recorded by aligning adequate number of different iriscodes from the same subject. Next, the position vector is secretly encoded using a random seed. Finally, the random bit sequence is stored as a protected template. These transformations produce lower recognition performance for noisy biometric data.

Hammerle-Uhl et al. [59] applied two different transformations i.e. block re-mapping and image warping onto iris texture evaluated by applying the method proposed in Ma et al. [66]. In the first transformation, the blocks in the iris texture are mapped randomly. In other transformation, the texture is again mapped based on a mesh grid mesh superimposed

over it. A user-specific key is utilized to distort the texture by offsetting each vertex in the original mesh by some amount. In their another work, Hammerle-Uhl et al. [60] applied block permutation onto the source iris texture obtained using wavelet transform . These method [59, 60] were reported with significant performance degradation.

Rathgeb et al. [61] proposed block permutation on iris textures to protect the iris template. However, they improved the performance by applying bloom filter to generate an alignment-free cancelable iris template [67]. The method [67] suffers against the claim of unlinkability.

Recently, Lai et al. [62] proposed a non-invertible transformation for iris template protection namely Indexing-First-One (IFO) hashing inspired by Min-hashing [68]. In their method, first, Hadamard product operator is applied on two distinct permutations of IrisCode. Next, the IrisCode is divided into equal sized windows. Further, they record the first occurrence of bit '1' of multiple random tokenized permuted IrisCode in each window to derive a cancelable template.

In contrast, the schemes such as fuzzy vault [33], fuzzy commitment [32], and secure sketches [29] have been introduced for cryptosystem based template protection. Dodis et al. [29] applied a hash function on error-tolerant biometric input to attain non-invertibility. In this approach, two functions are proposed, namely, fuzzy extractor and secure sketches. Fuzzy extractor applies a hash function on biometric input to generate a random string. This random string is utilized as a key. In contrast, secure sketch uses this random string to reconstruct the original template.

Juels and Wattenberg [32] proposed a state-of-the-art scheme for biometric cryptosystem known as fuzzy commitment. This approach applies a function on the codeword and binary biometric input to generate the template. The codeword is prepared with error-correcting codes to eliminate bit-errors. In verification, the codeword is evaluated for the query biometric data and matched using error-correcting codes. Lately, Juels and Sudan [33] introduces an encryption method namely Fuzzy Vault. In their method, the secret message are fed to a polynomial say $P(X)$ and its coefficients. The values related to polynomial are evaluated for different X. Each value in X are selected such that it denotes the biometric original feature. The set of pairs of values i.e. (X', Y') are merged with a set of chaff points (C_F^P) to derive a cancelable template (i.e. $(X', Y') \cup C_F^P$) at the encryption end. At the decryption end, error-correcting codes are applied to extract the (X', Y') out of $((X', Y') \cup C_F^P)$.

Bringer et al. [30] applied fuzzy commitment scheme [32] with an improved error-correcting mechanism. In this approach, a matrix is formed with two different binary Reed-Muller codes. Next, a 2-D iterative min-sum decoding is performed to retrieve a 40-bit cryptographic key. Wu et al. [63] proposed an iris cryptosystem based on key generation. The iris feature vector is corrected with Reed-solomon codes. Then, a hash function is applied to generate a cipher key. Reddy and Babu et al. [64] derived a key using password based transformation to encrypt the fuzzy vault [33].

A summary of various template protection schemes related to iris biometric are reported in Table 2.1.

Table 2.1: Summary of different iris template protection techniques

	Author	Applied scheme	Dataset used	Remarks
Cancelable biometric	Zuo et al. [54]	GRAY-COMBO, BIN-COMBO, GRAY-SALT, and BIN-SALT	MMU1 database	High EER
	Du et al. [55]	Random re-mapping, Non-invertible transform	ICE 2005 IUPUI remote	High EER for IUPUI database
	Ouda et al. [58]	BioEncoding Non-invertible transform	CASIA v1.0	Vulnerable to correlation attacks
	Hammerle-Uhl et al. [59]	Block remapping and Image warping	CASIA-v3-Interval	High EER
	Hammerle-Uhl et al. [60]	Wavelet transforms 1. Parameterised filters 2. Wavelet packets	CASIA-v3-Interval	User-specific key

Continued to next page

Table 2.1 – continued from previous page

Author		Applied scheme	Dataset used	Remarks
	Rathgeb et al. [61]	Bloom filter based feature transformation	CASIA-v3-Interval Left eye (1332 subjects)	Do not provide unlinkability
	Lai et al. [62]	Indexing-first-one hashing Non-invertible transform	CASIA-v3-Interval	Privacy invasion for less-sized hashed code
Biometric cryptosystem	Bringer et al. [30]	Fuzzy commitment	ICE 2005	EER very high
	Wu et al. [63]	Fuzzy vault	CASIA v1.0	Hash encoding with error-correction
	Reddy and Babu [64]	Hardened fuzzy vault	CASIA v1.0 MMU1 Database	-

2.2 Cancelable fingerprint biometric template generation

In literature over last few years, a number of researchers have introduced different transformations to generate the cancelable template. Different methods concerning cancelable biometric based transformation [22–26, 28, 35, 42, 43, 69–80] and biometric cryptosystems [31, 81–85] have been proposed in recent years. We discuss the existing literature of cancelable biometric in the following.

First, Ratha et al. [35] introduced the notion of cancelable biometric with three different types of transformations (Cartesian, polar, and functional) to provide privacy and security to the original biometric information. The Cartesian transformation method maps the fingerprint minutiae into cells of fixed size. The minutiae positions in the cells are permuted to derive the cancelable template. In polar transformation method, the minutiae positions are mapped onto a polar coordinate space. Further, the coordinate space is divided into sec-

tors, and sector positions are shuffled based on a key to generate the cancelable template. Functional transformation method alters the minutiae positions and orientation based on a parametric Gaussian function.

Boult et al. [69] proposed secure biotokens for fingerprint template protection. The method constructs a minutiae pair table which contains distance, relative orientation, and orientation of the line connecting two minutiae points. The features are then divided into quotient and modulus part. The quotient part is encrypted using RSA algorithm and modulus part is concatenated with the encrypted quotient to form a cluster. In verification stage, minutiae pair tables of the query and stored templates are traversed to construct clusters and to compute the comparison scores.

Lee et al. [70] proposed an alignment-free protected fingerprint template generation scheme using minutia orientation. They applied two different changing functions (i.e., positions and respective orientations) which are used to secure the minutiae information. A user-specific PIN is used for input to both changing functions. The stored template can thus be regenerated and revoked by altering the input parameters of the changing functions in the situation of compromise.

In BioHashing based approaches [26, 28], first, the original biometric template is exploited to inner product with the projection matrix. Next, a bit string is generated after discretization using a threshold determined experimentally. Later, Biohashing has been applied over other different biometric modalities for template protection.

Yang et al. [71] proposed a non-linear dynamic random projection scheme to increase the computational complexity against the inversion attack. Instead of conventional random projection utilized by BioHashing [26, 28], the projection matrix is dynamically constructed based on an index vector. From each index, a set of random vectors is used for projection. An index vector is created so that the imposter has no clue about the selected columns from the projection matrix.

Lee et al. [72] presented a method to derive cancelable fingerprint template based on 3-D array mapping. In this work, a minutia from the minutiae set is assigned as the reference, and remaining minutiae are aligned with respect to the reference minutiae. Then, the aligned minutiae points are mapped into a 3-D array based on the positions (*x*-*y* co-ordinate) and orientations of the minutiae points. The cells in the 3-D array are marked as 1, which include

minutiae points. The array is sequentially traversed to derive a bit-string. The derived bit-string is exploited to random permutation utilizing a user-specific PIN and minutiae type.

Wang et al. [73] proposed a template protection mechanism where many-to-one mapping is applied onto the pair-minutiae based bit-string evaluated using the method proposed by Jin et al. [86]. Next, discrete Fourier transform (DFT) has been applied to derive a complex vector. Then, a user-specific PIN is exploited over the complex vector to generate the protected template. Wang et al. [24] proposed another method for cancelable fingerprint template design using circular convolution. The procedure adopted till bit-string generation is identical to it's earlier method [73]. Then, a random sequence is derived by utilizing a user-specific PIN. Bit-string and random sequence are exploited to DFT, and product of both DFT's are computed. The cancelable template is stored by applying inverse-DFT and removing the first $(p-1)$ points from the output.

Das et al. [42] constructed a graph structure based on the minimum possible distance from core/delta point to remaining minutiae points. Hash values with minimum distances in the graph structure are stored as a protected template. Correspondence search algorithms [42] are used for verification of query template.

Liu et al. [43] proposed a template protection scheme which derives a protected fixed-length template viz., random local region descriptor (RLRD). In this scheme, a random reference point is selected initially. Next, Tico's sampling structure [87] is utilized to generate uniformly distributed sampling point structure around the random reference. The order of the sampling points is decided through a random seed. Finally, a protected template is derived as the angular width between the reference and sampling points. Further, gray-code encoding of sine and cosine of angular width is performed to generate a bit-string.

Wong et al. [75] proposed a multi-line code (MLC) for minutiae-based fingerprint template protection which is an extension of Wong et al. [74] work. In this method [74], the minutia set is divided into angular partitions with respect to a straight line drawn at the reference minutiae. Next, few sample points with equal distance to each other are taken with uniform distribution on the straight line. Circles are constructed on each of the sample points, and minutiae points falling in each lower region (semi-circle) are counted. A binary string is derived considering 1 if the count is greater than 0, and 0 otherwise. The result is stored as the cancelable template. In their extended work [75], the mean distance from minutiae to

the line is computed in each semicircle along the lines. The quantization is performed over the mean distances. The binary string is derived and permuted with a user-specific PIN to generate the cancelable template.

Ahmad et al. [76] proposed a cancelable fingerprint template design scheme using relative minutiae information in the polar coordinate system as described in [88]. In their method, the pair minutiae points greater than a predefined distance are selected first. Next, invariant features (distance, angle between line-segment to reference axis, and angle between minutiae orientation to line-segment) are employed to many-to-one sector mapping for template protection.

Farooq et al. [77] proposed a triangular transformation which derives a binary representation of minutiae features. The method utilizes the minutiae triplet features: length of each side, the angle subtended between each side, each minutiae orientation in the triplet, and the height of triplet. These features are quantized into 24 bits to derive a 2^{24}-bit binary representation. Further, three transformations (mutation, random permutation, and encryption by MD5 or SHA-1) have been performed to derive the protected template.

Sutcu et al. [78] introduced a geometric design which represents minutiae information into a fixed length string. The method computes mean of minutiae x and y coordinate as centroid. Next, a circle is constructed centered at centroid and divided into an arc of equal angular width. Then, a straight line is drawn in between each minutiae pair, and intersection with the circumference is marked. The number of intersection mark is collected sequentially for each arc to derive the transformed template.

Wang et al. [23] proposed a scheme which utilizes DFT for pair-minutiae bit string. In their work, the feature extraction is followed from the method proposed in [86]. Next, DFT is exploited to derive a complex sequence. Further, the complex sequence is fed to Finite-Impulse-Response (FIR) with a user-specific key to derive the protected template. The method performs optimally yet weak against attack via record multiplicity (ARM). In their future work, Wang et al. [79] conceived the same methodology till complex sequence generation. Next, the partial Hadamard based transformation is applied to protect original pair minutiae bit-string.

Sandhya et al. [80] proposed two different transformation which applies quantization over Delaunay triangle's features. Then, the quantized features are mapped to a 3-D array.

Next, the 3-D array is traversed in row-major oder to produce fixed length 1-D bit string. Finally, DFT is employed over 1-D bit string to derive protected template. In another work, Sandhya et al. [89] presented a protection method by integrating local minutiae structure and distance structure. The bit-strings derived are combined using a user-specific PIN to derive a protected template.

Cappelli et al. [90] introduced a state-of-the-art Minutiae Cylinder Code (MCC) algorithm which frames a 3-D cylindrical structure around minutiae neighborhood considering each minutia as a reference. Each cylinder of height (2π) and radius (r) is tessellated into a number of cells. Each cell stores the minutiae position and orientation in the neighborhood of each minutia taken as a reference at a time. A cylinder which contains less valid information is discarded. Two cylinders are verifiable if direction difference between two minutiae is less than a certain value. MCC is a fixed radius local minutiae construct which provides notable recognition performance.

Ferrara et al. [22] then proved that few genuine minutiae points (approximately 25.4%) could be correctly revealed by calculating likelihood between two cylinders. Later, a novel representation namely Protected-MCC (P-MCC) is proposed where a non-invertible transform has been applied onto MCC template incorporating binary-KL projection which provides a greater level of security and privacy. To overcome the non-revocability concern of P-MCC, Ferrara et al. [25] proposed a two-factor protected Minutiae Cylinder Code (2P-MCC) scheme which performs curtailed permutation onto cylinders in P-MCC using a secret key. This 2P-MCC method has a simpler implementation based on scrambling the bits using a secret key. Also, it allows a optimal trade-off between performance and security.

The current state-of-the-art concerning biometric cryptosystem is based on Fuzzy Vault and Fuzzy Commitment schemes. These two schemes, fuzzy vault and fuzzy commitment are proposed by Juels and Sudan [33] and Juels and Wattenberg [32], respectively. Fuzzy vault scheme involves the union of minutiae encoding using chaff points and polynomial projection whereas fuzzy Commitment stores biometric feature along with hash of identifiers and parity bit-string.

Li et al. [81] proposed a fingerprint based cryptosystem which utilizes fuzzy vault scheme. In their work, they employed orientation minutiae descriptor [87] and local minutiae structure [91] (relative distance, radial angle, and minutiae orientation) as invariant features.

Chaff points are merged with local structure and Huffman encoding is applied over descriptor. Further, both transformed descriptors are integrated to form a protected template.

Li et al. [82] proposed a cryptosystem where two stage fuzzy vault is applied over pair-polar minutiae descriptor considering each minutiae point as a reference. In the first stage, a cryptographic key is binded with the pair-polar structure by dividing the feature string and cryptographic key. Next, Shamir's secret sharing [92] is applied in the second stage. Finally, the protected template contains the union of these two outputs.

Yang et al. [83] considered Voronoi neighbor structures (VN_s) over minutiae points. They utilize only distinct triangles in the Voronoi structure. Next, VN_s are mapped into a three-dimensional (3D) array to generate fixed length binary string. Finally, template protection is achieved by using PinSketch [31] over bit string.

Jin et al. [84] derived cancelable template by extracting the invariant features and applying non-invertible transformation using their previous work [93]. The features involve minutiae quadruples. Next, the derived transformed template is divided into equal-sized blocks. Then, cryptographic key is blended with each block and finally concatenated each block to derive final cancelable template.

Arakala et al. [31] introduced a novel scheme which first evaluate minutiae descriptor and applied PinSketch scheme for fingerprint authentication. The enrollment process contains three operations including XOR, PinSketch, and pairwise hash operations. First, the minutiae positions are XORed with a random codeword generated using Bose, Chaudhuri, and Hocquenghem (BCH) codes. Next, it is fed to the PinSketch where syndrome based error-correction has been applied. Finally, the pairwise hash function using a random seed is applied to generate the hashed output. Hashed output, XORed output, and PinSketch encoded output is stored as a protected template.

Imamverdiyev et al. [85] evaluated Gabor filter-based FingerCode, a local binary pattern (LBP), and a local direction pattern (LDP) based features from fingerprint. Next, reliable bits are selected from the evaluated bit patterns from these three techniques. Then, Fuzzy Commitment Scheme is applied over the reliable bit-string to derive the protected template.

Recently, Akdogan et al. [94] introduced two novel biometric key agreement protocols namely, Secure Key Agreement-Pure Biometrics (SKA-PB) and Secure Key Agreement-Cancelable Biometrics (SKA-CB) to handle the unordered set of fingerprint features.

We summarize the existing cancelable fingerprint generation and biometric cryptosystem schemes in Table 2.2.

Table 2.2: Summary of different fingerprint template protection techniques

	Authors	Applied scheme	Dataset used	Remarks
Cancelable biometric	Ratha et al. [35]	Cartesian, polar and functional transformation	IBM 99 optical database	Rely on core/delta point
	Boult et al. [69]	RSA encryption	DB1 & DB2 of FVC2000, FVC2002 and FVC2004	High EER for all datasets
	Lee et al. [70]	Changing functions for position and orientation	FVC2002 DB1	Performance degrades for stolen-token PIN
	Jin et al. [28]	Biohashing	FVC2002	Privacy invasion if unique seed is compromised
	Yang et al. [71]	Non-linear dynamic random projection	FVC2002 DB2	Susceptible to ARM attack
	Lee et al. [72]	3-D array mapping	FVC2004	User-specific PIN
	Wang et al. [73]	Random projection based mapping	DB1-DB3 of FVC2002	User-specific PIN
	Wang et al. [24]	Curtailed circular convolution	FVC2002 DB1-DB3	User-specific PIN
	Das et al. [42]	Minimum distance graph from core/delta	DB1 & DB2 of FVC2002	Performs poor for low-quality fingerprint
	Liu et al. [43]	Local region structure around core/delta	DB1-DB3 of FVC2002	Rely on core/delta point
	Wong et al. [74]	Line-code generation	DB1 & DB2 of FVC2002, DB1 of FVC2004	EER very high; Large storage required

Continued to next page

Table 2.2 – continued from previous page

Authors	Applied scheme	Dataset used	Remarks
Wong et al. [75]	Binarized line-code generation	DB1 & DB2 of FVC2002 and FVC2004	High computation cost
Ahmad et al. [76]	Pair-polar co-ordinate transformation	FVC2002 DB1-DB3	High EER for FVC2002 DB3
Farooq et al. [77]	Minutiae triplet features; Bit-string generation	FVC2002 & FVC2004	High computation cost
Sutcu et al. [78]	Geometric transformation	Synthetic test dataset	Prone to security threats
Wang et al. [23]	Parametrized FIR filter applied onto bit-string features	DB1-DB3 of FVC2002	User-specific PIN
Wang et al. [79]	Partial Hadamard transform	DB1-DB3 of FVC2002	User-specific PIN
Sandhya et al. [80]	3-D array transformation on Delaunay triangle features	FVC2002 & FVC2004	Performs poor for low-quality fingerprints
Sandhya et al. [89]	Local and distant structures; Bit-vector quantization	FVC2002 & FVC2004	Quantization errors
Ferrara et al. [22]	Binary K-L projection onto MCC templates	FVC2002, DB2 of FVC2006	Hill-climbing attack
Ferrara et al. [25]	Random permutation on PMCC templates	FVC2002, DB1 of FVC2004, DB2 of FVC2006	-

Continued to next page

Table 2.2 – continued from previous page

	Authors	Applied scheme	Dataset used	Remarks
Biometric cryptosystem	Arakala et al. [31]	Fuzzy extractor; Minutiae descriptor	FVC2000, Private database	Quantization errors; Prone to security threats
	Li et al. [81]	Fuzzy vault, minutiae local descriptor	DB1 & DB2 of FVC2002	Large storage required
	Li et al. [82]	Fuzzy vault, Pair-polar minutiae structure	FVC2002, DB2 of FVC2004, DB2 and DB3 of FVC2006	Large storage required, Low performance
	Yang et al. [83]	Secure sketch; Modified Voronoi structure	FVC2000 DB1, FVC2002, DB2 of FVC2004	Fake local structure due to Voronoi distortion
	Jin et al. [84]	Chaffing and winnowing; Graph based Hamming embedding	FVC2002, DB2 of FVC2004	Low performance, Prone to different attacks
	Imamverdiyev et al. [85]	Fuzzy commitment; Reliable bit extraction	FVC2000	Discretization errors
	Akdogan et al. [94]	Secure key agreement	Verifinger sample database	High computation cost

2.3 Multimodal cancelable biometric system

In multimodal cancelable biometric system, multiple protected modalities are utilized for user authentication. In recent years, different methods have been proposed for cancelable multibiometric based authentication [95, 96] to achieve performance enhancement and template protection simultaneously. For multimodal biometric system, fusion can be performed at five different levels, namely, sensor, feature, decision, rank, and match-score levels [19]. We discuss the current state-of-the-art work on multimodal biometrics and multimodal cancelable biometrics for three possible levels of fusion [97]: (1) fusion at feature level, (2) fusion at score level, and (3) fusion at decision level, in the following.

2.3.1 Feature level fusion

Fusion at feature level refers to integrate different feature strings obtained from either multiple sensors for the same biometric trait, multiple instances of the same biometric trait, multiple units of the same biometric trait or multiple biometric traits. Here, verification is performed on the basis of this combined feature vector into the genuine or impostor category. Lately, several methods such as [89, 98, 99] utilized a user-specific PIN to combine features from different biometric modalities. The methods proposed in [95, 96, 100, 101] applied AND/OR rules to perform feature integration. In contrast, cryptographic techniques such as Fuzzy vault, Fuzzy Commitment, and Secure-sketch based schemes have also been applied to derive multibiometric templates in literature [102, 103]. Othman et al. [104] acquired two fingerprint impressions from two different fingers to create a new protected identity. Camlikaya et al. [105] incorporated feature level fusion over voice and fingerprint by evaluating mel frequency cepstral coefficients (MFCCs) from voice and minutiae points from fingerprint. The binary feature coefficients from voice are mapped to x-y coordinate positions by dividing each binary feature descriptor of a users into groups of 16 and using each 16 bits to generate one point (X,Y) in the 2-dimensional space. Next, the minutiae information is embedded into the computed voice features for privacy preservation. Rathgeb et al. [67] proposed a feature level integration scheme which evaluate iriscodes by applying two different feature extraction mechanisms [50, 66]. First, the iriscodes obtained from different biometric feature vectors are mixed together based on a user-specific key. Further, the mixed bit-string are mapped to bloom filter to derive a protected bit-string. In recent years, Rathgeb et al. [106] proposed Bloom filter-based integration scheme to combine face and iris features. However, ongoing research has been shifted to other fusion mechanism such as score/decision fusion due to the dependency over user-specific PIN and low performance in comparison to other fusion mechanism.

2.3.2 Score level fusion

Score level fusion combines match scores obtained from different classifiers/matchers. The verification is performed based on the fused or combined score value. In the last few years, approaches incorporating score level fusion [47–49, 107–125] have been extensively investi-

gated. However, works on score fusion for protected modalities have been scarcely reported. Existing score level fusion follows three different schemes. These include transformation-based, density-based, and classifier-based fusion schemes [19]. Here, we have discussed these score level fusion approaches since we have utilized these methods for comparison to our method.

2.3.2.1 Transformation based approaches

In these approaches, first, match scores are normalized to a common domain (e.g. in the interval [0,1]). Next, the fused score is derived by weighting different match scores, and this combined score is utilized for authentication. The approaches proposed in [107–116], have utilized the transformation based approaches for match-score level fusion.

Toh et al. [107] utilized weighted-sum rule-based fusion for hand geometry, fingerprint, and voice biometric. Four learning and decision scenarios have been investigated. The authors employed a model which requires a single training step for the verification. The experiments carried out show approximately 50% improvement over equal error rate (EER).

Snelick et al. [108] proposed an adaptive normalization procedure which is utilized to increase the separation between genuine and imposter distributions in the range [0,1]. This procedure is carried out using three functions: Two-Quadrics (QQ), Logistic, and Quadric-Line-Quadric. Next, different fusion techniques such as simple-sum, min-score, max-score, matcher weighting, and user weighting are applied for fusion onto face and fingerprint biometric modalities for 1000 subjects.

Jain et al. [109] analyzed the performance of existing normalization techniques and fusion methods for face, fingerprint, and hand geometry-based multimodal biometric system. The authors performed experimentation on a 100 user database. Further, they reported that tanh normalization followed by the simple sum of score fusion method gives better performance in comparison to other normalization techniques.

Lobrano et al. [110] introduced a new index named Score Decidability Index (SDI) which computes the coefficients of the linear combination for each classifier and pattern. SDI denotes the confidence with which a score value belongs to positive or negative distributions. Next, SDI values for different classifiers for a single pattern are exploited to averaging operation to derive fused score. For integration, mean-rule fusion method is utilized for fusion.

Poh et al. [111] proposed a novel normalization procedure which first, categorizes the user scores based on joint density computation. Next, F-norm is applied to estimate group-specific mean by maximum-a-posteriori (MAP) computation. Further, experimentations are performed on face, iris, and fingerprint modalities. In their another work, Poh et al. [126] applied a Gaussian Mixture Model-based fusion classifier. Next, B-ratio for each possible combination is evaluated and OR-switcher is utilized for fusion.

Hanmandlu et al. [113] utilized fuzzy triangular membership function for normalization. Next, they applied Einstein product t-norm on hand geometry, palmprint, and hand vein modalities. In their another work, Hanmandlu et al. [112] first, normalized the scores in the interval of [0,1] using min-max normalization technique. Next, they applied different variants of t-norm (such as Frank, Yager, Hamacher, Einstein product, and schweizer-sklar) to claim the potential usefulness of the t-norm based integration.

Wang et al. [114] applied Aczél-Alsina (AA) t-norm [114] to fuse match score information for dual iris and face biometric modalities expanding the interval between genuine and imposter distribution. In their method, combined features from dual iris and combined features from face (thermal face, visible face) are evaluated using 1-D log Gabor filter [50] and Gabor wavelets, respectively. Next, scores are computed and are then integrated using AA t-norm for verification.

Peng et al. [115] proposed constructed a virtual database of multiple finger biometric sources named: finger vein, fingerprint, finger-shape, and finger-knuckle. Before fusion, matching scores of the four biometric features are normalized into the range [0,1]. Then, t-norm based score-level fusion is applied for authentication. The authors claimed that Sugeno–Weber t-norm outperform other t-norms.

Kabir et al. [116] proposed two different score normalization techniques based on the overlap region between the genuine and impostor scores. Next, a novel confidence-based weighting technique based on the confidence value of the matching scores is applied which considers the mean-to-maximum of genuine scores and mean-to-minimum of impostor scores. Further, the evaluations are carried out onto three biometric traits, fingerprint, palmprint, and earprint.

A summary of transformation based multibiometric score fusion techniques are reported in Table 2.3.

Table 2.3: Summary of different transformation based score fusion techniques

Authors	Fused modalities/ Representations/ Features	Fusion scheme/ Methodology	Remarks
Toh et al. [107]	Hand geometry, fingerprint and voice	Weighted-sum rule	Selection of optimal threshold is required
Snelick et al. [108]	Adaptive normalization using two-quadratic, logistic and Quadric-Line-Quadric	simple-sum, min-score, max-score, matcher weighting, and user weighting schemes	Not suitable for open environment
Jain et al. [109]	Existing normalization techniques	Sum rule	Performance relies on kernel type and width
Lobrano et al. [110]	Score Decidability Index (SDI)	Mean rule	High FAR value corresponding to low EER
Poh et al. [111]	Face, fingerprint and iris	Group-specific score normalization	Deterministic partitioning of clients
Poh et al. [126]	Gaussian mixture model	OR switcher	Implicit Gaussian assumption on the score distribution
Hanmandlu et al. [112, 113]	Fuzzy triangular membership; Min-max normalization	Different Variants of t-norm	Low performance, High EER
Wang et al. [114]	Dual iris features from 1-D log gabor and face features from Gabor wavelets	Aczél-Alsina (AA) t-norm	Optimal parameter selection required
Peng et al. [115]	Finger-vein, finger-shape, fingerprint, finger-knuckle	t-norm	High EER value
Kabir et al. [116]	Fingerprint, palmprint and earprint modalities	Overlap-based anchor normalization; Confidence-based weighting	Prior information on genuine, imposter, score distribution is required

2.3.2.2 Classification based approaches

In these approaches, scores obtained from different matchers for the same subject are concatenated to form a feature vector. Next, a classifier is utilized to differentiate between

genuine and imposter users. The approaches proposed in [47, 48, 117–122] utilized the Classification based approaches for match-score level fusion.

Ma et al. [47] proposed an improved classifier using a tree model in a random forest. Each tree in a forest represents a classification axiom. The tree grows until the terminal node with the decision is reached based on the splitting rule. Beginning with Tree 1, we iterate the procedure for N^{th} tree in the forest. Next, number of votes are counted for the two classes. The class with higher number of votes is the verification output.

Tronci et al. [48] proposed a method which dynamically selects the matching score to provide a better separation between genuine and imposter. The selector provides a better separation in terms of area under ROC curve (AUC) providing smaller errors than individual matchers. The experiments are performed onto fingerprint modality.

In literature, many authors have applied DS theory [127–129] based fusion to combine modalities. DS theory combines evidences by computing the basic belief assignment (BBA) of each individual's score. Singh et al. [118] applied DS theory scheme on four different classifier outputs for fingerprint: minutiae-based verification, ridge-based verification, fingercode based verification, and pore-based verification. For each fingerprint image, each of the four classifier assigns a label true i.e. 1 to proposition i if $i \in T$, and remaining classes are assigned a label false i.e. 0. Next, the respective BBA are computed and combined using DS rule for verification.

Nguyen et al. [117] applied DS theory based fusion on match scores obtained from face, fingerprint, and iris. The authors evaluated three mass values corresponding to genuine class, imposter class, and uncertainty. Uncertainty mass is evaluated considering quality score and recognition performance of the particular biometric modality.

Miao et al. [119] proposed a fusion mechanism based on three kinds of bin-based classifiers: continuous, discontinuous, and pair-wise. These bin-based classifiers maps the match scores into a high-dimension space to reveal the hidden info associated with match scores. Further, high dimension match scores are integrated using ensemble learning methods such as AdaBoost. The authors performed experimentation on face and iris modalities.

Recently, Kumar et al. [120], Mezai et al. [121], and Sadhya et al. [122] have proposed the approaches concerning transformation-based score fusion. Kumar et al. [120] investigated ACO to evaluate weights for different biometric modalities taking part in the fusion. The four

fusion rules are considered for combination i.e. sum, product, exp, and tanh. Further, the appropriate weights for these four rules are evaluated for score fusion. Mezai et al. [121] performed score level fusion utilizing Denoeux model [130] to transform the match scores into belief assignments. Finally, DS theory and proportional conflict redistribution (PCR) rules of combinations are applied to integrate the belief assignments. Sadhya et al. [122] considered four soft biometric traits for combination i.e. height, weight, age, and gender. Further, they applied Bayesian classifier with modified conditional probability function. Gaussian probability function and log based weighted fusion are used to achieve better performance.

The classification-based score fusion approaches are summarized in Table 2.4.

Table 2.4: Summary of different classification based score fusion techniques

Authors	Fused modalities/ Representations/ Features	Fusion scheme/ Methodology	Remarks
Ma et al. [47]	Random tree forest	Voting scheme	Requires exhaustive training
Tronci et al. [48]	AUC features	Dynamic score selection	Exhaustive searching required
Singh et al. [118]	Basic belief assignment	DS theory	Large amount of training time required
Nguyen et al. [117]	Genuine mass, imposter mass, uncertainty mass with quality score	DS theory	Performance degrades for low quality images
Miao et al. [119]	Ordinal iris+LBP face	Bin-based classifiers	Insufficient training samples may lead to incorrect decision
Kumar et al. [120]	ACO based weight estimation	Sum, product, exp, tanh rules	Misclassification due to overlap region
Mezai et al. [121]	Belief assignment	DS theory with PCR rules	Incorrect selection of confidence parameters degrades the performance
Sadhya et al. [122]	Minutiae features+SURF face features+BMI for soft biometric	Bayesian classifier; Conditional probability function	-

2.3.2.3 Density based approaches

In these approaches, scores from multiple matchers are concatenated to form a feature vector. Next, match-score densities are evaluated to form a set of training scores. The approaches proposed in [49, 123–125] have employed the classification based approaches for match-score level fusion. The existing approaches in literature utilize kernel density estimator (KDE) or a mixture of Gaussians (MOG) for density estimation.

Nanni et al. [123] utilized MOG [131] estimation using expectation-maximization (EM). Next, support vector machine (SVM) and AdaBoost of neural network classifier are applied on fingerprint, palmprint, hand geometry, and face biometric traits. Likelihood ratio test along with a random subspace of different classifiers is applied for integration.

Nandakumar et al. [49] used a Gaussian mixture model for genuine and imposter density estimation. Next, likelihood ratio fusion rule is applied to match scores and estimated densities. The integration is performed for face, iris, fingerprint, and speech modalities.

Dass et al. [125] proposed a modified kernel density estimator in which the marginal density is computed as a mixture of continuous and discrete components. Next, the joint density is estimated using copula functions. Further, fusion is performed by combining the marginal densities using product rule. Experimental evaluations are carried out on MSU-multimodal and NIST-multimodal databases.

Tao et al. [124] introduced a method for multibiometric score fusion which involves computation of likelihood ratio under Naive Bayes approximation. Likelihood ratio has been computed directly by ROC curves of individual classifiers involved in the fusion using a limited number of operational points. The authors carried out their evaluations on 2-D and 3-D face, face video, and speech biometric modalities.

A summary of different density-based methods are presented in Table 2.5.

2.3.3 Decision level fusion

Information fusion at decision level occurs where each classifier/matcher independently adduces its decision. The classifier/matcher can make out either positive or negative class for accepting or rejecting a user in a context of biometric based authentication systems. In the last decade, several methods for decision level fusion applied over single biomet-

Table 2.5: Summary of different density based score fusion techniques

Authors	Fused modalities/ Representations/ Features	Fusion scheme/ Methodology	Remarks
Nanni et al. [123]	Mixture of Gaussian	Sum rule	Insufficient decision if limited number of samples
Nandakumar et al. [49]	Gaussian mixture model	LR fusion rule	Complex density estimation
Dass et al. [125]	Kernel density estimator	Product rule	Incorrect model leads to deficient fusion rule
Tao et al. [124]	LR from ROC curves	Naive LR test	-

ric trait have been extensively investigated. These methods include AND/OR rule [132], majority voting [133–135], Behavior-Knowledge Space method [136, 137], Bayesian classifier combination [138], fuzzy integrals [139, 140], and Dempster-Shafer theory of evidence [128, 141, 142]. However, work on decision fusion for cancelable modalities have been scarcely reported.

A very few methods have been reported in the literature under decision level cancelable multibiometric verification. Kelkboom et al. [95] applied AND/OR rule-based fusion for the protected modalities. Gomez-Barrero et al. [96] proposed a novel framework for template creation, template encryption, and verification after decision fusion using OR rule of fusion. The 'AND' rule agrees upon if and only if all the classifiers categorize the input in the same class. In contrast, the 'OR' rule assign the input to the class if at least one of the classifiers categorizes the input for the same class. These two combination methods are the simplest among all methods of decision level integration for different classifiers.

2.3.4 Hybrid fusion

Hybrid fusion involves two or more fusion schemes to overcome the limitations of the individual fusion schemes if applied in combination. In literature, only few researchers [143–147] have proposed hybrid multibiometric systems which are utilized for comparison to our method and are described in the following.

Tao et al. [143] introduced a unique way of hybrid fusion by integrating multiple Receiver Operating Characteristics (ROC) curves. First, ROCs for different modalities are derived by their match scores. Next, the integration is performed using AND and OR rules with the optimal operating points and thresholds. Next, the optimal thresholds are applied while fusing to compute overall detection rate. This method is evaluate on face databases.

Azom et al. [144] applied hybrid feature level and score level fusion mechanism onto face and iris biometric modalities. First, the features from face and iris are extracted by applying PCA, LDA, LBPH, spPCA, and mPCA methods. Next, feature level integration is performed for different features for iris and face biometrics individually. Next, score fusion is performed onto match scores obtained from LDA for face and LBPH for iris. Next, sum rule is applied for hybrid fusion.

Grover et al. [145] proposed a hybrid fusion approach where the error rates are integrated for different threshold points using the PSO algorithm. First, Frank T-norm has been applied onto the scores of left and right finger-knuckle-prints. Next, hybrid PSO [148] is utilized on fused left and fused right finger-knuckle-print scores. The error rates for different threshold values are converted into the fuzzy sets using triangular membership functions. Further, global fuzzy error rates are computed by utilizing total distance criterion (TDC).

Razavi et al. [146] proposed an hybrid rank and decision fusion method to integrate vein patterns from both hands. First, the binarized statistical image features (BSIFs) algorithm is used to extract features. Next, true positive identification rank has been evaluated based on the CMC curve by sorting match scores. Simultaneously, a 'top rank-decision matrix' is constructed for rank of each identifier to calculate the value of importance. Further, identification is performed using computed weight and importance value.

Recently, Kabir et al. [147] proposed three different hybrid fusion methods based on feature and score level fusions. In their first method, feature level fusion is applied on the features extracted from different biometric modalities initially. Next, features corresponding to the lowest EER are encoded to the fused output for hybrid integration. In their second method, the genuine and imposter scores are separated from fused feature set and lowest-EER feature set. Next, confidence for genuine and imposter scores are evaluated to compute the weights. Further, score fusion is performed for user verification. In third, sum rule is applied on scores obtained from the fused feature set and the lowest-EER feature set.

Table 2.6: Summary of different hybrid fusion techniques

Authors	Fused modalities/ Representations/ Features	Fusion scheme/ Methodology	Remarks
Tao et al. [143]	ROC curves; Operating point and threshold	AND rule & OR rule	Low performance
Azom et al. [144]	PCA, LDA, LBPH, sp-PCA and mPCA features	Sum rule	Large feature vector; More execution time
Grover et al. [145]	Topothesy-fractal dimension features	Frank t-norm for score fusion and PSO for decision fusion	Exhaustive empirical evaluations
Razavi et al. [146]	BSIFs features	Top-rank-decision matrix; Importance value estimation	Best suited for identification only
Kabir et al. [147]	Earprint, palmprint and fingerprint features	Lowest EER-based feature fusion; Confidence-based weighting for score level and sum rule for decision fusion	High FAR value

A summary of different hybrid fusion methods for multibiometric verification are reported in Table 2.6.

