Multimodal Template Protection Schemes for Iris and Fingerprint Biometrics

Submitted in partial fulfillment of the requirements

for the award of the degree of

DOCTOR OF PHILOSOPHY

Submitted by

Dilip Kumar Vallabhadas

(Roll No. 701956)

Under the supervision of

Prof. M. Sandhya

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

NATIONAL INSTITUTE OF TECHNOLOGY WARANGAL

TELANGANA - 506004, INDIA

APRIL 2024

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
NATIONAL INSTITUTE OF TECHNOLOGY WARANGAL
TELANGANA - 506004, INDIA

THESIS APPROVAL FOR Ph.D.

This is to certify that the thesis entitled, Multimodal Template Protection Schemes for Iris and Fingerprint Biometrics, submitted by Mr. Dilip Kumar Vallabhadas [Roll No. 701956] is approved for the degree of DOCTOR OF PHILOSOPHY at National Institute of Technology Warangal.

Examiner

Research Supervisor
Prof. M. Sandhya
Dept. of Computer Science and Engg.
NIT Warangal
India

Chairman
Prof. R. Padmavathy
Dept. of Computer Science and Engg.
NIT Warangal
India

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
NATIONAL INSTITUTE OF TECHNOLOGY WARANGAL
TELANGANA - 506004, INDIA

CERTIFICATE

This is to certify that the thesis entitled, Multimodal Template Protection Schemes for Iris and Fingerprint Biometrics, submitted in partial fulfillment of requirement for the award of degree of DOCTOR OF PHILOSOPHY to National Institute of Technology Warangal, is a bonafide research work done by Mr. Dilip Kumar Vallabhadas [Roll No. 701956] under my supervision. The contents of the thesis have not been submitted elsewhere for the award of any degree.

Research Supervisor
Prof. M. Sandhya
Dept. of Computer Science and Engg.
NIT Warangal
India

Place: NIT Warangal

Date: 24 April, 2024

DECLARATION

This is to certify that the work presented in the thesis entitled "*Multimodal Template Protection Schemes for Iris and Fingerprint Biometrics*" is a bonafide work done by me under the supervision of Prof M. Sandhya was not submitted elsewhere for the award of any degree.

I declare that this written submission represents my ideas in my own words, and where others ideas or words have been included, I have adequately cited and referenced the original sources. I also declare that I have adhered to all principles of academic honesty and integrity and have not misrepresented or fabricated or falsified any idea/date/fact/source in my submission. I understand that any violation of the above will be cause for disciplinary action by the institute and can also evoke penal action from the sources which have thus not been properly cited or from whom proper permission has not been taken when needed.

Dilip Kumar Vallabhadas
(Roll No. 701956)
Date: 24-04-2024

ACKNOWLEDGMENTS

I would like to express my sincere gratitude and appreciation to my supervisor, Prof. M. Sandhya, for her invaluable guidance throughout the completion of this work. Her continuous support, timely feedback, and constructive discussions have played a pivotal role in helping me achieve my objectives. I am grateful for the ample time she dedicated to reviewing my work and providing insightful suggestions for improvement. Her mentorship not only shaped me as a researcher but also as an individual. I have been inspired by her words, actions, and values, which have demonstrated the qualities of a great teacher and a compassionate human being. Her unwavering dedication and commitment to excellence have left a profound impact on me. I aspire to embody these remarkable qualities throughout my life.

I would like to express my heartfelt gratitude to all the members of my Doctoral Scrutiny Committee (DSC), namely Prof. R. Padmavathy, Prof. Ch. Sudhakar, Dr. Ilaiah Kavati, and Dr. Naga Srinivasarao Batta. Their valuable comments and suggestions during the oral presentations have greatly enriched my research work. I am truly fortunate to have had the opportunity to attend lectures by esteemed professors such as Dr E. Suresh Babu, Dr M. Sandhya, Dr U.S.N. Raju, and Dr K. Madhavi Reddy. Their knowledge and expertise have been instrumental in broadening my understanding of the field.

I am immensely thankful to Prof. P. Radha Krishna, Dr. Ravichandra Sadam, and Prof. R. Padmavathy, Heads of Dept. of CSE and chairmans of DSC, during my tenure for providing adequate facilities in the department to carry out the oral presentations. I wish to express my thanks to all the esteemed faculty members of the Department of Computer Science and Engineering at NIT Warangal. I would also like to extend my heartfelt gratitude to Prof. N.V. Ramana Rao and Prof. Bidyadhar Subudhi, the Director of NIT Warangal, for their unwavering support and encouragement throughout my research endeavour. I would like to extend special gratitude to Dr. Gujjala Raghavendra for his unwavering love, support, and valuable suggestions throughout this journey. I am truly fortunate to have been part of such a remarkable institution and to have received support from all these individuals

who have contributed to my academic and personal development.

I would like to express my heartfelt gratitude to my seniors, M Mahesh Kumar, Amilpur Santhosh, J Pavan, K Suresh, Vinay Raj, and B. Umamaheswara Sharma, as well as my co-scholars, G Punnam Chander, Medipaly Rampavan, Ch Rajesh, Prakash, Asif M.d, Murukesan, Rajasekar, and A Srinivas for their invaluable support and selfless cooperation throughout my Ph.D. journey. Their presence and assistance have been truly remarkable, and I am deeply thankful for their unwavering support and readiness to help me at any time. In particular, I would like to express a special thanks to Punnam Chander, Rampavan, Rajesh, and Prakash for their unconditional love, support, and constant presence in both the joyful and challenging moments of my personal life and research work. Their friendship has been a source of strength and motivation, and I am forever grateful to have such amazing individuals by my side. Without the support and camaraderie of these remarkable individuals, my Ph.D. journey would have been much more challenging. I am truly blessed to have such incredible friends in my life, and I will cherish their friendship and support forever.

I am immensely grateful to my father, Vallabhadas Raju; my mother, Vallabhadas Bujji; my wife, Tirupathi Sony; and my sisters Kalpana and Lakshmi for their unwavering love, support, and prayers throughout my journey. Their constant encouragement and support have been my pillars of strength, giving me the confidence and motivation to overcome challenges and pursue excellence.

Dilip Kumar Vallabhadas

Dedicated to

Family, Friends & Teachers

ABSTRACT

Nowadays, with the advancement of technology, everything has been automated. Traditional authentication systems use ID cards, passwords, or PIN for identification. These systems have several limitations like password may easily be forgotten, hacked, or guessed, and ID cards could be misplaced, robbed, shared, or damaged. These limitations can be solved by using a biometric-based automatic recognition system. Biometrics is an area of science dealing with a person's physical and behavioural characteristics. As these characteristics are distinct for each user, they provide a reliable solution for authentication. The authentication systems which use a single biometric trait are known as unimodal biometric authentication systems. These systems face the challenges such as high security, poor recognition, and robustness against spoofing attacks. The systems which use more than one trait are known as multimodal biometrics authentication systems. These systems are more reliable, robust, and resistant to spoofing attacks. However, these authentication systems face challenges related to the privacy and security of the data. This biometric data is prone to various attacks like Hill Climbing, Brute Force, Record Multiplicity, Spoofing etc. To safeguard this information, we use a technique known as Biometric Template Protection (BTP). This research uses Iris and Fingerprint to develop a multimodal authentication system. These patterns are more resistant to genetic and environmental conditions throughout life. In addition, due to their randomness in pattern, there are fewer mismatches in the recognition system. This thesis presents a variety of multimodal template protection schemes designed for diverse applications that overcome various vulnerabilities and give a better balance of security and performance.

The main objectives of this thesis include: (i) To develop a homomorphic encryption based template protection technique for high-security applications, (ii) To develop an alignment-free cancelable template protection technique, (iii) To develop a cancelable technique that uses deep CNN for enhanced security and performance, and (iv) To design a hybrid template protection technique that provides confidentiality and integrity.

In this thesis, to achieve the mentioned objectives, we proposed a multimodal template protection technique using Local Random Projection and Homomorphic Encryption. Ini-

tially, features are extracted from both traits and combined to generate a fused template. Later, local random projection (LRP) is used on this template to create a reduced, revocable, and unlinkable template. Finally, fully homomorphic encryption (FHE) is applied to the created template to protect the user's privacy, as all template operations are performed on encrypted data.

Secondly, an alignment-free 3-D cancelable shell is developed for a multimodal authentication system. First, features are extracted from the fingerprint. Then, using a user key set, a 2D spiral curve is generated from fingerprint features. Next, iris features are extracted using a pre-trained VGG-16 model and then random projection is applied to generate an iris feature vector. This generated feature vector is combined with the fingerprint shell to construct a secured 3-D shell.

Thirdly, a cancelable template using Deep Binarization and Feature-Hashed Random Projection is developed for a multimodal authentication system. First, the features are extracted from both traits using a pre-trained Convolutional Neural Network(CNN) model. Next, these features are converted to binary codes by using deep binarization and combined on which AdditionRotationXor(ARX) operation is performed to generate fused features. The feature-hashed random projection is then used to generate secured templates.

Lastly, a hybrid template protection techni que is developed using Block-Xor and signcryption. Initially, features from both traits are extracted utilizing a pre-trained Convolutional Neural Network (CNN) model. These extracted features undergo a deep binarization process, transforming them into binary codes. These binary codes are then fused using the Block-xor operation. To improve security, the signcryption operation is used to ensure the integrity and confidentiality of biometric data.

The experimental results of this research demonstrate the effectiveness of template protection in biometric authentication system. The proposed methods outperform existing methods, offering improved security and performance. These developments can transform multimodal biometric template protection, offering better security and accuracy in authentication across various applications, ensuring enhanced data protection and user privacy.

Contents

List of Figures

List of Tables

List of Algorithms

List of Notations

f_ir	Iris feature vector
f_fp	Fingerprint feature vector
f_v	Fused feature vector
f_t	Fused template
b_s	Block size
l	length of feature vector
R_p	Random projection matrix
R_{lrp}	Local Random projection matrix
F_m	Feature seed matrix
U_m	User seed matrix
T_p	Tuning parameter
M	Message
HD	Hamming Distance
HUD	Hausdorff Distance
CS	Cosine Similarity
U-ID	User ID
R_2	Polynomial Ring over a binary field
χ	Discrete Gaussian distribution
R_q	Uniform Random Distribution
a	Random polynomial from R_q

q	large prime
t	small prime
Δ	q/t used to scale message M
u	Small Random polynomial from R_2
e	Random error polynomial from χ
e_1, e_2	Small Random polynomial from χ
$[.]_{P'}$	polynomial arithmetic modulo q
δ_{pk}	public key
δ_{sk}	secret key
δ_{ek}	evaluation key
A, B	Iris and Fingerprint reference templates
A', B'	Iris and Fingerprint probe templates
N	Degree of polynomial
F	Finite field
P'	Large Prime number
f(x)	Hyperelliptic Curve
D	divisor for hyperelliptic curve

Chapter 1

Introduction

The rapid advancement of technology has made person authentication a critical aspect of numerous applications. Traditional token-based systems, which rely on passwords or PINs, are vulnerable to a variety of threats, including theft, easy password guessing, credential sharing, and phishing assaults [1]. These systems often lack the additional security provided by two-factor authentication, resulting in compromised accounts and potential data breaches. The challenges of forgotten passwords, high maintenance costs, and the inability to authenticate actual identity highlight their limitations [2]. As technology progresses, these systems struggle to keep up, becoming increasingly outdated in the face of evolving security risks. With its improved security features, ease of use, and flexibility, biometric systems present a strong alternative to the drawbacks of conventional token-based authentication. Biometrics refers to the use of a person's unique physiological and biological characteristics to identify an individual [3]. These properties comprise of physical features like fingerprints, face recognition, iris and DNA, as well as behavioral features such as gait, voice recognition and keystroke dynamics. One of the primary advantages is the high level of security it provides, as biometric traits such as fingerprints, face, or iris patterns are unique to each individual, making it extremely difficult for unauthorized access[4, 5]. Additionally, biometric systems eliminate the need for users to remember passwords or carry physical tokens, enhancing convenience and reducing the risk of identity theft [6]. These systems have numerous applications in various fields, including security and access control, identification at airports and border crossings, authentication for online banking

and transactions, and forensic analysis in law enforcement [7]. Biometric technology's flexibility and reliability make it useful for improving security, optimizing operations, and ensuring accurate identification in various scenarios.