2.4 Summary

In this chapter, we present a survey on cancelable template generation techniques with iris, fingerprint, and multimodal traits under feature transformation and biometric cryptosystem mechanism. Cryptographic methods are not suitable for cancelable templates as they reform the template and generate a poor matching rate. Hence, we have focused on feature transformation mechanism for cancelable template generation in our work. From the survey of cancelable iris template generation schemes, we can observe that existing methods underperform due to rotational inconsistencies caused by tilt head while capturing the image. Even for genuine subject, it may result in poor intra-class Hamming distance causing performance degradation. The different attacks such as hill-climbing, correlation or stolen-token attacks can be launched for illicit use of biometric data which reduce the reliability of the system. In literature, several template protection methods are reported for fingerprint biometric. In

existing techniques, the alignment, translation, and scale deformations present in the input fingerprint samples can degrade the performance. To manage these deformations, majority of the existing approaches utilize the core and delta points (singularities) of an input fingerprint for registration. However, it is not possible to identify the singular points from fingerprint images of all subjects. Moreover, the accurate detection of core point from an arch type or a poor quality fingerprint image is a challenging task. Few approaches in the literature utilize fixed-radius transformation. These approaches may cause performance degradation if the minutiae points are on the edge of the radius. Due to noise or local distortion these minutiae could be considered inside the radius for first sample and outside the radius for second sample for the same fingerprint. Additionally, a number of approaches failed to yield a perfect, non-revocable, and secure cancelable template. The template can be reconstructed against different attacks such as Attack-via-record-multiplicity (ARM), pre-image, and cross-matching attack. Finally, under cancelable multi-biometric, there exist three possible level of fusion. Most of the feature level multimodal protection approaches involve concatenation, random projection or transformation based on a user-specific PIN for privacy protection. These approaches lead to a minor performance improvement over the unimodal biometric system. Moreover, if a protected multi-biometric template gets compromised, there is no possibility to prevent the loss of original biometric information. For score level integration methods, the limitation lies in the complex density estimation for density based methods. Also, it may suffer from the local minimum problem. Few classifier based approaches provide an incorrect decision in scenarios where sufficient training samples are absent. However, score level fusion is favored owing to the factors such as ease of fusion and freedom to choose any feature extraction and matching algorithms. Despite many benefits, many commercial firms provide access only on the basis of the final decision or recognition output. Further, if the involved matchers are non-homogeneous or do not have the same scale, score level fusion becomes a challenging task. Hence, there is a need of a hybrid fusion involving score level as well as decision level fusion which would overcome the limitations of the score as well as decision fusion if a combination of both fusion mechanism is employed.

Chapter 3

Cancelable iris template generation

Biometric-based recognition systems have overcome major issues of traditional human authentication systems. However, security theft and privacy invasion are two passive issues that still persist in effective deployment of biometric-based authentication systems. To overcome these issues, we propose a novel cancelable iris template generation method which employs a mapping between a decimal vector and a randomized binary look-up table. Our work consists of a number of tasks as shown in Fig. 3.1. First, iris images are pre-processed using Masek's [50] and Daugman's [65] techniques, and IrisCode features are extracted in form of 0-1 matrix using 1-D Log-Gabor filter [50] with phase quantization from the pre-processed iris images. Thereafter, rotation-invariant IrisCode is generated from the original IrisCodes, and the rotation invariant IrisCode is transformed into a row vector. In the next step, we find the consistent bits from the row vectors and generate the consistent bit vector which is used in decimal encoding. Finally, a look-up table is created to map the decimal encoded vector and to generate the cancelable template. These steps are discussed in this chapter.

The rest of this chapter is organized as follows. In Section 3.1, we describe the pre-processing and IrisCode extraction mechanism applied over input iris image. Section 3.2 talks about the invariant feature extraction from the IrisCodes which includes rotation-invariant code generation, row vector formation, and consistent bit extraction. Cancelable template generation technique are presented in Section 3.3 which is composed of two steps, i.e. decimal encoding and look-up table mapping. Section 3.4 provides the experimental evaluations and comparison with the existing approaches. The security analysis of our method is discussed in Section 3.5. Finally, Section 3.6 summarizes the chapter.

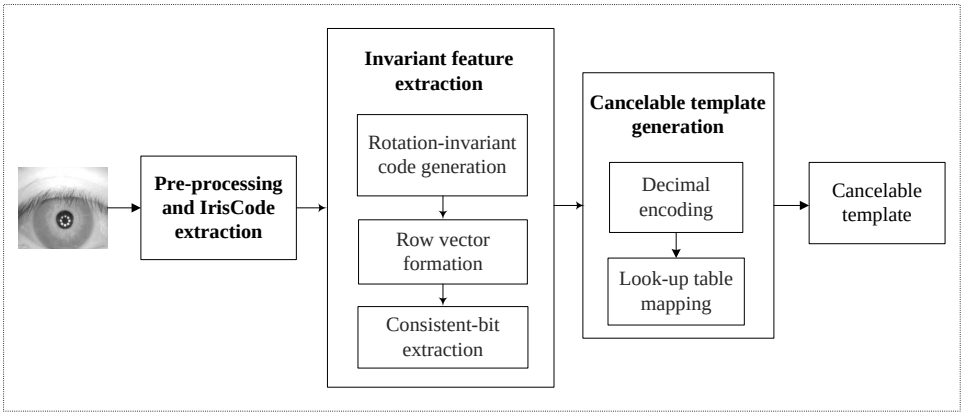


Figure 3.1: Block diagram of the proposed cancelable iris template generation method

3.1 Pre-processing and IrisCode extraction

The pre-processing includes iris segmentation followed by iris normalization and image enhancement. Segmentation is performed to extract the iris region and to remove the eyelids, eyelashes and other noises from the eye image to avoid performance degradation. In our approach, circular hough transformation [50] is applied to detect the iris and pupil circles using the parameters: radius and center co-ordinates. First, iris boundary is detected from the eye image and then, pupil boundary is located from the detected iris region instead of the whole eye image, since the pupil is always within the iris region. Eyelids are detected from the image using parabolic curve parameter instead of the circle parameters [50]. Due to illumination variations and the different imaging conditions, the radial size of the pupil may change accordingly. Therefore, the iris region is normalized using Daugman's rubber sheet model [50, 65] to compensate for these variations. Normalization process maps each point in the iris region to a polar coordinate. Thereafter, local histogram analysis [50] based enhancement technique is applied to the normalized iris image. This reduces the effect of non-uniform illumination and produces a well-distributed texture image. Reflection regions are characterized by high intensity values close to 255 to avoid low contrast. A simple thresholding operation [50] is performed to remove the reflection noise. The details of techniques involved in pre-processing can be found in the report [50]. Fig. 3.2 shows the enhanced normalized iris image.

Figure 3.2: Enhanced image after normalization

Normalized iris image is transformed into a 0-1 form of binary matrix by convolving 1-D Log-Gabor filter [50] to the normalized image. Each row in the normalized iris image is considered as a 1-D signal for convolution. The frequency response of 1-D Log-Gabor function is represented in Eq. 3.1.

$$G(f) = \exp\left(\frac{-\left(\log\left(\frac{f}{f_0}\right)\right)^2}{2\left(\log\left(\frac{\sigma}{f_0}\right)\right)^2}\right) \tag{3.1}$$

where, f_0 and σ represent center frequency and bandwidth of the filters, respectively. The function produces real and imaginary components which are phase quantized to get IrisCode in the form of 0-1.

3.2 Invariant feature extraction

It is quite difficult to match iris image with rotational inconsistencies caused by tilt head while capturing the image. Even for genuine subject, it may result in poor intra-class Hamming distance [149] causing performance degradation. Hence, it is desired to compute invariant features from the extracted IrisCodes.

3.2.1 Rotation-invariant code generation

To employ rotation-invariance, we perform 8-bit left and 8-bit right rotation for each IrisCode of a particular subject. For this purpose, the whole circular iris pattern is considered to have 512 columns. Hence, shifting of one column is equivalent to 360/512=0.703125 degree to a maximum of 8 columns [65] generating 5.625 degree rotation. Next, we consider 'V' number of IrisCodes per subject to achieve invariance. The value of V is determined empirically (for details see Section 3.4.3). We randomly choose one IrisCode as reference from all V

IrisCodes. Hamming distances are calculated between the reference IrisCode and 17 other IrisCodes which are derived from each remaining IrisCode by shifting 8-columns in both directions one at a time. The IrisCode having minimum Hamming distance is further utilized to form row vector and consistent bit extraction. Here, the rotation-invariance is employed to achieve superior performance with respect to original IrisCodes [Please see Table 3.3].

It may be noted that we are not storing any reference IrisCode as this would cause a direct leakage of target IrisCode, if the database has been compromised. In the verification stage, the verifiable template is exploited with 8 bit left and right rotations. The minimum distance is calculated using Eq. 3.2.

$$\text{min\_dist} = \min_{k} \{Icode(r) \oplus shift\,(Icode(q), k)\} \tag{3.2}$$

where, *min_dist* represents the Hamming distance between reference IrisCode ($Icode(r)$) and the given Iriscode ($Icode(q)$) with *k* number of shifts. Here, *k* varies from -8 to 8. *k*=-8 represents 8 bits left shift and *k*=8 represents 8 bits shift to right direction.

3.2.2 Row vector formation

In row vector formation, the rotation-invariant iris samples are stored in row vectors by merging the next row to the previous one since it is easy to apply any transformation on 1-D vector instead of 2-D matrix because we need to traverse in one direction only in the case of 1-D vector. The row vector (R_v) is formed as:

$$R_v\,[j + i \times col\_dim] = Icode\,(i, j) \tag{3.3}$$

where, *col_dim* is the width of column, and R_v is the output row vector for IrisCode (Icode). For example, a row vector of 1×24, which is obtained from the IrisCode of 4×6 is shown in Fig. 3.3. Furthermore, any transformation can be applied on the row vector.

3.2.3 Consistent bit extraction

After generating the row vector from all rotation-invariant IrisCodes, the consistent bits are extracted by considering significant bits in the row vector. Consistent bits are those bits in

IrisCodes which are less likely to change. The consistent bit vector (C_b) is derived after aligning and summing up *V* IrisCodes in order to examine the occurrence of corresponding bits. The consistent bit vector contains same number of bits as in row vector. Hollingsworth et al. [150] presented a mathematical proof for inconsistent bits and its impact on performance. The model observed that the probability (*p*) of a bit flip does not affect the False Match Rate (FMR). However, bit flip rate affects the False Non-Match Rate (FNMR) performance. Hence, we empirically tested our approach with different values of *p* to improve the FNMR. The bit indices that have higher probability of occurrence across various samples of the same IrisCodes are collected in C_b. Moreover, the bits in the original IrisCodes are protected using probability constraint.

In this work, a bit is taken into account if the probability of occurrences is greater than or equal to the threshold p_{th}, across the '*V*' row vectors as defined in Eq. 3.4 and Eq. 3.5:

$$C_b(i) = \begin{cases} 1 & for \quad p(i) \geqslant p_{th} \\ 0 & \quad elsewhere \end{cases} \tag{3.4}$$

$$p(i) = \frac{\sum_{v=1}^{V} R_v(i)}{V} \tag{3.5}$$

where, *V* is total number of samples of a subject and $p(i)$ is the probability of i^{th} bit in the samples of a particular subject. We have considered V = 4 and p = 0.75 in our method [Please see Section 3.4.3].

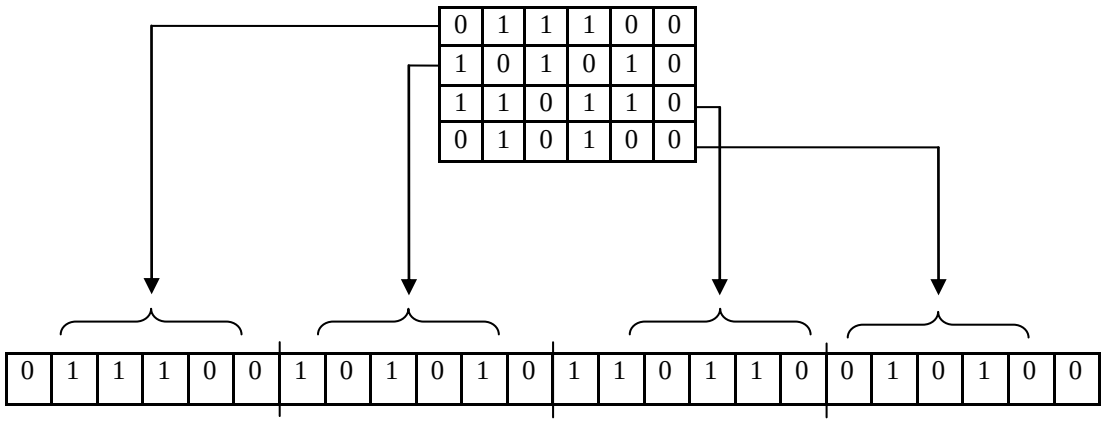


Figure 3.3: Example of creating row vector

3.3 Cancelable template generation

Cancelable template generation involves two steps, i.e. decimal encoding and look-up table mapping. First, decimal vector is derived from the invariant features. Next, a randomized mapping is performed between decimal vector and look-up table. We discuss these steps in the following subsections.

3.3.1 Decimal encoding

It is difficult to apply any transformation function into the entire consistent bit vector as it comprises of 32768 bits. Therefore, consistent bit vector is partitioned into fixed size blocks. The value of block-size (*m*) is considered as multiple of 2 to the power to get consistent words of *m* bits. If it does not equal to powers of 2 then the partition will not be a perfect and some bits will be left over.

The decimal vector is derived from the partitioned consistent bit vector. Each partitioned word is converted into decimals. The conversion of a word from binary to positive integer seizes the right most bit as the least significant bit. For example, we consider the value of *m* = 4 for a given row vector of size 24 bits. Therefore, the row vector is divided into 6 words, each having 4 bits as shown in Fig. 3.4. The size of decimal vector will be 2^m including positive integers in the range of 0 to $2^m - 1$.

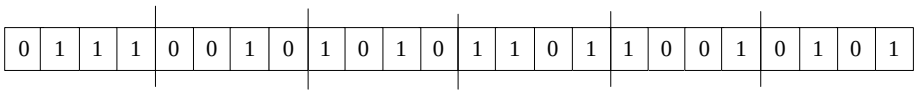


Figure 3.4: Partitioned vector

The decimal vector will comprise large values of positive integers corresponding to large value of *m*. The words in the consistent bit vector are mapped to the corresponding decimal values. The mapping for given consistent bit vector is illustrated in Fig. 3.5.

3.3.2 Look-up table mapping

A binary look-up table (LUT) of size R×C is generated with random values 0 and 1 for each user. Here, R and C represent the size of decimal vector and the size of each word,

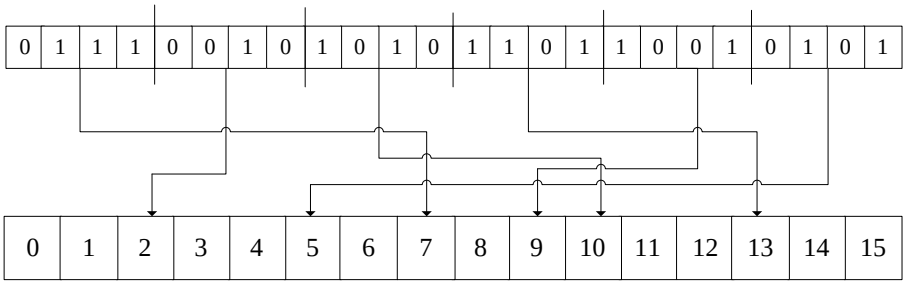


Figure 3.5: Mapping of word to decimal vector

respectively. The size of the table (i.e. number of rows and columns) depends on the value of *m*. The LUT consists R= 2^m and C=m number of rows and columns, respectively. The LUT is filled randomly as defined here:

$$LUT\,(i,j) = rand\,(0,1)\,, \text{for } i = 0,1,...,2^m - 1 \; and \; j = 0,1,...,(m-1) \tag{3.6}$$

where, $LUT(i,j)$ represents the (i,j) position in the look-up table. For example, if we have word length 4, then the table must have at least 2^4 = 16 rows. To differentiate among the different words, we map the decimal vector to a corresponding word utilizing a look-up table. The corresponding word is positioned at the right most bit position. Fig. 3.6 illustrates the mapping procedure.

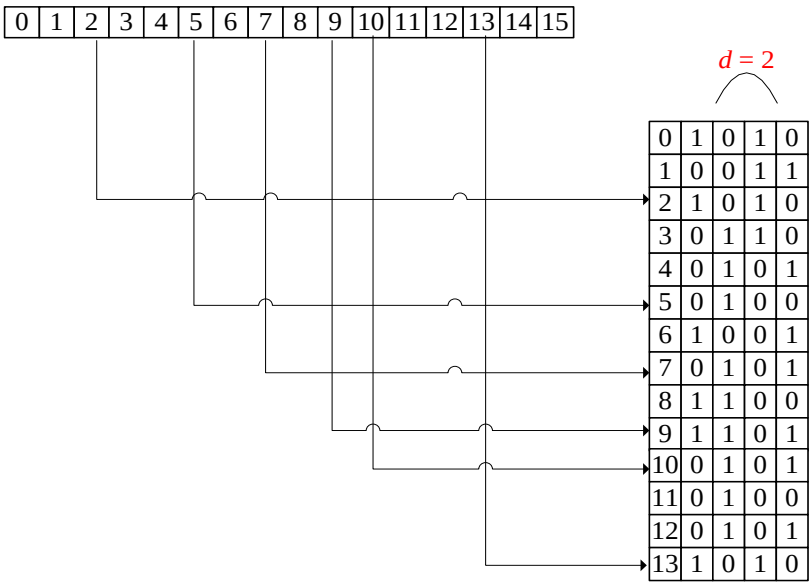


Figure 3.6: Mapping from decimal vector to look-up table

More than one word can be mapped to the same positive integer which prevents the attacker to employ reverse mapping. There is a possibility that all entries of a particular row or more than one row are either 0 or 1. In this situation, the use of these entries is vulnerable to privacy invasion attacks, as this makes imposter's task easy. Therefore, look-up table should maintain approximately same number of 0's and 1's in a randomized manner.

The mapping is performed between the decimal vector and the corresponding row of the LUT. Each row in LUT consists of *m* bits. We can choose *d* bits ($\leq m$) to generate the final template. These bits are referred to as check bits. For example, if *d* = 2 as shown in Fig. 3.6, then 2 bits from the 2^{nd} and 3^{rd} positions are selected from the mapped entries in the LUT. It may be noted that these 2 bits can be chosen from any position in the LUT. Therefore, the final template consists of 12 bits if we choose 2 bits from each word as depicted in Fig. 3.7.

Different templates can be derived using different values of *m*, but look-up table is kept fixed for every *m*. If we select all bits from each block i.e. *d*=*m*, the number of matching will be less across all bits in the stored and verifiable templates. Hence, performance will degrade. We have evaluated our method with different values of d for a fixed value of m (please see Section 3.4.3, Table 3.2) and observed that performance degrades when m=d.

Finally, matching is performed in the transformed domain by measuring the dissimilarity between two templates. We have computed Hamming distance between two templates to measure the dissimilarity. Hamming distance (HD) is sum of non-equivalent bits (exclusive-OR) between the stored and query templates as defined in Eq. 3.7:

$$\text{Hamming Distance}\,(HD) = \frac{1}{N}\sum_{i}^{N} S_i \oplus Q_i \tag{3.7}$$

where, Q_i and S_i are the i^{th} bits of the query and stored templates, respectively. N is the total number of bits in the template.

0	1	1	0	1	0	1	0	1	0	0	1

Figure 3.7: Final template

3.4 Experimental results and analysis

In this section, we present the details of experimental design and results to illustrate performance of the proposed method and the effect of the different parameters as well as comparison with the existing approaches.

3.4.1 Database

We have chosen three widely used iris databases (CASIA-V 1.0, CASIA IrisV3-Interval, ICE 2005) for evaluation of our proposed method. The CASIA-V 1.0 [151] database consists of 756 images of 108 eyes. Each subject has 7 images captured in two sessions; 3 in first and 4 in second session. The CASIA-iris V3 Interval [51] database includes 2639 images captured from 249 different subjects. The prime motive behind using these databases is to compare our proposed method with the existing approaches in [55, 58–60] since their results are reported on the same database. The ICE 2005 database [52] from National Institute of Standards and Technology (NIST) consists of 2953 images composed of 244 subjects. The results obtained from this database are compared with [55].

3.4.2 Experimental design

In our experiments, we have considered left and right eyes as different subjects because iris pattern is different for left and right eyes. We require 4 images per subject to create rotation invariant template at the time of enrollment and 1 image for verification. Hence, we consider the subjects which have at least 5 images. The experiment is performed on 348 subjects containing 177 subjects of left eye and 171 subjects of right eye iris patterns for CASIA-V3-Interval [51] database. To evaluate imposter score, iris template of each subject is matched against the corresponding templates of other subjects, yielding 1197019 different inter-class comparisons. To evaluate genuine score, each iris pattern is matched with other iris patterns of the same subject resulting a total of 7223 different intra-class comparisons. For ICE 2005 dataset [52], the experiment is performed on 210 subjects containing 109 subjects of left eye and 101 subjects of right eye iris patterns resulting into 6560 intra-class comparison and 1386127 inter-class comparison. The experiment performed on CASIA-V 1.0 [151] database outputs a total of 432 genuine comparisons and 80892 imposter comparisons.

To evaluate our method, each database is randomly divided into two partitions, keeping 4 samples in the first partition and the rest in the second partition. The first partition is utilized for enrollment and the second partition for verification. We have conducted a number of experiments using different parameter values. We repeatedly perform each experiment 10 times as the enrollment and test samples are chosen randomly. The average performance for 10 trials is reported in the chapter. We have used CASIA-V3-Interval [51] database to choose the values of different parameters. We have also evaluated our method with CASIA-V 1.0 [151] and ICE 2005 [52] databases using the chosen parameter values.

The efficiency of the proposed method is evaluated by different performance measures such as FAR, FRR, and EER. These terms have been already defined in Eq. 1.1-1.4 in Chapter 1. The values of these performance metrics are evaluated from the genuine and imposter scores. Genuine score refers to matching an iris pattern of a subject with other patterns of the same subject, whereas imposter score is derived by comparing an iris pattern of each subject against the iris patterns of all other subjects. The effectiveness of a biometric system can be illustrated graphically by plotting a Receiver Operating Characteristic (ROC) curve with GAR against the FAR.

3.4.3 Validation of parameters

The proposed method uses four parameters to generate the different cancelable templates. These parameters are: number of samples used for rotation-invariance (V), block-size (m), number of check bits (d) and different look-up tables. In this section, we highlight the impact of the different parameters on the performance of our approach. We have validated all these parameters with respect to CASIA-V3-Interval [51] database.

- *Number of samples (V) used for rotation-invariance*:

  Before formation of row vector, the derived IrisCodes are aligned to eliminate rotational deviation caused due to head tilt while acquisition. We consider 'V' number of samples of the same user to achieve rotation-invariance. From the rotation-invariant IrisCode, we generate row vector followed by consistent bit vector, which considers the different probability values (p). To validate the parameter V and p, we have conducted a number of experiments with different values of V=2,3...,6 and p=0.33, 0.4,...,0.83.

Table 3.1: EER for number of samples used for aligning IrisCodes

V	EER								
	p=0.33	p=0.4	p=0.5	p=0.6	p=0.66	p=0.75	p=0.8	p=0.83	p=1
2	-	-	-	-	-	-	-	-	3.12
3	-	-	-	-	2.03	-	-	-	2.89
4	-	-	1.93	-	-	0.43	-	-	2.03
5	-	0.82	-	0.48	-	-	0.57	-	2.18
6	1.73	-	1.04	-	0.43	-	-	0.73	3.03

The performance is measured with respect to EER and results are reported in Table 3.1. It has been experimentally observed that EER reduces for $V>3$. For high values of V, the EER does not deviate much. Hence, we have considered V=4. The results reported in Table 3.1, show that we achieve the minimum value of EER for p= 0.75. However, EER increases when we consider p=1, that means all bits of a particular position in four row vectors are same. The reason of getting higher EER is that number of consistent bits are less for p=1. Therefore, it has been concluded that masking out inconsistent bits using p=0.75 improves the recognition accuracy firmly.

- *Block size (m)*:

  The row vector is divided into fixed size blocks of size *m*. Different values of *m* produce different Hamming distances for the same subject; therefore, the parameter *m* has an impact on the efficiency of the proposed method. Moreover, a change in *m* may result in the generation of different biometric templates. To validate the parameter *m*, we have evaluated the proposed method with *m* = 2, 4, 8, 16 and 32, and measure the performance with respect to ERR. We can also choose different values of *d* for each *m*. Table 3.2 shows the EER for different values of *m* and *d*. From Table 3.2, we observe that the EER is high for *m*=2 because of less variation in bits of different words. This leads to very low separability in intra-class comparisons. For *m*=4, less value of EER is obtained as variability in bits increases for different words. We also observe that for higher values of *m*, ERR is less as the bit difference is more.

  The ROC curves for different values of *m* with *d*=2 are shown in Fig. 3.8. Fig. 3.8 shows that the EER obtained for *d*=2 are 2.08%, 1.73%, 1.49%, 1.47%, and 1.47% for

Table 3.2: EER for different values of m and d

Block size(m)	Number of check bits(d)	EER
2	2	2.08
4	2	1.73
	4	1.01
8	2	1.49
	4	0.91
	8	1.09
16	2	1.47
	4	0.43
	8	0.82
	16	1.04
32	2	1.47
	4	0.44
	8	0.80
	16	1.03
	32	1.09

m=2, 4, 8, 16, and 32, respectively on CASIA-V3-Interval dataset [51]. It has been observed that there is not much difference in EER for m = 16 and m = 32. Therefore, we conclude that m=16 is the best value to preserve the performance.

- *Check bits (d)*:

  Final cancelable template is generated by selecting d bits from the mapped entries of the look-up table. The parameter d is responsible for security and revocability as various cancelable templates can be generated by varying the value of d (see Table 3.6). The ROC curves for different values of d with m=16 are shown in Fig. 3.9. The EER obtained for m=16 are 1.47%, 0.43%, 0.82%, and 1.04% for d=2, 4, 8, and 16 on CASIA-V3-Interval database [51], respectively. It has been observed from Fig. 3.9 that d=4 is the best value to preserve the performance. Therefore, it can be concluded that the best recognition accuracy is obtained for m=16 and d=4.

- *Effect of different look-up table*:

  The look-up tables are constructed using randomly generated 0-1 values. Sometime it may happen that table is biased for either 0 or 1 that makes the proposed approach non-revocable. A modification in the look-up table leads to alter the random bits for

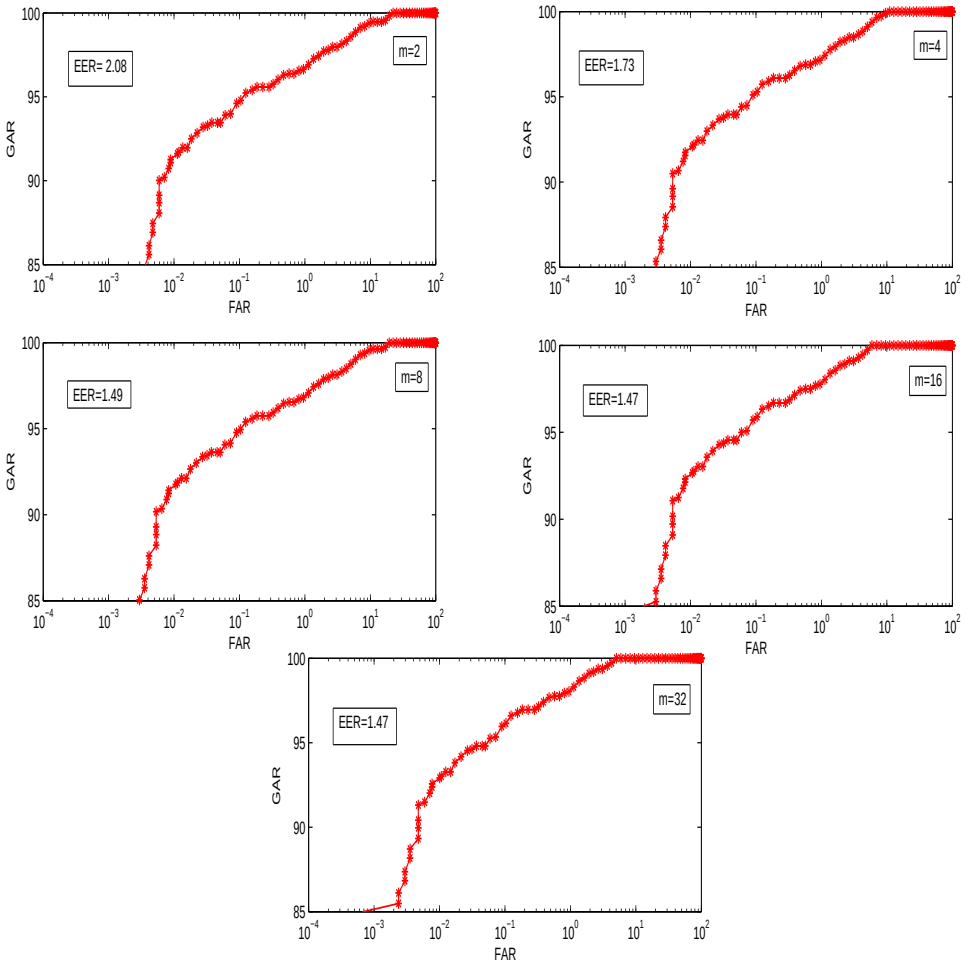
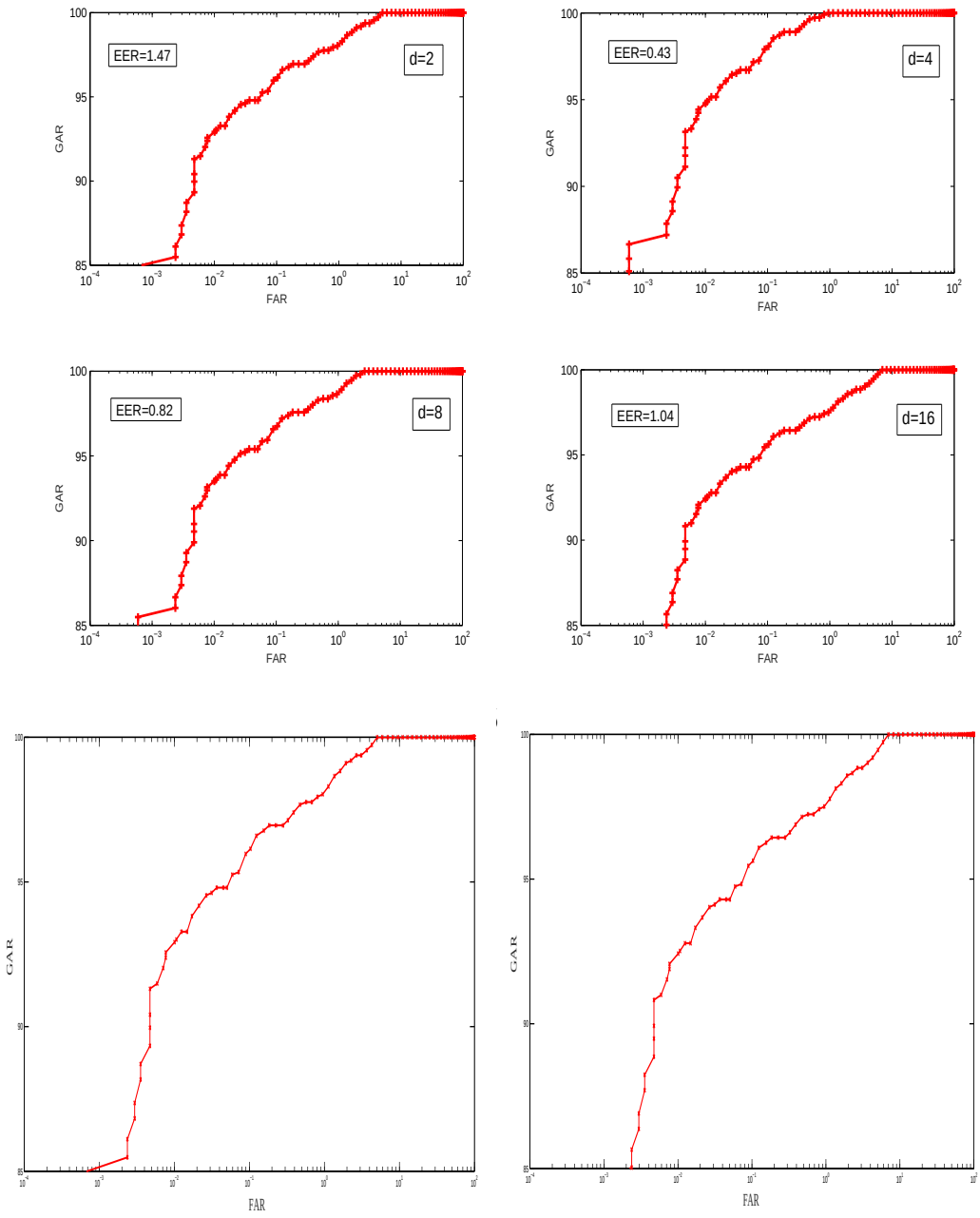


Figure 3.8: ROC curves for m = 2, 4, 8, 16, and 32, respectively

deriving a new template. We have chosen two sets of different look-up tables. Both sets contain different look-up tables for different subjects, however the look-up table of a subject in the first set is different from the look-up table of the same subject in other set. First, we have evaluated the performance with the m=16 and d=4 using first set of look-up tables. Then, we have performed the same experiment using second set of look-up tables. The ROC curves for the two experiments are shown in Fig. 3.10(a) and Fig. 3.10(b). We observe EER of 0.43 and 0.46 with the first and second set of look-up tables, respectively. Therefore, it is clear that change in the look-up table will less affect the overall performance.

The performance is evaluated by tuning all the three parameters m, d, and LUT for CASIA V3 Interval database. The tuned values of parameters are further utilized to evaluate the performance for other two databases. The EER corresponding to the tuned parameters are used for comparison with state-of-the-art.



(a) ROC for LUT set 1 (b) ROC for LUT set 1

Figure 3.10: ROC curves for $m = 16$ and $d = 8$ for two different look-up tables

3.4.4 Baseline comparison

Baseline comparison refers to the comparison of performances before and after cancelable transformation. In this experiment, first we compute the performance using original IrisCodes. Next, we extract the consistent bit vector and compute the performance. Then, we apply the proposed approach to derive cancelable template. Matching between query and

stored templates is performed in the transformed domain. Table 3.3 shows the EER obtained from the original (unprotected) IrisCode, consistent bit vector, and cancelable template for different databases. From Table 3.3, the EER for original Iriscodes and consistent bit vector depicts the significance of rotation-invariance. We have evaluated the performance for rotationally aligned IrisCodes which shows an EER of 0.28, 0.37 for CASIA V 1.0, EER of 0.39, 0.43 for CASIA V-3.0 Interval, and 0.53, 0.79 for ICE 2005 databases without applying cancelable transformation and after applying cancelable transformation, respectively as described in Table 3.3. The reported results in Table 3.3 shows that performance is degraded by 0.09%, 0.093%, and 0.329% for CASIA-V 1.0, CASIA-V3-Interval, and ICE 2005 databases with respect to consistent bit vector, respectively. Therefore, we conclude that performance degradation produced by the transformation is very low and the cancelable transformation preserves the recognition performance.

Table 3.3: Baseline comparison

Dataset	EER		
	Original Iriscode without rotation-invariance	Without cancelable transformation with rotation-invariance	With cancelable transformation with rotation-invariance
CASIA-V 1.0	3.95	0.28	0.37
CASIA-V3-Interval	4.11	0.39	0.43
ICE 2005	4.39	0.53	0.79

3.4.5 Comparison with other state-of-the-art methods

We have analyzed performance of the proposed method for different values of parameters and observed that the best accuracy of EER=0.43% is achieved corresponding to the parameter values m=16 and d=4. The objective of the approaches reported in [30, 55, 58–60, 63, 64, 67] is same with our work. Hence, we compare our work with these approaches only.

The approaches in [30, 63] used CASIA-V 1.0 [151] database and the approaches in [58–60, 64, 67] used CASIA-V3-Interval [51] database. ICE 2005 [52] database is used by Du et al. [55]. The summary of the results of the existing approaches and our proposed approach are reported in Table 3.4. Form Table 3.4, we observe that the best result reported in existing literature is EER=0.84 and EER=1.06 for CASIA-V3-Interval [51] and ICE 2005

[52] databases, respectively whereas our approach gives EER of 0.37, 0.43, and 0.79 for CASIA-V1.0 [151], CASIA-V3-Interval [51], and ICE 2005 [52] databases, respectively. From the reported results, it is evident that our approach performs better for CASIA-V3-Interval [51] and ICE 2005 [52] databases, respectively over the existing approaches.

3.5 Security analysis

A cancelable biometrics system needs to satisfy the four security constraints of revocability, irreversibility, and diversity by preserving the recognition accuracy. In this section, we analyze our method against these requirements. The analysis of different well known attacks against templates generated by our algorithm is also presented in this section.

3.5.1 Non-invertibility analysis

The term, irreversibility refers to the computational hardness in recovering the true IrisCodes. Recall that a randomized look-up table is maintained to map decimal entries and certain digits are selected from the mapped entries to generate a cancelable template. Moreover,

Table 3.4: Performance comparison with existing methods

Methods	EER			Remarks
	CASIA-V 1.0	CASIA-V3-Interval	ICE 2005	
Bringer et al. [30]	6.65/0 FRR/FAR	-	-	fuzzy commitment scheme, EER very high
Wu et al. [63]	5.55/0 FRR/FAR	-	-	BC(Hash encoding with error-correcting codes)
Reddy and Babu et al. [64]	-	9.8/0 FRR/FAR	-	Hardended fuzzy vault
Hammerle-Uhl et al. [59]	-	1.3	-	block transformation
Ouda et al. [58]	-	1.3	-	Non-invertible transformation
Du et al. [55]	-	-	1.06	For IUPUI database 2.95 EER
Hammerle-Uhl et al. [60]	-	0.84	-	EER 0.76 for partial dataset
Rathgeb et al. [67]	-	2.6	-	Non-invertible transformation
Proposed method	0.37	0.43	0.79	Non-invertible tranformation

our approach does not allow the storage of any parameter except the look-up table for each subject. Therefore, an imposter would need to learn the entire procedure to have any chance of compromising the security of the iris template. From the security frame of reference, acquiring the consistent bit vector of an IrisCode is as severe as recovering the true IrisCode itself since it contains the most significant bit information. Therefore, we apply a probability constraint for the evaluation of the consistent bit vector from the IrisCode. In addition to this, utilization of different values of *m*, different Look-up tables, and selection of different *d* bits ensure robustness of the approach. In this section, we analyze three different scenarios to test the irreversibility of the method.

3.5.1.1 Compromised look-up table and protected template

In this case, we assume that an attacker is able to reveal the stored look-up table and protected template of a user. From the size of the look-up table and protected template the value of m and d may be computed. Now, to reconstruct the original IrisCode, the attacker has to compute the mapped locations in the look-up table from the protected template. For this purpose, an attacker can divide the protected template (PT) into L number of bit sequences of the length of d bits where $L = Len_{PT}/d$ as shown in Fig. 3.11. Len_{PT} is the length of the protected template. Next, each bit sequence would be searched in each row of the look-up table to find the mapped location. The number of attempts required to find a match corresponding to a bit sequence in a single row is ${}^{m}C_{d}$ and ${}^{m}P_{d}$ when d bits are taken from the look-up table to generate the protected template in order and without any order, respectively. We denote this number of attempts as M_r. There are 2^d possible bit sequences in the protected template and 2^m number of rows in the look-up table. Hence, the attacker requires $2^d \times 2^m \times M_r$ number of attempts to find mapped locations for all bit sequences of the protected template from all rows of the look-up table. It may be noted that the substring matching cannot be utilized as the positions of d bits may not necessarily be consecutive. For example, if the length of the original template is 32768; the value of m and d are 16 and 4, respectively then the size of the protected template is 8192, and the number of attempts to find possible mapped locations for all bit sequences of the protected template is 1908 million and 45801 million when d bits are selected in order and without any order, respectively to generate the protected template. Further, each bit sequence of the protected template can be

found in multiple rows of the look-up table which could be considered as a set of possible mapped entries of that bit sequence. Figure 3.11 shows that the set of possible mapped locations is $\{1, 3, 7\}$ as the 2^{nd} bit sequence is found in the 1^{st}, 3^{rd}, and 7^{th} rows in the look-up table. Similarly, the attacker can generate L number of sets of possible mapped locations corresponding to all bit sequences of the protected template. We assume that the number of possible mapped locations for the i^{th} bit sequence is N_i. Hence, the total number of attempts to generate the original decimal vector from the sets of possible mapped locations is $N_{MT} = N_1 \times N_2 \times \cdots \times N_i \times \cdots \times N_L$.

As a result, the number of computations required to derive the decimal vector from the compromised look-up table and protected template is $2^d \times 2^m \times M_r + N_{MT}$. Moreover, even if the attacker derives the consistent-bit vector from the computed decimal vector; it would be hard to retrieve the original template as the attacker does not know the positions of consistent bits out of 32768 bits.

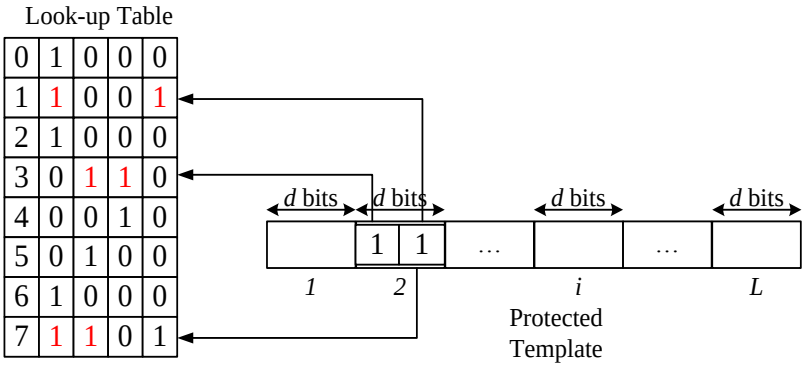


Figure 3.11: Mapping from protected template to look-up table

3.5.1.2 Compromised protected template and value of *m*

Assume that an attacker infiltrates the protected template and the value of m. In this scenario, an attacker has to reconstruct the look-up table and derive the decimal vector to obtain the original IrisCode. The reconstruction of the look-up table is computationally hard as the number of attempts required to reconstruct the original look-up table is $2^{2^m \times m}$ because there are $2^m \times m$ number of cells in the look-up table and the value of each cell is either 0 or 1. Now, there are $2^{2^m \times m}$ possible look-up tables and the attacker has to derive the decimal vector corresponding to each look-up table. The number of computations required to generate dec-

imal vector for single look-up table is $2^d \times 2^m \times M_r + N_{MT}$ as discussed in Section 3.5.1.1. Therefore, the total number of computations required to derive the decimal vector from the compromised protected template, and value of m is $2^{2^m \times m} \times \left(2^d \times 2^m \times M_r + N_{MT}\right)$. For example, we assume that the size of the look-up table is 16×4, and 2 bits are selected in order as well as without any order from the look-up table to generate the protected template. We also assume that the size of the protected template is 8 bits which contains 4 mapped locations, and each set has 2 entries. The number of attempts required to generate the decimal vector is 7.4×10^{21} when the bits are selected in order and 1.4×10^{22} when the bits are not selected in any particular order. These values are comparable with those of Du et al. [55] and Hammerle-Uhl et al. [59] methods.

3.5.1.3 Compromised look-up table

In this case, we assume that an attacker reveals the stored look-up table but no information about the protected template. In this situation, the value of m is known to the attacker. However, the attacker would not be able to reconstruct the original template as the look-up table comprises random 0-1 entries. From random 0-1 entries, it is impossible to retrieve any information about the true IrisCode.

3.5.2 Revocability analysis

It is necessary that a new template must be issued if the stored template is stolen/compromised. The new template should be uncorrelated to the previously compromised templates though they are derived from the same biometric information. It is a necessary requirement for a biometric template protection scheme to generate numerous transformed templates from the same iris and they should differ with other templates to prevent cross-mating of templates across various applications.

1820 templates can be generated for the same sample of each subject corresponding to m=16 and d=4. We have selected 100 different templates randomly from this combination and matched with the original enrolled templates to obtain pseudo-imposter distribution. The mean and variance of genuine, imposter, and pseudo-imposter distribution for different values of *m* is shown in Table 3.5. Table 3.5 indicates that mean and variance for pseudo-

Table 3.5: Mean and variance of imposter (μ_i & σ_i), pseudo-imposter (μ_{pi} & σ_{pi}) and genuine distributions (μ_g & σ_g) for different values of *m*

Block size(*m*)	μ_i	σ_i	μ_{pi}	σ_{pi}	μ_g	σ_g
2	0.4834	0.0019	0.3980	0.02783	0.1132	0.0043
4	0.4802	0.0018	0.3893	0.02871	0.1241	0.0052
8	0.4789	0.0016	0.3741	0.02889	0.1534	0.0059
16	0.4770	0.0015	0.3692	0.03112	0.1784	0.0072
32	0.4698	0.0013	0.3591	0.03156	0.1837	0.0080

imposter distribution is near to the imposter distribution and far from genuine distribution. This signifies that the derived templates are dissimilar to enrolled templates for the same iris pattern. Although, the templates are generated from same iris pattern, they are uncorrelated with each other. Therefore, claim of revocability is preserved.

3.5.3 Diversity analysis

It is essential for a template protection mechanism that numerous derived templates should not match over various applications to avoid cross-matching. To evaluate this criterion, we employ different combination of *m* and *d* from the mapped row of Look-up table. The selection of *d* bits from the mapped instances in Look-up table can derive many templates for a particular subject. Table 3.6 shows the possible number of templates generated using different values of *d*. Further, we can also generate different templates by choosing different Look-up tables.

The parameters illustrated in Section 3.4.3 shows that multiple templates can be generated for a single subject; they can still significantly be distinguished from the original

Table 3.6: Total number of possible templates for different values of m and d

Block size(*m*)	Possible templates		
	d = 2	*d* = 3	*d* = 4
2	${}^{2}C_{2}$=1	-	-
4	${}^{4}C_{2}$=6	${}^{4}C_{3}$=4	-
8	${}^{8}C_{2}$=28	${}^{8}C_{3}$=56	${}^{8}C_{4}$=70
16	${}^{16}C_{2}$=120	${}^{16}C_{3}$=560	${}^{16}C_{4}$=1820
32	${}^{32}C_{2}$=496	${}^{32}C_{3}$=4960	${}^{32}C_{4}$=35960

template which means an individual can enroll different templates of the same subject at different physical applications without cross-matching. Therefore, the experiments validate the property of diversity.

3.5.4 Other attacks

We also analyze the possibility of different types of attacks namely Attacks via Record Multiplicity, pre-image, cross-matching, distinguishing and annealing attacks to validate the robustness of the proposed work:

3.5.4.1 Correlation attack

To avoid correlation attack, the proposed approach uses different values of *m* and *d* to derive multiple templates across various applications. If an imposter is able to reveal the two templates of the same user, it would not be possible to link the i^{th} bit in two templates derived using different values of *m* and *d*. It is also possible to permute the bits in derived template or it can be XORed with a random sequence before deploying it to a new application. This random sequence will be dependent on the value of *m*. For example, if *m*=4, random sequence will have 8192 bits, which is computationally hard to invent for an imposter.

3.5.4.2 Hill-climbing attack

The primary idea behind hill climbing attack is to consecutively modify a biometric input to verification system in order to reconstruct the original IrisCode. The attacker observes the matching score returned by the system at each attempt and tries to maximize the matching score. The process of attempts with modified input continues until no significant improvement in matching score is observed. In our approach, consistent bit vector is considered after aligning the different IrisCodes. The bits which are less likely to change across different IrisCodes of the same subject are treated as consistent bits. For example, if we have four IrisCodes 0110, 0010, 0101, and 0100, then the consistent bit vector we consider is 0100. Here, the attacker needs to know the position of consistent bits to launch the hill-climbing attack. The consistent bits are selected based on probability constraint. Hence, the attacker has to match all possible bit vectors to obtain the desired score for verification. Moreover,

the attacker has to apply all possible combination of parameters (m and d) to derive the cancelable template which is hard to invent.

3.5.4.3 Stolen-token scenario

This is a scenario where the same token i.e. look-up table is utilized for template generation for all subjects. The stolen token, combined with his own biometric input is utilized for verification. If the attacker gets access to the block size (m) and check bits (d), it will be impossible to reconstruct the original template as look-up table comprise of random 0-1 entries. This will avoid the condition of stolen-token and aid more revocability to our approach. Under stolen-token (same key) scenario, the experimental results are provided in Section 3.4. Our method achieves, an EER close to 0%, in case of different-key scenario.

3.6 Summary

In this chapter, we have presented a novel cancelable iris template generation method which is able to derive a new and unique template from the original biometric template in case the stored transformed template is compromised. Further, the approach also satisfies the four design criteria of irreversibility, revocability, diversity, and accuracy. The proposed method utilizes look-up table mapping to protect the original IrisCodes. Our approach uses 1-D Log-Gabor filter to generate iris code which is further partitioned into a number of fixed size words. The proposed method generates cancelable templates by mapping the decimal vector into look-up table. The significant performance improvement is achieved by our approach as it involves consistent-bit vector over rotation invariant IrisCodes for enrollment. We achieve 0.37%, 0.43%, and 0.79% EER for CASIA-V1.0, CASIA V3-Interval, and ICE 2005 databases, respectively which indicates that our approach performs better than the existing approaches after applying the transformation. If the cancelable template is compromised, the parameters utilized in our experiment or the look-up table entries can be altered to derive another unique protected template.

Chapter 4

Cancelable fingerprint template generation

In fingerprint-based authentication, computation of invariant features from the minutiae points results in significant performance improvement over the original minutiae information. In addition, a non-invertible, diverse and revocable template protection mechanism is essential to maintain secrecy. In this work, we propose a novel cancelable fingerprint template generation method based on ridge feature transformation. Ridge-based features are computed for the nearest neighbor structure drawn for each reference minutiae point. Next, the Cantor pairing function is applied to encode the ridge features, and the logarithm function is used to uniformly distribute the paired features. Finally, the random projection is utilized to derive a non-invertible protected template. Figure 4.1 displays the overall design flow for the proposed method which consists of different tasks involved in our approach. The rest of the chapter is organized as follows. In Section 4.1, we describe the techniques utilized for pre-processing and minutiae extraction. Our proposed two steps feature extraction process is presented in Section 4.2. Section 4.3 narrates the cancelable template generation mechanism. The matching procedure between the stored and query templates is described in Section 4.4. Section 4.5 demonstrates experimental results obtained with different databases as well as compares the proposed method with the existing cancelable template generation approaches. Section 4.6 provides the security analysis of our method. Finally, Section 4.7 summarizes this chapter.

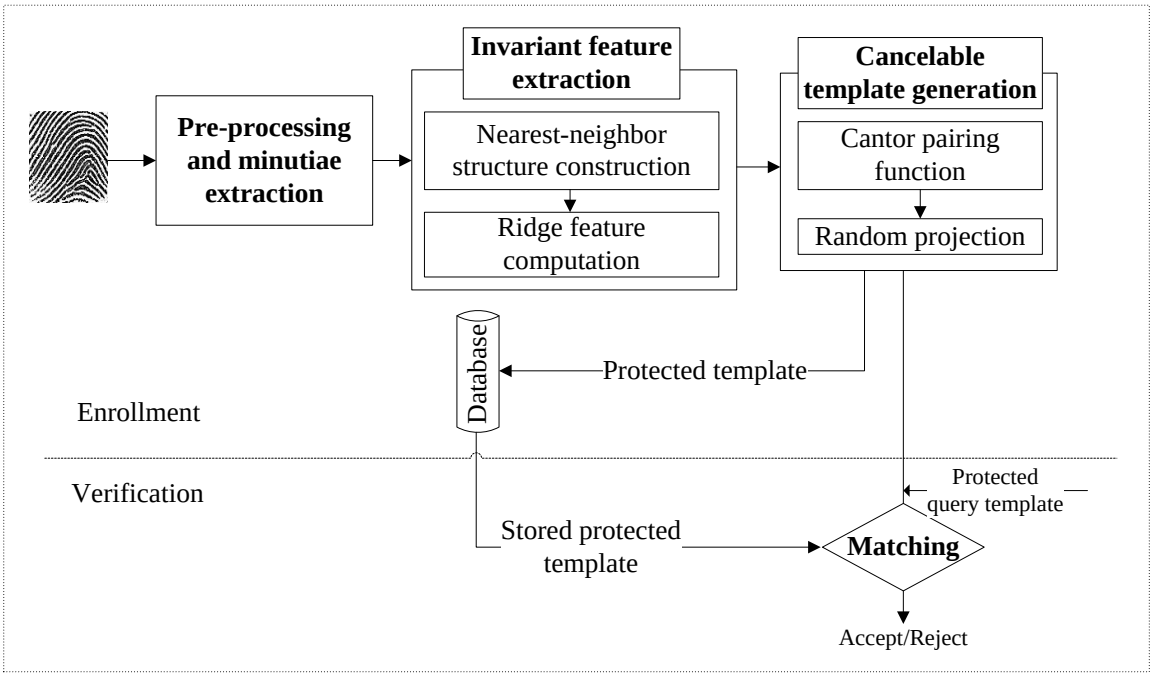


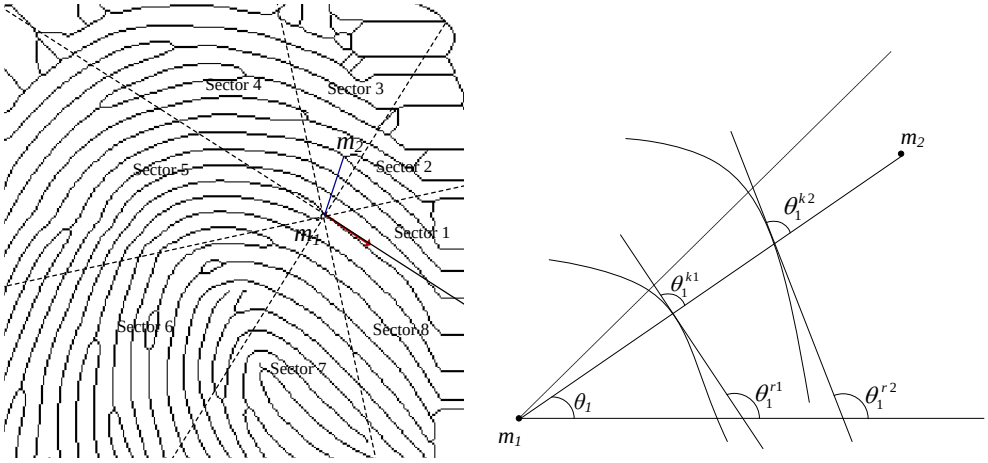
Figure 4.1: Block diagram of the proposed cancelable fingerprint template generation method

4.1 Pre-processing and minutiae extraction

Fingerprint images may have different levels of contrast throughout the image. Pre-processing is performed to enhance the quality of input fingerprint image subsequently reducing the noise. In literature, different methods have been proposed to reduce noise and detect minutiae points from input fingerprint image. In this work, the pre-processing and extraction of minutiae points are performed by following the method presented in [152]. The extracted minutiae points are denoted as follows:

$$\begin{aligned} V_{up} &= \{m_i\}_{i=1}^{n} \\ m_i &= (x_i, y_i, \theta_i) \end{aligned} \tag{4.1}$$

where, V_{up} represents the set of untransformed (raw) minutia points detected from the input fingerprint and *n* is the total number of minutiae points in V_{up}. The i^{th} minutiae point is denoted by m_i where (x_i, y_i) and θ_i are the coordinate positions and orientation, respectively. Also, a thinned fingerprint image is obtained during preprocessing step which is further used for the invariant features extraction.



(a) Nearest neighbor structure onto ridge-based coordinate system

(b) Ridge-based feature computation

Figure 4.2: Ridge feature extraction

4.2 Invariant feature extraction

There is an utmost need of evaluating invariant features to achieve optimal performance. The proposed feature extraction involves two steps: nearest neighbor structure construction and ridge feature computation. These steps are described in the following subsections.

4.2.1 Nearest neighbor structure construction

We use minutiae information to create the nearest neighbor structure on the thinned fingerprint image. First, one of the minutiae point from V_{up} is selected as a reference minutia. Next, a nearest neighbor structure is formed in the vicinity of reference minutiae point considering the ridge-based co-ordinate system as depicted in Fig. 4.2(a). In ridge-based co-ordinate system, reference axis coincides with the orientation of the selected reference minutiae. Further, we divide the fingerprint region into 's' sectors of equal angular width around reference minutia in an anti-clockwise direction. In each sector, the nearest neighbor minutiae point is identified by selecting the minimum distance from the reference minutiae point. This procedure is followed for all minutiae points in V_{up}. It may be noted that if there is no minutia located in any of the sectors, we assign the nearest neighbor to be 0 in that sector. Further, we do not take into account the sectors with no minutiae point at the time of comparison. We consider eight sectors (s = 8) in our method as shown in Fig. 4.2(a). In Fig. 4.2(a), m_2 is the nearest neighbor of reference minutiae m_1 in sector 3.

4.2.2 Ridge feature computation

Accuracy of the fingerprint-based verification system could be affected by translation, rotation, and scale deformations produced while acquisition. Hence, it is necessary to compute invariant features from the input fingerprint image. In this work, we consider ridge count and average ridge orientation between the nearest neighbor minutiae and the reference minutiae in each sector as invariant features. To compute these features, first, the reference minutiae and the nearest neighbor minutiae points are identified. Then, we compute the number of ridges along the straight line between these two minutiae in the thinned image and denote the ridge count in the j^{th} sector as rc_j. Figure 4.2(a) shows a descriptive example where ridge count between the nearest neighbor minutiae point (m_2) and the reference minutiae point (m_1) is 2. To compute ridge orientation, a tangent is drawn at the intersection point of the line and ridge. Next, we measure the angle subtended by the tangent and straight lines between two minutiae points for each ridge crossing the straight line. For example, the orientation ($\theta_1^{k_1}$) of the first ridge in the first sector as shown in Fig. 4.2(b) is evaluated as:

$$\theta_1^{k_1} = \theta_1^{r_1} - \theta_1$$

where, θ_1 denotes the slope of line connecting nearest neighbor minutiae to reference minutiae point in the first sector. $\theta_1^{r_1}$ is the angle subtended by tangent line from the first ridge crossing and reference axis. In a similar manner, we calculate the orientation $\theta_1^{k_2}$ for the second ridge in the first sector and compute the mean ridge orientation for the first sector. The mean ridge orientation for the j^{th} sector, denoted as ro_j is calculated using Eq. 4.2.

$$ro_j = \text{round}\left[\frac{\left(\theta_j^{r_1} - \theta_j\right) + \left(\theta_j^{r_2} - \theta_j\right) + \text{.....} + \left(\theta_j^{r_{NR_j}} - \theta_j\right)}{NR_j}\right] \tag{4.2}$$

where, NR_j represents the total number of ridges between the reference and nearest minutiae point in the j^{th} sector. Similarly, we find ridge count and mean ridge orientation for all minutiae and store it as $\left\langle \langle rc_{ij}, ro_{ij} \rangle_{j=1}^{s} \right\rangle_{i=1}^{n}$, where s is the number of sectors and n is the total number of minutiae points.

4.3 Cancelable template generation

After invariant feature extraction, we generate cancelable fingerprint template which includes two steps, i.e. Cantor pairing and random projection. These steps are discussed in the following subsections.

4.3.1 Cantor pairing function

The Cantor pairing function [153, 154] is utilized to uniquely encode two natural numbers into a single natural number. Let N = 0, 1, 2, 3,.... be the set of positive integers, and $N \times N$ be the set of all ordered pairs of non-negative integers. A bijection from $N \times N$ to N is called the Cantor pairing function which is defined as in Eq. 4.3.
Consider a function: $\pi : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$
such that:

$$\pi(k_1, k_2) := \frac{1}{2}(k_1 + k_2)(k_1 + k_2 + 1) + k_2 \forall\, (k_1, k_2) \in \mathbb{N}^2 \tag{4.3}$$

The motive of applying Cantor paring function is to encode the evaluated ridge features i.e rc and ro into one. This pairing maps multiple features into one from which it is hard to find the original ridge features. For each minutiae point, we compute the paired output of ridge features (rc and ro) for each sector and store in a 2D matrix as defined in Eq. 4.4.

$$\begin{aligned} C^P\,(i,j) = \;& \tfrac{1}{2}\,(rc_{ij} + ro_{ij})\,(rc_{ij} + ro_{ij} + 1) + ro_{ij} \\ & \forall\;\; i \in [1, n] \text{ and } j \in [1, s] \end{aligned} \tag{4.4}$$

where, $rc_{i,j}$ and $ro_{i,j}$ represent the ridge features (i.e. ridge count and mean ridge orientation) between the nearest minutiae in the j^{th} sector corresponding to the i^{th} reference minutiae. $C^P\,(i,j)$ is paired output of ridge features of the j^{th} sector with respect to the i^{th} reference minutiae. Next, we apply pointwise logarithm operation onto the paired output, C^P. Here, the motivation to apply the logarithm operation is to obtain a uniform distribution of C^P which is utilized to minimize EER. Log function is defined in Eq. 4.5 and the base (b) of log function is chosen empirically (for details see Section 4.5.3). For instance, if an input

fingerprint image comprising n minutiae points is divided into 's' sectors, the matrix C^P would result into $n \times s$ entries. After applying the log function, we obtain the log template ($\mathcal{L}$) of size $n \times s$.

$$\mathcal{L}(i,j) = \log_b \left(C^P(i,j) \right) \tag{4.5}$$

4.3.2 Random projection

In order to derive non-invertible and revocable cancelable template, we apply random projection on log template ($\mathcal{L}$). A random projection matrix ($\mathcal{R}$) of size $s \times t$ where $t < s$ is derived using a random seed κ. Moreover, each of the entries of $\mathcal{R}$ is computed from a Gaussian independent and identical distribution (i.i.d.) with mean equal to zero. Now, each row of log template ($\mathcal{L}$) is projected onto random projection matrix ($\mathcal{R}$) to derive the cancelable template (C^T) of size $n \times t$ as shown in Eq. 4.6 where, rank($\mathcal{R}$)=r.

$$C^T = \mathcal{L} \cdot \mathcal{R} \tag{4.6}$$

A system of linear equations claims a unique solution when ranks of the coefficient matrix as well as the augmented matrix are same. Further, if rank becomes lower than the unknowns present (i.e. $r < t$), the linear system leads to infinite solutions [Please see Appendix A.1]. Hence, $\mathcal{R}$ is one of those infinite solutions of Eq. 4.6. This random projection based transformation guarantees the privacy and security of the proposed method. An imposter has no clue about $\mathcal{L}$ even if the protected template gets compromised. Further, if we consider the worst case of stolen C^T and $\mathcal{R}$, it would be hard to retrieve $\mathcal{L}$ from infinitely many possible solutions (Please see Section 4.6.1). The user's original information cannot be compromised even if an adversary obtains the stored fingerprint template because of the randomness present in the $\mathcal{R}$.

4.4 Matching

The comparison between enrolled and query templates is performed in the protected domain to maintain secrecy. We compute local and global similarities to evaluate overall comparison score. We use Dice coefficient to measure the local similarity between the enrolled and query

templates as utilized in [75]. Finally, the likelihood of the enrolled and query templates being the two fingerprint of the same subject is measured to compute the global similarity score.

4.4.1 Local similarity score

Let us consider, the enrolled and query protected templates are denoted by $C^T_{n\times t}$ and $Q^T_{m\times t}$, respectively where m and n represent the number of minutiae in the query and enrolled templates, respectively. To evaluate the local similarity score, each row of C^T is cross-matched with all rows in Q^T by computing the inner product of $C^T(i,:)$ and $Q^T(j,:)$ where $i \in 1, 2, \cdots, n$ and $j \in 1, 2, \cdots, m$. We obtain a similarity matrix $sim(i,j) \in \mathbb{R}^{n\times m}$ after applying the Eq. 4.7.

$$sim\,(i,j) = \frac{2C^T(i,:)\cdot Q^T(j,:)}{\|C^T(i,:)\|^2 + \|Q^T(j,:)\|^2} \tag{4.7}$$

where $i \in [1,n]$ and $j \in [1,m]$.

The i^{th} row of C^T and the j^{th} row of Q^T are considered as verifiable iff $sim(i,j)$ = max $([sim(i,1), sim(i,2), ..., sim(i,n)])$ and $sim(i,j)$ = max $([sim(1,j), sim(2,j), ..., sim(m,j)])$ are valid simultaneously. Therefore, each of the entries in similarity matrix is re-evaluated to eliminate double comparison in the following manner:

Let,

$$\Gamma_{C^T} = [\Gamma_{C^T(1)}, \ldots, \Gamma_{C^T(i)}, \ldots \Gamma_{C^T(n)}]$$

$$\text{where, } \Gamma_{C^T(i)} = max(sim(i,1), \ldots, sim(i,m)$$

and

$$\Gamma_{Q^T} = [\Gamma_{Q^T(1)}, \ldots, \Gamma_{Q^T(i)}, \ldots, \Gamma_{Q^T(m)}]$$

$$\text{where, } \Gamma_{Q^T(j)} = max(sim(1,j), \ldots, sim(n,j)$$

be the maximum scores acquired for all minutiae in C^T and Q^T, respectively. Next, we construct a binary mask $A \in \{0,1\}^{n\times m}$, which records the positions of the coinciding maxima;

$$A(i,j) = \delta(\Gamma_{C^T(i)} == \Gamma_{Q^T(j)}) \tag{4.8}$$

where $\delta(\cdot)$ returns 1 when the nested condition is true and 0, otherwise. Hence, the filtered similarity matrix is represented by Eq. 4.9:

$$\hat{S} = sim \odot A \tag{4.9}$$

where, $\odot$ represents element-wise multiplication.

4.4.2 Global similarity score

To perform overall comparison score between C^T and Q^T, the likelihood of C^T and Q^T being two instances of the same fingerprint is measured. From the similarity matrix ($\hat{S}$) obtained in Eq. 4.9, we calculate the comparison score ($\mathfrak{S}$) with the following equation:

$$\mathfrak{S} = \frac{\sum_{i=1}^{n}\sum_{j=1}^{m}\widehat{S(i,j)}}{min(m,n)} \tag{4.10}$$

Algorithm 1 describes the overall comparison procedure.

4.5 Experimental results and analysis

In this section, we present the details of experimental design and results to illustrate the performance of the proposed method. We also analyze the effect of the different parameters as well as comparison with the existing approaches.

4.5.1 Database selection

We have conducted our experiments on publicly available fingerprint databases FVC2002, FVC2004, and FVC2006, and each database contains four sets namely, DB1, DB2, DB3, and DB4 since most of the authors of biometrics research community utilize FVC databases [53]. Further, FVC databases contain variety of images including rotated fingerprints, scaled images due to pressure, images from elderly people, and poor quality images with dry and moistened fingerprints. Each set of the first two databases comprises of 100 subjects with 8 images per subject. Each set of the FVC2006 database includes 140 subjects with 12 images per subject.

Algorithm 1 Comparison

Input: Cancelable template ($C^T_{n\times t}$), Query template ($Q^T_{m\times t}$)
Output: Comparison score ($match\_score$)

Initialize : $sim(n,m) \leftarrow 0$, $S(n,m) \leftarrow 0$
for $i = 1$ to n **do**
  $R^M_1 \leftarrow C^T[i]$
  for $j = 1$ to m **do**
    $R^M_2 \leftarrow Q^T[j]$
    // Evaluate similarity score as described in Eq. 4.7
    $sim[i,j]$ = InnerProduct(R^M_1, R^M_2)
  end for
end for
$\Gamma_{C^T} \leftarrow [\Gamma_{C^T(1)}, \ldots, \Gamma_{C^T(i)}, \ldots \Gamma_{C^T(n)}]$
where, $\Gamma_{C^T(i)} = max(sim(i,1), \ldots, sim(i,m)$
$\Gamma_{Q^T} \leftarrow [\Gamma_{Q^T(1)}, \ldots, \Gamma_{Q^T(i)}, \ldots, \Gamma_{Q^T(m)}]$
where, $\Gamma_{Q^T(j)} = max(sim(1,j), \ldots, sim(n,j)$
for $i = 1$ to n **do**
  for $j = 1$ to m **do**
    $S[i,j] \leftarrow (\Gamma_{C^T}[i] = \Gamma_{Q^T}[j])$ // Re-evaluate similarity score to avoid double comparison as described in Eq. 4.8
  end for
end for
$\hat{S} = sim \odot S$
$match\_score(\mathfrak{S}) = \frac{sum(sim(:))}{min(m,n)}$ // Evaluate Eq. 4.10

4.5.2 Experimental design

In accordance with the ISO standard [37], we have incorporated FMR, FNMR, EER, and GMR metrics to evaluate the performance of our method as defined in Eq. 1.1-1.4 in Chapter 1. The computation of these performance metrics involves the evaluation of genuine and imposter scores. Genuine score refers to the comparison of a fingerprint impression of a subject with the other impressions of the same subject, whereas imposter score is derived by comparing a fingerprint impression of each subject against the fingerprint impressions of all other subjects. Also, we have used standard FVC protocol and 1VS1 protocol to compute the performance of our method. These protocols are discussed as follows:

- In 1VS1 protocol, the first fingerprint image of each subject is compared with the second fingerprint image of the same subject to compute FNMR. To measure FMR, the first image of each subject is compared with the first image of the other subjects. This results to measure 100 genuine and $^{100}C_2$ =4950 imposter scores for each of the

FVC2002 and FVC2004 databases. For each set of FVC2006 database, 140 genuine and ${}^{140}C_2$=9730 imposter scores are computed.

- In the FVC protocol, each fingerprint image of a subject is compared with the remaining fingerprint images of the same subject to compute the FNMR and to evaluate the FMR, the first fingerprint image of each subject is compared with the first fingerprint image of different subjects. This results in providing ${}^{8}C_2 \times 100$=2800 genuine and ${}^{100}C_2$=4950 imposter scores computation for each set of FVC2002 and FVC2004 databases. For each set of FVC2006, ${}^{12}C_2 \times 140$=9240 genuine and ${}^{140}C_2$=9730 imposter scores are computed.

4.5.3 Validation of parameters

The proposed method utilizes two parameters to derive the protected fingerprint template. These parameters are: number of sectors (s) in the nearest neighbor structure [see section 4.2] and log-base value (b) [see section 4.4]. In this section, we highlight the impact of these parameters on the performance of our approach. We have validated these parameters with respect to dataset DB1 of FVC2002, DB3 of FVC2004 and DB1 of FVC2006 using FVC protocol since they have good quality images.

1. *Number of sectors (s)*: After conducting the pre-processing steps, we divide a input fingerprint image into s number of sectors with an equal angular width in the ridge-based co-ordinate system. To validate parameter the s, we have performed exhaustive testing considering different angular widths with 15° interval. We have considered s = 24, 12,..., and 4 corresponding to angular width 15°, 30°, ..., and 90°, respectively. To carry out this experiment, we have considered log-base value (b) as 1.2. The performance is measured with respect to EER, and results are reported in Table 4.1. It has been observed that the method yield best result for s = 8 on dataset DB1 of FVC2002, DB3 of FVC2004, and DB1 of FVC2006. Further, the performance of the method is degraded for the smaller values of s as the transformation becomes sensitive to noise. We also observe that the EER increases for higher values of s as there are more sectors with 0 minutiae points. Hence, we have considered s = 8 for all other experimental evaluations here.

Table 4.1: EER for different number of sectors in the nearest neighbor structure

Angular width	Number of sectors (s)	EER (in %)		
		FVC2002 DB1	FVC2004 DB3	FVC2006 DB1
15	24	5.03	7.89	11.32
30	12	3.91	6.75	8.03
45	8	1.75	3.97	5.14
60	6	2.17	4.64	6.38
90	4	3.81	5.44	7.19

2. *Log-base value (b)*: We apply the log function onto the paired output derived using Cantor pairing function to obtain the uniform features distribution. We have conducted a number of experiments by considering the different values of b = 1.1, 1.2, 1.3,..., 2 and measured the performance in terms of EER for dataset DB1 of FVC2002, DB3 of FVC2004, and DB1 of FVC2006 as reported in Table 4.2. The experimental evaluation illustrates that the method performs the best on b = 1.2. We observe that small value of b amplifies the distribution of paired output reducing EER. Further, EER gets increased as the discrimination between features of the different subjects gets reduced for higher values of b. Therefore, we consider b = 1.2 to evaluate the performance of our method.

Table 4.2: EER for different values of b

Log-base (b)	EER (in %)		
	FVC2002 DB1	FVC2004 DB3	FVC2006 DB1
1.1	2.13	4.03	6.84
1.2	1.75	3.97	5.14
1.3	2.43	4.87	7.04
1.4	4.07	5.13	8.93
1.5	5.51	6.83	9.94
1.6	6.91	8.03	11.53
1.7	8.12	10.23	13.18
1.8	10.03	11.89	14.91
1.9	11.36	13.97	16.12
2	12.89	14.64	17.9

4.5.4 Performance evaluation

To measure the performance of our method, we have conducted two sets of experiments. We evaluate the performance under the same key and different key scenario in the first and second set of experiments, respectively. Each experiment is conducted 10 times, and the average performance of 10 trials is reported in this chapter.

4.5.4.1 Same key scenario

This scenario represents the practical situation where an imposter illicitly accesses the random projection matrix ($\mathcal{R}$). We have evaluated this scenario by assigning the same $\mathcal{R}$ to each user present in the database.

FVC2002: For FVC2002 database, the ROC curves are displayed in Fig. 4.3 for FVC and 1VS1 protocols. Out of all datasets of FVC2002, the method exhibit low EER on DB1 and DB2 for both protocols due to the presence of more number of good quality images as compared to other datasets of FVC2002. In case of DB2 dataset, we obtain an EER of 0 due to less number of intra-class comparisons for 1VS1 protocol. Further, 1^{st} and 2^{nd} images of a subject in FVC2002 DB2 are acquired in the same session and have less variation and distortion than the other six images. However, images in DB3 and DB4 dataset of FVC2002 contain relatively poor quality images with less number of minutiae points as compared to dataset DB1 and DB2. As a result, we achieve high EER for DB3 and DB4 datasets under both protocols.