1.1 Biometric Authentication System(BAS)

As seen in Figure 1.1, there are two stages in a biometric authentication system such as Enrollment and Authentication [8]. In addition, it involves five steps: acquiring data, pre-processing, extracting features, building a template, and matching [9]. The first step, Data Acquisition, involves collecting biometric data from the user using specialized sensors. These sensors capture various biometric traits such as fingerprints, facial features, iris patterns, voice, or gait. The collected data may include unwanted background information and noise, which leads to the second step, Pre-processing. In this step, advanced algorithms are used to remove irrelevant data and noise, ensuring that only the essential biometric information remains, thereby enhancing the accuracy of the system. After pre-processing, the third step is Feature Extraction, where the system identifies and extracts distinctive features from the acquired biometric traits. These features serve as unique identifiers for each individual and play a crucial role in accurate identification. The extracted features are then utilized in the fourth step, Template Generation, where templates are created based on the extracted features. These templates serve as digital representations of the biometric traits and are stored securely in the system's database for future reference. Finally, the fifth step, Matching which determines the similarity between the templates during the identification or verification process. This step involves comparing the template generated(probe template) from the user's biometric data with the templates stored(reference template) in the database. Based on the degree of similarity, the system determines whether the user is genuine or an imposter. If the match score is within a predefined threshold, the user is authenticated, granting access to the system. However, if the match score falls below the threshold, the user is rejected, preventing unauthorized access.

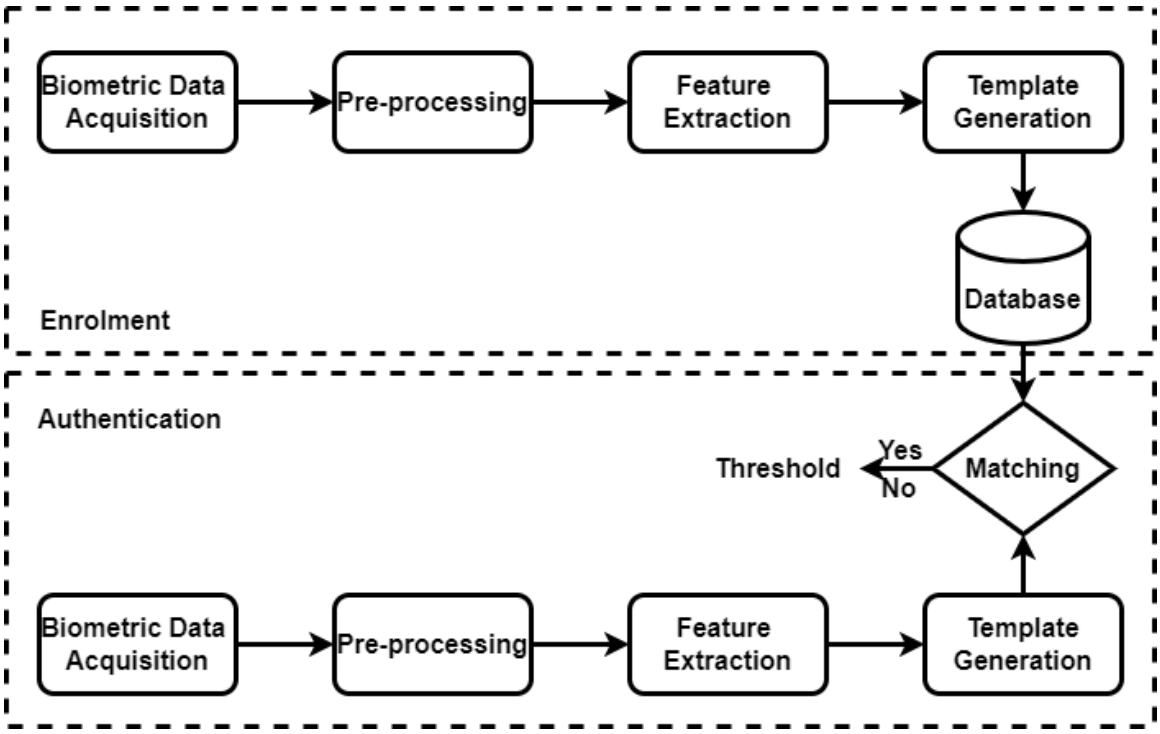


Figure 1.1: Biometric Authentication System

1.2 Attacks on BAS

Ratha et al. [10] proposed a model that gives various vulnerable points where an attacker can attack the biometric system. They have identified eight attack points which are shown in Figure 1.2. These attack points are further categorized into four distinct groups based on the nature of the attack.

1.2.1 Attacks on Hardware

Attacks on hardware specifically target sensors by manipulation or spoofing of biometric data to deceive the system. In these attacks, adversaries use fake or fabricated biometric traits to gain unauthorized access. For example, an attacker may use a high-resolution image [11] or a 3D-printed copy of a fingerprint [12] to a sensor, misleading it into recognizing the fake biometric as genuine. To prevent such attacks, advanced sensor technologies must be implemented that can detect and differentiate between genuine biometric features and unauthorized attempts [13, 14, 15]. Furthermore, adding modern anti-spoofing techniques

and ensuring the physical security of sensor hardware can help reduce the danger of unauthorized access via hardware assaults in biometric systems.

1.2.2 Attacks on Communication Channels

Attacks on the communication channels of a biometric system take place when someone interferes with the connections between its different modules [16, 17, 18]. For example, an attacker might intercept the channel between the sensor and the feature extractor by using a replay attack, where they replay previously recorded biometric data instead of real-time data. They could also target the channel between the feature extractor and the matcher, substituting real biometric features with fake ones which are called as synthesized feature vector attack. Additionally, the attacker might tamper with the channel between the matcher and the database, either by replaying data, denying access to legitimate users, or making the system unavailable altogether. Finally, the channel between the matcher and the application could be compromised if the attacker overrides the final decision, making the system to accept the attacker as a genuine user.

1.2.3 Attacks on Modules

This type of attack targets specific components or modules within the biometric system. Attackers aims their efforts at specific modules like feature extractor, template generator, and decision module. For example, at the feature extractor, the attacker attempts to replace it with a malicious program, like a Trojan horse, designed to generate predetermined and fake feature sets. This would deceive the system into recognizing these fake features as genuine, compromising the overall security [19]. Similarly, at the matcher module, the attacker could substitute it with a Trojan horse program that always produces high scores, tricking the system into granting access to unauthorized users [16].

1.2.4 Attacks on Database

These attacks focus on the stored templates within the biometric system's database, which are crucial for the authentication process [20, 21]. Attackers aim to compromise or manip-

ulate this reference data to gain unauthorized access to the system. They may attempt to alter the templates by changing the stored biometric information to match their own data. Alternatively, attackers could attempt to steal the templates directly, duplicating them and using them for unauthorised access later. Another method is forging the templates to create a fake biometric data that appears genuine to the system.