FVC2004: For FVC2004 database, the ROC curves are shown in Fig. 4.4 for both protocols. The method provides a high value of EER on DB2 for both protocols as the first two images of the DB2 dataset are heavily distorted. In addition, the small overlap area corresponding to the images of stored and the query template is another reason for less accuracy on DB2 of FVC2004. For example, if we consider the images of stored and query template, as 96_1.tif and 96_2.tif, the genuine matching attempt fails. This is because 96_1.tif contains the region below the core point, whereas 96_2.tif contains region above the core point. Since the proposed system relies on minutiae neighborhood, the lack of corresponding minutiae pair due to limited overlapping area from the stored and query template pair

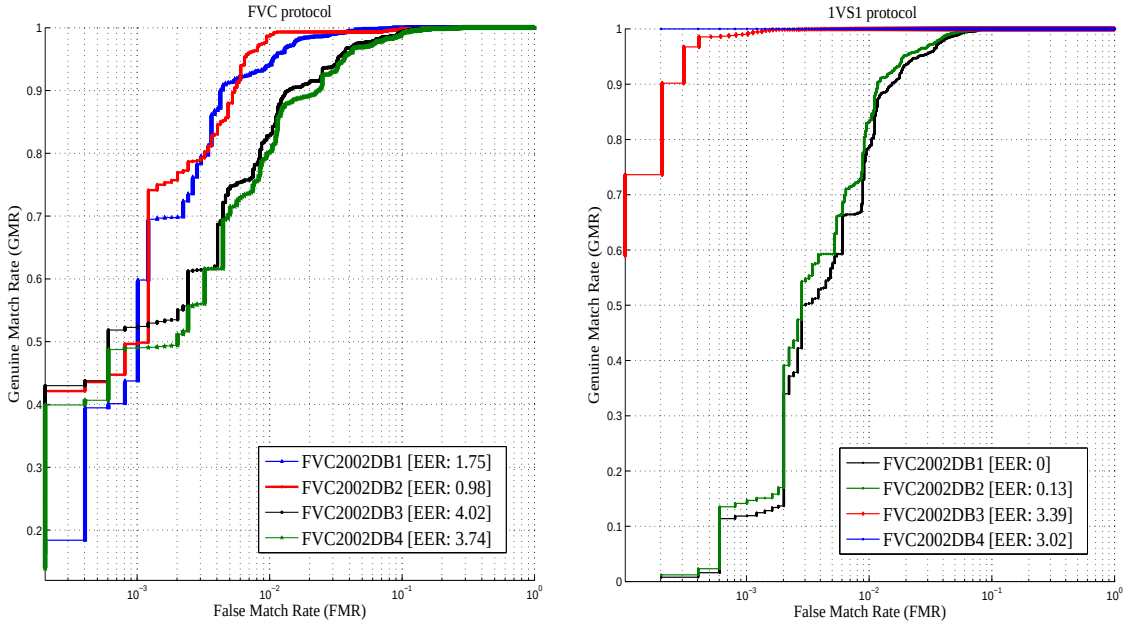


Figure 4.3: ROC curves for FVC2002 under FVC and 1VS1 protocols

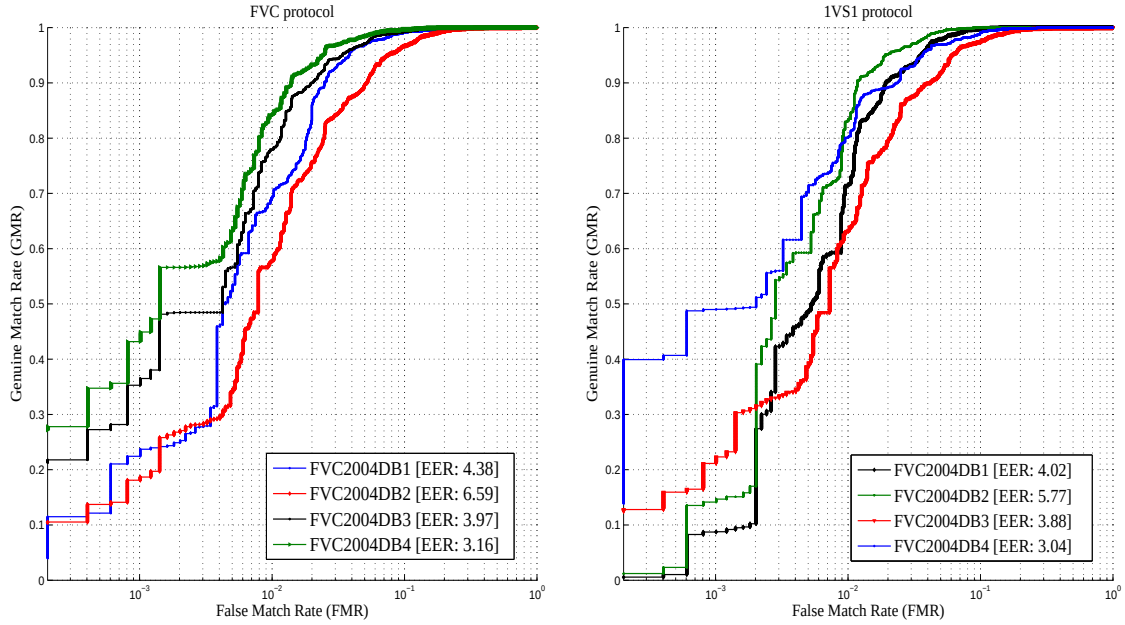


Figure 4.4: ROC curves for FVC2004 under FVC and 1VS1 protocols

causes comparison trial to fail. The method performs better on DB4, in comparison to other datasets of FVC2004 database in both protocols. Nevertheless, we achieve high EER for all four datasets of the FVC2004 database since all the users were requested to put deliberate perturbations at the time of acquisition [53].

FVC2006: For FVC2006 database, the ROC curves are shown in Fig. 4.5 for FVC as well as 1VS1 protocols. All these four datasets (DB1, DB2, DB3 and DB4 of FVC2006) are selected among the heterogeneous populations (i.e., manual workers and elderly people) allowing the most difficult fingerprints according to quality index with explicit distortions such as large amounts of rotation and displacement, wet/dry impressions, etc. The dataset DB1 contains small sized poor quality images with missing minutiae. Therefore, the method produces high EER on the DB1 dataset. The method performs optimally on the DB2 dataset for both protocols due to the presence of relatively good quality images. Datasets DB3 and DB4 consist of more number of poor quality images in comparison to DB2. Therefore, it is observed that the performance of the method degrades heavily for DB3 and DB4 datasets of FVC2006 database.

Further, we also observe that the proposed method performs better with 1VS1 protocol compared to standard FVC protocol. The reason lies in the number of genuine verification attempts. In case of 1VS1 protocol, the first two images of the same user are utilized, whereas all eight images from each user are utilized in the genuine verification for the standard FVC protocol. However, we achieve high EER for 1VS1 protocol as compared to FVC protocol for the DB3 and DB4 datasets of the FVC2006 database since the first two images are noisy and involve non-overlapping regions.

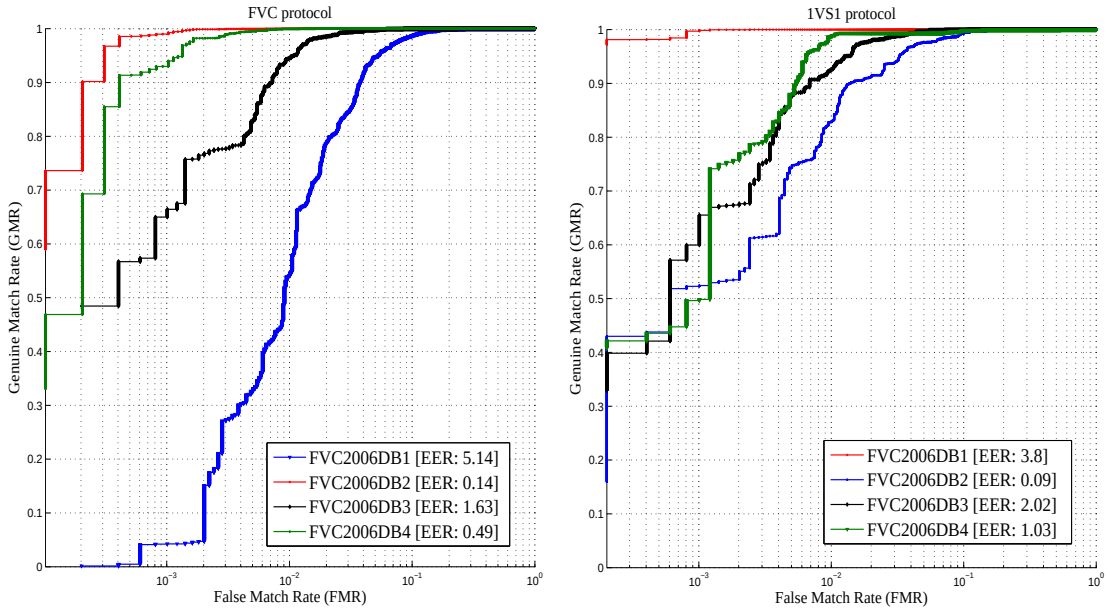


Figure 4.5: ROC curves for FVC2006 under FVC and 1VS1 protocols

4.5.4.2 Different key scenario

In the second set of experiment, we assign the different projection matrices to different users by altering the seed value and test our method for both the protocols. For FVC2002, our method performs ideal for all datasets (EER = 0) with both protocols. Moreover, we achieve an EER of 0 for DB1 and DB2 datasets of FVC2004. DB3 and DB4 datasets consist of more number of poor quality images with very few or missing minutiae in comparison to datasets DB1 and DB2. For DB3 and DB4 dataset, the method gives EERs of 0.08 and 0.03, respectively. For FVC2006, we achieve an EER close to 0 for DB1, DB2, DB3, and DB4 using FVC and 1VS1 protocols. Therefore, it is evident that the performance of the method in the different key scenarios is almost ideal for all datasets.

4.5.5 Baseline comparison

To perform a fair comparison, the verification performance of the proposed cancelable biometric system is analyzed with respect to the baseline biometric system (i.e., original ridge features). Further, a comparison process relying on the original minutiae should be taken into account, since the employed ridge-based representation is already part of the process generating the proposed protected templates. Therefore, we compare the performance of the method under three scenarios i.e. original minutiae comparison, original ridge features comparison, and protected templates comparison. In this experiment, first, we compute the performance for original minutiae comparison based on adaptive image enhancement method proposed by Bartunek et al. [155]. The approach involves publicly available Bozorth3 minutiae matcher [156] from NIST to evaluate the performance. Next, we compute the performance using original ridge features of the query and stored templates. Further, we apply the proposed approach to derive cancelable template and compare the stored and query templates in the transformed domain. Table 4.3 reports the EERs obtained from this experiment for different databases. It has been observed that the proposed ridge-based computation outperforms the original minutiae comparison since Bozorth3 does not perform well for poor quality fingerprint images with fewer minutiae points. Further, Bozorth3 is not robust against the alignment and scale deformations present between the stored and query templates. Therefore, it is evident that the proposed method performs better than the Bozorth3 matcher.

For FVC protocol, the reported results in Table 4.3 exhibit that there is a minor degradation of 0.19%, 0.15%, 0.05%, and 0.07% in the performance for DB1, DB2, DB3, and DB4 of FVC2002, 0.053%, 0.07%, 0.033%, and 0.04% for DB1, DB2, DB3, and DB4 of FVC2004, and 0.04%, 0.14%, 0.037%, and 0.32% for DB1, DB2, DB3, and DB4 of FVC2006, respectively with reference to original ridge features. The performance degradation occurs due to cancelable transformation. For 1VS1 protocol, the reported results in Table 4.4 indicate that the performance is degraded by 0%, 0.85%, 0.08%, and 0.09% for DB1, DB2, DB3, and DB4 of FVC2002, 0.05%, 0.11%, 0.04%, and 0.05% for DB1, DB2, DB3, and DB4 of FVC2004, and 0.048%, 2.0%, 0.09%, and 0.17% for DB1, DB2, DB3, and DB4 of FVC2006, respectively with reference to original ridge features. Therefore, we can conclude that performance degradation produced by the transformation is very low.

Table 4.3: Baseline comparison for FVC protocol

Dataset	EER											
	Original minutiae comparison				Without cancelable transformation				With cancelable transformation			
	DB1	DB2	DB3	DB4	DB1	DB2	DB3	DB4	DB1	DB2	DB3	DB4
FVC2002	2.8	2.3	6.5	3.9	1.47	0.89	3.81	3.49	1.75	0.98	4.02	3.74
FVC2004	9.6	5.9	6.2	6.6	4.14	6.12	3.84	3.03	4.38	6.59	3.97	3.16
FVC2006	5.2	1.39	2.91	1.27	4.93	0.12	1.57	0.37	5.14	0.14	1.63	0.49

Table 4.4: Baseline comparison for 1VS1 protocol

Dataset	EER											
	Original minutiae comparison				Without cancelable transformation				With cancelable transformation			
	DB1	DB2	DB3	DB4	DB1	DB2	DB3	DB4	DB1	DB2	DB3	DB4
FVC2002	0.91	1.02	4.3	3.89	0	0.07	3.13	2.77	0	0.13	3.39	3.02
FVC2004	4.65	6.30	4.72	3.95	3.81	5.19	3.69	2.89	4.02	5.77	3.88	3.04
FVC2006	4.87	1.04	2.65	2.83	3.62	0.03	1.83	0.88	3.8	0.09	2.02	1.03

4.5.6 Comparison with other state-of-the-art methods

The approaches in [23, 69–71, 73, 76, 79] utilized FVC 2002 database to evaluate the performance of their method using standard FVC protocol. Further, Wong et al. [74] also evaluated

the performance on DB1 of FVC2004. In addition to each dataset of FVC2002, Ferrara et al. [22,25] evaluated their methods on DB1 of FVC2004 and DB2 of FVC2006. The authors, Yang et al. [71] and Wang et al. [23] evaluated the performance on DB2 of FVC2002 with the 1VS1 protocol. Ferrara et al. [22, 25] also evaluated their methods on DB2 of FVC2006 and each datasets of FVC2002 database for 1VS1 protocol. Therefore, we compare our method with these current state-of-the-art approaches [22, 23, 25, 69–71, 73, 74, 76, 79] in the literature. Table 4.5 and 4.6 summarize the comparison of different state-of-the-art methods in terms of EER on different FVC datasets for 1VS1 and FVC protocols, respectively. From Table 4.5, we observe that the best result reported in existing literature is EER = 0, 0.02, 3.43, 3.37, and 0.03 for FVC2002DB1, FVC2002DB2, FVC2002DB3, FVC2002DB4, and FVC2006DB2, respectively, whereas our approach yields EER of 0, 0.13, 3.39, 3.02, and 0.09 for FVC2002DB1, FVC2002DB2, FVC2002DB3, FVC2002DB4, and FVC2006DB2, respectively. From Table 4.6, we observe that the best result reported in existing literature is EER = 1, 0.99, 5.24, 4.84, 10.36, and 0.17 for FVC2002DB1, FVC2002DB2, FVC2002DB3, FVC2002DB4, FVC2004DB1, and FVC2006DB2, respectively, whereas our approach gives EER of 1.75, 0.98, 4.02, 3.74, 4.38, and 0.14 for FVC2002DB1, FVC2002DB2, FVC2002DB3, FVC2002DB4, FVC2004DB1, and FVC2006DB2, respectively. However, we can observe that the performance of the proposed method for the DB2 dataset of FVC2002 and FVC2006 is slightly lower than [22] in 1VS1 protocol, and the EER of FVC2002DB1 is lower than that of Wang et al. [79], but it is comparable.

The proposed method outperforms existing methods due to the improvements in invariant feature evaluation, feature encoding, and random projection based transformation. We evaluate ridge features (i.e. ridge count and mean ridge orientation) in comparison to the pair-minutiae distance [76], relative orientation based methods [70, 76], and the geometrical transformation based techniques [74]. In our method, ridge features are utilized to cope up scale, translational, and rotational deformations in comparison to the other existing literature described in Section 2.2 of Chapter 2. The methods proposed by Yang et al. [71] and Boult et al. [69] applied quantization over feature string. Hence, a small perturbation may output a different index or regions. Our approach performs better as it involves ridge-based co-ordinate system to evaluate features. In our method, logarithm and random projection transformations lead to superior performance over other techniques since these reduce the

intra-class variation and seize substantial discrimination among templates of different users. In addition, it involves simpler (less complex) transformation in comparison to DFT based approaches [23, 73, 79] in literature. The methods proposed in [22, 25] are vulnerable to annealing attack [157]. Our method performs better than the methods proposed by Ferrara et al. [22, 25] since it overcomes the scenario of annealing attack [157] [See Section 4.6.4]. Hence, it is evident that the proposed transformation outperforms the existing methods.

Table 4.5: Performance comparison with existing methods for 1VS1 protocol

Datasets		Methods			
		Yang et al. [71]	Ferrara et al. [22]	Wang et al. [23]	Proposed method
FVC 2002	DB1	-	0	3	0
	DB2	0.72	0.02	2	0.13
	DB3	-	3.43	7	3.39
	DB4	-	3.37	-	3.02
FVC 2006	DB2	-	0.03	-	0.09

Table 4.6: Performance comparison with existing methods for FVC protocol

Datasets		Methods										
		Ahmad et al. [76]	Wang et al. [73]	Lee et al. [70]	Wong et al. [74]	Yang et al. [71]	Boult et al. [69]	Ferrara et al. [22]	Ferrara et al. [25]	Wang et al. [23]	Wang et al. [79]	Proposed method
FVC 2002	DB1	9	3.5	3.4	4.69	-	2.1	1.88	3.3	4	1	1.75
	DB2	6	4	-	5.03	4.53	1.2	0.99	1.8	3	2	0.98
	DB3	27	7.5	-	-	-	-	5.24	7.8	8.5	5.2	4.02
	DB4	-	-	-	-	-	-	4.84	6.6	-	-	3.74
FVC 2004	DB1	-	-	-	10.36	-	-	-	6.3	-	-	4.38
FVC 2006	DB2	-	-	-	-	-	-	0.17	0.3	-	-	0.14

" – " indicates that the author(s) have not reported the results or results are reported for partial dataset, in their work.

4.6 Security analysis

The security of the derived protected template is guaranteed when an adversary has no information about the transformation. If an adversary unveils any information about cancelable transformation, the security of the proposed system is guaranteed by three factors: non-invertibility, revocability, and diversity. In this section, we analyze our method with respect to these three contexts.

4.6.1 Non-invertibility

The term, non-invertibility refers that it should be computationally infeasible to derive the original fingerprint template from the protected template. Note that a randomized projection matrix ($\mathcal{R}$) is utilized to generate a cancelable template from the log template ($\mathcal{L}$). To meet the non-invertibility requirement, we have adopted a reference architecture proposed by Breebaart et al. [39]. Figure 4.6 shows the reference architecture where the protected template (C^T), random projection matrix ($\mathcal{R}$), and the parameters (s, b) can be presumed as pseudo-identity, auxiliary data, and supplementary data, respectively.

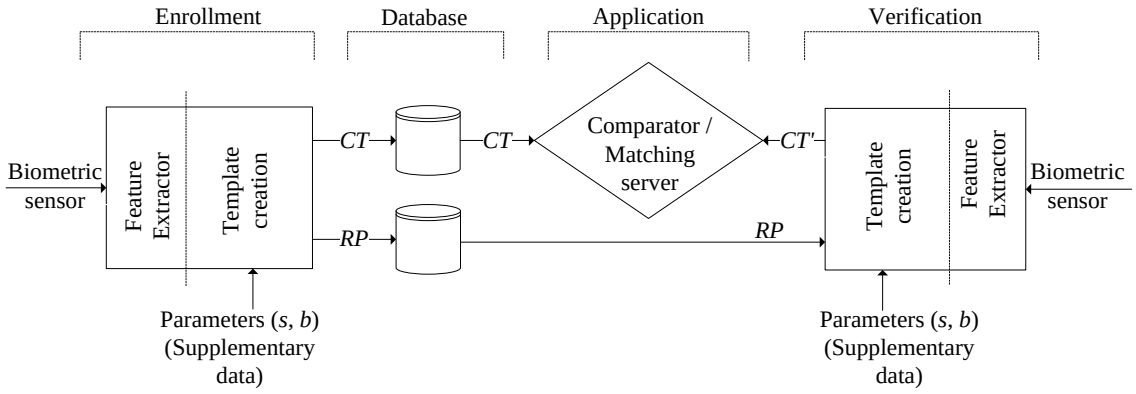


Figure 4.6: Reference architecture for the creation, storage, and verification of the protected template

In the reference architecture, the protected template (C^T) is derived at the enrollment phase. The biometric sample, ridge features, and the parameter (s, b) are destroyed after the successful verification of the query protected template with the stored template. Due to privacy preservation, protected template may be / parameters may be either issued for a limited period or may require revocation when compromised. Moreover, the biometric characteristics may get affected due to aging effects. Hence, it requires renewal after a validity period regulated through watch list. The protected template C^T along with the $\mathcal{R}$ and supplementary data (s, b) are stored in the database. During verification, a protected query template ($C^{T'}$) is generated from the issued $\mathcal{R}$, biometric sample, and the parameters (s, b). Next, the stored protected template (C^T) and the query protected template ($C^{T'}$) are forwarded to a comparator/matching server via the communication interface to verify the identity. In this section, we analyze the criterion of non-invertibility with three different

architectural components i.e. database, matching server, and communication interface for information exchange.

4.6.1.1 Compromised database

In this scenario, an attacker can reveal the database i.e. protected template (C^T) and the random projection matrix ($\mathcal{R}$). On the possession of this information, the attacker would not be able to retrieve the log template ($\mathcal{L}$) since the size of $\mathcal{R}$ is $s \times t$ where $t < s$ and the entries of $\mathcal{R}_{s\times t}$ are independent and identically distributed (i.i.d.) Gaussian random variables. Evaluation of $\mathcal{L}_{n\times s}$ from $C^T_{n\times t}$ results to find a solution for underdetermined system because it is hard to find s unknowns from t linearly independent equations where $t < s$. Further, it has also been proved in Du et al. [158] that if the projection matrix follows the condition $t \leq \frac{s}{2}$ and entries in $\mathcal{R}$ are i.i.d., it is very hard to find the $\mathcal{L}$ from C^T. Moreover, even if the attacker achieves supplementary information (s, b), it would be infeasible to unveil the $\mathcal{L}$ as analyzed in the third scenario i.e. compromised communication interface.

4.6.1.2 Compromised matching server

Let us assume that an attacker unveils matching server i.e. the stored protected template (C^T) and query protected template ($C^{T'}$). Next, an attacker tries to evaluate $\mathcal{L}$ by correlating the information contained in C^T and $C^{T'}$. In this situation, an attacker would not be able to retrieve $\mathcal{L}$ since he does not have any information about the $\mathcal{R}$.

4.6.1.3 Compromised communication interface

In this scenario, an attacker may have control over communication interface between the database and matching server. In this situation, the adversary would be able to estimate the stored protected template (C^T), query protected template ($C^{T'}$), and the random projection matrix ($\mathcal{R}$). On the possession of these information, the attacker may utilize C^T and $\mathcal{R}$, or $C^{T'}$ and $\mathcal{R}$ to retrieve the log template ($\mathcal{L}$). This situation is identical to the first scenario i.e. compromised database. Further, the attacker may correlate C^T and $C^{T'}$ to evaluate $\mathcal{L}$. This situation is same as the second scenario i.e. compromised matching server.

Further, we assume that the attacker unveils the approximate $\mathcal{L}$ by applying known key distinguishing attack. In this situation, the imposter tries to estimate C^P or approximate C^P using the value of parameter b. However, it would not be possible to retrieve the original

ridge features since inversion involves the computation of a square root which gives one to many correspondences as defined in Eq. 4.11-4.14.

$$w = \left\lfloor \frac{\sqrt{8\,C^P + 1} - 1}{2} \right\rfloor \tag{4.11}$$

$$t = \frac{w^2 + w}{2} \tag{4.12}$$

$$ro = C^P - t \tag{4.13}$$

$$rc = w - ro \tag{4.14}$$

where, rc, ro, and C^P represent the ridge count, mean ridge orientation, and transformed paired output, respectively. w and t are intermediate values in the calculation and $\lfloor\rfloor$ is the floor function. Hence, it would be very hard to invert C^P to attain original ridge features. Therefore, it can be stated that our method preserves the criterion of non-invertibility.

4.6.2 Revocability

The term revocability refers to the design of a new protected template if stored template gets leaked. The newly generated template should be adequately dissimilar to the compromised one. In this work, a new protected template can be issued just by altering $\mathcal{R}$. To ensure the potent revocability, the biometric templates that are derived by applying different $\mathcal{R}$s for the same user in different applications, should not be able to verify each other. Here, the random projection is motivated by the Johnson-Lindenstrauss (JL) lemma described in [159]. The lemma states that:

L_1: For any $0 < \epsilon < 1$ and an integer k, let t be a positive integer such that $t \geq t_0 = \mathcal{O}(\epsilon^{-2} log\ k)$. For any set B of k points in $\Re^s$, there exists a map $f : \Re^s \rightarrow \Re^t$ such that: for all $u, v \in B$,

$$(1 - \epsilon) \left\|u - v\right\|^2 \leqslant \left\|f(u) - f(v)\right\|^2 \leq (1 + \epsilon) \left\|u - v\right\|^2 \tag{4.15}$$

where, u and v are two randomly derived vectors in the s-dimensional Euclidean space, $u, v \in \Re^s$. For inner-product based similarity, it states that:

$$\frac{u.v}{\|u\|.\|v\|} = \frac{Au.Av}{\|Au\|.\|Av\|} \pm \mathcal{O}(\epsilon)$$

This lemma provides a proof that the similarity between any two vectors can be preserved up to a factor of ϵ when these vectors are projected onto a random t-dimensional subspace. Such type of mapping can be performed by utilizing a matrix containing orthonormal columns as described in Lemma 5.2 of [160]. The lemma states that:

L_2: Let $\mathcal{R}$ be a matrix of size $s \times t$ where $t < s$. Each of the entries of $\mathcal{R}$ are i.i.d. Gaussian random variable with zero mean and variance $\frac{1}{s}$, $r_{ij} \sim s(0, \frac{1}{s})$, i=1,$\cdots$,s , j=1,$\cdots$, t. Let $W = \mathcal{R}^T\mathcal{R}$ and $W^{'} = \mathcal{R}\mathcal{R}^T$; then,

$$E(w_{i,j}) = \begin{cases} 1, & i = j \\ 0, & i \neq j \end{cases} \qquad Var(w_{i,j}) = \begin{cases} \frac{2}{s}, & i = j \\ \frac{1}{s}, & i \neq j \end{cases} \tag{4.16}$$

$$E(w^{'}_{i,j}) = \begin{cases} \frac{t}{s}, & i = j \\ 0, & i \neq j \end{cases} \qquad Var(w^{'}_{i,j}) = \begin{cases} \frac{2t}{s^2}, & i = j \\ \frac{t}{s^2}, & i \neq j \end{cases} \tag{4.17}$$

where, $w_{i,j}$ and $w^{'}_{i,j}$ are elements of W and $W^{'}$, respectively.

The output here confirms that $E[\mathcal{R}^T\mathcal{R}] = I$, where I denotes an identity matrix. The elements of $\mathcal{R}^T\mathcal{R}$ are centered around their mean with very small variance. This suggests that vectors with random directions are close to orthogonal (i.e. $\mathcal{R}^T\mathcal{R} \approx I$). Further, it is obvious that if $r_{ij} \sim s(0, \frac{1}{s})$, then, $E[\|r_j\|^2] = E[\sum_{i=1}^{s} r_{ij}^2] = 1$ and $Var[\|r_j\|^2] = Var[\sum_{i=1}^{s} r_{ij}^2] = \frac{2}{s}$, where r_j denotes individual columns of $\mathcal{R}$. This mathematical proof ensures that columns in $\mathcal{R}$ are saturated around 1 which signifies that the vectors in $\mathcal{R}$ are nearly orthonormal. For revocable template generation, we evaluate the probability of false match when biometric data of same user is exploited with different random projection matrices, denoted as P_{fm}. Therefore, the revocability i.e. probability of a protected template being revocable can be defined as: $P_r = 1 - P_{fm}$. The higher value of P_r corresponds to better revocability. In general, zero P_{fm} cannot be obtained if we apply random projection directly onto $\mathcal{L}$. Further, this probability can be reduced by adding an extra vector $d \in \Re^s, d_i >> th$ to the $\mathcal{L}$,

$\mathcal{L}' = \mathcal{L} + d$, where th denotes threshold of verification system [161]. In a similar manner, the biometric templates with $P_r \approx 1$ could be derived, if different random projection matrices are exploited on the original template of the same user nullifying the record multiplicity attack [162]. In this work, we achieve P_r= 0.982 corresponding to a threshold, th=0.65.

We also verify this security aspect empirically by generating 100 different protected templates using 100 different projection matrices from the same finger. Next, we perform a comparison of these 100 templates with the originally enrolled template to obtain the pseudo-imposter scores. We achieve mean and variance of (0.7519; 0.018), (0.3982; 0.177), and (0.3563; 0.189) for genuine, imposter, and pseudo-imposter distributions, respectively. These values indicate that mean and variance for the pseudo-imposter distribution are at a distant to genuine distribution and near towards the imposter distribution. Moreover, we obtain FMR = 0, which depicts that all queries are rejected. This signifies that the derived templates are dissimilar to the enrolled templates for the same finger. Although, the templates are generated from the same finger pattern, they are uncorrelated to each other. Therefore, the claim of revocability is preserved.

4.6.3 Diversity

The characteristics of diversity state that it should derive numerous templates and these derived templates should not provide positive biometric claim over other applications to avoid cross-matching. In our method, multiple fingerprint templates can be derived by choosing the different projection matrices ($\mathcal{R}$) with the different seed values (κ). In addition, the two parameters illustrated in Section 4.5.3; the number of sectors (s) and log-base value (b) can be utilized to derive numerous templates. The derived protected templates are sufficiently different from the raw fingerprint template which indicates that a user can enroll itself with different templates in different applications without any cross-matching. Hence, it has been confirmed that the method validates the property of diversity.

4.6.4 Other attacks

We also analyze the possibility of different types of attacks namely Attacks via Record Multiplicity, pre-image, cross-matching, distinguishing and annealing attacks to validate the robustness of the proposed work:

4.6.4.1 Attack via Record Multiplicity (ARM)

This is a scenario where the attacker employs multiple stolen protected templates with or without associated parameters to generate original template [163]. If the attacker is able to reveal enough protected templates and their corresponding random projection matrices, the series of linear equations can be solved to obtain the approximate entries of log template. Further, if the projection matrix follows the conditions $t \leq \frac{s}{2}$, and entries in $\mathcal{R}$ are i.i.d., it is very hard to find the $\mathcal{L}$ from C^T. If adversary is able to retrieve the C^T and corresponding $\mathcal{R}$s from different applications, he can append $\mathcal{R}$s column-wise such that [$\mathcal{R}_1$ $\mathcal{R}_2$ $\cdots$ $\mathcal{R}_n$] = s. Further, the adversary solves linear system of equations to obtain the original log template, $\mathcal{L}$. In spite of this effort, he would not be able to generate the actual $\mathcal{L}$ because different applications utilize different samples of the same subject where the intra-variance is present among the features. Hence, $\mathcal{L}$ would not be exactly same for different samples of the same subject. Moreover, it would be very unlikely that the attacker is able to reveal different protected templates alongwith the corresponding $\mathcal{R}$ for the same user from different applications. Further, even if the attacker is able to compute approximate $\mathcal{L}$, he has to compute C^P by inverse log operation using b value. From paired output C^P, the attacker has to evaluate Eq. 4.11-4.14 to compute ridge features. As inversion of paired output, C^P results into multiple values, it would be very hard to evaluate original ridge features (rc, ro). Therefore, it is evident that our approach is resilient enough against ARM attack when a user enrolls himself by different impressions of same fingerprint. However, if the user uses same biometric impressions for different applications, the proposed technique may not resist over ARM attack. This limitation would be looked in the future.

4.6.4.2 Pre-image attack

In this attack, the attacker can utilize multiple protected instances to derive a pre-image instance. Knowledge of security can also be challenged using feature order with different projection matrices to create a fake template. Biohashing based methods [26–28, 164] derive binary string by projecting feature vectors with user-specific random numbers. In contrast, the bit-string could be easily exploited to disclose original minutiae information. Moreover, the projection matrix in Biohashing is not only a square matrix but also have orthonormal row vectors i.e. $R_{proj} \cdot R_{proj}^T$=I, where R_{proj}^T is the pseudo-inverse of R_{proj}, and I is the iden-

tity matrix. This makes the Biohashing methods vulnerable to pre-image attack. However, the proposed random projection based transformation is different to the methods involving Biohashing. Here, the random projection is utilized to hide the log template among infinitely many possible solutions. Also, our method does not depend on the order of feature components while generating the original as well as the protected template. Further, any value could not be investigated from two projected feature vectors in any position due to a difference in the size of enrolled and query templates. Hence, pre-image attack could not be utilized to derive the original template in our method.

4.6.4.3 Cross-matching attack

The cross-matching attack refers to the scenario where an adversary is able to compromise the databases stored in different applications. The protected templates each from different applications are analyzed to restore the original template. However, the random projection transformation described in Eq. 4.6 avoids any possibility of cross-matching attack across different applications.

4.6.4.4 Distinguishing attack

In distinguishing attack [165], an imposter tries to utilize the same protected template captured from different applications to derive the original template by correlating the information. To prevent this, different protected templates can be utilized in different applications. However, the attacker can retrieve different protected templates (C^T) along with the known random projection matrices ($\mathcal{R}$) from different applications in the known-key distinguishing attack. In this situation, the attacker would be able to unveil log template ($\mathcal{L}$). Further, he may estimate the paired output (C^P) or approximate C^P using the value of b or approximately equal to b. However, it is not possible to derive original ridge features since the Cantor pairing function is irreversible as defined in Eq. 4.11-4.14.

4.6.4.5 Annealing attack

In this attack [157], the protected template is divided into multiple regions, and some regions of a sample template are paired with some regions of the reference template to evaluate similarity score. If the similarity score exceeds the threshold, the vicinity corresponding to

sample's region is included in the gummy template. This step is repeated until it outputs a gummy template including all matched vicinities. Our approach is robust against this type of attack due to the following reasons:

1. Our approach evaluates the nearest neighbor minutiae point for each minutiae point causing different radii to different minutiae points. Hence, it is very hard to map the gummy template with the original template which is derived from the multiple regions with the variable radius.

2. Ridge features are utilized for neighboring minutiae in each sector instead of relative distances or the directional difference between minutiae pairs. Here, the measured ridge features are invariant to inter-ridge distances and locations of minutiae points.

4.7 Summary

In this work, we have proposed alignment free cancelable fingerprint template generation technique. The proposed technique does not rely on detection of singular points. We divide the input fingerprint image into a number of sectors of equal angular width considering each minutia as a reference and use the nearest neighbor minutiae in each sector to compute transformation invariant ridge count and mean ridge orientation features from each sector. Cantor pairing function is applied to encode these features uniquely. Further, the pointwise logarithm operation is exploited to yield uniformly distributed features. Finally, a random projection is adopted to derive a non-invertible and revocable cancelable template. Experimental evaluation performed over four datasets of FVC2002, FVC2004, and FVC2006 databases depicts that the significant performance improvement is achieved as compared to the current state-of-the-art techniques. Moreover, the security analysis of our work confirms that our approach fulfills the desired characteristics of template protection schemes and preserves the recognition performance too.

Chapter 5

Score-level fusion for cancelable multi-biometric verification

Integration of scores from multiple biometric modalities has become promising to alleviate the limitations of unibiometric systems such as sensitivity to outliers, erroneous authentication caused by intra-class variability and low verification performance due to poor quality. As a multimodal biometric system is able to attain performance improvement, template security schemes aim to protect original biometric data. The compositions of these two schemes achieve a win-win scenario for the template protection and performance enhancement. In this work, we propose a two-level score level fusion approach for integrating the scores obtained from cancelable templates of different biometric modalities. As a result, we achieve a significant improvement in overall recognition performance providing secure authentication for the different application. At the first level, scores from multiple matchers are combined using a novel mean-closure weighting (MCW) technique to achieve the desired score for a particular biometric modality. The proposed solution is based on the region of uncertainty between the genuine and imposter distribution. Further, the derived scores from different modalities are integrated using a novel rectangular area weighting (RAW) technique at the second level to obtain the overall fused score. The block diagram of the proposed fusion framework is illustrated in Fig. 5.1. The remainder of this chapter is organized as follows. Section 5.1 briefly describes the existing methods utilized to compute match scores. The proposed score level fusion scheme is described in Section 5.2. Section 5.3 narrates the verification of identity based on the combined scores. Section 5.4 demonstrates and analyzes experimental results as well as compares the proposed method with some existing score-level

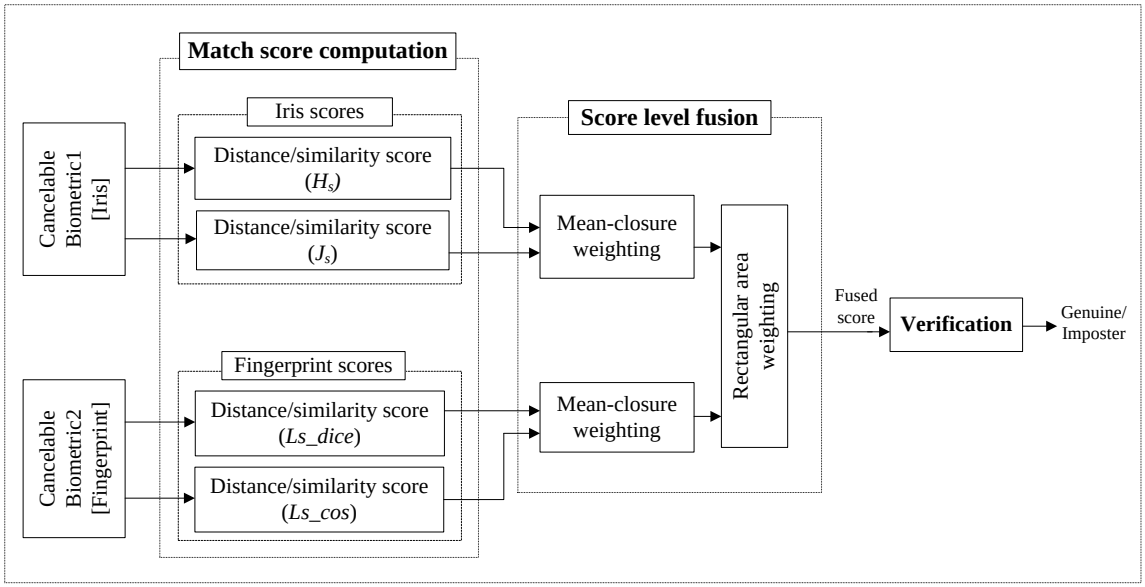


Figure 5.1: Block diagram of the proposed score level fusion framework

fusion approaches. Security analysis of the proposed cancelable mulibiometric verification is described in Section 5.5. Finally, Section 5.6 summarizes the chapter.

5.1 Match score computation

In this section, we present the distance/similarity metrics utilized to compute match scores for cancelable iris and fingerprint biometric. The computation of match scores involves the comparison between cancelable enrolled and cancelable query template. The scores computed from individual biometric systems represent either dissimilarity (distance) or similarity measure. Therefore, it is needed to convert all the scores alike in nature. In this work, we transform all the scores into similarity measure following the common practice.

5.1.1 Cancelable iris match scores computation

The comparison between cancelable enrolled and cancelable query template is performed to evaluate match scores for iris biometric. To derive cancelable iris template, we apply the same methodology proposed in chapter 3. For convenience, we briefly describe this method. First, iris images are pre-processed using Masek's [50] and Daugman's [65] techniques. Then, IrisCodes are extracted in the form of a 0-1 matrix using 1-D Log-Gabor filter [50]

with phase quantization from the pre-processed iris images. Thereafter, 8-bit left and right shifting is performed to derive rotation-invariant IrisCode and the rotation invariant IrisCode is transformed into a row vector. Next, the decimal vector is derived by partitioned the row vector into fixed size blocks. Then, a Look-up table is created to map the decimal-encoded vector and to generate the cancelable template. Finally, matching between the protected enrolled and protected query iris template is performed in the transformed domain to measure the match score. First, we compute the similarity in Hamming domain for its simplicity in the evaluation. Hamming distance (HD) is the sum of non-equivalent bits (exclusive-OR) between the stored and query templates. The Hamming similarity is computed by subtracting normalized Hamming distance from one, as defined in Eq. 5.1:

$$\text{Hamming similarity } (H_s) = 1 - \frac{1}{N}\sum_{i}^{N} E_i \oplus Q_i \tag{5.1}$$

where, Q_i and E_i are the i^{th} bits of the query and enrolled templates, respectively. N is the total number of bits in the template.

Next, Jaccard similarity is evaluated between the protected query and protected enrolled iris template. Jaccard similarity is the overlap of bits in E and Q except the ill condition i.e. 0-0 overlap as defined in Eq. 5.2. Jaccard similarity is computed to elude the ill match condition (0-0 match) between the protected query and protected enrolled templates.

$$\text{Jaccard similarity } (J_s) = \frac{N_{11}}{N_{01} + N_{10} + N_{11}} \tag{5.2}$$

where,

N_{11}: Number of positions where E, Q both have a value of 1,

N_{01}: Number of positions where value in E is 0 and Value in Q is 1,

N_{10}: Number of positions where value in E is 1 and Value in Q is 0.

5.1.2 Cancelable fingerprint match scores computation

Cancelable enrolled and cancelable query fingerprint templates are compared to calculate match scores for fingerprint biometric. To derive cancelable fingerprint template, we apply

the method as proposed in chapter 4. For reader's clarity, we describe the method briefly. First, the input fingerprint image is preprocessed to obtain the thinned image and to extract the minutiae information. Next, we form a nearest-neighbor structure around each minutiae point using the ridge-based co-ordinate system and compute the ridge features from the thinned image and minutiae information. Thereafter, we apply cantor pairing function to encode the ridge features uniquely. Finally, the random projection is applied to the paired output to derive the protected template. In the verification stage, the same procedure is followed to generate the protected template from the query fingerprint.

Matching between enrolled and query templates is performed in the transformed domain to maintain security. We adopt the inner product based similarity measures since similarity computation requires measuring the likelihood between the rows in the protected enrolled template (E) to the rows in protected query templates (Q). First, we utilize Dice coefficient to measure local similarity (Ls_dice) between each row of the enrolled and that of query templates as utilized in [75] as defined in Eq. 5.3.

$$Ls\_dice\ (i, j\,) = \frac{2E(i,:) \cdot Q(j,:)}{||E(i,:)\ ||^2 + ||Q(j,:)\ ||^2} \tag{5.3}$$

Further, we apply cosine similarity (Ls_cos) between each row of the enrolled and that of query templates to compute the normalized dot product as defied in Eq. 5.4.

$$Ls\_cos\ (i, j\,) = \frac{E(i,:) \cdot Q(j,:)}{\sqrt{||E(i,:)\ ||^2}\sqrt{||Q(j,:)\ ||^2}} \tag{5.4}$$

Next, we re-evaluate each element in local similarity matrix to avoid double matching. For this purpose, we acquire those positions where the maximum scores in $E(i,:)$, and $Q(j,:)$ coincides to obtain the filtered similarity matrix. Next, global similarity score is obtained by summing up the entries in filtered matrix and dividing by a minimum of the minutiae points in E and Q. Finally, the likelihood of the enrolled and query template being the two fingerprints of the same subject is measured to compute the global similarity scores.

5.2 Score level fusion

In general, there is a need for score normalization so that the match scores are transformed into a common interval (e.g. in the interval of [0,1]). But, normalization is not required in this work because the methods utilized in score computation generate the scores in the interval of [0,1]. However, the proposed work can be extended to the situations where the scores from different biometric modalities follow different distribution range or scores derived through different matchers may have a different range instead of [0,1]. In these situations, we can utilize the RHE normalization [166] to guarantee a meaningful score integration since it is found to be sensitive to outliers. RHE minimizes the score-sets to be normalized because of the fact that raw scores have richer information content than the normalized score. In the following, we have proposed a novel mean-closure weighting (MCW) mechanism followed by rectangular area weighting (RAW) method for optimal weight estimation. The proposed model achieves the optimal weights for different matchers corresponding to each of the regions present in the FMR/FNMR curve including the uncertainty region. Further, the fused score is utilized for multimodal verification. In this work, we evaluate the scores from protected iris and protected fingerprint biometric to explore the potential significance of cancelable multimodal biometrics with respect to security, privacy and performance improvement over the unimodal biometric system.

5.2.1 Mean-closure weighting (MCW)

Let us consider, Hamming similarity and Jaccard similarity measure to be matcher 1 and matcher 2, respectively where the scores from two matchers (s_h, s_j) are to be integrated. On the basis of Fig. 5.2, we can indicate five possible regions for different scores of any matcher. The gray color regions (i.e. R_1 and R_2) represents the region of confidence where both the regions are able to classify the scores accurately. Region 3 (R_3), region 4 (R_4), and region 5 (R_5) falls into the uncertainty where it is very difficult to classify the match scores. Therefore, it is necessary to assign more weights to the scores lying into the confidence region (i.e. R_1 and R_2) and relatively less weights to the scores in the region of uncertainty while evaluating the fused score. In this work, we estimate the weights on the basis of mean-closure metric which measures the separation of scores from mean of the matcher's

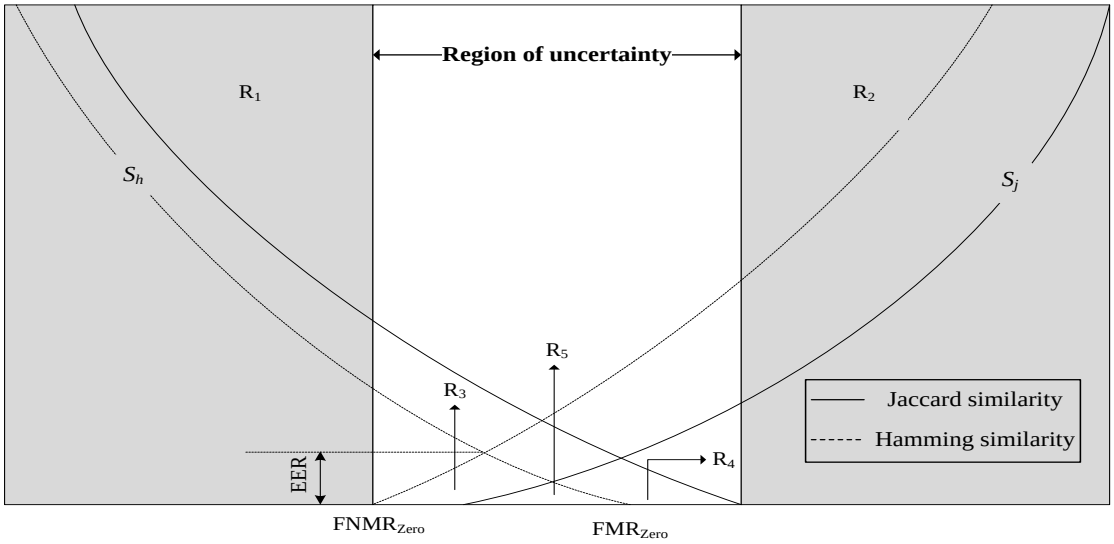


Figure 5.2: Explanatory diagram for region of uncertainty present in FMR/FNMR curve; FMR_{Zero}, $FNMR_{Zero}$, and EER correspond to matcher 1 i.e. Hamming similarity

genuine and imposter distribution for different users. The ratio of these two decides whether the user's score is close to genuine or imposter distribution of matcher 1 or matcher 2. We represent these notations as (i, m) for every pair of user and matcher. The mean-closure (Mc_i^m) for a of user-matcher pair (i, m) in a multibiometric system is defined as:

$$Mc_i^m = \left(\frac{\mu_i^m\left(gen\right) - s_m}{\mu_i^m\left(imp\right) - s_m} \right)^2 \tag{5.5}$$

where, $\mu_i^m\left(gen\right)$ and $\mu_i^m\left(imp\right)$ represents the mean of genuine distribution and mean of imposter distribution, respectively. Here, s_m denotes the similarity score. Further, the estimated weight for each matcher using MC weighting is computed as follows:

$$w_i^m = \frac{mc_i^m}{\sum_{i=1}^{M} mc_i^m} \tag{5.6}$$

where, w_i^m is the weight for matcher m, and M is the number of matchers for a particular modality. $0 \leq w_i^m \leq 1, \forall i, \forall m$, and $\sum_{m=1}^{M} w_i^m = 1, \forall i$.

Here, the weights are proportional to corresponding mean-closure i.e. more accurate matcher attains higher weights than those of less accurate matcher for user i. This user-specific score weighting scheme deals optimal with the scores lying in the region of uncertainty. Applying the weights, we achieve fused scores from different matchers of a modality.

5.2.2 Rectangular area based weighting (RAW)

In this method, the weights are estimated based on the rectangular area containing a region of uncertainty for the individual modalities in a multibiometric system. The rectangular area (RA) is evaluated using Eq. 5.7.

$$RA = EER \times (FMR_{zero} - FNMR_{zero}) \tag{5.7}$$

where, FMR_{zero} and $FNMR_{zero}$ are the points where FMR and FNMR become zero, respectively as shown in Fig. 5.3.

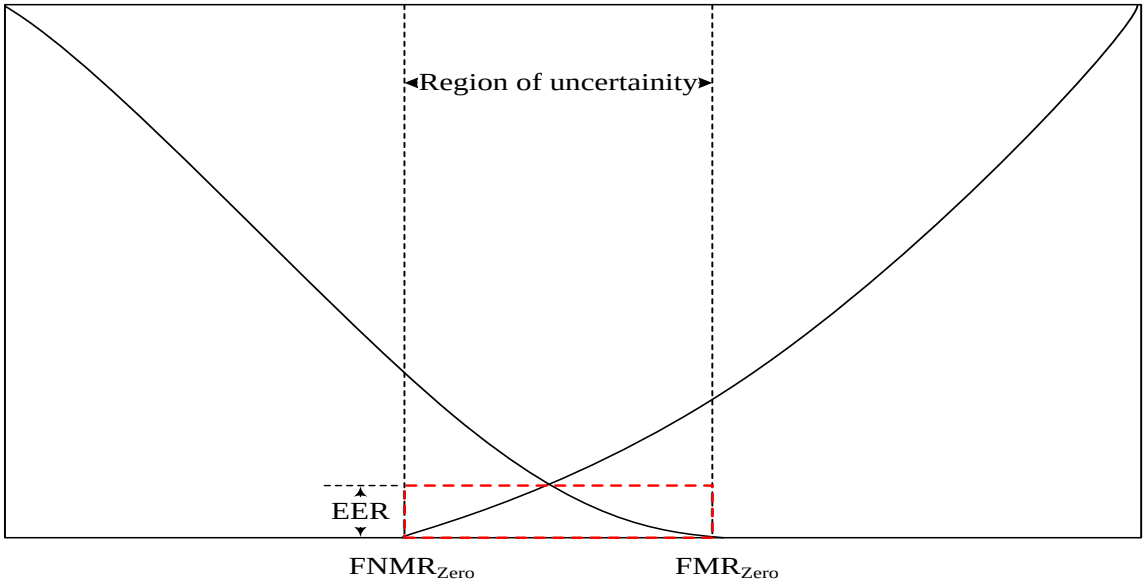


Figure 5.3: Explanatory diagram for RA containing region of uncertainty

Assuming that the estimated weight for modality k is represented as w_k, the estimated weight for modality N in a multi-biometric system using RAW technique is computed as follows:

$$w_k = \frac{\frac{1}{RA_k}}{\sum_{k=1}^{N} \frac{1}{RA_k}} \tag{5.8}$$

where, $0 \leq w_k \leq 1, \forall k, \forall N$. The estimated weights are applied in an inversely proportional manner for the available scores of the modalities i.e. lower weight for the modality that provides a larger rectangular area and vice versa.

5.3 Verification

The verification is performed by employing a threshold (t) to fused score (F_s) as defined in Eq. 5.9. In this way, a user's identity can be verified to be a genuine or an imposter.

$$Result = \begin{cases} Accept; & \text{if } F_s > t \\ Reject; & otherwise \end{cases} \tag{5.9}$$

5.4 Experimental results and analysis

To perform successful multimodal verification, we present a number of experiments to demonstrate the performance of our proposed score level fusion method. Subsection 5.4.1 describes the databases utilized in our work to integrate scores from different modalities. Subsection 5.4.2 narrates the experimental settings and performance metrics to quantify the results for each database. Furthermore, the performance of the proposed method is presented in Subsection 5.4.3. Subsection 5.4.4 presents the baseline comparison. Also, we compare the proposed methodology with the other approaches in order to specifically measure the effectiveness of the proposed approach in Subsection 5.4.5. Statistical evaluation of our approach is presented in Subsection 5.4.6.

5.4.1 Database

We evaluate the performance of our method onto three virtual databases involving iris and fingerprint modalities. The virtual databases are created due to the underlying cost and efforts related to multimodal database creation. Most of the multibiometric system proposed in literature utilize a virtual database constructed by pairing a user from one modality with a user from another modality. This pairing assumes that biometric traits of a user are independent. For iris, we use the CASIA V-3-Interval [51] database maintained by the Chinese Academy of Science and Multimedia university database (MMU1) [167]. The CASIA V-3-Interval database contains 2639 high-quality iris images from 249 users collected in two different sessions while MMU1 comprises of left and right iris images for 46 users. Considering left iris and right iris as different subjects, we find that there are 117 left and 121 right

iris subjects from 348 total subjects from 249 users of CASIA V-3-Interval which contain at least 7 samples per subject. In MMU1 database, we consider a dataset of 92 users with 5 iris samples assuming left and right iris as a different subject. For fingerprint, we use datasets DB1, DB2 of FVC2002 [53] database containing a total of 800 images of 100 subjects with eight samples each.

Virtual_A: The first virtual database comprises of 100 subjects where iris images are randomly selected from 121 right iris subjects of CASIA V-3 Interval and fingerprint from FVC2002DB1 with 7 samples per subject.

Virtual_B: The second virtual database comprises of 92 subjects where iris images are selected from MultiMedia university version-1 (MMU1) database [167] and fingerprint from FVC2002DB2 [53] with 5 samples per subject.

Virtual_C: Third virtual database comprises of 100 subjects chosen from 117 left iris subjects of CASIA V-3 Interval [51] and FVC2002DB2 [53] with 7 samples per user.

The larger context of this work is the hybrid fusion over the three described virtual multimodal databases for verification. The example images of the two modalities for Virtual_A, Virtual_B, and Virtual_C databases are shown in Fig. 5.4.

5.4.2 Experimental design

Cancelable template for iris and fingerprint are generated and are compared to derive intra-class (i.e. genuine) scores and inter-class (i.e. imposter) scores. The match scores are evaluated by adopting the FVC protocol as described in 4.5.2. As a result, the experiment is performed on 100 subjects resulting into 2100 intra-class comparison and 4950 inter-class comparisons for Virtual_A database. For Virtual_B database, 920 intra-class comparisons and 4186 inter-class comparisons are measured to evaluate the performance. We evaluate 2100 genuine comparison and 4950 imposter comparison for Virtual_C database. First, the match scores from iris and fingerprint from different matchers are integrated by applying the proposed MCW method. As a result, the fused iris and fused fingerprint scores are obtained. Next, we apply RAW method to combine these scores. Further, the performance of our method is evaluated using the four metrics as defined in Eq. 1.1-1.4 of Chapter 1.

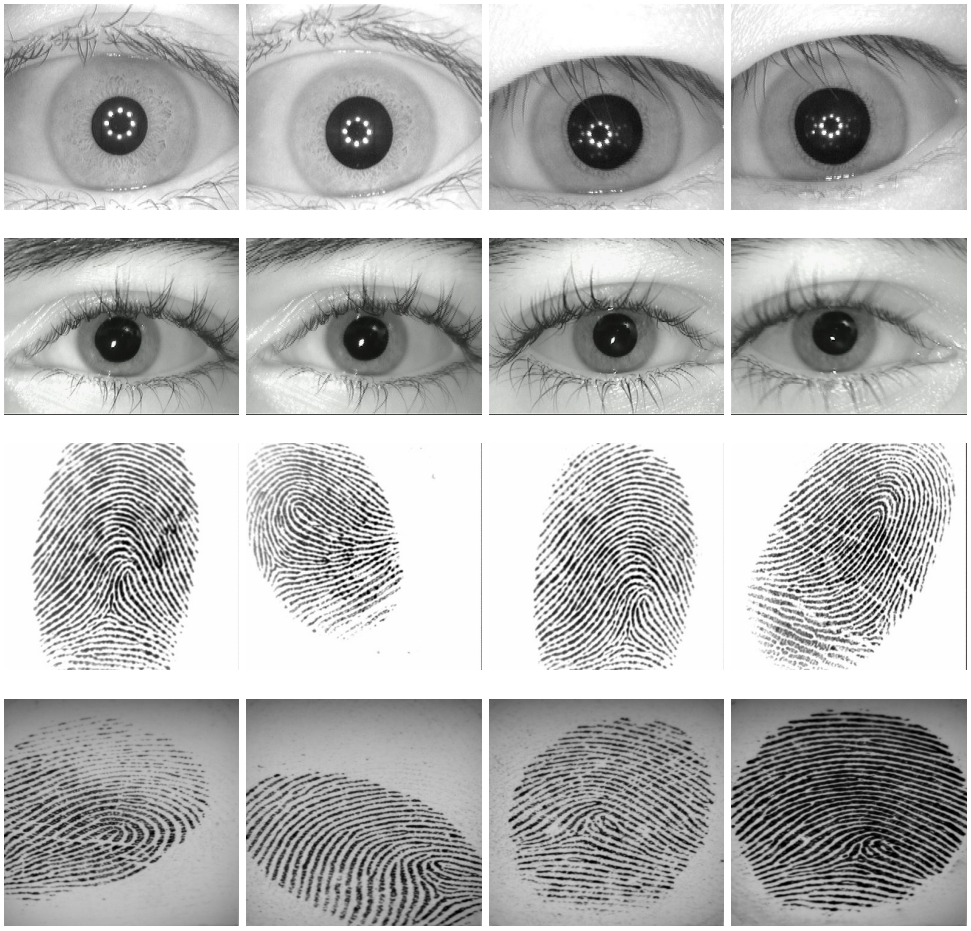


Figure 5.4: First and second rows indicate sample images from CASIA V-3.0 Interval and MMU1 databases; third and fourth rows show the example images from FVC2002DB1 and FVC2002DB2 databases, respectively

5.4.3 Performance evaluation

We evaluate EER values and ROC curves for unimodal and multimodal databases to estimate the performance of our method. Further, the performance in term of GMR @ 0.01% FMR is also calculated since a biometric system deployed in a security application is considered to be efficient if it has low EER and high GMR at low FMR [168].

Virtual_A: The multimodal biometric performance of Virtual_A is evaluated utilizing the scores obtained from CASIA V-3 Interval and FVC2002DB1. First, the performance for individual modalities (i.e. iris and fingerprint) taking part in fusion is evaluated. Next, we evaluate the performance for the multimodal biometric system. The ROC curve for Virtual_A multimodal database is shown in Fig. 5.5 which demonstrate the performance for the scores

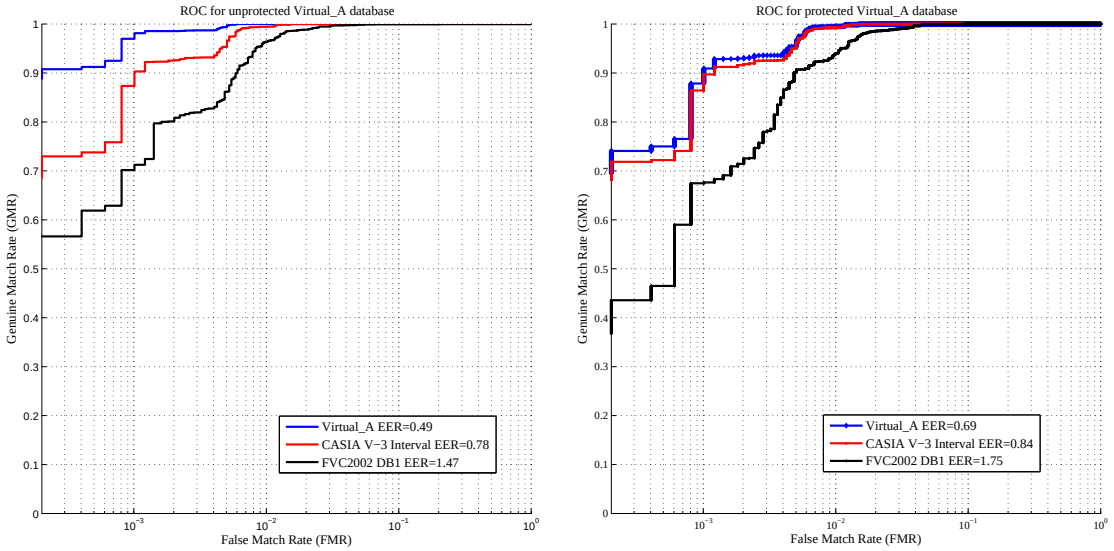


Figure 5.5: ROC curves for Virtual_A database

obtained in the unprotected and protected domain. From Fig. 5.5, it has been observed that the performance of the multibiometric system is better than that of a unimodal biometric system utilizing the proposed approach for both (unprotected and protected) domains.

Virtual_B: In a similar manner, the Virtual_B database comprising MMU1 iris and FVC2002DB1 is tested against our method. Figure 5.6 illustrates the ROC curve for the Virtual_B database. We also demonstrate the ROC curves for individual modalities comprising Virtual_B. It can be noticed from Fig. 5.6 that the proposed multibiometric system outperforms over the unimodal system for scores obtained through original and cancelable biometric systems.

Virtual_C: In the similar way, the performance of Virtual_C database is evaluated along with the performance for individual modalities. Figure 5.7 illustrates the performance in the unprotected and protected domain. The reported results demonstrate the superiority for both domains over the unimodal biometric system utilizing the proposed approach.

The evaluation carried out onto three virtual databases affirms the robustness of the proposed schemes. Further, we also evaluate the performance of our method in terms of GMR @ 0.01% FMR and results are reported in Table 5.1 for the three virtual databases, respectively. The GMR @ 0.01% FMR would validate the efficacy for secure application's perspective. From Table 5.1, it is evident that the performance of the multibiometric system using the

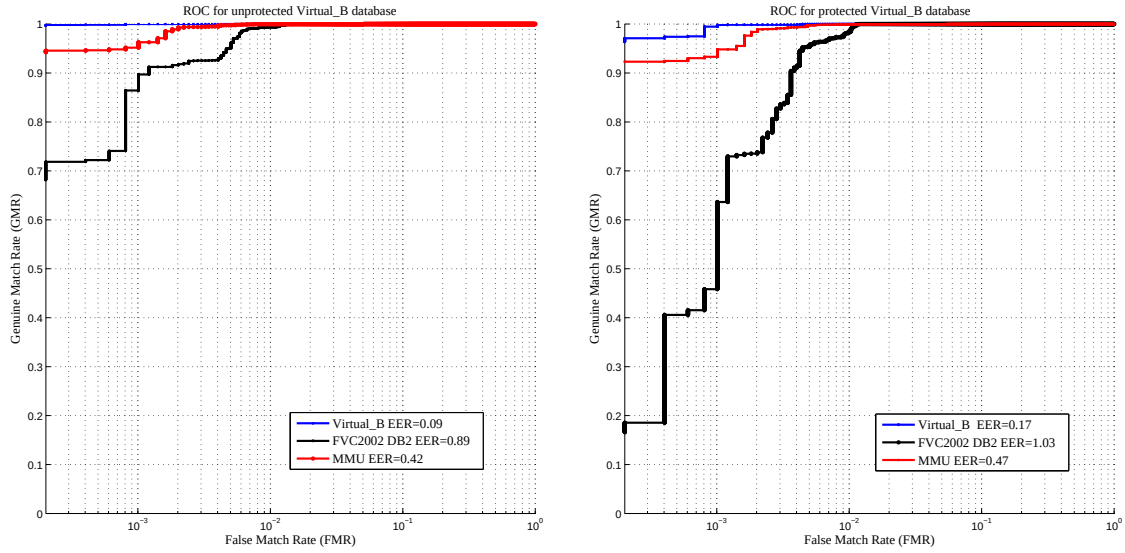


Figure 5.6: ROC curves for Virtual_B database

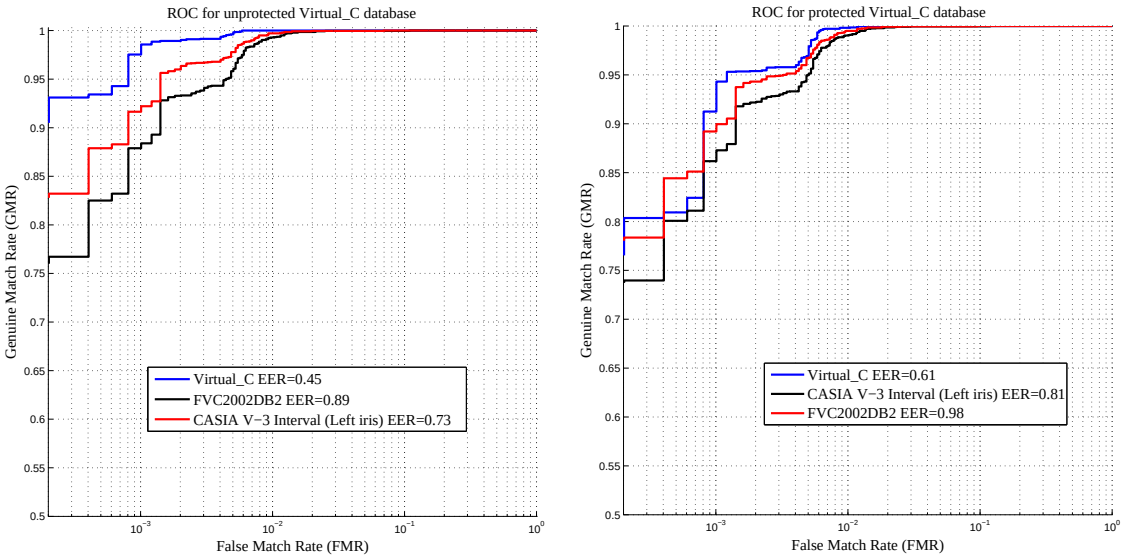


Figure 5.7: ROC curves for Virtual_C database

proposed method is better that that of unimodal systems. The performance for the Virtual_B database is higher than that of Virtual_A and Virtual_C databases since there is a relative minimal overlap between the genuine and imposter score distributions. The extent of overlap is evaluated by decidability index d', which is defined as:

$$d' = \frac{|\mu_1 - \mu_2|}{\sqrt{\frac{\sigma_1^2+\sigma_2^2}{2}}} \tag{5.10}$$

where, μ_1 and μ_2 represent the genuine mean and imposter mean distributions, respectively; and the variances of the genuine and imposter score distributions are represented by σ_1 and σ_2, respectively. The value of d' should be higher if the genuine and imposter distributions are more separable. We achieve the d' of 2.74, 3.01, and 2.81 for Virtual_A, Virtual_B, and Virtual_C databases, respectively. The score distributions for Virtual_A, Virtual_B, and Virtual_C databases are shown in Fig. 5.8. From Fig. 5.8, it is evident that the proposed fusion scheme achieves the optimal separation between genuine and imposter distributions for these three virtual databases.

5.4.4 Baseline comparison

We have also evaluated the performance with respect to the scores obtained using original biometric templates along with the protected template. From Fig. 5.5, Fig. 5.6 and Fig. 5.7, it is evident that the performance is degraded by 0.29%, 0.47%, and 0.26% for Virtual_A, Virtual_B, and Virtual_C databases, respectively. Therefore, we can conclude that performance degradation produced by the cancelable transformation is very low.

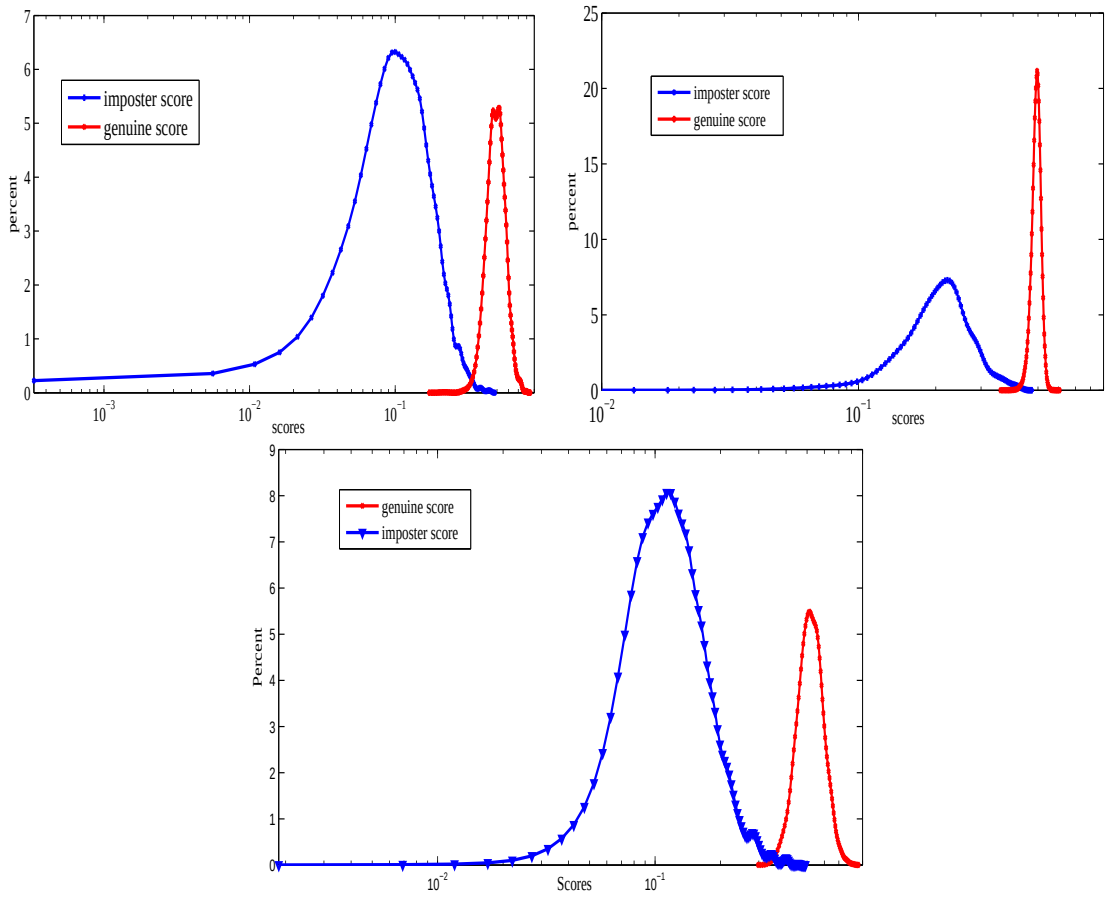


Figure 5.8: Distribution curves of the fused matching scores

5.4.5 Comparison with other state-of-the-art methods

To evaluate the robustness of the proposed fusion approach, we have implemented four other well-established weighted fusion methods for comparison in addition to the relevant density and classification based fusion techniques. These existing weighted techniques are briefed in the following.

EER weighted (EERW): In this method [108], the weights are assigned based on the EER of the individual matchers. EER is the value at which the FMR and FNMR hold equality. The weight for modality k using EERW is evaluated as:

$$w_k = \frac{\frac{1}{EER_k}}{\sum_{k=1}^{N} \frac{1}{EER_k}}$$

where, EER_k is the EER for matcher k.

d-prime weighted: The d-prime based weighting technique [108] measures the separation between the genuine and impostor scores. Larger separation between the genuine and the impostor scores corresponds to the better performance of a biometric system. The d-prime metric for modality k, $d_k^{'}$ is defined as:

$$d_k^{'} = \frac{\mu_k^G - \mu_k^I}{\sqrt{\sigma_k^{G^2} + \sigma_k^{I^2}}}$$

where, μ_k^G and μ_k^I are the mean for genuine and imposter distributions, respectively whereas σ_k^G and σ_k^I are the standard deviations of the genuine and impostor score distributions, respectively. In d-prime weighted (DPW) technique, the estimated weight of modality k is defined as follows:

$$w_k = \frac{d_k^{'}}{\sum_{k=1}^{N} d_k^{'}}$$

Fisher's discriminant ratio weighted (FDRW) technique: In this technique [169], the weights of the matchers are estimated based on the separability of the genuine and impostor scores in a multi-biometric system. The FDR of a biometric system is defined as:

$$FDR_k = \frac{\left(\mu_k^G - \mu_k^I\right)^2}{{\sigma_k^G}^2 + {\sigma_k^I}^2}$$

The estimated weight is proportional to the computed value of FDR i.e. a high-performance biometric authentication system has a high value of FDR. The weight based on $FDRW$ technique for modality k is computed as:

$$w_k = \frac{FDR_k}{\sum_{k=1}^{N} FDR_k}$$

Mean-to-Extrema weighted (MEW) technique: In this technique [170], weights are estimated using the mean of the scores distribution and its maxima i.e. the two extremes of the overlap region. The mean-to-extrema (ME) for a matcher is computed as:

$$ME_k = \left(Max_k^I - \mu_k^I\right) + \left(\mu_k^G - Max_k^G\right)$$

For modality k, the weight using the MEW technique is computed using the equation:

$$w_k = \frac{MEW_k}{\sum_{k=1}^{N} MEW_k}$$

It has been analyzed that DPW [108], MEW [170], and FDRW [169] techniques only involve the scores outside the uncertainty region to estimate the weight which results the performance sensitive to outliers. Furthermore, EER cannot be considered as weight estimation factor since a matcher with a lower EER may have higher FMR than the other one. In this work, the weights for individual matcher's are estimated based on the rectangular overlap area in order to assign the less weight to the weak matcher. Hence, the performance of the proposed method is better than that of the EERW [108], DPW [108], FDRW [169], and MEW [170] methods.

We also implemented few relevant density-based[1] and classification-based[2] methods to perform a robust comparative analysis. Table 5.1 reports the EER(%) and GMR @ 0.01%

[1] `https://msu.edu/dingyaoh/WebpageofGUI/FusionTool.htm`, `http://www.lx.it.pt/mtf/mixturecode.zip`

[2] `http://www.ti3.tu-harburg.de/rump/intlab/`

Table 5.1: Performance comparison with existing methods

Methods	EER						GMR @0.01% FMR					
	Virtual_A		Virtual_B		Virtual_C		Virtual_A		Virtual_B		Virtual_C	
	unprotected	protected	unprotected	protected	unprotected	protected	unprotected	protected	unprotected	protected	unprotected	protected
Density-based methods												
Nandakumar et al. [49]	0.89	1.03	0.77	0.95	0.81	0.99	99.01	98.82	99.23	98.90	99.06	99.89
Nanni et al. [123]	1.25	1.48	1.03	1.20	1.17	1.41	98.65	98.45	98.91	98.75	98.71	98.49
Tao et al. [124]	0.98	1.19	1.08	1.31	0.93	1.12	98.90	98.70	98.83	98.69	98.94	98.79
Classification-based methods												
Tronci et al. [48]	1.35	1.62	0.55	0.68	1.29	1.57	98.53	98.30	99.43	99.25	98.60	98.41
Nguyen et al. [117]	1.52	1.72	0.97	1.28	1.48	1.69	98.39	98.13	98.93	98.70	98.45	98.21
Transformation-based (weighting) methods												
EERW [108]	0.59	0.77	0.21	0.32	0.55	0.71	99.11	98.53	99.63	99.06	99.17	98.62
DPW [108]	0.52	0.73	0.14	0.29	0.49	0.66	99.29	98.72	99.81	99.29	99.38	98.82
FDRW [169]	0.89	0.98	0.28	0.42	0.84	0.93	98.60	98.09	99.05	98.78	98.70	98.23
MEW [170]	0.91	1.09	0.34	0.49	0.87	1.06	98.39	97.90	98.81	98.71	98.46	98.04
Proposed score fusion	**0.49**	**0.69**	**0.09**	**0.17**	**0.45**	**0.61**	**99.59**	**98.89**	**99.97**	**99.64**	**99.69**	**98.93**

FMR, obtained using the proposed and existing weighting (transformation) [108, 169, 170], density based [49,123,124], and classification based [48,117] approaches. From Table 5.1, it has been observed that the proposed multi-biometric system (i.e. cancelable iris - cancelable fingerprint system), provides lower EER and higher GMRs @ 0.01% FMR than that of the existing fusion techniques. Also, the best performance in terms of EER (i.e. 0.69%, 0.17%, and 0.61%) and GMR @ 0.01% FMR (i.e. 98.89%, 99.64%, and 98.93%) are achieved using the proposed weighting technique for the three virtual multimodal databases additionally providing secure authentication.

5.4.6 Statistical evaluation of score fusion method

The performance of any biometric system is affected by the size of the database and image comprising the database. ROC curves and verification performance are not enough to validate the overall performance for the multibiometric system. In the literature, the statistical significance of the achieved performance is evaluated by a commonly used method proposed in [171] which utilizes the Half Total Error Rate (HTER) and Confidence Interval (CI). Hence, we test our method against these two parameters. HTER is computed as:

$$HTER = \frac{FMR + FNMR}{2}$$

In order to compute CI around HTER, we look for the bound $\sigma \times z_{\alpha/2}$. Here, σ and $z_{\alpha/2}$ are defined as [171]:

$$\sigma = \sqrt{\frac{FMR(1-FMR)}{4 \cdot NI} + \frac{FNMR(1-FNMR)}{4 \cdot NG}}$$

$$z_{\alpha/2} = \begin{cases} 1.645 & \text{for} \quad 90\%\, CI \\ 1.960 & \text{for} \quad 95\%\, CI \\ 2.576 & \text{for} \quad 99\%\, CI \end{cases}$$

where, NG and NI represents the total number of intra-class comparisons and the total number of inter-class comparisons, respectively. We evaluate HTER and CI for the three virtual databases using the FMR and FNMR. The statistical evaluation is carried out at 0.01% FMR, and results are reported in Table 5.2. From Table 5.2, it has been observed that HTER lies between 0.02 ± 0.05 with 95% confidence for all three virtual databases. This validates the achieved performance in our method. In the runner-up DPW [108] method, the HTERs for Virtual_A, Virtual_B, and Virtual_C database are 0.73, 0.27, and 0.69, respectively. Also, the CI around HTER lies in between 0.02 ± 0.08 for these three virtual databases which is inferior than the proposed method. This confirms the statistical soundness of the proposed fusion method over the state-of-the-art.