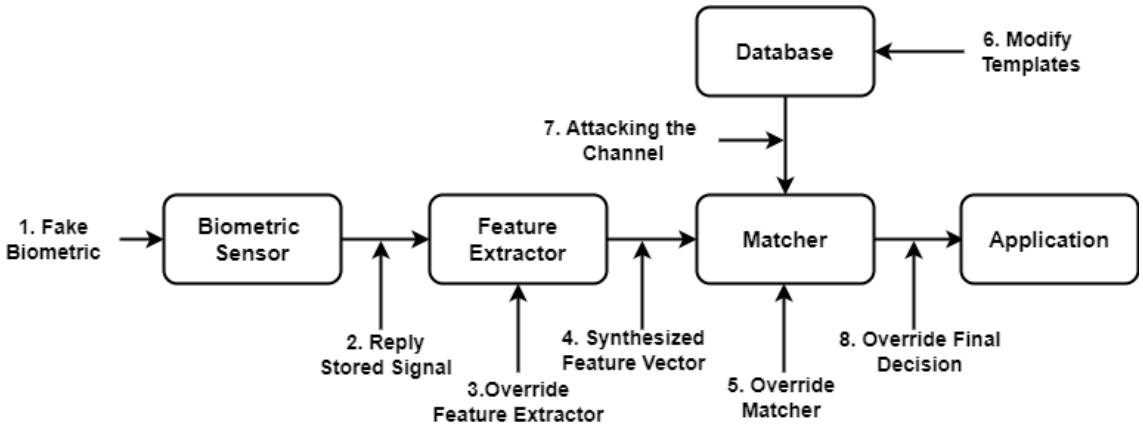


Figure 1.2: Attacks on BAS

1.3 Biometric Template Protection

A template is a digital representation of unique biometric traits extracted from a raw sample, such as a fingerprint, iris, face, or voice. These characteristics are transformed into a numerical code that uniquely identifies a person.

When the templates in the database are accidentally exposed to an unauthorized user, the data is lost and cannot be used again. If the template is stored in the database without any protection, it is vulnerable to several attacks as we have discussed in 1.2.4. To prevent such attacks, biometric template protection (BTP) [22] is used which secures the templates in the database without compromising the system's accuracy. According to ISO/IEC standard 24745, the templates created by BTP must meet the following requirements [23].

- **Diversity:** The templates that are generated for a single user should be distinct and cannot be linkable with other templates.

- **Irreversibility:** Even if the secured template is available, the template is altered in such a manner that reconstructing the actual biometric is impossible.
- **Revocability:** If a template is compromised, the authentication system must allow the user to create a different template with the same biometric features.
- **Performance:** The new BTP approach should not degrade the accuracy of the biometric system.

1.4 Types of BTP

Biometric template protection methods are divided into four types: Cancelable Biometrics, Bio-cryptosystems, Hybrid method and Homomorphic Encryption-based systems [24]. The classification is shown in Figure. 1.3.

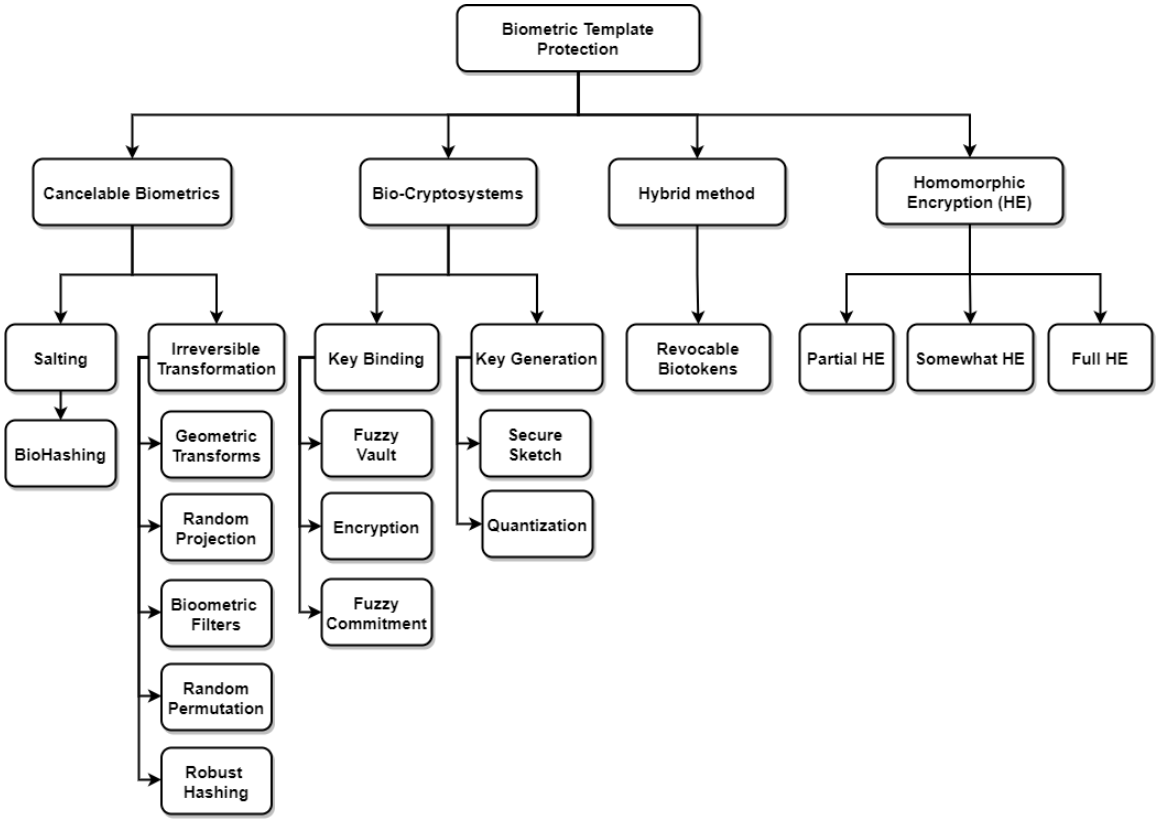


Figure 1.3: Types of Biometric Template Protection techniques

1.4.1 Cancelable Biometrics

Cancelable biometrics are the schemes in which a biometric template is transformed into an irreversible template [25], and the verification is performed on that template as shown in Figure 1.4. These are categorized into two types 1) Salting, where an invertible function is used to transform the features [26, 27, 28, 29, 30]. The key used for authentication must be securely stored or retrieved. This approach has a low FAR. By changing the user-specific keys provided during authentication it enables the straightforward revocation of compromised templates. 2) Irreversible Transformation, where they use irreversible transformations, generating transformation keys during authentication [31, 32, 33, 34, 35]. This method enhances security by making the original biometric data irrecoverable. Non-invertible transforms offer better revocability and diversity than salting methods, balancing discriminability and non-invertibility in their design.