Further, the comparative analysis shows that the proposed fusion method outperforms over the existing weighting approaches. Also, we obtain a substantial improvement over recognition performance through the efficient fusion of match scores from cancelable biometric modalities providing secrecy over different applications. As described above, the substantial improvement over runner-ups i.e. existing fusion methods lies in achieving (i)

Table 5.2: Confidence interval (CI) around HTER of the *d*-prime weighting (DPW) and proposed fusion methods

Methods	HTER			Confidence interval (%) around HTER for								
				90%	95%	99%	90%	95%	99%	90%	95%	99%
	Virtual_A	Virtual_B	Virtual_C	Virtual_A			Virtual_B			Virtual_C		
DPW [108]	0.73	0.27	0.69	0.03	0.045	0.059	0.047	0.061	0.078	0.035	0.049	0.063
Proposed method	**0.67**	**0.13**	**0.58**	**0.02**	**0.038**	**0.047**	**0.04**	**0.049**	**0.052**	**0.027**	**0.044**	**0.057**

minimal EER amongst all, (ii) highest GMR@ 0.01%FMR (required for security applications), (iii) no requirement of learning, (iv) deals optimally with the region of uncertainty and weight computation utilizing all set of scores.

5.5 Security analysis

The cancelable multimodal biometric verification should satisfy the criteria of template protection as described in Section 1.3 in Chapter 1. These criteria are analyzed in the following subsections with respect to our method.

5.5.1 Non-invertibility

In the proposed score fusion scheme, the verification is performed between the protected stored and query templates which is shared between the database and the query user. Further, the look-up table and random projection matrices are stored at the authentication server. Also, there is no communication between the templates and authentication server. Hence, the template cannot be reconstructed since there is no access to the auxiliary information. Hence, the criterion of non-invertibility gets satisfied.

5.5.2 Revocability

The look-up table and random projection matrices along with the associated parameters can be modified to generate different cancelable templates and stored in the database for iris and fingerprint biometric modality. In such a way, the whole database can be again protected with new cancelable templates. These cancelable templates for would be different enough from each other for the same or different subjects.

5.5.3 Diversity

In this work, an alteration to look-up table or random projection matrix results to generate many different templates. This fulfills the criterion of diversity.

5.6 Summary

In this work, the score level fusion is performed onto the match scores obtained from cancelable biometric templates. The proposed two-level fusion method applies MCW and RAW at the first and second level, respectively. RAW utilizes the rectangular area containing region of uncertainty for each modality while MCW computes the optimal score for each matcher to be fused. The weighting techniques incur the minimal computational complexity without the need of any learning. Experimental evaluations vindicate that the proposed two-level cancelable multibiometric fusion method attains better performance compared to the cancelable unimodal biometric systems in terms of EER, d', and GMR for the three virtual databases. Further, the comparative analysis shows that the proposed fusion method outperforms over the existing weighting approaches. Also, we obtain a substantial improvement over recognition performance through the efficient fusion of match scores from cancelable biometric modalities providing secrecy over different applications.

Chapter 6

Hybrid fusion scheme for cancelable multi-biometric verification

Among the five different fusion levels, score level fusion is favored owing to the factors such as ease of fusion, and freedom to choose any feature extraction and matching algorithms [172]. Despite many benefits, many commercial firms provide access only on the basis of the final decision or recognition output. Further, if the involved matchers are non-homogeneous or do not have the same scale, score level fusion becomes a challenging task. Hence, we have chosen score level as well as decision level fusion which would overcome the limitations of the score as well as decision fusion if a combination of both fusion mechanism is employed.

To the best of our knowledge, our method is the first to incorporate the hybrid fusion for protected multimodal verification utilizing MCW based score level and DS theory-based decision fusion. The workflow diagram of the proposed hybrid fusion framework for cancelable multimodal biometric verification is shown in Fig. 6.1. The block diagram comprises three major blocks i.e. score computation, hybrid fusion, and verification. Score computation evaluates score from the different matchers applied on the protected iris and protected fingerprint templates. Hybrid fusion module includes score level followed by decision level fusion schemes. Score fusion is carried out using MCW to combine different matchers corresponding to each biometric modality whereas decision fusion integrates the decision outcome of individual modality using Dempster-Shafer (DS) theory of evidence. The organization of the remaining chapter is as follows. The preliminaries of DS theory are presented in Section 6.1. Section 6.2 briefly describes the match score computation from the protected modalities.

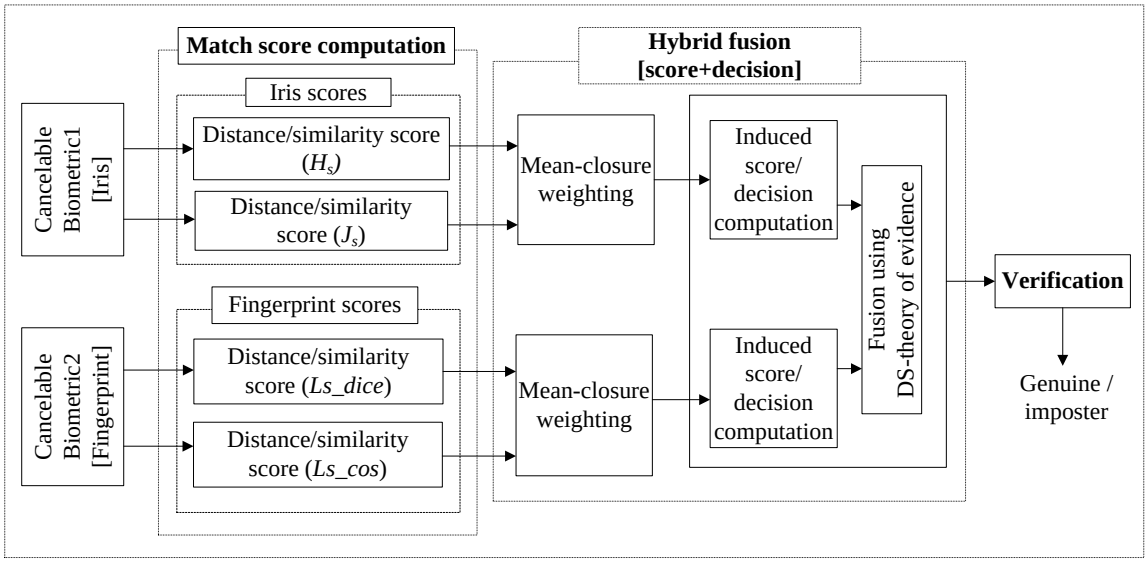


Figure 6.1: Block diagram of the proposed hybrid fusion framework

The hybrid fusion involving score and decision level fusion methods is presented in Section 6.3. Section 6.4 narrates the verification procedure to classify user either a genuine or an imposter. Experimental evaluations are presented in Section 6.5, and Section 6.6 discusses the security analysis. Section 6.7 summarizes the chapter.

6.1 Preliminaries on Dempster-Shafer theory

In Bayesian theory, the probabilities are assigned to each individual proposition form a set of mutually exclusive propositions. Alternatively, DS theory assigns masses to each combination of events. Unlike DS theory, the probability theory is unable to discriminate between ignorance and uncertainty due to sketchy information. Fundamentally, the Bayesian theory departs DS theory in the aspect of handling ignorance. DS theory does not assign belief to ignorance or to a falsified hypothesis. The mass is assigned particularly to the subsets for which we seek to assign belief. This implies neither belief nor disbelief for the evidence to a certain value. Hence we have utilized DS theory in our work.

Consider, θ be a finite set of all possible hypotheses known as a frame of discernment. The power set 2^θ contains all subsets of θ including a null set (ϕ) and itself. Each subset in the power set is referred as a focal element and assigned a value in between [0, 1] on the basis of their evidence. A value of 1 corresponds to total belief and 0 for no belief. In general,

the assigned value is named as basic belief assignment (BBA). In DS theory [168], BBA is assigned to each subset i.e. hypothesis also called as the mass of the individual proposition,

$$m : 2^{\theta} \rightarrow [0, 1] \,. \tag{6.1}$$

If $\theta = \{A, B\}$ then $2^{\theta} = \{\varnothing, A, B, \theta\}$. The mass function fulfills the following criteria:

$$\sum_{a_i \in 2^{\theta}} m\left(A_i\right) = 1, \quad m\left(\varnothing\right) = 0 \tag{6.2}$$

where $\varnothing$ represents the empty set. The measure of belief is defined by the function $bel : 2^{\theta} \rightarrow [0, 1]$,

$$bel\left(A\right) = \sum_{B \subseteq A, B \neq \varnothing} m\left(B\right). \tag{6.3}$$

The bel can also be formally defined as:

$$bel_{Y,t}^{\theta,\Re}\left[E_{Y,t}\right]\left(w_0 \in A\right) = x \tag{6.4}$$

This means the degree of belief x for the classifier Y at time t when $w_0 \in A$. Here, $E_{Y,t}$ represents the evidential information known to classifier Y at time t. For ease in representation, we use $bel(A)$ instead of $bel_{Y,t}^{\theta,\Re}\left[E_{Y,t}\right]\left(w_0 \in A\right)$. Next, plausibility ($pl$) is measured as:

$$pl : 2^{\theta} \rightarrow [0, 1] \,, \quad pl\left(A\right) = 1 - bel(\neg A) = \sum_{B \cap A \neq \varnothing} m\left(B\right) \tag{6.5}$$

If θ defines the set of all possible hypotheses, then the level of uncertainty is denoted by $m\left(\theta\right)$. In a hypothesis, beliefs and disbeliefs may not sum to 1 and may attain 0 value. A value of 0 signifies no evidence present for the hypothesis. The DS theory based aggregation involves the following steps:

- The measure of belief is evaluated based on the facts from the different sources of information. As compared to Bayesian theory, the masses are not distributed among classes.

- Dempster rule of combination is applied to aggregate belief measure obtained from the available information and facts.

For different sources of information, $(1, 2, \cdots, N)$, Dempster's rule of combination is described in Eq. 6.6:

$$m_{1,2,\cdots,N}(A) = \frac{\sum_{B_i \cap \cdots \cap B_k = A} m_1(B_i) \cdot \cdots \cdot m_N(B_k)}{1 - K} \tag{6.6}$$

where $A, B_1, \ldots, B_N \subseteq \theta,$ and

$$K = \sum_{B_i \cap \cdots \cap B_k = \varnothing} m_1(B_i) \cdot m_2(B_j) \ldots m_N(B_k) \tag{6.7}$$

where K denotes the conflict present between evidences; 1-K is the normalization factor.

6.1.1 Updation of masses

In a majority of the scenarios, mass updation is required if any new evidence or belief is encountered. Suppose, $E \subset \theta$ and E_d be the evidence not present in E. If this new evidence provides the exact value of E_d, then bel(A) is updated based on the following condition rule:

$$bel[E_d](A) = bel(A \cup \neg E) - bel(\neg E) \tag{6.8}$$

After the computation of the masses, the classification is performed onto the training set. One of the aggregation rules is applied to evaluate total conflicting mass. Next, the winner-take-all assignment is utilized to compute $A(k)$, which is defined in Eq. 6.9:

$$m(A_k) = \max_{A_j} m(A_j), \quad j = 1, \ldots M + 1 \tag{6.9}$$

where $M + 1$ represents is the total number of classes including the class of rejection and $A_{M+1} = \theta$.

6.2 Match score computation

Match score computation requires the matching between cancelable stored and cancelable query template for iris and fingerprint biometric traits. To derive cancelable templates, we apply the similar methodology as proposed in chapter 3 and chapter 4, respectively. We have evaluated Hamming and Jaccard similarity from cancelable iris biometric as described in Section 5.1.1 of Chapter 5. For cancelable fingerprint biometric, we have computed Dice and Cosine similarity measure as presented in Section 5.1.2 of Chapter 5.

6.3 Hybrid score and decision level fusion

After match scores evaluation, it is required to normalize the match scores into a common interval (e.g., in the interval of [0,1]). Here, the normalization is not needed as different matchers already generate the scores in the interval of [0,1]. Hybrid fusion scheme comprises of two techniques: MCW-based score fusion to integrate match scores from different matchers corresponding to individual biometric modality; DS-theory based decision fusion to integrate combined match scores from different modality. These techniques are presented in the following.

6.3.1 Mean-closure weighting (MCW)

In this work, score fusion is carried out on the basis of mean-closure (MC) metric to measure the separation of scores from the mean of the matcher's genuine and imposter distribution. MCW based score fusion technique has been described in Section 5.2.1 of Chapter 5.

6.3.2 Fusion using DS-theory of evidence

In the proposed fusion framework, DS theory [127, 128] is applied to combine the matcher's decision of individual biometric modalities. For each input image, the matchers assign either a label accept i.e., 1 to the hypothesis i, $i \in \theta$ or not accept i.e., 0. Hence, there are two focal elements for each matcher i and $\neg i = \theta - i$, where i is for confirming the hypothesis and $\neg i$ is for not accepting a particular hypothesis for mass assignment as shown in Table 6.1. We

Table 6.1: Basic belief assignment function

Matchers	Basic belief assignments (BBA)	
	Class: Accept (Gen)	Class: Not accept (Imp)
Matcher 1	$m_1(Gen)$	$m_1(Imp)$
Matcher 2	$m_2(Gen)$	$m_2(Imp)$

compute the corresponding predictive rates for every matcher, which are then used to assign their BBA. The predictive rate of a matcher P_k for an output class k is the ratio of the number of users classified correctly to the total number of users classified as class k.

After applying the MCW method to combine score from the different matchers for a particular modality, we utilize DS theory of evidence to integrate the scores from different modality to obtain the overall score/decision. For this purpose, we evaluate decision induced scores from the fused score and apply DS theory framework to obtain a final decision output. In the proposed method, when the j^{th} matcher classifies the result $k \in (c+1)$ for the match score S_j, it is denoted that for all instances the likelihood of k being the correct class is P_k, and the likelihood of k not being the actual class is (1-P_k). The induced score/decision output is computed by multiplying P_{kj} with the respective match score S_j for the j^{th}matcher. This score is then utilized as basic belief assignment or mass $m_j(k)$ as defined in Eq. 6.10:

$$m_j\left(k\right) = P_{kj} \cdot S_j \tag{6.10}$$

where j= 1 or 2 corresponds to the two matchers; one for the output achieved through integrating two different matchers for protected iris modality and other for the output obtained by integrating both matchers for protected fingerprint templates. In a similar way, $m_j\left(\neg k\right)$; with $m\left(\theta\right)$ = 1 indicates the measure of disbelief. After the evaluation of induced score, the mass of each evidence or classifier is combined iteratively as described in Eq. 6.11:

$$m_{final} = m_1 \oplus m_2 \oplus m_3 \oplus m_4 \tag{6.11}$$

where, $\oplus$ represents the Dempster rule of combination (see Eq. 6.6). Here, we need not have to deal with the computation cost associated with DS theory [128] since verification involves only two classes (accept, reject).

6.4 Verification

The utmost verification decision for a user to be genuine/imposter is attained by employing a threshold (t) to m_{final} as defined in Eq. 6.12. The verification procedure has already been narrated in Section 5.3.

$$\text{Result} = \begin{cases} Accept; & \text{if } m_{final} > t \\ Reject; & otherwise \end{cases} \tag{6.12}$$

6.5 Experimental results and analysis

To perform successful multimodal verification, we present a number of experiments to demonstrate the performance of our proposed hybrid fusion framework encompassing score and decision level fusion. Subsection 6.5.1 describes the databases utilized in our work for experimentation. Subsection 6.5.2 narrates the experimental settings and performance metrics to quantify the results for each database. The performance of the proposed method is evaluated in Subsection 6.5.3. Subsection 6.5.4 presents baseline comparison to compare the performance of the method under the protected and unprotected scenario. Subsection 6.5.5 validates the achieved performance statistically. Next, we compare the proposed methodology with the other approaches in order to specifically measure the effectiveness and robustness of the proposed approach in Subsection 6.5.6.

6.5.1 Database

The performance of the proposed hybrid fusion is evaluated on the three virtual databases. The description of the three databases (i.e. Virtual_A, Virtual_B, and Virtual_C) has already been given in Section 5.4.1.

6.5.2 Experimental design

After generation of the protected template for iris and fingerprint, enrolled and query templates are compared to derive intra-class (i.e., genuine) scores and inter-class (i.e., imposter)

scores. We adopt the FVC protocol to obtain the match scores as described in Section 4.5.2. First, the match scores from iris and fingerprint from different matchers are integrated by applying the proposed MCW method. As a result, the fused iris and fused fingerprint scores are obtained. Next, we evaluate induced score (decision output) from the computed match scores. Finally, we apply the DS theory of evidence to combined induced scores. The final decision output is compared with a predefined threshold to verify the user's identity. Further, the performance of our method is evaluated using the four performance metrics FMR, FNMR, EER, and GMR as defined in Eq. 1.1-1.4 in Chapter 1.

6.5.3 Performance evaluation

After the generation of the protected templates for iris and fingerprint, stored protected and query protected template are compared with each other to calculate match scores. Next, MCW and DS theory have been applied for score and decision level fusion, respectively. To carry out the experimental evaluation, we perform training onto one set of each database. For each experiment, half of the total subjects are considered to train fusion retaining another half to test the performance of the proposed fusion framework if new evidence is encountered. For each experiment, the training set is required first to find the parameters for decision fusion. In decision-level fusion, the parameters refer to the masses of the respective hypothesis. The masses have been computed for each induced score/decision output from different modality. These computed masses are combined using Eq. 6.6. Final verification decision is obtained by comparing the fused decision/score with a pre-defined threshold (see Eq. 6.12). We evaluate EER values and ROC curves for unimodal and multimodal databases. Further, the performance in term of GMR @ 0.01% FMR is computed since a biometric system deployed in a security application is considered to be efficient if it has low EER and high GMR at low FMR [168].

The multimodal biometric performance of Virtual_A is evaluated utilizing the scores obtained from CASIA V-3 Interval and FVC2002DB1. First, the performance for individual modalities (i.e., iris and fingerprint) taking part in fusion is evaluated. Next, we evaluate the performance of the multimodal biometric system. The ROC curve for the Virtual_A multimodal database is shown in Fig. 6.2 which demonstrate the performance for the scores obtained in the unprotected and protected domain. From Fig. 6.2, it has been observed that

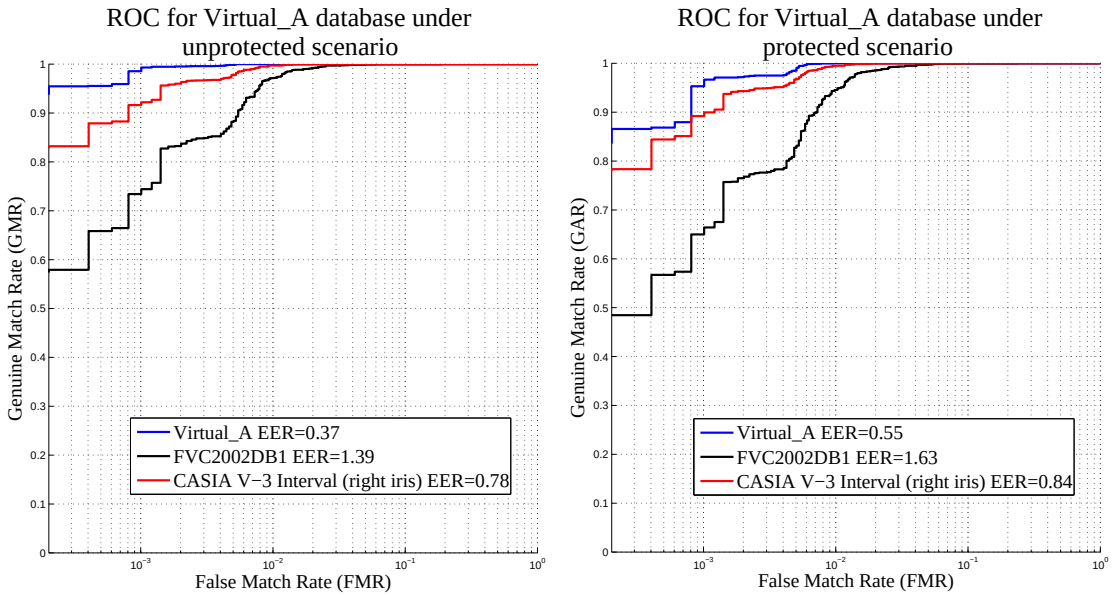


Figure 6.2: ROC curves for Virtual_A database

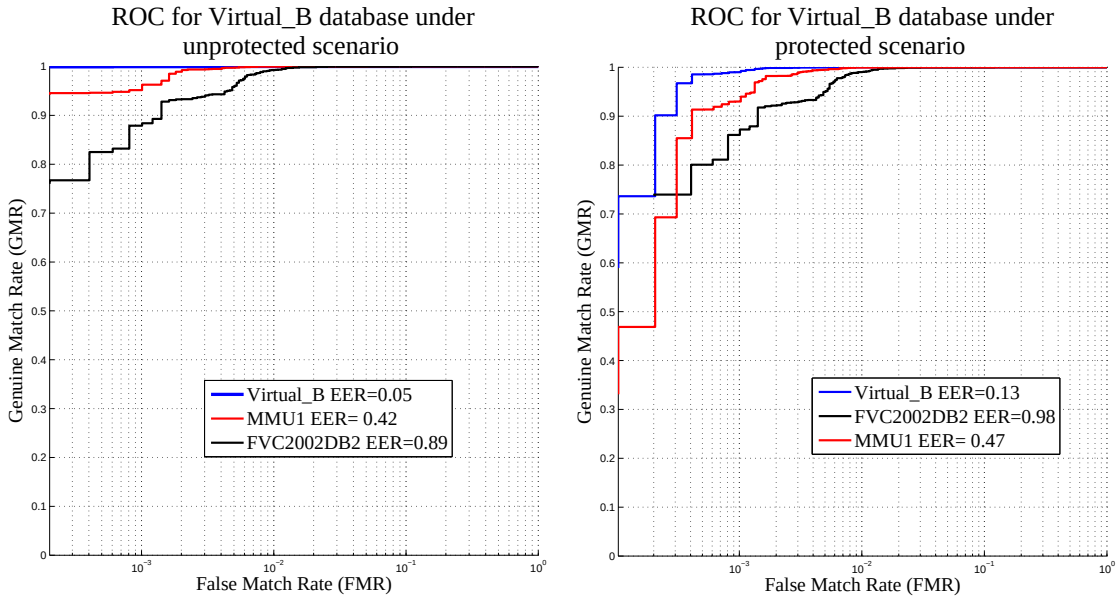


Figure 6.3: ROC curves for Virtual_B database

the performance of the multibiometric system is better than that of a unimodal biometric system utilizing the proposed approach for both domains.

In a similar manner, the Virtual_B database comprising MMU1 iris and FVC2002DB1 is tested against our method. Figure 6.3 illustrates the ROC curve for the Virtual_B database. We also demonstrate the ROC curves for individual modalities comprising Virtual_B which clearly shows the superior performance for both of the scenarios.

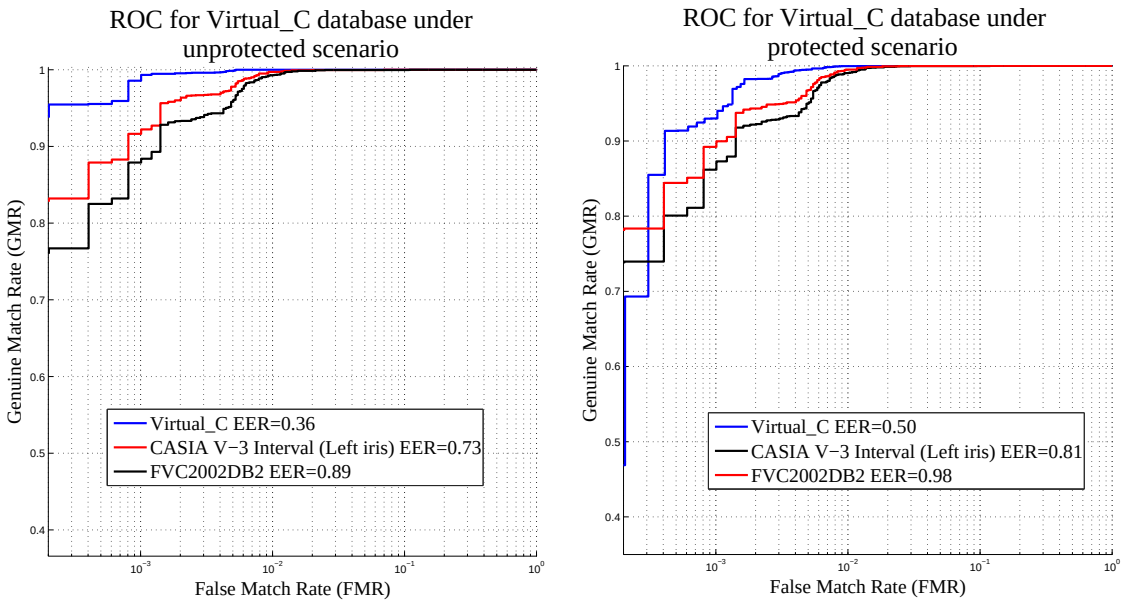


Figure 6.4: ROC curves for Virtual_C database

Further, the performance for the Virtual_C database comprising CASIA V-3 Interval iris and FVC2002DB2 is evaluated. The ROC curves for individual modality along with unprotected multimodal is shown in Fig. 6.4. It can be noticed from Fig. 6.4 that the proposed multibiometric system achieves better performance over the unimodal and unprotected multibiometric system for decisions obtained through original and cancelable biometric systems.

In the proposed method, the performance is degraded by 0.32%, 0.60%, and 0.28% for Virtual_A, Virtual_B, and Virtual_C datasets, respectively under protected scenario as evident from the Fig. 6.2, Fig. 6.3, and Fig. 6.4. Therefore, we conclude that performance degradation produced by the cancelable transformation is very low. Further, we also evaluate the performance of our method in terms of GMR @ 0.01% FMR and results are reported in Table 6.3 for Virtual_A, Virtual_B, and Virtual_C databases, respectively. From Table 6.3, it is evident that the performance of the multibiometric system using the proposed method is better than that of other existing fusion schemes. The performance for the Virtual_B database is higher than that of Virtual_A and Virtual_C since there is a relative minimal overlap between the genuine and imposter score distributions. The extent of overlap is evaluated by decidability index d', which is defined as:

$$d' = \frac{|\mu_1 - \mu_2|}{\sqrt{\frac{\sigma_1^2 + \sigma_2^2}{2}}} \tag{6.13}$$

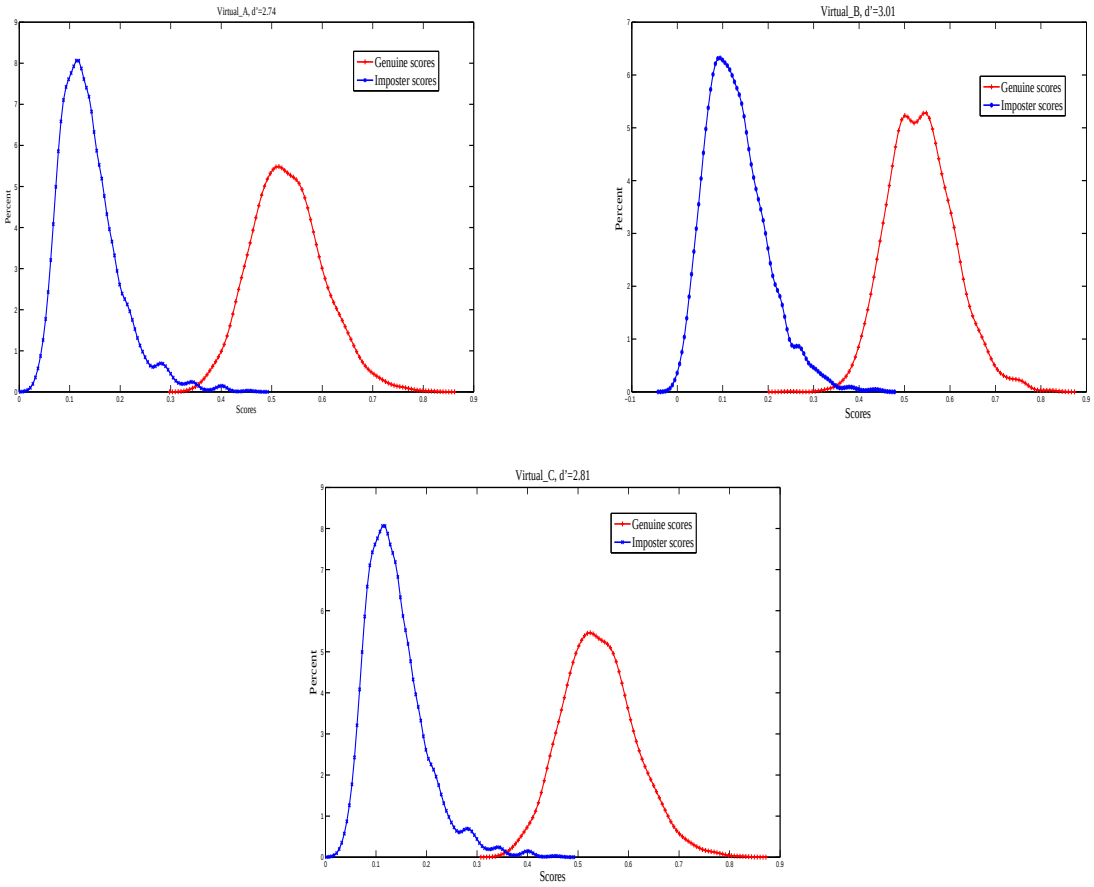


Figure 6.5: Distribution curves of the fused matching scores

where, μ_1 and μ_2 represent the genuine mean and imposter mean distributions, respectively; and the variances of the genuine and imposter score distributions are represented by σ_1 and σ_2, respectively. The value of d' should be higher if the genuine and imposter distributions are more separable. We achieve approximately equal values of d' for Virtual_A, Virtual_B, and Virtual_C databases. The score distributions for all three virtual databases are shown in Fig. 6.5. From Fig. 6.5, it is evident that the proposed fusion scheme achieves the optimal separation between genuine and imposter distribution for both the virtual databases.

6.5.4 Baseline comparison

Baseline comparison refers the comparison of verification performance between the protected multimodal and unprotected multimodal biometric system. In this work, we evaluate the performance obtained by combined scores from different modalities (fused iris and fused fingerprint) and final decision output under protected and unprotected scenarios. Further,

we compare the performance of the proposed hybrid fusion framework with respect to the above-mentioned verification systems. Figure 6.6 represents the performance achieved in different scenarios for Virtual_A, Virtual_B, and Virtual_C databases. Each of the figure comprise of (i) performances obtained by applying MCW over match scores from different matchers corresponding iris i.e. Score fusion [Protected iris], Score fusion [unprotected iris], Score fusion [Protected fingerprint], Score fusion [unprotected fingerprint], (ii) Hybrid fusion applied over iris and fingerprint modalities i.e. Hybrid fusion [Protected] and Hybrid fusion [Unprotected].

Figure 6.6 illustrates that hybrid fusion framework obtains 0.37 and 0.55 of EER under unprotected and protected scenario, which is superior in comparison to fused iris unprotected (0.59), fused fingerprint unprotected (1.10), fused iris protected (0.67), and fused fingerprint protected (1.23) for the Virtual_A databases. For the Virtual_B database, the proposed method achieves an EER of 0.05 and 0.13 under unprotected and protected scenario which performs better than the results obtained in fused iris unprotected (0.23), fused fingerprint unprotected (0.69), fused iris protected (0.31), and fused protected protected (0.77) verification systems. Similarly, we obtain superior results for Virtual_C database also. Hence, it has been confirmed that hybrid fusion framework outperforms over individual score fusion systems for all three databases.

6.5.5 Statistical evaluation of hybrid fusion method

The statistical evaluation of the proposed fusion scheme is affected by database size and the image quality of the database. Hence, it would not be sufficient to rely upon only ROC curves and EER. In our work, we have evaluated our method using the statistical test introduced by Bengio et al. [171] which utilizes half total error rate (HTER) and confidence interval (CI). The details of this statistical test has already been described in Section 5.4.6.

As per the statistical test, we evaluate HTER and CI for these three databases using the FMR and FNMR. The statistical evaluation is carried out at 0.01% FMR, and results are reported in Table 6.2. From Table 6.2, it has been observed that HTER lies between 0.02 ± 0.05 with 95% confidence for the three chimerical databases which validates the achieved performance from our method.

Table 6.2: Confidence interval around HTER of the proposed hybrid fusion

Database	HTER (%)	Confidence Interval (%) around HTER for		
		90%	95%	99%
Virtual_A	0.54	0.02	0.033	0.043
Virtual_B	0.14	0.04	0.039	0.048
Virtual_C	0.52	0.03	0.042	0.050

6.5.6 Comparison with other state-of-the-art methods

To validate the performance of our method, we compare our proposed hybrid fusion scheme with other recent methodologies in literature. Besides hybrid fusion methods [143, 145], we include few other recent state-of-the-art fusion approaches based on score level [117, 120, 121, 147, 173] and decision level fusion [95, 122]. As described in performance evaluation,

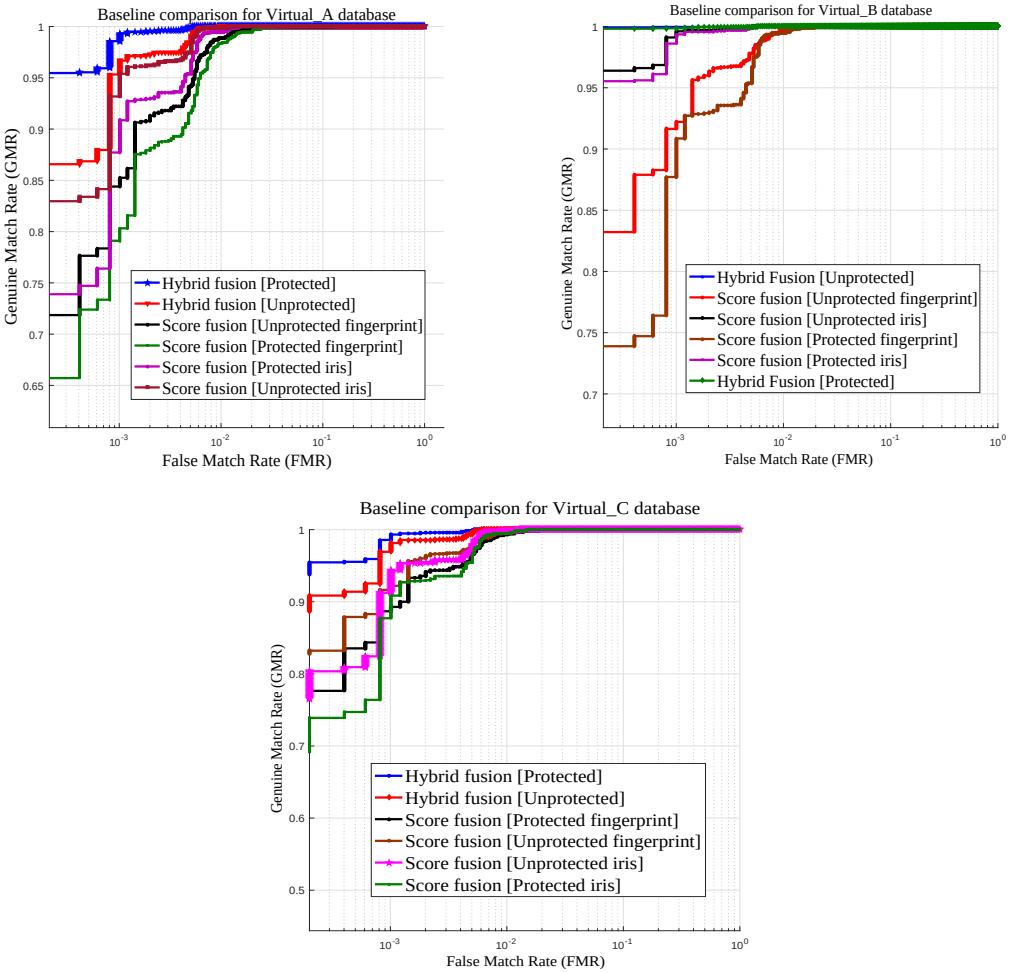


Figure 6.6: Baseline comparison for three databases

it can be observed that the proposed method performs optimally than the other approaches with respect to EER (see Figure 6.2-6.4). The superior performance is due to the extent of overlap ($d^{'}$) i.e. separability between the genuine and imposter distributions, as shown in Fig. 6.5. This also proves that the proposed method is less sensitive to the outliers since the separability between distributions is significantly higher than the existing methods.

First, the proposed hybrid fusion method is compared with other existing hybrid decision fusion schemes proposed in [143, 145]. In case of Virtual_A database, the technique proposed in [145] performs better than the proposed method, but it involves complex evaluation for global error optimization using PSO. The decision fusion methods involve AND rule and OR rule-based fusion proposed by Kelkboom et al. [95] and Bayesian classifier fusion proposed by Sadhya et al. [122]. Table 6.3 reports the EER and GMR @ 0.01% FMR, obtained using the proposed and existing weighting techniques. From the reported results in Table 6.3, it has been observed that the performance of AND rule and OR rule combination methods gets degraded in case the individual classifiers does not perform well. Hence, these two methods are rarely recommended in practice. Additionally, it can be analyzed from Table 6.3 that the proposed hybrid fusion outperforms the individual score level methods [117, 120, 121, 147, 173]. The proposed hybrid multi-biometric system (i.e., cancelable iris - cancelable fingerprint system), provides lower EER and higher GMRs @ 0.01% FMR than a majority of the existing techniques. Also, the best performance in terms of EER (i.e. 0.55, 0.13 and 0.50) and GMR @ 0.01% FMR (i.e. 99.29%, 99.70% and 99.33%) are achieved using the proposed method for the three virtual multimodal databases. Also, it is confirmed that the performance is enhanced by (48%,66%), (72%,86%), and (49%,38%) over unimodal cancelable systems for Virtual_A (iris, fingerprint), Virtual_B (iris, fingerprint), and Virtual_C (iris, fingerprint) databases, respectively.