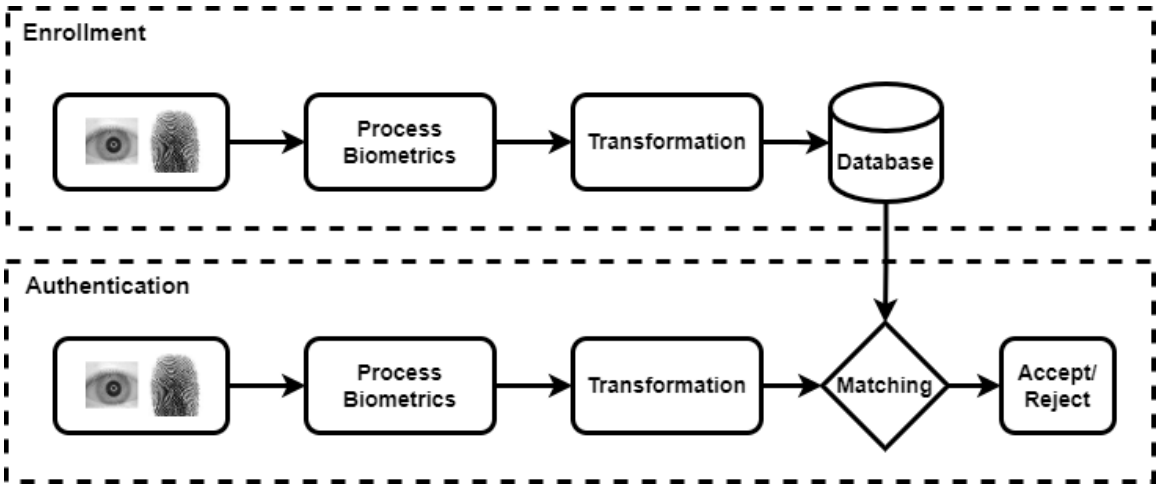


Figure 1.4: Cancelable System Architecture

1.4.2 Bio-cryptosystems

Bio-cryptosystems are the schemes in which cryptographic techniques are applied for biometric data protection [36]. These are divided into two types 1) Key Binding scheme, where we perform a cryptographic operation on the data based on the key provided by the user [37]. This process creates a secure link between the key and the biometric data, ensuring its protection as shown in Figure 1.5. Examples of Key Binding schemes include

the fuzzy vault method [38, 39, 40, 41, 42], encryption techniques [43, 44, 45, 46, 47], and fuzzy commitment protocols [48, 49, 50, 51, 52]. These methods encrypt or protect biometric data using the user's chosen key, making it unreadable without the corresponding key. 2) Key Generation scheme, where the cryptographic key is generated using the biometric trait to perform the cryptographic operation [53] as shown in Figure 1.6. This approach eliminates the need for the user to provide a key separately. Examples of Key Generation schemes include secure sketch methods [54, 55, 56, 57, 56] and quantization techniques [58, 59, 60, 61, 62].

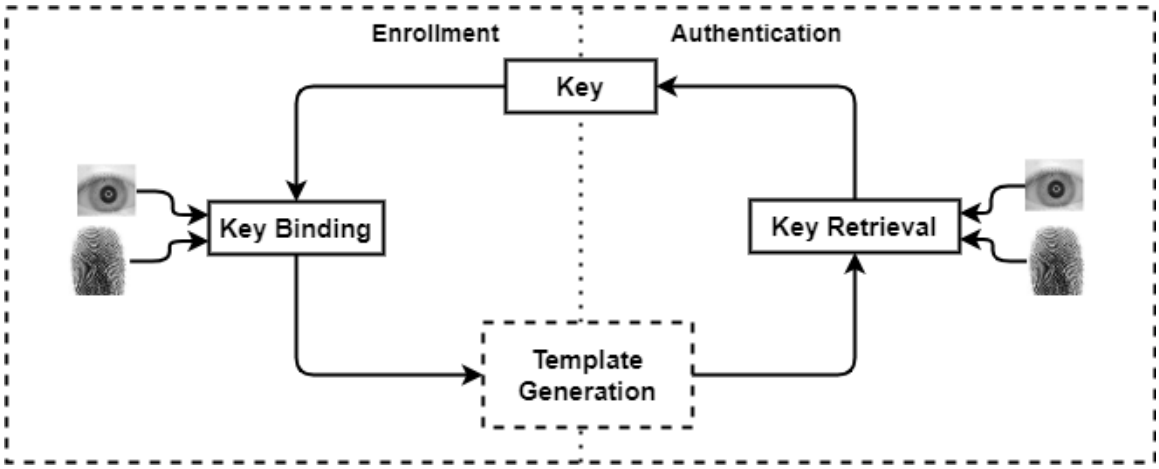


Figure 1.5: Key Binding Scheme

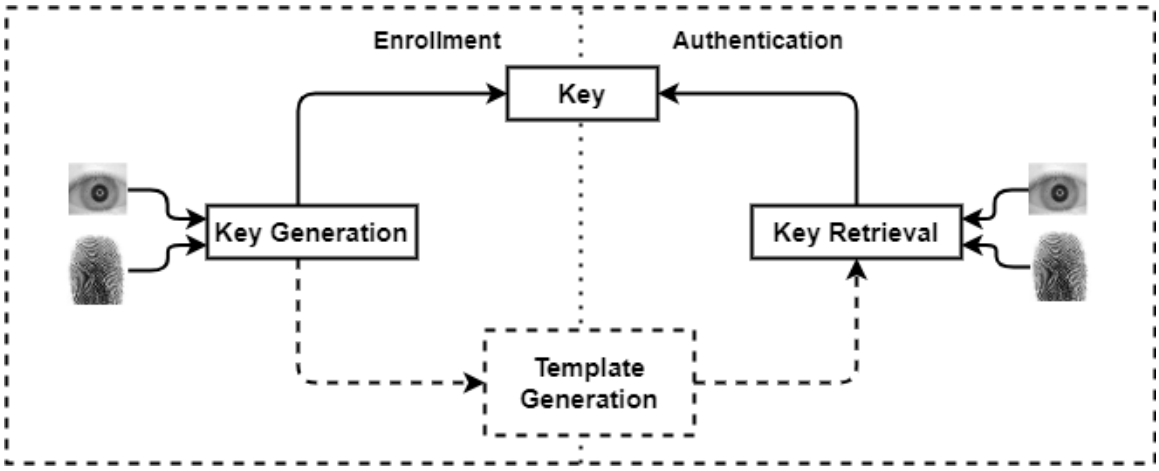


Figure 1.6: Key Generation Scheme

1.4.3 Hybrid method

To solve the limitations of using only cancelable biometrics or biometric cryptosystems, Biometric Template Protection Schemes introduces a hybrid solution [63]. These hybrid techniques enhance security by combining cancelable biometrics and biometric cryptosystems [64, 65, 66, 67, 68]. By integrating the transformation capabilities of cancelable biometrics with the cryptographic approaches of biometric cryptosystems, these hybrid schemes provide a comprehensive solution for biometric data protection that balances performance and security.

1.4.4 Homomorphic Encryption

Bio-cryptosystems and cancelable biometrics perform poorly when working on unprotected data or require auxiliary data (AD) for verification [53]. An attack on this AD can expose sensitive information, affecting the system's security and the subject's privacy. HE can be used as an alternative for those approaches that require AD, which provides privacy and security by allowing us to perform operations like additions and multiplications on the encrypted data[69] as shown in Figure 1.7. HE is of three types [69, 70, 71] (1) Partial homomorphic encryption (PHE) allows either additions or multiplications in an encrypted domain but not both [72, 73, 74, 75]. (2) Somewhat homomorphic encryption (SHE) allows additions and multiplications but for a limited number of times [76, 77, 78, 79]. (3) Fully homomorphic encryption (FHE) allows additions and multiplications in the encrypted domain any number of times [80, 81, 82, 83].

1.5 Unimodal and Multimodal

Unimodal biometrics refers to biometric systems that rely on a traits for authentication, such as a single fingerprint or face. These systems are commonly used in real-world applications for their simplicity and ease of implementation. However, unimodal biometric systems face several challenges that can impact their reliability and effectiveness [84]. Firstly, they often encounter noisy data, such as fingerprints with scars or low light face

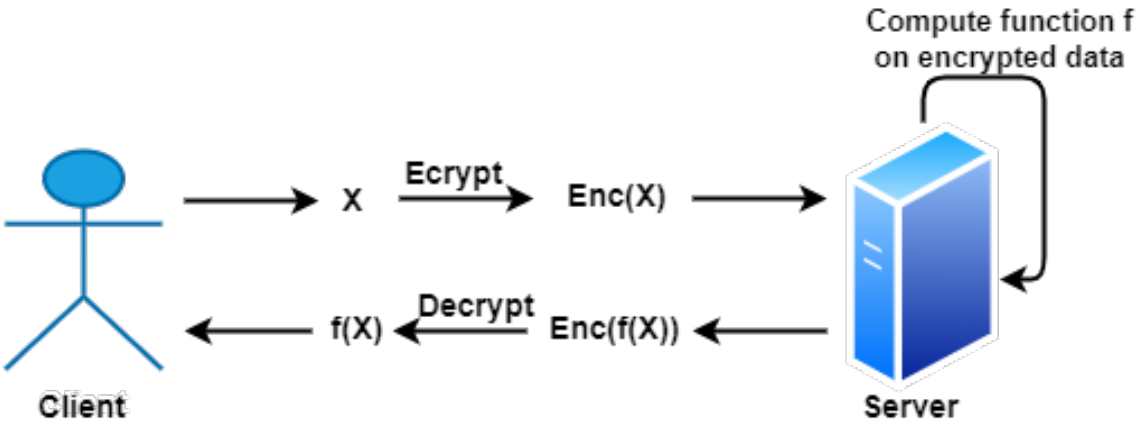


Figure 1.7: Homomorphic Encryption Scheme

images. This noise can be caused by a variety of circumstances, including defective sensors or poor environmental conditions. Secondly, variations within the same class of users, caused by incorrect interactions during authentication, can lead to authentication errors. Thirdly, in biometric systems with a large user base, similarities between different individuals' biometric features can create confusion. This can limit the system's ability to accurately distinguish between users. Finally, unimodal systems are susceptible to spoof attacks, in which attackers utilise forged biometric samples to mislead the system.

Multimodal biometric systems, utilize multiple straits for authentication. This approach combines two or more biometric traits, such as fingerprints, facial features, iris patterns, voice, or hand geometry, to enhance the accuracy and reliability of the authentication process [85]. By integrating multiple biometric modalities, multimodal systems aim to improve security, overcome the limitations of individual traits, and provide a more robust means of user authentication.

1.6 Types of Fusion

The following are the fusion types that can be performed for designing a multimodal biometric [86].

- **Sensor-level Fusion**

  This is a basic level fusion where the raw data from the sensor is combined in the

form of pixels, signals, etc. Here, the raw data is fused without performing any preprocessing. It combines two or more instances of the same biometric obtained from the same or separate sensors (with the same compatibility) [87].

- **Feature-level Fusion**

  In this type of fusion, the feature vectors which are generated after preprocessing are merged to create a single feature vector that is used for authentication. Fusion at the feature-level is supposed to produce superior recognition results as it contains more biometric characteristic information. However, it has also been shown that feature-level fusion enhances accuracy when features from diverse modalities are compatible [88].

- **Score-level Fusion**

  In score level fusion, individual scores produced by matching features with previously saved templates are combined to make a final choice. Scores are commonly computed using the average, min-max, and highest score approaches [89].

- **Decision-level Fusion**

  In this level of fusion, each modality is classified independently, i.e., each biometric trait is processed separately, and features are extracted. These feature vectors are used in the further process of classification. Once all traits have been classified separately, then all those outputs are combined to get the final classification [90].

1.7 Performance Metrics

Our proposed work is evaluated based on the following metrics [91].

- False Acceptance Rate (FAR): It is the fraction of times an impostor is identified as a legitimate user by the authentication system.

$$FAR = \frac{\textit{imposter scores above the threshold}}{\textit{all imposter scores}}$$

- False Rejection Rate (FRR): It is the fraction of times a legitimate user is misidentified as an impostor by the authentication system.

$$FRR = \frac{\textit{genuine scores below the threshold}}{\textit{all genuine scores}}$$

- Genuine Acceptance Rate (GAR): It is the fraction of times an authentication system properly detects a genuine user. It can also be calculated using FRR i.e. GAR = 1 - FRR.

$$GAR = \frac{\textit{genuine scores exceeding threshold}}{\textit{all genuine scores}}$$

- Equal Error Rate (EER): It is the error value at which FRR and FAR are equal. The smaller the equal error rate value, the better the biometric system's accuracy.