6.6 Security analysis

In this section, we present a general security model with all the components to perform exhaustive security analysis for our method and discuss the three major requirements needed for template protection as described in Section 1. For reader's clarity, we also describe each assumption taken into account for the entities associated with the verification procedure

Table 6.3: Performance comparison with existing fusion methods

Methods	Performance (EER,GMR @0.01%)					
	Virtual_A		Virtual_B		Virtual_C	
	unprotected	protected	unprotected	protected	unprotected	protected
Score level fusion methods						
Dwivedi et al. [173]	0.49, 99.59	0.69,98.89	0.09, 99.97	0.17, 99.64	0.45, 99.49	0.61, 99.25
Kabir et al. [147]	0.47, 99.44	0.62, 98.73	0.11, 99.80	0.17, 99.59	0.59, 99.12	0.71, 98.50
Nguyen et al. [117]	0.84, 98.81	1.12, 98.63	0.37, 99.49	0.45, 99.29	0.62, 99.28	0.79, 98.97
Kumar et al. [120]	0.69, 99.18	0.78, 98.91	0.29, 99.58	0.41, 99.34	0.65, 99.30	0.83, 98.81
Mezai et al. [121]	0.95, 98.85	1.19, 98.71	0.87, 98.99	1.10, 98.79	0.73, 99.18	0.89, 99.09
Decision level fusion methods						
Kelkboom et al. [95] [AND rule]	1.52, 98.39	1.72, 98.13	0.97, 98.93	1.28, 98.70	0.78, 99.10	0.95, 98.91
Kelkboom et al. [95] [OR rule]	1.41, 98.51	1.62, 98.32	0.81, 99.02	1.04, 98.83	0.69, 99.21	0.85, 99.01
Sadhya et al. [122]	1.01, 98.87	1.23, 98.70	0.55, 99.35	0.64, 99.23	0. 53, 99.38	0.67, 99.19
Hybrid fusion methods						
Grover et al. [145]	0.34, 99.55	0.52, 99.39	0.09, 99.90	0.15, 99.81	0.42, 99.36	0.60, 99.27
Tao et al. [143]	0.52, 99.32	0.68, 99.07	0.19, 99.76	0.27, 99.61	0.51, 99.41	0.68, 99.24
Proposed fusion	**0.37, 99.64**	**0.55, 99.29**	**0.05, 99.98**	**0.13, 99.70**	**0.36, 99.55**	**0.50, 99.33**

providing a more general perspective of how the multimodal fusion framework deals with different threats or privacy invasion attempts. An explanatory diagram (see Fig. 6.7 (left)) illustrates the verification procedure adopted for an unprotected scenario for two entities:

Client: The client performs data acquisition, feature extraction, and represents the features in the form of verifiable templates. Next, it computes the similarity score between the query and stored template. Finally, user's identity is verified based on a predefined threshold.

Server: The server maintains the true biometric template for each user present in the database and shares these templates with the client for verification. To strengthen the privacy of a user, the server must send client's biometric data without pulling any other information and protect the biometric information stored in the database simultaneously.

In contrast, a different security model is utilized for verifying protected biometric template is shown in Fig. 6.7 (right). In the protected scenario, all the biometric information which is either stored or communicated between client and server are transformed (i.e., protected). Hence, the mentioned entities play the following roles:

Client: The client first acquires the data and extracts the features. Next, it applies a cance-

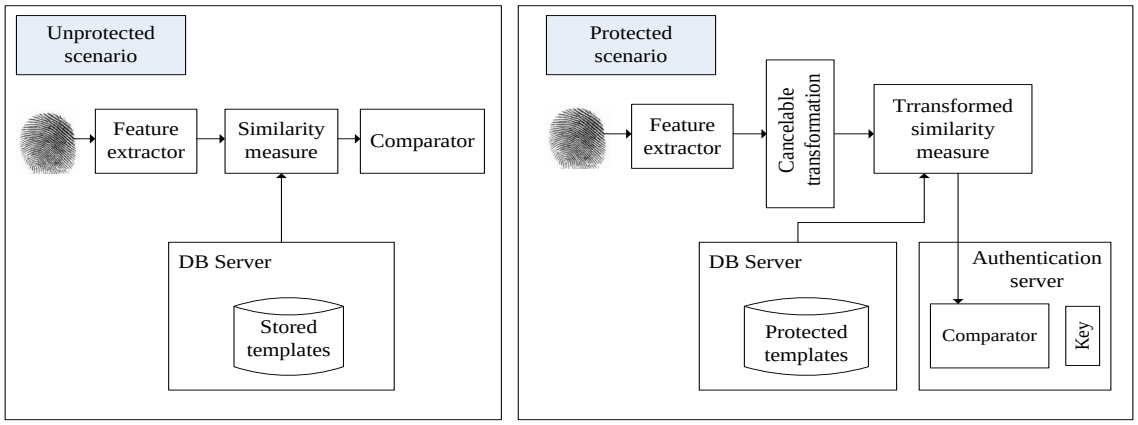


Figure 6.7: Unprotected vs. protected biometric verification

lable transformation to derive protected biometric templates and stores it onto DB server.

DB server: It contains the database consisting of only protected templates and shares these templates with the client for verification.

Authentication server: It comprises the user-specific key and comparator. Also, it computes the final verification decision by comparing stored and query template.

The following assumptions are taken into account to perform secure authentication in a multi-biometric framework:

- An imposter may get access to any one of the server but the DB server and authentication server would not intrigue.
- The client does not know the user-specific key hence it can neither extract the original template from the protected one nor the similarity score obtained through protected modalities assuming that the client serves honestly. As a result, there is no invasion possible of biometric information in the communication link.
- Similarly, the authentication server would not be allowed to access either the original template or stored protected template avoiding any trace for instigating biometric data. Also, it is assumed that all involved entities adopt the protocol and thus the score evaluated by the clients are correct.

Based on the security model illustrated in Fig. 6.8, the privacy-preserving authentication in a multi-biometric fusion framework should exhibit the following requirements:

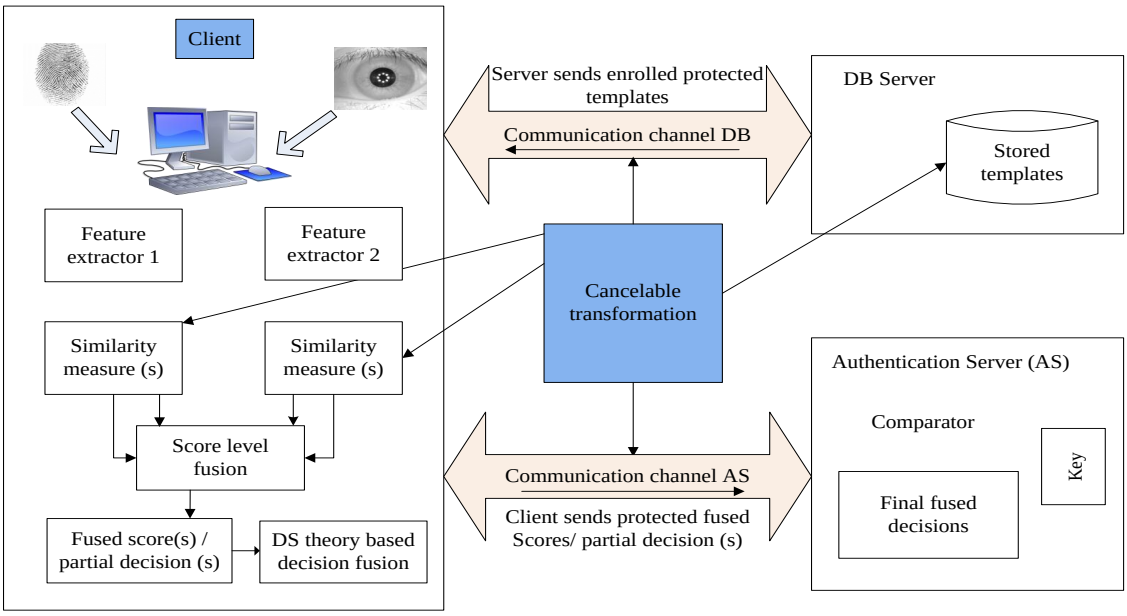


Figure 6.8: Security model: Hybrid fusion

1. The client alone should have access to the original biometric template,

2. Only the protected template should be stored in the DB server. Hence,it can never be visible to any other entity,

3. The match score/ decision output cannot be transmitted as it may be utilized to launch inversion/ hill climbing attacks.

To ensure the privacy protection, the authentication system should fulfill the three requirements, i.e. non-invertibility, diversity, and revocability as described in Section 1.3. We will investigate these three criteria in the following subsections.

6.6.1 Non-invertibility

In our multimodal biometric fusion framework, only the protected template is shared/communicated between DB server and client to compute the match scores/decision outputs. Moreover, only the user-specific key is known to the authentication server. The authentication server can never get access to the stored and query protected template. Further, the client is not allowed to send any information to the extracted original template. Hence, it would be impossible for the client or any of the servers to trace any information related to

template information since decisional composite residuosity in an NP-hard problem. Therefore, we can conclude that our approach meets the requirement of non-invertibility based on the ISO/IEC 24745 standard [174].

6.6.2 Revocability

To ensure potent revocability, the user-specific key can be altered to derive a new protected template and stored in the DB server. This way, the whole database could be re-secured with retransformed templates. This would avoid the impersonation of different users. These transformed templates for same or different subjects would be uncorrelated from each other. No information could be retrieved from these uncorrelated templates since the scores/decision outputs from different modalities are computed in the protected domain.

In the proposed scheme, only the server is allowed to access the protected scores/ decision outputs from different modalities. Hence, inversion attack and Hill-climbing attacks [175] are impossible to launch for an attacker, since he would not get the desired feedback to reconstruct the original template.

6.6.3 Diversity

In our approach, either a look-up table or random projection matrix or both of these can be altered to derive the numerous protected template corresponding to an instance of any subject. This ensures the criteria of diversity.

6.7 Summary

In this chapter, we have proposed a novel hybrid fusion scheme for protected multi-biometric template verification based on score and decision level combination. Fusion at decision level is performed using DS theory of evidence and MCW weighting is employed to combine scores from different matchers corresponding to each modality. MCW weighting does not involve any learning incurring minimal computation complexity, and DS theory exhibit a signification performance improvement thereby avoiding the uncertainty present in the matchers making ie efficiently applicable in military and government's security applications. Fusing

the output of different matchers at the score or decision level allows the freedom to choose and evaluate any feature extraction or matching algorithm. In our method, score normalization is not required at any stage since the utilized matchers provide the scores already in the range [0,1]. In theory, the experimental evaluation carried out over three virtual databases depicts that the proposed fusion method will always outperform over the unibiometric authentication, and in practice, it also attain performance improvement better than the existing hybrid fusion and other conventional fusion schemes for multibiometric verification. Also, the performance evaluation showed that verification could be carried out in the transformed domain with no degradation. Further, the security analysis of our work ensures that our approach fulfills the desired characteristics of non-invertibility, revocability, and diversity thereby preserving the recognition accuracy.

Chapter 7

Conclusions and future research directions

The main objective of our research is to explore efficient cancelable template generation schemes for iris and fingerprint traits with their utilization for multibiometric verification. The outcomes of our research are discussed in Chapter 3 to 6 in this thesis. In this chapter, we summarize some salient features of our research contributions. This research enlightens over invariant feature extraction, cancelable template generation mechanism, and multimodal biometric verification using cancelable iris and fingerprint templates. We also manifest over the performance of the introduced methods and their strength in terms of security and sustainability to different attacks. Finally, we give some future research directions in our area of research.

7.1 Invariant feature extraction mechanism

In cancelable biometric systems, an important aspect is computation of invariant features. These features are extracted in such a way that it reduces the rotation, scale, and translation deformations present at the time of acquisition. At the same time, the feature extraction mechanism should retrieve a significant amount of information to produce best verification performance. In the following, we summarize how we have achieved this objective with respect to iris and fingerprint biometric information.

Majority of the iris template protection techniques consider the IrisCode generation from iris texture pattern [50, 65, 66]. Among these feature encoding techniques, Ma et al. [66]

outperform other existing techniques. However, we have utilized 1-D log Gabor filter [50] due to the low computation cost in comparison to other existing techniques. Further, it also provides translation and scale invariant features. For rotation-invariance, we perform 8-bit left and right rotation on IrisCodes. The IrisCode with minimum Hamming distance with the reference is selected as rotation-invariant IrisCode.

From our study of existing literature [35, 42, 43, 176], we have observed that various fingerprint template protection schemes incorporate core/singular points for registration. However, the detection of underlying information is not feasible due to partial or poor-quality fingerprints images. Hence, we have proposed ridge features with reference to a ridge-based coordinate system where the orientation of the reference minutiae coincides/overlaps with the reference axis. This alleviates the acquisition associated deformations described above.

In our cancelable multibiometric verification schemes, the match scores corresponding to cancelable iris and cancelable fingerprint templates are utilized. These templates are derived by utilizing rotation-invariant IrisCodes and ridge features.

The summary of iris, fingerprint, and multimodal biometric feature representation is provided in Table 7.1.

Table 7.1: Feature representation of different template protection approaches

Cancelable biometric	Features	Invariant characteristic	
Iris	1-D log Gabor filter	Scale	Normalization of iris images
		Translation	Iris localization
		Rotation	8-bit left, 8 bit right rotation of IrisCodes
Fingerprint	Ridge features Ridge count, mean ridge orientation	Scale and translation	Ridge features [Ridge count, and mean ridge orientation]
		Rotation	Ridge-based coordinate system
Multimodal score fusion	Match score from cancelable iris, cancelable fingerprint biometric	Scores from invariant features	Invariant features from cancelable iris and cancelable fingerprint
Multimodal hybrid fusion	Match score from cancelable iris, cancelable fingerprint biometric	Scores from invariant features	Invariant features from cancelable iris and cancelable fingerprint

7.2 Cancelable template generation schemes

Secure template generation is another important concern in protected biometric verification system. It may be noted that utilization of user-specific key alongwith the associated parameters immensely influences the recognition performance. Here, we summarize our investigation to achieve template protection for iris and fingerprint, and multimodal biometric trait. Most of the existing iris template protection techniques employ different kind of transformation on iris codes such as logical operations [54], bit distortion based on a user-specific key [55, 59, 61], and hashing mechanisms [62]. Nevertheless, these methods directly exploit iris codes to user-specific keys yielding them prone to privacy invasion. On the contrary, we have derived consistent bits by aligning different rotation-invariant IrisCodes and created a decimal vector by dividing consistent bit vector. Next, a lookup table is maintained for mapping decimal vector entries in a random way. The check bits are selected from the mapped entries to derive the cancelable iris template. This proposed protection scheme serves the purpose of securing IrisCodes since there is no relationship between check bits and decimal vector, and, purpose of performance improvement due to the usage of consistent bit vector.

From the current literature, we observe that few of the fingerprint template protection approaches [43, 78] follow fixed-radius transformation. These approaches may cause performance degradation if the minutiae points are at the edge of the radius. Owing to noise or local distortion, these minutiae could be considered inside the radius for the first sample and outside the radius for the second sample for the same fingerprint. Further, the approaches proposed in [76, 78] applied a transformation considering a threshold onto the number of minutiae points to derive the protected template. Certain methods [72, 74] directly use the position and direction information of minutiae points to derive a protected fingerprint template. However, selection of invariant features from the minutiae points results in significant performance improvement over the original minutiae information. Further, BioHashing and its variants [26–28, 177] are proved to be impractical if the unique seed is compromised and the approaches introduced in [22, 25, 77] require a large number of computations. In contrast, we have proposed cancelable fingerprint template generation method based on ridge features and random projection-based transformation. The applied random projection follows a Gaussian independent and identical distribution (i.i.d.) with mean equal to zero thereby securing

the original ridge features. To conclude, the ridge-based feature extraction mechanism and random projection operation addresses the limitations of the existing approaches and outperform state-of-the-art.

7.3 Cancelable multimodal biometric verification

Generally, three possible level of fusion i.e., feature, score, and decision are used in multimodal biometric verification system. Most of the feature level multimodal protection approaches [98, 99, 104, 106, 178, 179] involve concatenation, random projection, or transformation based on a user-specific key for privacy protection. The approaches proposed in [98, 99, 104, 106, 178, 179] lead to a minor performance improvement over the unimodal biometric system. Moreover, if a protected multi-biometric template gets compromised, there is no possibility to prevent the loss of original biometric information. Owing to ease in fusion, score level fusion is the most favored integration technology in literature. Existing work on score fusion utilize three categories of schemes i.e. transformation, classification, and density-based fusion. An insufficient number of training samples and complex density estimation are the two critical issues in classification-based [47, 48, 118], and density-based approaches [49, 123, 125], respectively. Exisitng transformation-based methods [107–112, 115, 126, 180] do not involve any training except the appropriate normalization and computation of combination weights. Further, they require exhaustive empirical evaluation. Among the three categories described above, we adopt the transformation-based fusion to mitigate the limitations of the previous score level fusion approaches and try to improve the overall accuracy. Also, traditional score fusion methodologies have not considered the scores from cancelable biometric template yet. Here, we combine match scores from the protected modalities to achieve performance improvement and secure authentication. Earlier, we have proposed the techniques to derive cancelable iris and cancelable fingerprint templates. Therefore, we integrate the scores obtained from multiple matchers applied on cancelable iris and cancelable fingerprint templates in this work. However, the proposed fusion framework could be extended to other biometric traits also. To the best of our knowledge, our method is the first to incorporate the two-level fusion utilizing novel mean closure weighting (MCW) and rectangular area weighting (RAW) method to estimate weights for the protected modalities. MCW decides whether the user's score is closer to genuine or imposter

distribution for any matcher. This user-specific score weighting scheme performs better for the scores lying in the region of uncertainty by assigning more weight to the scores lying into the confidence region and vice-versa. Next, we apply a novel rectangular area weighting (RAW) method to evaluate the fused scores, where the weights are estimated based on the rectangular area containing the region of uncertainty for the individual modalities. To conclude, we can state that the proposed fusion scheme outperforms the existing transformation, density, and classification-based methods and provides a secure authentication utilizing multiple biometric modalities.

Despite many benefits, many commercial firms provide access only on the basis of the final decision or recognition output. Further, if the involved matchers are non-homogeneous or do not have the same scale, score level fusion becomes a challenging task. Hence, we have chosen score level as well as decision level fusion which would overcome the limitations of the score as well as decision fusion if a combination of both fusion mechanisms is employed. Previously, we have introduced a two-level score fusion scheme which utilizes MCW and RAW techniques. However, the limitations of our earlier work lie in the aspect of performance and security. Moreover, the prior work does not perform well if non-homogeneous matchers are present for different modalities in any biometric authentication system. In a nutshell, we extend this work in the following aspect as compared to our previous work. We have applied the MCW to combine scores from individual matchers corresponding to one particular biometric modality. Then, DS theory of evidence is employed to combine the fused scores achieved from different biometric modalities. DS theory based fusion is utilized to mitigate the uncertainty associated with non-homogeneous matcher's output. Further, the proposed hybrid fusion technique can be efficiently applied for verification decision making in security infrastructure, defense, governments, and industries. To the best of our knowledge, our method is the first to incorporate the hybrid fusion for the protected multimodal verification utilizing MCW based score level and DS theory-based decision fusion.

7.4 Performance

The performance of a cancelable biometric based authentication system relies on the invariant feature extraction and template protection transformation. The performance has been

evaluated in terms of the four metric as described in Eq. 1.1-1.4 in Chapter 3. The experimental results of the proposed schemes for unimodal and multimodal biometric traits substantiate the accuracy of our proposed methods. In Table 7.2, we summarize the proposed cancelable iris, fingerprint, and multimodal biometric verification techniques.

The consistent bit-based feature computation and lookup table-based transformation allows us to derive a diverse, irreversible, and revocable template sustaining different kinds of attack without compromising the accuracy. An exhaustive empirical evaluation has been carried out with different benchmark iris databases. We have achieved an average EER of 0.53 for all iris databases (see Table 7.2 and Fig. 7.1). The method has also been shown to perform better than the best of the existing approaches [See Section 3.4.5]. The experimental results indicate that our cancelable iris template generation approach can be applied to any real time iris biometric-based verification system.

Our cancelable fingerprint template protection approach is capable of achieves a higher accuracy with the required security measure. We have performed an extensive study with different benchmark fingerprint databases, and the average results of all fingerprint databases are reported in Table 7.2 which indicates that the proposed fingerprint template protection scheme can achieve on the average 2.52 and 3.0 of EER for all fingerprint databases under 1VS1 and FVC protocol, respectively. Hence, we can conclude that the proposed protection scheme attains optimal performance and outperforms the existing techniques.

Comprehensive evaluation on three virtual user databases shows the effectiveness of our proposed multimodal cancelable biometric verification approaches. The proposed score fusion approach can achieve an average of 0.49 EER for all virtual databases. In a similar way, we obtain an average of 0.39 EER and an average of 99.53% of GMR@0.01% FMR for hybrid fusion approach. Furthermore, we have achieved and an average GMR of 99.15% and 99.53% at 0.01% FMR for score level fusion and hybrid level fusion, respectively. We

Table 7.2: Average performances of different template protection approaches

Proposed methods	EER
Cancelable iris template generation	0.53
Cancelable fingerprint template generation	3.0
Cancelable multimodal biometric verification: Score level fusion	0.49
Cancelable multimodal biometric verification: Hybrid fusion	0.39

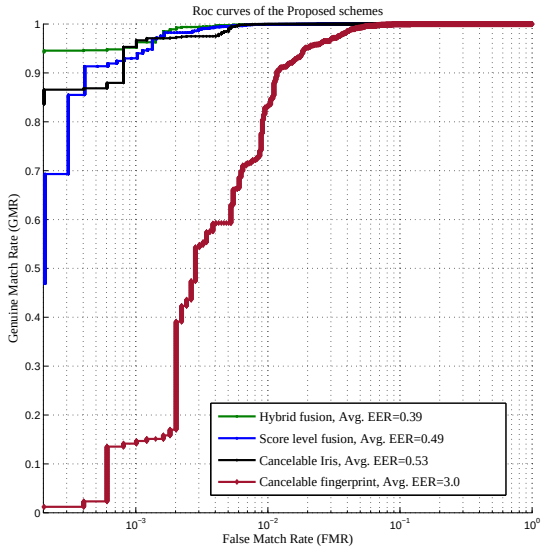


Figure 7.1: Average ROC curves for the proposed schemes

have observed that our multibiometric score fusion approach performs better than the existing score fusion approaches, and hybrid fusion scheme outperforms existing decision and hybrid fusion approaches. It is evident from the experimental results that our proposed multimodal cancelable biometric verification approach can be applied to any large-scale application. Further, the proposed approaches can handle any number of biometric traits for a multimodal biometric based verification system.

7.5 Security analysis

In cancelable iris template generation, we have performed a rigorous security analysis with respect to revocability, irreversibility and diversity, and also tested our method against possible attacks such as correlation, hill-climbing, and stolen-token attack in this dissertation. A discussion for the same is provided in Section 3.5 of Chapter 3. In a similar way, the proposed fingerprint template protection scheme is analyzed with respect to the necessary criteria of cancelable template generation as mentioned above. Further, the method is also analyzed against different types of attacks such as pre-image attack, cross-matching attack, distinguishing attack, and annealing attack. This analysis has been discussed in Section 4.6 of Chapter 4. The security analysis demonstrates that the proposed approaches fulfill the desired criteria and are robust enough to prevent such attacks.

For cancelable multibiometric verification methods constituting match scores from cancelable iris and cancelable fingerprint, the security analysis concerning the necessary criteria confirms the robustness of the proposed score fusion mechanism. The security analysis is presented in Section 5.5 of Chapter 5. For the hybrid fusion mechanism, we have assumed a hybrid fusion security model with different assumption for the entities associated with the verification procedure. This provides a more general perspective of how the multimodal fusion framework deals with different threats or privacy invasion attempts. The security model alongwith the discussion over the three requirement is narrated in Section 6.6 of Chapter 6. The analysis confirms that the authentication system fulfills the three requirements and is robust enough to sustain different kind of attacks.

7.6 Future directions

Though, we have made significant improvement in the development of biometric template protection and fusion methods to facilitate the design of a robust biometric verification systems, this thesis also delivers various future pathways for research. Few of them are indicated in the following:

1. In the cancelable iris template generation scheme, one limitation of our approach is that it requires 4 iris images per subject to generate rotation invariant template which are captured at the time of enrollment. Hence, there is a scope to propose invariant template generation from a single iris image.

2. We have investigated the log Gabor filter for IrisCode features generation in our cancelable iris template generation. In future, we would explore on other iris feature extraction techniques for performance enhancement.

3. In iris template protection scheme, a look-up table mapping based transformation is introduced. Although the proposed method outperforms against stolen-token scenario, there is need for secure look-up table generation.

4. We have investigated random projection based transformation with Gaussian independent and identical distribution (iid) entries. Introducing a more robust template protection mechanism can be a future area of research.

5. In our fingerprint template protection scheme, the proposed transformation may get affected due to ARM attack if the attacker reveals different protected templates from different applications. Hence, we are keen to proceed in the direction of handling ARM attack over random projection based transformation.

6. The performance of the template protection schemes degrades for low quality or partial biometric images. Therefore, the future scope lies in handling these types of images for the purpose of biometric template protection.

7. Most of the existing schemes for template protection, including ours, are designed with the public benchmark biometric databases with the limited number of subjects in the order of thousands. However, there is no such large database whose sizes are in the order of millions for the research community. Hence, acquiring a large biometric database with different biometric traits is a promising research direction.

8. We have explored the multimodal verification schemes using scores and decisions for protected biometric modalities. The experimentation has been performed on virtual databases with approximately 100 subjects. In future, it is hoped that the proposed approach would be tested on large databases containing 1000 subjects with more than two modalities. Additionally, we aim to validate our method onto benchmark databases such as WVU multimodal, BioSecure, and Biosec databases in future.

9. In this thesis, we have utilized iris and fingerprint biometric traits for cancelable template generation and incorporated these protected modalities for multibiometric verification. However, there are different biometric modalities other than iris and fingerprint. The template protection with those modalities are yet to be addressed.

10. In future, we shall focus on sequential and parallel decision level fusion for the protected and unprotected multimodal biometric systems to aid robustness and to reduce the computation cost.

11. Finally, a formal cost-effective model of a cancelable biometric system based on performance (EER and GMR), speed up, physical cost of the system, and adequate security needs to be designed in order to enable researchers to rapidly develop a cancelable biometric system that should be most appropriate for the application on hand.

Bibliography

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

[2] A. K. Jain, P. Flynn, and A. Ross, *Handbook of Biometrics*. Berlin, Heidelberg: Springer-Verlag, 2007. [Online]. Available: https://doi.org/10.1007/978-0-387-71041-9

[3] "Personal identity verification (PIV) of federal employees and contractors," https://www.nist.gov/publications/personal-identity-verification-piv-federal-employees-and-contractors, Accessed on: 2013-09-05.

[4] "IAFIS,integrated automated fingerprint identification system," https://www.fbi.gov/services/information-management/foipa/privacy-impact-assessments/iafis, Accessed on: 2015-08-28.

[5] "Iris Recognition Immigration System, UK," http://workpermit.com/tags/iris-recognition-immigration-system, Accessed on: 2016-05-11.

[6] "Iris Scans at Amsterdam Airport Schiphol," https://www.schiphol.nl/en/privium/, Accessed on: 2017-04-25.

[7] "CLEAR Program, CLEAR airport security and automate security," https://www.clearme.com/home, Accessed on: 2015-09-14.

[8] "Orlando international airport will be first to utilize biometrics to expedite international travel," https://www.orlandoairports.net/press/2018/04/18/orlando-international-airport-will-be-first-to-utilize-biometrics-to-expedite-international-travel/, Accessed on: 2014-11-19.

[9] "The eyes have it," http://www.accessexcellence.org/WN/SU/irisscan.html, Accessed on: 2017-04-25.

[10] "Cross U.S. Borders, department of homeland security," https://www.dhs.gov/how-do-i/cross-us-borders, Accessed on: 2017-09-13.

[11] "US-VISIT: entry and exit system," https://www.immihelp.com/visas/usvisit.html, Accessed on: 2017-11-19.

[12] "Entering the UK, home office UK border agency," https://www.gov.uk/uk-border-control, Accessed on: 2015-11-19.

[13] J. Daugman, "Iris recognition at airports and border-crossings," in *Encyclopedia of Biometrics*, S. Z. Li and A. Jain, Eds. Springer, Boston, USA, 2009, pp. 819–825.

[14] "Canadian passenger accelerated service system (CANPASS) – Private aircraft program,canada border services agency," https://www.cbsa-asfc.gc.ca/prog/canpass/privateair-eng.html, Accessed on: 2018-09-14.

[15] T. Huang, Z. Xiong, and Z. Zhang, "Face recognition applications," in *Handbook of Face Recognition*, S. Z. Li and A. K. Jain, Eds. Springer, London, 2011, pp. 617–638.

[16] "AADHAR unique identification authority of india," https://uidai.gov.in/, Accessed on: 2015-09-30.

[17] "TSA, Transportation security administration," https://www.tsa.gov/, Accessed on: 2016-09-06.

[18] "VERIDUM: Hands on security," https://www.veridiumid.com/blog/healthcare-data-breaches-demand-biometric-security/, Accessed on: 2016-08-28.

[19] A. A. Ross, K. Nandakumar, and A. K. Jain, *Handbook of Multibiometrics*. New York, USA: Springer-Verlag, 2006.

[20] A. K. jain, K. Nandakumar, and A. Nagar, "Biometric template security," *EURASIP Journal on Advances in Signal Processing*, vol. 2008, no. 113, pp. 1–17, 2008.

[21] C. Rathgeb and A. Uhl, "A survey on biometric cryptosystems and cancelable biometrics," *EURASIP Journal on Information Security*, vol. 2011, no. 1, pp. 3–25, 2011.

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

[23] S. Wang and J. Hu, "A blind system identification approach to cancelable fingerprint templates," *Pattern Recognition*, vol. 54, no. 6, pp. 14 – 22, 2016.

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

[25] M. Ferrara, D. Maltoni, and R. Cappelli, "A two-factor protection scheme for MCC fingerprint templates," in *IEEE International Conference of the Biometrics Special Interest Group (BIOSIG)*, Darmstadt, Germany, 2014, Sep. 10-12, pp. 1–8.

[26] A. B. Teoh, Y. W. Kuan, and S. Lee, "Cancellable biometrics and annotations on biohash," *Pattern Recognition*, vol. 41, no. 6, pp. 2034 – 2044, 2008.

[27] G. I. Davida, Y. Frankel, and B. Matt, "On enabling secure applications through off-line biometric identification," in *IEEE Symposium on Security and Privacy*, Oakland, USA, 1998, May 6, pp. 148–157.

[28] A. T. B. Jin, D. N. C. Ling, and A. Goh, "Biohashing: two factor authentication featuring fingerprint data and tokenised random number," *Pattern Recognition*, vol. 37, no. 11, pp. 2245 – 2255, 2004.

[29] Y. Dodis, L. Reyzin, and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," in 23^{rd} *International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT)*, vol. 3027, Interlaken, Switzerland, 2004, May 2-6, pp. 523–540.

[30] J. Bringer, H. Chabanne, G. Cohen, B. Kindarji, and G. Zemor, "Theoretical and practical boundaries of binary secure sketches," *IEEE Transactions on Information Forensics and Security*, vol. 3, no. 4, pp. 673–683, 2008.

[31] A. Arakala, J. Jeffers, and K. J. Horadam, "Fuzzy extractors for minutiae-based fingerprint authentication," in 2^{nd} *International Conference on Biometrics (ICB)*, Seoul, Korea, 2007 Aug. 27-29, pp. 760–769.

[32] A. Juels and M. Wattenberg, "A fuzzy commitment scheme," in 6^{th} *ACM Conference on Computer and Communications Security*, Singapore, 1999, Nov. 1-4, pp. 28–36.

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

[34] "Cyber security software & solutions | FireEye," https://www.fireeye.com/solutions.html, Accessed on: 2016-08-28.

[35] N. K. Ratha, S. Chikkerur, J. H. Connell, and R. M. Bolle, "Generating cancelable fingerprint templates," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 29, no. 4, pp. 561–572, 2007.

[36] "ISO/IEC 24745:2011 information technology – security techniques – biometric information protection," https://www.iso.org/standard/52946.html, 2011, Accessed on: 2015-11-19.

[37] "ISO/IEC 2382-37:2012 information technology – vocabulary – part 37: biometrics 2012," https://www.iso.org/standard/55194.html, 2012, Accessed on: 2015-11-19.

[38] "ISO/IEC 19795-1:2006 information technology – biometric performance testing and reporting – part 1: Principles and framework," https://www.iso.org/standard/41447.html, 2006, Accessed on: 2015-11-19.

[39] J. Breebaart, C. Busch, J. Grave, and E. Kindt, "A reference architecture for biometric template protection based on pseudo identities," in *Proceedings of the Special Interest Group on Biometrics and Electronic Signatures*, Darmstadt, Germany, 2008, Sep. 11-12.

[40] K. Nandakumar, A. K. Jain, and S. Pankanti, "Fingerprint-based fuzzy vault: Implementation and performance," *IEEE Transactions on Information Forensics and Security*, vol. 2, no. 4, pp. 744–757, 2007.

[41] J. Pillai, V. Patel, R. Chellappa, and N. Ratha, "Sectored random projections for cancelable iris biometrics," in *IEEE International Conference on Acoustics Speech and Signal Processing (ICASSP)*, Dallas, USA, 2010, March, 14-19, pp. 1838–1841.

[42] P. Das, K. Karthik, and B. Chandra Garai, "A robust alignment-free fingerprint hashing algorithm based on minimum distance graphs," *Pattern Recognition*, vol. 45, no. 9, pp. 3373–3388, 2012.

[43] E. Liu, H. Zhao, J. Liang, L. Pang, H. Chen, and J. Tian, "Random local region descriptor (RLRD): A new method for fixed-length feature representation of fingerprint image and its application to template protection," *Future Generation Computer Systems*, vol. 28, no. 1, pp. 236–243, 2012.

[44] K. Zhou and J. Ren, "PassBio: Privacy-preserving user-centric biometric authentication," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 12, pp. 3050–3063, 2018.

[45] Q. Gao and C. Zhang, "Constructing cancellable template with synthetic minutiae," *IET Biometrics*, vol. 6, no. 6, pp. 448–456, 2017.

[46] M. Tarek, O. Ouda, and T. Hamza, "Robust cancellable biometrics scheme based on neural networks," *IET Biometrics*, vol. 5, no. 3, pp. 220–228, 2016.

[47] Y. Ma, B. Cukic, and H. Singh, "A classification approach to multi-biometric score fusion," in *Proceedings of the 5th International Conference on Audio- and Video-Based Biometric Person Authentication (AVBPA)*, Hilton Rye Town, USA, 2005, July 20-22, pp. 484–493.

[48] R. Tronci, G. Giacinto, and F. Roli, "Dynamic score selection for fusion of multiple biometric matchers," in *14th IEEE International Conference on Image Analysis and Processing (ICIAP)*, Modena, Italy, 2007, Sep. 10-14, pp. 15–22.

[49] K. Nandakumar, Y. Chen, S. C. Dass, and A. Jain, "Likelihood ratio-based biometric score fusion," *IEEE transactions on pattern analysis and machine intelligence*, vol. 30, no. 2, pp. 342–347, 2008.

[50] L. Masek, "Recognition of human iris patterns for biometric identification," Univ. of Western Australia, Tech. Rep., 2003.

[51] "CASIA iris image database version 3.0," http://www.cbsr.ia.ac.cn/Databases.htm, Accessed on: 28-02-2014.

[52] P. Phillips, K. Bowyer, P. Flynn, X. Liu, and W. Scruggs, "The iris challenge evaluation 2005," in *2nd IEEE International Conference on Biometrics: Theory, Applications and Systems (BTAS)*, Arlington, USA, 2008, Sep. 29-Oct. 1, pp. 1–8.

[53] "Fingerprint Verification Competition," https://biolab.csr.unibo.it/FVCOnGoing/UI/Form/Home.aspxp, Accessed on: 11-05-2015.

[54] J. Zuo, N. Ratha, and J. Connell, "Cancelable iris biometric," in *19th IEEE International Conference on Pattern Recognition (ICPR)*, Tampa, USA, 2008, Dec. 9-11, pp. 1–4.

[55] E. Y. Du, K. Yang, and Z. Zhou, "Key incorporation scheme for cancelable biometrics," *Journal of Information Security*, vol. 2, no. 4, pp. 185 – 194, 2011.

[56] L. Nanni, S. Brahnam, and A. Lumini, "Biohashing applied to orientation-based minutia descriptor for secure fingerprint authentication system," *Electronics Letters*, vol. 47, no. 15, pp. 851–853, 2011.

[57] A. T. B. Jin and T. Connie, "Remarks on biohashing based cancelable biometrics in verification system," *Neurocomputing*, vol. 69, no. 16–18, pp. 2461 – 2464, 2006.

[58] O. Ouda, N. Tsumura, and T. Nakaguchi, "Tokenless cancelable biometrics scheme for protecting iris codes," in *20th IEEE International Conference on Pattern Recognition (ICPR)*, Istanbul, Turkey, 2010, Aug. 23-26, pp. 882–885.

[59] J. Hämmerle-Uhl, E. Pschernig, and A. Uhl, "Cancelable iris biometrics using block re-mapping and image warping," in *International Conference on Information Security*, vol. 5735, Pisa, Italy, 2009, pp. 135–142.

[60] J. Hammerle-Uhl, E. Pschernig, and A. Uhl, "Cancelable iris-templates using key-dependent wavelet transforms," in *IEEE International Conference on Biometrics (ICB)*, Madrid, Spain, 2013, June 4-7, pp. 1–8.

[61] C. Rathgeb and C. Busch, "Comparison score fusion towards an optimal alignment for enhancing cancelable iris biometrics," in *Fourth IEEE International Conference on Emerging Security Technologies (EST), 2013*, Cambridge, UK, 2013, Sep. 9-11, pp. 51–54.

[62] Y.-L. Lai, Z. Jin, A. B. J. Teoh, B.-M. Goi, W.-S. Yap, T.-Y. Chai, and C. Rathgeb, "Cancellable iris template generation based on indexing-first-one hashing," *Pattern Recognition*, vol. 64, no. C, pp. 105 – 117, 2017.

[63] X. Wu, N. Qi, K. Wang, and D. Zhang, "A novel cryptosystem based on iris key generation," in *Fourth IEEE International Conference on Natural Computation*, vol. 4, Jinan, China, 2008, Oct. 18-20, pp. 53–56.

[64] E. Reddy and I. Ramesh Babu, "Performance of iris based hard fuzzy vault," in *8th IEEE International Conference on Computer and Information Technology Workshops*, Sydney, Australia, 2008, July 8-11, pp. 248–253.

[65] J. Daugman, "How iris recognition works," in *IEEE International Conference on Image Processing*, vol. 1, Rochester, NY, USA, 2002, Sep. 22-25, pp. 33–36.

[66] L. Ma, T. Tan, Y. Wang, and D. Zhang, "Efficient iris recognition by characterizing key local variations," *IEEE Transactions on Image Processing*, vol. 13, no. 6, pp. 739–750, June 2004.