- Separability measures: The d' and ks-test provide a measurement for the degree of separation between the genuine and imposter score probability density.

  - d-prime(d'): The d' value is defined as the standard deviation difference between the means of the genuine and imposter probability distributions. The higher the d' value the better the system can differentiate genuine and imposter.

$$d' = \frac{|\mu_G - \mu_I|}{\sqrt{\sigma_G^2 - \sigma_I^2}}$$

  - ks-test: The KS-test is a non-parametric statistical procedure used to determine whether two sets of biometric data have the same underlying distribution. It has a scale of 0 to 1. If the ks-test value is near to one, it means that the distributions are well separated.

1.8 Motivation & Objectives

1.8.1 Motivation

In the rapidly evolving field of biometric security, the primary challenge lies in safeguarding user privacy while maintaining system performance. The exposure of biometric templates to unauthorized users poses a serious problem, resulting in the implementation of strong Biometric Template Protection (BTP). The existing literature on BTP has identified a critical gap in addressing issues related to the need for auxiliary data during template construction. This research gap motivates us to focus on developing a BTP technique that utilizes homomorphic encryption operating on encrypted data. The proposed work aims to significantly enhance security by eliminating the need for auxiliary data, and reducing template size, thereby improving system performance. As some applications need high performance, given the increased computational complexity associated with implementing Full Homomorphic Encryption (FHE), some applications require high performance; hence, a BTP strategy that prioritizes system performance is required. As a result, this thesis introduces a cancelable scheme ensuring high performance without compromising the security of biometric templates. The technique focuses on eliminating trait alignment issues to enhance system efficiency. Notably, cancelable techniques in the literature are vulnerable to various attacks when auxiliary data is used. This thesis presents a cancelable technique that uses deep CNN-based feature extraction, with a main focus on improving system security by addressing alignment and rotational invariance issues. This aims to counter attacks involving auxiliary data, ensuring resistance against potential threats. Acknowledging that attackers can modify data even when templates are protected using various BTP mechanisms, we designed a hybrid protection strategy. This technique combines digital signatures and encryption technologies to provide an additional layer of security for biometric templates, ensuring confidentiality and integrity. This dual strategy seeks to strengthen the system's resistance to potential attacks while ensuring overall robustness.

1.8.2 Objectives

The following objectives formulated in this thesis are:

Objective 1: To develop a homomorphic encryption-based template protection technique for high-security applications that eliminates the need for auxiliary data.

Objective 2: To develop an alignment-free cancelable template protection technique for enhancing performance without compromising security.

Objective 3: To develop a cancelable technique that uses deep CNN-based feature extraction, with a focus on eliminating alignment and rotational invariant issues for enhanced security.

Objective 4: To develop a hybrid protection technique that combines both sign and encryption for providing confidentiality and integrity to the templates.

1.9 Summary of the contributions

In this section, an overview of chapter-wise contributions to this thesis has been presented. Each subsection presents a summary of the contributions of the corresponding chapter.

1.9.1 To develop a homomorphic encryption-based template protection technique for high-security applications that eliminates the need for auxiliary data.

The contributions of this work are listed below.

1. We present a method called Local Random Projection (LRP), which reduces the template size by using random projection based on features extracted from the biometric traits.

2. Our method generates a multimodal cancelable template without any AD, thereby avoiding information leakage.

3. To improve the system's accuracy and solve the rotational inconsistency problem, we generate a rotational invariant code.

4. We utilize a batching scheme to reduce computational time by simultaneously performing multiplication on multiple ciphertexts.

5. Our method has been evaluated on Children Multimodal Biometric Database, with LRP on fused templates, and LRP on individual templates, where we get an Equal Error Rate(EER) of 0.0214% by using LRP on fused template technique. The lower the equal error rate value, the higher the system's accuracy.

1.9.2 To develop an alignment-free cancelable template protection technique for enhancing performance without compromising security.

The contributions of this work are listed below.

- We proposed an alignment-free method that doesn't require singularity points or ridge count for fingerprint.

- We extracted features from Iris using a pre-trained VGG-16 and random-projection model.

- We created a secure 3-D shell using a non-invertible transformation which preserves the security and performance of the system.

- Our technique was evaluated on CASIA V1 & FVC 2004, CASIA V3 & FVC 2006, and the Children Multimodal Biometric Database and achieved an EER of 0.032%, 0.09% and 0.015%, respectively.

1.9.3 To develop a cancelable technique that uses deep CNN-based feature extraction, with a focus on eliminating alignment and rotational invariant issues for enhanced security.

The contributions of this work are listed below.

- An architecture for the protection of multibiometric templates is proposed, based on the concepts of deep binarization and feature hashing random projection.
- Unlike traditional random projection, feature-hashed random projection generates an irreversible template by considering the local features of the feature vector and user seed using SHA3-512 hashing.
- This study explores the model's effectiveness on different feature-level fusion methods like concatenation and Xor.

1.9.4 To develop a hybrid protection technique that combines both sign and encryption for providing confidentiality and integrity to the templates.

The contributions of this work are listed below.

- A multimodal system is proposed to safeguard the biometric templates, based on the concepts of Block-Xor, sign, and encryption.
- Our proposed technique provides both confidentiality and integrity by integrating encryption and digital signature in a single operation, providing efficiency and minimizing computational overhead. 0.5cm
- Block-xor is employed to generate irreversible templates.
- The templates generated by combining Iris and Fingerprint satisfy all of the criteria of biometric template protection such as cancelability, diversity, security, and performance.

1.10 Organization of the Thesis

The main goal of this thesis is to create a template protection mechanism for multimodal biometric data. The thesis consists of seven chapters, each covering a specific area of the research, as briefly stated below.

Chapter 1: This chapter serves as a thorough introduction to the thesis topic, presenting an overview of the objectives and summarizing the work done to achieve these objectives.

Chapter 2: This chapter provides an overview of the latest advancements in the field of biometrics, with particular emphasis on multimodal template protection techniques.

Chapter 3: In this chapter, a template protection technique based on homomorphic encryption is developed. The method utilizes Local Random Projection to reduce the template size and generate an irreversible template. Experimental results indicate that the proposed approach enhances the performance of the system compared to existing techniques while also improving security.