[67] C. Rathgeb and C. Busch, "Cancelable multi-biometrics: Mixing iris-codes based on adaptive bloom filters," *Computers & Security*, vol. 42, no. 5, pp. 1 – 12, 2014.

[68] A. Z. Broder, M. Charikar, A. M. Frieze, and M. Mitzenmacher, "Min-wise independent permutations," *Journal of Computer and System Sciences*, vol. 60, no. 3, pp. 630 – 659, 2000.

[69] T. E. Boult, W. J. Scheirer, and R. Woodworth, "Revocable fingerprint biotokens: accuracy and security analysis," in 17^{th} *IEEE International Conference on Computer Vision and Pattern Recognition (CVPR)*, Minneapolis, USA, 2007, June 17-22, pp. 1–8.

[70] C. Lee, J.-Y. Choi, K.-A. Toh, and S. Lee, "Alignment-free cancelable fingerprint templates based on local minutiae information," *IEEE Transactions on Systems, Man, and Cybernetics*, vol. 37, pp. 980–992, 2007.

[71] B. Yang, D. Hartung, K. Simoens, and C. Busch, "Dynamic random projection for biometric template protection," in 4^{th} *IEEE International Conference on Biometrics: Theory Applications and Systems (BTAS)*, Washington, USA, 2010, Sep. 27-29, pp. 1–7.

[72] C. Lee and J. Kim, "Cancelable fingerprint templates using minutiae-based bit-strings," *Journal of Network and Computer Applications*, vol. 33, no. 3, pp. 236 – 246, 2010.

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

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

[75] W. J. Wong, A. B. Teoh, M. D. Wong, and Y. H. Kho, "Enhanced multi-line code for minutiae-based fingerprint template protection," *Pattern Recognition Letters*, vol. 34, no. 11, pp. 1221 – 1229, 2013.

[76] T. Ahmad, J. Hu, and S. Wang, "Pair-polar coordinate-based cancelable fingerprint templates," *Pattern Recognition*, vol. 44, no. 10-11, pp. 2555 – 2564, 2011.

[77] F. Farooq, R. Bolle, T.-Y. Jea, and N. Ratha, "Anonymous and revocable fingerprint recognition," in 17^{th} *IEEE International Conference on Computer Vision and Pattern Recognition (CVPR)*, Minneapolis, USA, 2007, June 17-22, pp. 1–7.

[78] Y. Sutcu, H. T. Sencar, and N. Memon, "A geometric transformation to protect minutiae-based fingerprint templates," in *SPIE Proceedings on Biometric Technology for Human Identification*, Orlando, USA, 2007, April 9-13, pp. 65 390E–65 390E.

[79] S. Wang, G. Deng, and J. Hu, "A partial hadamard transform approach to the design of cancelable fingerprint templates containing binary biometric representations," *Pattern Recognition*, vol. 61, no. 1, pp. 447 – 458, 2017.

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

[81] P. Li, X. Yang, K. Cao, X. Tao, R. Wang, and J. Tian, "An alignment-free fingerprint cryptosystem based on fuzzy vault scheme," *Journal of Network and Computer Applications*, vol. 33, no. 3, pp. 207 – 220, 2010.

[82] C. Li and J. Hu, "A security-enhanced alignment-free fuzzy vault-based fingerprint cryptosystem using pair-polar minutiae structures," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 3, pp. 543–555, March 2016.

[83] W. Yang, J. Hu, S. Wang, and M. Stojmenovic, "An alignment-free fingerprint biocryptosystem based on modified voronoi neighbor structures," *Pattern Recognition*, vol. 47, no. 3, pp. 1309 – 1320, 2014.

[84] Z. Jin, A. B. J. Teoh, B.-M. Goi, and Y.-H. Tay, "Biometric cryptosystems: A new biometric key binding and its implementation for fingerprint minutiae-based representation," *Pattern Recognition*, vol. 56, no. 8, pp. 50 – 62, 2016.

[85] Y. Imamverdiyev, A. B. J. Teoh, and J. Kim, "Biometric cryptosystem based on discretized fingerprint texture descriptors," *Expert Systems with Applications*, vol. 40, no. 5, pp. 1888 – 1901, 2013.

[86] Z. Jin, A. Teoh, T. Ong, and C. Tee, "A revocable fingerprint template for security and privacy preserving," *KSII Transactions on Internet and Information Systems*, vol. 4, no. 6, pp. 1327–1342, 12 2010.

[87] M. Tico and P. Kuosmanen, "Fingerprint matching using an orientation-based minutia descriptor," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 25, no. 8, pp. 1009–1014, 2003.

[88] Z. Jin, T. S. Ong, C. Tee, and A. B. J. Teoh, "Generating revocable fingerprint template using polar grid based 3-tuple quantization technique," in *IEEE 54th International*

Midwest Symposium on Circuits and Systems (MWSCAS), Seoul, South Korea, 2011, Aug. 7-10, pp. 1–4.

[89] M. Sandhya and M. V. N. K. Prasad, "Securing fingerprint templates using fused structures," *IET Biometrics*, vol. 6, no. 3, pp. 173–182, 2017.

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

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

[92] "Shamir's secret sharing," https://www.cs.tau.ac.il/~bchor/Shamir.html, Accessed on: 2017-08-06.

[93] Z. Jin, M.-H. Lim, A. B. J. Teoh, and B.-M. Goi, "A non-invertible randomized graph-based hamming embedding for generating cancelable fingerprint template," *Pattern Recognition Letters*, vol. 42, no. 6, pp. 137 – 147, 2014.

[94] D. Akdogan, D. K. Altop, L. Eskandarian, and A. Levi, "Secure key agreement protocols: Pure biometrics and cancelable biometrics," *Computer Networks*, vol. 142, no. C, pp. 33 – 48, 2018.

[95] E. J. C. Kelkboom, X. Zhou, J. Breebaart, R. N. J. Veldhuis, and C. Busch, "Multi-algorithm fusion with template protection," in *3rd IEEE International Conference on Biometrics: Theory, Applications, and Systems*, Washington, USA, 2009, Sep. 28-30, pp. 1–8.

[96] M. Gomez-Barrero, E. Maiorana, J. Galbally, P. Campisi, and J. Fierrez, "Multi-biometric template protection based on homomorphic encryption," *Pattern Recognition*, vol. 67, no. 7, pp. 149 – 163, 2017.

[97] C. Rathgeb and C. Busch, *Biometric template protection: state-of-the-art, issues and challenges*, ser. Security. Institution of Engineering and Technology, 2017. [Online]. Available: http://digital-library.theiet.org/content/books/10.1049/pbse004e_ch8

[98] P. P. Paul and M. Gavrilova, "Multimodal cancelable biometrics," in 11^{th} *IEEE International Conference on Cognitive Informatics and Cognitive Computing*, Kyoto, Japan, 2012, Aug. 22-24, pp. 43–49.

[99] Y. Chin, T. Ong, A. Teoh, and K. Goh, "Integrated biometrics template protection technique based on fingerprint and palmprint feature-level fusion," *Information Fusion*, vol. 18, no. 7, pp. 161 – 174, 2014.

[100] Y. Sutcu, Q. Li, and N. Memon, "Secure biometric templates from fingerprint-face features," in 17^{th} *IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, Minneapolis, USA, 2007, June 17-22, pp. 1–6.

[101] M. Gomez-Barrero, C. Rathgeb, G. Li, R. Ramachandra, J. Galbally, and C. Busch, "Multi-biometric template protection based on bloom filters," *Information Fusion*, vol. 42, no. 7, pp. 37 – 50, 2018.

[102] A. Nagar, K. Nandakumar, and A. K. Jain, "Multibiometric cryptosystems based on feature-level fusion," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 1, pp. 255–268, Feb 2012.

[103] S. Cimato, M. Gamassi, V. Piuri, R. Sassi, and F. Scotti, "Privacy-aware biometrics: Design and implementation of a multimodal verification system," in *IEEE Annual Computer Security Applications Conference (ACSAC)*, Anaheim, USA, 2008, Dec. 8-12, pp. 130–139.

[104] A. Othman and A. Ross, "On mixing fingerprints," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 1, pp. 260–267, Jan 2013.

[105] E. Camlikaya, A. Kholmatov, and B. Yanikoglu, "Multi-biometric templates using fingerprint and voice," in *SPIE Defence and Security Symposium for Biometric Technology for Human Identification V*, vol. 6944, Orlando, USA, 2008, March 16-20, p. 69440I.

[106] C. Rathgeb, M. Gomez-Barrero, C. Busch, J. Galbally, and J. Fierrez, "Towards cancelable multi-biometrics based on bloom filters: a case study on feature level fusion of face and iris," in 3^{rd} *IEEE International Workshop on Biometrics and Forensics (IWBF)*, Gjovik, Norway, 2015, March 3-4, pp. 1–6.

[107] K.-A. Toh, X. Jiang, and W.-Y. Yau, "Exploiting global and local decisions for multimodal biometrics verification," *IEEE Transactions on Signal Processing*, vol. 52, no. 10, pp. 3059–3072, 2004.

[108] R. Snelick, U. Uludag, A. Mink, M. Indovina, and A. Jain, "Large-scale evaluation of multimodal biometric authentication using state-of-the-art systems," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 27, no. 3, pp. 450–455, March 2005.

[109] A. Jain, K. Nandakumar, and A. Ross, "Score normalization in multimodal biometric systems," *Pattern recognition*, vol. 38, no. 12, pp. 2270–2285, 2005.

[110] C. Lobrano, R. Tronci, G. Giacinto, and F. Roli, "Dynamic linear combination of two-class classifiers," in *Joint IAPR International Workshops on Statistical Techniques in Pattern Recognition (SPR) and Structural and Syntactic Pattern Recognition (SSPR)*, Cesme, Turkey, 2010, Aug. 18-20, pp. 473–482.

[111] N. Poh, J. Kittler, A. Rattani, and M. Tistarelli, "Group-specific score normalization for biometric systems," in 20^{th} *IEEE International Conference on Computer Vision and Pattern Recognition*, San Francisco, USA, 2010, June 13-18, pp. 38–45.

[112] M. Hanmandlu, J. Grover, A. Gureja, and H. Gupta, "Score level fusion of multimodal biometrics using triangular norms," *Pattern Recognition Letters*, vol. 32, no. 14, pp. 1843 – 1850, 2011.

[113] M. Hanmandlu, J. Grover, V. K. Madasu, and S. Vasirkala, "Score level fusion of hand based biometrics using t-norms," in *IEEE International Conference on Technologies for Homeland Security (HST)*, Waltham, USA, 2010, Nov. 8-10, pp. 70–76.

[114] N. Wang, L. Lu, G. Gao, F. Wang, and S. Li, "Multibiometrics fusion using aczél-alsina triangular norm," *KSII Transactions on Internet and Information Systems (TIIS)*, vol. 8, no. 7, pp. 2420–2433, 2014.

[115] J. Peng, A. A. A. El-Latif, Q. Li, and X. Niu, "Multimodal biometric authentication based on score level fusion of finger biometrics," *Optik-International Journal for Light and Electron Optics*, vol. 125, no. 23, pp. 6891–6897, 2014.

[116] W. Kabir, M. O. Ahmad, and M. N. S. Swamy, "Normalization and weighting techniques based on genuine-impostor score fusion in multi-biometric systems," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 8, pp. 1989–2000, 2018.

[117] K. Nguyen, S. Denman, S. Sridharan, and C. Fookes, "Score-level multibiometric fusion based on dempster shafer theory incorporating uncertainty factors," *IEEE Transactions on Human-Machine Systems*, vol. 45, no. 1, pp. 132–140, 2015.

[118] R. Singh, M. Vatsa, A. Noore, and S. K. Singh, "Dempster-shafer theory based classifier fusion for improved fingerprint verification performance," in 5^{th} *Indian Conference on Computer Vision, Graphics and Image Processing (ICVGIP)*, Madurai, India, 2006, Dec. 13-16, pp. 941–949.

[119] D. Miao, M. Zhang, Z. Sun, T. Tan, and Z. He, "Bin-based classifier fusion of iris and face biometrics," *Neurocomputing*, vol. 224, no. 1, pp. 105 – 118, 2017.

[120] A. Kumar and A. Kumar, "Adaptive management of multimodal biometrics fusion using ant colony optimization," *Information Fusion*, vol. 32, no. B, pp. 49 – 63, 2016.

[121] L. Mezai and F. Hachouf, "Score-level fusion of face and voice using particle swarm optimization and belief functions," *IEEE Transactions on Human-Machine Systems*, vol. 45, no. 6, pp. 761–772, 2015.

[122] D. Sadhya and S. K. Singh, "Construction of a bayesian decision theory-based secure multimodal fusion framework for soft biometric traits," *IET Biometrics*, vol. 7, no. 3, pp. 251–259, 2018.

[123] L. Nanni, A. Lumini, and S. Brahnam, "Likelihood ratio based features for a trained biometric score fusion," *Expert Systems with Applications*, vol. 38, no. 1, pp. 58–63, 2011.

[124] Q. Tao and R. Veldhuis, "Robust biometric score fusion by naive likelihood ratio via receiver operating characteristics," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 2, pp. 305–313, 2013.

[125] S. C. Dass, K. Nandakumar, and A. K. Jain, "A principled approach to score level fusion in multimodal biometric systems," in 5^{th} *International Conference on Audio and Video-Based Biometric Person Authentication (AVBPA)*, Hilton Rye Town, USA, 2005, Jul. 20-22, pp. 1049–1058.

[126] N. Poh, A. Ross, W. Lee, and J. Kittler, "A user-specific and selective multimodal biometric fusion strategy by ranking subjects," *Pattern Recognition*, vol. 46, no. 12, pp. 3341–3357, 2013.

[127] P. Smets, *Decision Making in a Context where Uncertainty is Represented by Belief Functions*. Heidelberg: Physica-Verlag HD, 2002, pp. 17–61.

[128] G. Shafer, *A mathematical theory of evidence*. Princeton university press, 1976.

[129] G. M. Provan, "A logic-based analysis of dempster-shafer theory," *International Journal of Approximate Reasoning*, vol. 4, no. 5, pp. 451 – 495, 1990.

[130] T. Denœux and M.-H. Masson, *Dempster-Shafer Reasoning in Large Partially Ordered Sets: Applications in Machine Learning*. Springer Berlin Heidelberg, 2010, pp. 39–54. [Online]. Available: https://doi.org/10.1007/978-3-642-11960-6_5

[131] M. A. T. Figueiredo and A. K. Jain, "Unsupervised learning of finite mixture models," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 24, no. 3, pp. 381–396, 2002.

[132] G. Rogova, "Combining the results of several neural network classifiers," *Neural Networks*, vol. 7, no. 5, pp. 777 – 781, 1994.

[133] R. Battiti and A. M. Colla, "Democracy in neural nets: Voting schemes for classification," *Neural Networks*, vol. 7, no. 4, pp. 691 – 707, 1994.

[134] C. Ji and S. Ma, "Combinations of weak classifiers," *IEEE Transactions on Neural Networks*, vol. 8, no. 1, pp. 32–42, 1997.

[135] L. Lam and S. Y. Suen, "Application of majority voting to pattern recognition: an analysis of its behavior and performance," *IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans*, vol. 27, no. 5, pp. 553–568, 1997.

[136] Y. S. Huang and C. Y. Suen, "A method of combining multiple experts for the recognition of unconstrained handwritten numerals," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 17, no. 1, pp. 90–94, 1995.

[137] H.-J. Kang, K. Kim, and J. H. Kim, "Optimal approximation of discrete probability distribution with kth-order dependency and its application to combining multiple classifiers," *Pattern Recognition Letters*, vol. 18, no. 6, pp. 515 – 523, 1997.

[138] L. Xu, A. Krzyzak, and C. Y. Suen, "Methods of combining multiple classifiers and their applications to handwriting recognition," *IEEE Transactions on Systems, Man, and Cybernetics*, vol. 22, no. 3, pp. 418–435, 1992.

[139] T. Murofushi and M. Sugeno, "A theory of fuzzy measures: Representations, the choquet, and null sets," *Journal of Mathematical Analysis and Applications*, vol. 159, no. 2, pp. 532 – 549, 1991.

[140] S.-B. Cho and J. H. Kim, "Combining multiple neural networks by fuzzy integral for robust classification," *IEEE Transactions on Systems, Man, and Cybernetics*, vol. 25, no. 2, pp. 380–384, 1995.

[141] M. Beynon, B. Curry, and P. Morgan, "The dempster-shafer theory of evidence: an alternative approach to multicriteria decision modelling," *Omega*, vol. 28, no. 1, pp. 37–50, 2000.

[142] M. Fontani, T. Bianchi, A. D. Rosa, A. Piva, and M. Barni, "A framework for decision fusion in image forensics based on dempster-shafer theory of evidence," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 4, pp. 593–607, 2013.

[143] Q. Tao and R. Veldhuis, "Hybrid fusion for biometrics: Combining score-level and decision-level fusion," in *IEEE Conference on Computer Vision and Pattern Recognition Workshops*, Anchorage, USA, 2008, Jun. 23-28, pp. 1–6.

[144] V. Azom, A. Adewumi, and J. R. Tapamo, "Face and iris biometrics person identification using hybrid fusion at feature and score-level," in *IEEE International Conference on Pattern Recognition Association of South Africa and Robotics and Mechatronics (PRASA-RobMech)*, Port Elizabeth, South Africa, 2015, Nov. 26-27, pp. 207–212.

[145] J. Grover and M. Hanmandlu, "Hybrid fusion of score level and adaptive fuzzy decision level fusions for the finger-knuckle-print based authentication," *Applied Soft Computing*, vol. 31, no. C, pp. 1 – 13, 2015.

[146] S. M. Razavi, M. Taghipour-Gorjikolaie, and N. Mehrshad, "Multimodal biometric identification system based on finger-veins using hybrid rank–decision-level fusion technique," *IEEJ Transactions on Electrical and Electronic Engineering*, vol. 12, no. 5, pp. 728–735, 2017.

[147] W. Kabir, M. O. Ahmad, and M. N. S. Swamy, "Weighted hybrid fusion for multimodal biometric recognition system," in *IEEE International Symposium on Circuits and Systems (ISCAS)*, Florence, Italy, 2018, May 27-30, pp. 1–4.

[148] K. Veeramachaneni, L. A. Osadciw, and P. K. Varshney, "An adaptive multimodal biometric management algorithm," *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*, vol. 35, no. 3, pp. 344–356, 2005.

[149] J. G. Daugman, "Uncertainty relation for resolution in space, spatial frequency, and orientation optimized by two-dimensional visual cortical filters," *Journal of The Optical Society of America A-optics Image Science and Vision*, vol. 2, no. 7, pp. 1160–1169, 1985.

[150] K. Hollingsworth, K. Bowyer, and P. Flynn, "The best bits in an iris code," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 31, no. 6, pp. 964–973, 2009.

[151] "CASIA iris image database 1.0," http://www.cbsr.ia.ac.cn/Databases.htm, Accessed on: 28-02-2014.

[152] J. Abraham, J. Gao, and P. Kwan, "Fingerprint matching using a hybrid shape and orientation descriptor," pp. 25–56, 2011. [Online]. Available: https://www.intechopen.com/books/state-of-the-art-in-biometrics/fingerprint-matching-using-a-hybrid-shape-and-orientation-descriptor

[153] M. Lisi, "Some remarks on the cantor pairing function," *Le Matematiche*, vol. 62, no. 1, pp. 55–65, 2007.

[154] G. Cantor, *Contributions to the Founding of the Theory of Transfinite Numbers*. New York: Dover, 1955.

[155] J. S. Bartunek, M. Nilsson, B. Sallberg, and I. Claesson, "Adaptive fingerprint image enhancement with emphasis on preprocessing of data," *IEEE transactions on image processing*, vol. 22, no. 2, pp. 644–656, 2013.

[156] C. I. Watson, M. D. Garris, E. Tabassi, C. L. Wilson, R. M. McCabe, and S. Janet, "User's guide to NIST fingerprint image software 2 (NFIS2)," *National Institute of Standards and Technology*, 2004, Accessed on: 2014-11-19.

[157] A. Pashalidis, "Simulated annealing attack on certain fingerprint authentication systems," in *International Conference of the Biometrics Special Interest Group (BIOSIG)*, Darmstadt, Germany, 2013, Sep. 5-6, pp. 1–11.

[158] W. Du, Y. S. Han, and S. Chen, "Privacy-preserving multivariate statistical analysis: Linear regression and classification," in *SIAM International Conference on Data Mining*, Florida, USA, 2004, Apr. 22-24, pp. 222–233.

[159] W. B. Johnson, J. Lindenstrauss, and G. Schechtman, "Extensions of lipschitz maps into banach spaces," *Israel Journal of Mathematics*, vol. 54, no. 2, pp. 129–138, 1986.

[160] K. Liu, H. Kargupta, and J. Ryan, "Random projection-based multiplicative data perturbation for privacy preserving distributed data mining," *IEEE Transactions on knowledge and Data Engineering*, vol. 18, no. 1, pp. 92–106, 2006.

[161] Y. Wang and K. N. Plataniotis, "An analysis of random projection for changeable and privacy-preserving biometric verification," *IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics)*, vol. 40, no. 5, pp. 1280–1293, 2010.

[162] F. Quan, S. Fei, C. Anni, and Z. Feifei, "Cracking cancelable fingerprint template of ratha," in *IEEE International Symposium on Computer Science and Computational Technology*, vol. 2, Shanghai, China, 2008, Dec. 20-22, pp. 572–575.

[163] W. J. Scheirer and T. E. Boult, "Cracking fuzzy vaults and biometric encryption," in *Biometrics Symposium*, Baltimore, USA, 2007, Sep. 11-13, pp. 1–6.

[164] T. Connie, A. Teoh, M. Goh, and D. Ngo, "Palmhashing: a novel approach for cancelable biometrics," *Information Processing Letters*, vol. 93, no. 1, pp. 1 – 5, 2005.

[165] W. Yang, J. Hu, and S. Wang, "A delaunay quadrangle-based fingerprint authentication system with template protection using topology code for local registration and security enhancement," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 7, pp. 1179–1192, 2014.

[166] M. He, S.-J. Horng, P. Fan, R.-S. Run, R.-J. Chen, J.-L. Lai, M. K. Khan, and K. O. Sentosa, "Performance evaluation of score level fusion in multimodal biometric systems," *Pattern Recognition*, vol. 43, no. 5, pp. 1789 – 1800, 2010.

[167] "Multimedia university version-1.0, MMU1 iris image database," www.cs.princeton.edu/~andyz/downloads/MMUIrisDatabase.zip, Accessed on: 25-04-2015.

[168] S. Prabhakar and A. K. Jain, "Decision-level fusion in fingerprint verification," *Pattern Recognition*, vol. 35, no. 4, pp. 861 – 874, 2002.

[169] N. Poh and S. Bengio, "A study of the effects of score normalisation prior to fusion in biometric authentication tasks," IDIAP, IDIAP-Report, Idiap-RR-69-2004, 2004.

[170] N. Damer, A. Opel, and A. Nouak, "Biometric source weighting in multi-biometric fusion: Towards a generalized and robust solution," in *22nd IEEE European Signal Processing Conference (EUSIPCO)*, Lisbon, Portugal, 2014, Sep. 1-5, pp. 1382–1386.

[171] S. Bengio and J. Mariéthoz, "A statistical significance test for person authentication," in *Proceedings of Odyssey: The Speaker and Language Recognition Workshop*, Toledo, Spain, 2004, May 31 - Jun. 3, pp. 237–244.

[172] T. Joshi, S. Dey, and D. Samanta, "Multimodal biometrics: state of the art in fusion techniques," *International Journal of Biometrics*, vol. 1, no. 4, pp. 393–417, 2009.

[173] R. Dwivedi and S. Dey, "Score-level fusion for cancelable multi-biometric verification," *Pattern Recognition Letters*, 2018. [Online]. Available: https://doi.org/10.1016/j.patrec.2018.04.022

[174] K. Simoens, J. Bringer, H. Chabanne, and S. Seys, "A framework for analyzing template security and privacy in biometric authentication systems," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 2, pp. 833–841, 2012.

[175] E. Maiorana, G. E. Hine, and P. Campisi, "Hill-climbing attacks on multibiometrics recognition systems," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 5, pp. 900–915, 2015.

[176] R. Bolle, J. Connell, and N. Ratha, "System and method for distorting a biometric for transactions with enhanced security and privacy," 2004, US Patent 6,836,554, Granted on: 2004-12-28.

[177] A. Kong, K.-H. Cheung, D. Zhang, M. Kamel, and J. You, "An analysis of biohashing and its variants," *Pattern Recognition*, vol. 39, no. 7, pp. 1359 – 1368, 2006.

[178] A. M. Canuto, F. Pintro, and J. C. Xavier-Junior, "Investigating fusion approaches in multi-biometric cancellable recognition," *Expert Systems with Applications*, vol. 40, no. 6, pp. 1971 – 1980, 2013.

[179] W. Yang, S. Wang, J. Hu, G. Zheng, and C. Valli, "A fingerprint and finger-vein based cancelable multi-biometric system," *Pattern Recognition*, vol. 78, no. 6, pp. 242 – 251, 2018.

[180] L. Nanni, A. Lumini, M. Ferrara, and R. Cappelli, "Combining biometric matchers by means of machine learning and statistical approaches," *Neurocomputing*, vol. 149, no. B, pp. 526–535, 2015.

[181] W.-H. Steeb and Y. Hardy, *Problems and solutions in introductory and advanced matrix calculus*, 2^{nd} ed. World Scientific, 2016. [Online]. Available: https://www.worldscientific.com/doi/abs/10.1142/10135

[182] J. Kalunga, "Integrating fingerprint biometrics system into the military police database: The case of zambia army," University of Zambia, Tech. Rep., 2015.

Appendix A

Random projection based non-invertible transformation

A.1 Propositions: Random projection

Proposition 1: A linear non-homogeneous system of equations such as $C^T = \mathcal{L} \cdot \mathcal{R}$ including s unknowns and n equations contain an infinite number of solutions.

Proof: Initially, we claim that $C^T = \mathcal{L} \cdot \mathcal{R}$ is solvable. It is evident from Eq. 4.6 in the chapter 4 that C^T is a linear combination of columns of $\mathcal{R}$, which states that C^T lies in the column space of $\mathcal{R}$. Hence, rank($\mathcal{R}$)=rank([$\mathcal{R}$ C^T]). Due to same rank of coefficient matrix and augmented matrix, a solution exists for $C^T = \mathcal{L} \cdot \mathcal{R}$.

Next, since rank($\mathcal{R}$)= $r < t$, there are infinitely many possible solutions to Eq. 4.6 in chapter 4. The proposition illustrates that C^T is concealed among infinitely many possible solutions which become infeasible to an attacker even if he/she unveils C^T and $\mathcal{R}$. The attacker would not be able to achieve true biometric template as evaluation of pseudo-inverse results obsolete as shown in the following example:

Example: Say, we have one row of log template and random projection matrix as follows:

$$\mathcal{L} = \begin{bmatrix} 2.5 & 1.3 & 3 & 4.51 \end{bmatrix} \text{ and } \mathcal{R} = \begin{bmatrix} 1.52 & -2.72 & 4.28 & -3.2 \\ 3 & -1.3 & 0.69 & -2.1 \\ -0.76 & 1.36 & -2.14 & 1.6 \end{bmatrix}$$

Hence, rank($\mathcal{R}$)=2 and,

$$C^T = \mathcal{L} \cdot \mathcal{R} = \begin{bmatrix} -1.328 & -1.591 & -0.664 \end{bmatrix}$$

is corresponding protected template.

Let ${}_i^p\mathcal{L}$ represents the pseudo-inverse $\mathcal{L}$. ${}_i^p\mathcal{L}$ is computed as:

${}_i^p\mathcal{L} = \mathcal{R}^\dagger \cdot C^T$=[-0.3579 0.0993 0.0240 0.1927],
where, $\mathcal{R}^\dagger$ denotes pseudo-inverse of $\mathcal{R}$. Concurrently, we evaluate another solution manually,
${}_i^p\mathcal{L}^\ddagger$=[0 0 0.3396 0.8692]. Hence, it is verified that ${}_i^p\mathcal{L} \cdot \mathcal{R} = C^T$ and ${}_i^p\mathcal{L}^\ddagger \cdot \mathcal{R} = C^T$.

This random projection based transformation guarantees the privacy and security of the proposed method. An imposter has no clue about $\mathcal{L}$ even if the protected template gets compromised. Further, if we consider the worst case of stolen C^T and $\mathcal{R}$, it would be very hard to retrieve $\mathcal{L}$ from infinitely many possible solutions. We illustrate this with a mathematical proof [181]:

Proposition 2: An under-determined system of linear equations either contains an infinite number of solutions or become inconsistent.

Proof: Consider this linear and under-determined system, $C^T = \mathcal{L} \cdot \mathcal{R}$ (see Eq. (6) in the revised manuscript).

We assume that $C^T = \mathcal{L} \cdot \mathcal{R}$ has infinitely many solutions. Let P be the $n \times s$ matrix,

$$P = \begin{pmatrix} 1 & 0 & \cdot & \cdot & \cdot & 0 & 0 \\ 0 & 1 & \cdot & \cdot & \cdot & 0 & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \cdot & \cdot & \cdot & 1 & 0 \end{pmatrix}_{n \times s}$$

We define $\hat{\mathcal{R}} := P \cdot \mathcal{R}$. Further we evaluate,

$$\bar{\mathcal{L}} = \min_{x} \left\| P \cdot \mathcal{R} - C^T \right\|_2^2$$

subject to the constraint $\left\| \mathcal{L} \cdot \mathcal{R} - C^T \right\|_2^2 = 0$. For evaluation of $\bar{\mathcal{L}}$, the $(\lambda \mathcal{L}^T \mathcal{L} + P^T P)^{-1}$ must exist for all $\lambda > 0$, this is non-trivial. Hence, $\bar{\mathcal{L}}$ achieved may look similar as $\mathcal{L}$, but it would not be identical.

Appendix B

Case study: Automated integrated fingerprint biometric system for military organization

The current military authentication systems have a lot of security and privacy vulnerabilities in terms of mechanism and applications. These vulnerabilities are mostly discovered at the time of identifying visitors and dependents living in military cantonment. In general, the visitors were being identified using user identities, National Register of Citizens (NRCs) or traveling documents. This procedure introduces security concerns such as impersonation and masquerading if anyone possesses someone else's identity. This case study deals with the situation if no proper record and identification parameters are found with dependents and children living in the military cantonment or barracks. Few other security concerns in this case study are traced from the heart of Zambia's Army Headquarters offices which host civil functions such as wedding and other social meetings.

B.1 Requirement of the new system

Development of a new system are divided into iris/fingerprint biometrics and military database requirements. These two requirements are integrated to form an automated integrated fingerprint biometric system for military organization (AFBSMO). The integration of biometric application into military database provides the defense architecture with the

stipulated security resilience. In addition, AFBSMO would aid military personnel an efficient service and document delivery system. However, the product must be narrated and modeled in a best possible manner to be fit into software development processes. It would contain documentation of the proposed system as it transverse from one development stage to another.

B.2 Product perspective

The AFBSMO is a latest security system which was intended to replace the present manual visitor/staff authentication in the Zambia Army [182]. Figure B.1 shows the context diagram with external entities and system interfaces. The system is expected to mature over several version/releases, and ultimately installed at a number of barracks and formations.

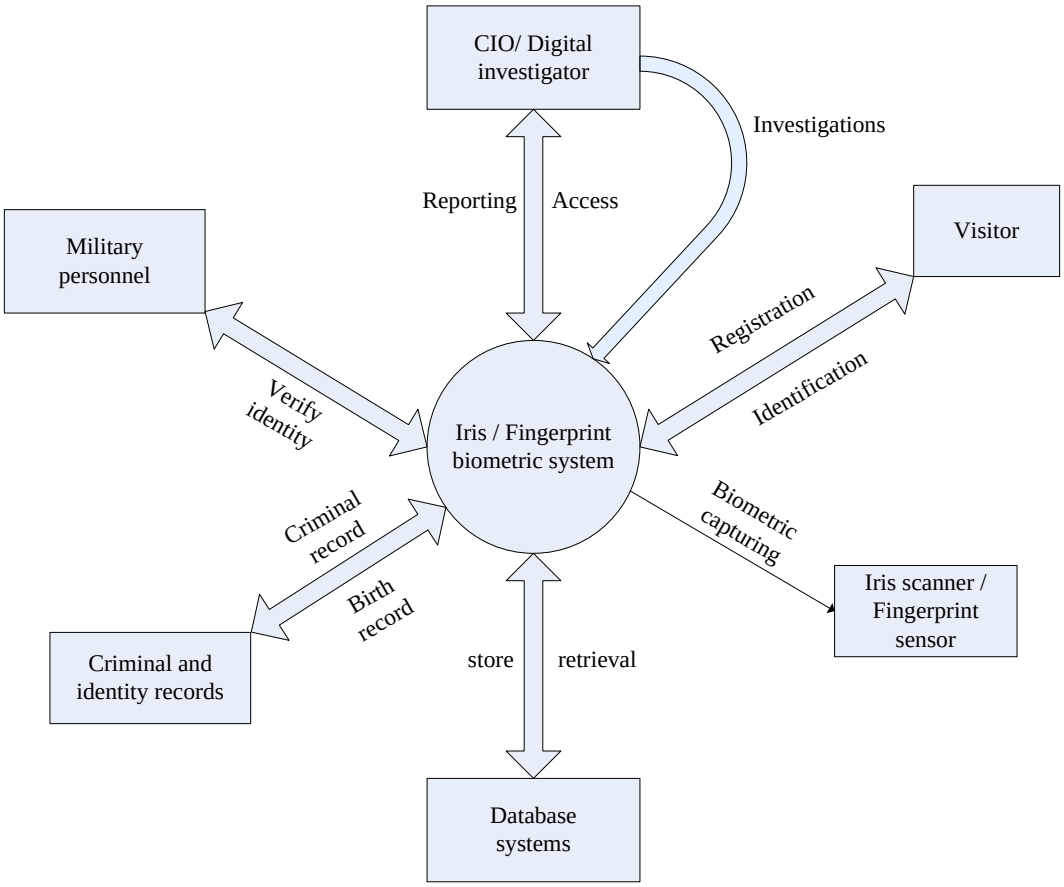


Figure B.1: AFBSMO context diagram

B.3 Objectives and process management

The objective behind the development of this new system is to amend the security concerns observed in the present manual system. These concerns should be mitigated in order to upgrade military area security clause and services. The security clauses and services can only be improved through automation at the application level. The improvements are sought through fetching information such as applicant details, fingerprint template, officer information recording, criminal data investigations, and human-descriptive information. The first module is the iris/fingerprint biometric authentication system which should be installed at entry/exit points or checkposts for secure access control. The second module is to ask visitors/staff to produce automated service identification card. The last module includes collection of security information from the guests. Figure B.2 represents different processes, actors, and data flow for this new automated system.

B.3.1 Military personnel database

The military database is utilized to handle operations at peace time and war times. It consists of record/log tables, queries and procedures committed for personnel duties.

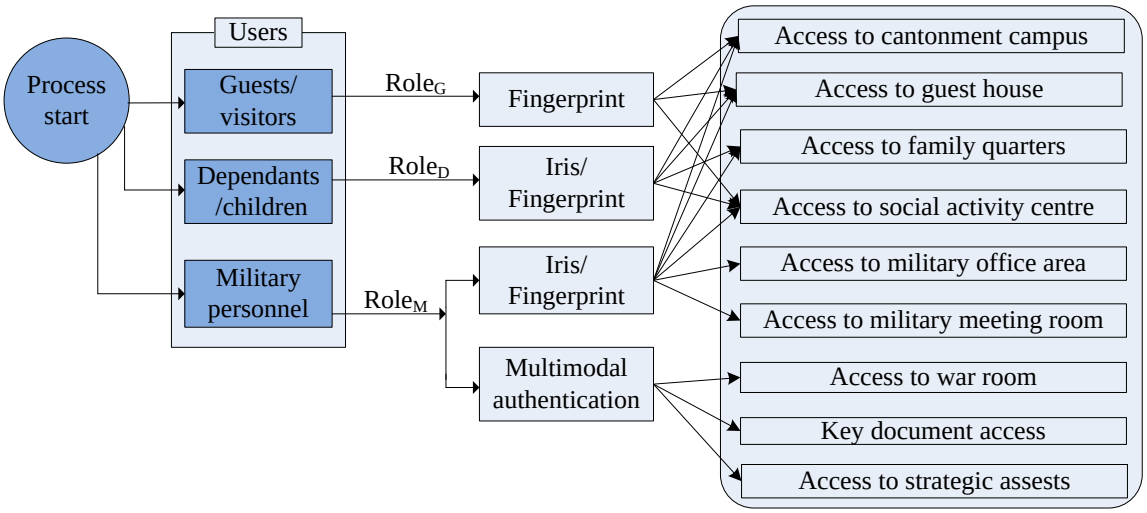


Figure B.2: Users and their roles for different applications

B.3.2 Roles of military personnel

The Military personnel are devoted to supply tactical defense support to the Zambia Army in military operations. If deployed, few roles the regimental military personnel includes:

- General investigation in peace times
- War/crime scene inspection in war time
- Collection of criminal evidence
- Reconnaissance patrols
- Prisoner handling
- Search operations and road blocks
- General policing duties within operational bases
- Foreign personnel and military training
- Provide close protection operatives for senior military personnel on operations

B.3.3 Military personnel functioning

The military personnel unit is responsible to maintain law and order within the military region. The unit is deployed at entry/exit points for traffic control, and to provide security to offices, offices personnel, installations, ammunition units, and the barracks.

As illustrated in Fig. B.2, civilian/Guests have to disclose their fingerprint to get verified. The guests/visitors can only access the cantonment campus area, guest houses and social activity center. Foreigners are compelled for security clearance from Ministry of Defense each time they need to visit a barrack. For dependents or children living inside the campus have to use their biometric information such as iris or fingerprint to access the cantonment campus, family quarters and social activity center. For this purpose, military personnel capture ten fingerprints from each and manually record their voice. Their duty also includes keeping database of disciplinary record of service personnel, offenses committed and identity information of officers in active service and reserve forces. Military personnel also use their

biometric information to access their barracks, quarters, and social activity center. For more sophisticated or privileged access, multibiometric verification may be performed (e.g. iris and fingerprint) utilizing more than a single modality. Sophisticated access includes access to war room, key documents, strategic assets, missiles, and radar rooms etc.