Chapter 4: This chapter presents an alignment-free multimodal cancelable template protection scheme by generating 3-D shells. Features are first extracted from the fingerprint, then a 2D spiral curve is created using a user key set. Next, iris features are extracted using a pre-trained VGG-16 model, and feature vector-based random projection is applied to generate an iris feature vector. This vector is combined with the fingerprint shell to construct a secured 3-D shell, which is then saved in the database for matching.

Chapter 5: This chapter presents a cancelable template protection scheme designed to address alignment and rotational invariant issues, thereby enhancing the security and performance of the system. Initially, features are extracted from the iris and fingerprint using a pre-trained Convolutional Neural Network (CNN) model. The extracted features are then deep binarized, to generate binary codes. These binary codes are fused using the AdditionRotationXor (ARX) operation, which adds a layer of complexity to the representation. Later, feature-hashed random projection is performed on these fused features by using a user seed and a feature seed to generate a secured template. The cancelability feature assures that these templates can be regenerated if compromised, providing another degree of protection to the entire system.

Chapter 6: This chapter introduces a template protection strategy aimed at providing confidentiality and integrity to the templates through the use of Block-Xor and Signcryption. Initially, features are extracted from the iris and fingerprint, using a pre-trained Convolutional Neural Network (CNN) model. After extraction, these features are converted into binary codes using a deep binarization process. Next, the binary codes are combined using the Block-Xor operation. Later Signcryption is performed on these fused features, which is a cryptographic approach that combines signature and encryption functionalities into a single operation. These secured templates generated by the Block-Xor and signcryption processes are stored on a server for authentication. This ensures the integrity, authenticity, and confidentiality of the data.

Chapter 7: This chapter provides a comprehensive summary of the contributions made in the thesis, highlighting the significant findings and discussing potential future directions for extending the proposed works.

Chapter 2

Related Work

This chapter provides a thorough review of various multimodal template protection techniques. Section 2.1 examines the literature on cancelable systems, while Section 2.2 focuses on Bio-Crypto Systems. Section 2.3 covers the use of hybrid approaches for biometrics, whereas Section 2.4 concentrates on literature relevant to homomorphic encryption-based systems. Finally, a summary is provided in Section 2.5.

2.1 Cancelable Systems

Cancelable biometrics are the schemes in which a biometric template is transformed into an irreversible template, and the verification is performed on that template. As shown in Figure. 1.3, these are categorized into two types.

2.1.1 Salting

Salting in BTP technique which uses an invertible function to transform biometric features. Due to the reversibility of the transformation, the key must be securely stored. Salting methods typically yield a low FAR due to the use of keys.Compromised templates can be easily revoked by altering user-specific keys. El-Rahiem et al. [92] created a cancellable multi-biometric recognition system that uses neural style transfer and bio-hash. The system integrates fingerprint, face image, and finger vein data, which is converted

using style transfer and used as cancellable templates after bio-hashing. The analysis demonstrates the system's improved performance both statistically and visually. Zheng et al [93] introduces a multimodal biometric authentication system that uses Index-of-Max (IoM) hashing and Alignment-Free Hashing (AFH), which is mathematically expressed as $T_k(V) = \sum_{i>j} \delta(d(i,j) - k)\delta(v_i, 1)\delta(v_j, 1)$. IoM hashing provides good security, while AFH has low template storage, computational cost, and privacy issues. It supports a variety of biometric features (binary and real-valued), allowing for fusion with AND, OR, and XOR operators in the binary representation. Bedad et al. [94] proposed a multi-instance fingerprint biometric system that uses deep learning together with biohashing. Initial features are extracted using a pre-trained ResNet-50 model. These vectors are then merged to create a combined feature vector. Finally, the resulting fused vector is protected using a feature transformation technique called as Biohashing. Khurshid et al. [95] presents a novel approach to enhance the security of a multimodal biometric system utilizing fingerprint and hand geometry traits. Firstly, fingerprint feature vectors are transformed using block-based hashing (BBH). Secondly, the average of hand geometry feature vectors is used for transforming their respective vectors. The resulting transformed feature vectors for both modalities are utilized to create secure templates. Zhong et al. [96] introduces a novel multi-biometrics system merging palmprint and DHV recognition. Using DHN deep learning for palmprint and BGM graph matching for DHV, this method encode biometric images into 128-bit binary codes. This approach optimizes feature combinations from both modalities to enhance recognition accuracy across pixel, feature, score, and decision levels. Jeng et al. [97] introduces a new multimodal system for personal authentication.The proposed method integrates features from varying ranges using shuffle coding, including dimension adjustment, standardization, and fusion coding. Two methods are explored: Method 1 uses feature scaling to produce a binary code representing normalized feature values' distance. In Method 2, hashing and a projection framework maximize features on a hyperplane, quantizing hash values into binary code sequences. The final fusion code is generated by XOR operations.

2.1.2 Irreversible Transformation

It uses irreversible modifications with a key generated during authentication, ensuring that the original biometric data cannot be recovered and therefore increasing security. When compared to salting techniques, these methods offer better diversity and revocability. Rathgeb et al. [98] presented a multi-instance cancelable system using both iris. Initially, features are extracted from both the iris and divided into several blocks. These blocks are combined by using an adaptive bloom filter to create a cancelable template. R Dwivedi et.al [99] developed a new fusion for generating multimodal cancelable templates. The proposed hybrid fusion approach considers the similarity scores generated by various matchers for each trait. MCW score fusion method is used to merge the separate scores collected from multiple matchers as it determines the best weight for all the matcher for each modality. The generated scores are next fed to the DS theory to produce the final decision. Yang et al. [100] proposed a multimodal cancelable system that uses fingerprint and finger vein. At first, features are extracted from both traits. Three types of fusions are evaluated in this paper where a new transformation named Enhanced partial DFT is used which is expressed as $Y' = M\tilde{b}$ is applied to the features to generate cancelable templates. Ghouzali et al. [101] presented a cancelable multimodal system using face and fingerprint. In order to create a cancelable template, chaotic maps are used for the face, and the torus automorphism technique is used for the fingerprint. Feature-level fusion is performed to generate a cancelable template. Walia et al. [102] proposed a multi-biometric system. Initially, normalized sparse graphs are constructed by comparing the key images with the raw input images. These graphs are combined using cross-diffusion to generate a fused vector. These graphs are fused adaptively by considering the weights that are generated from the adaptive weight generation module using image quality which generate a cancelable templates. Gupta et al. [103] proposed a multimodal cancelable system using fingerprint and iris. LBP is used to extract features from these traits that are represented as coordinates on a plane on which random projection is performed. These projected features are then represented as cylindrical coordinates using the equations $P_i^k(\theta, \rho, z) = f\left(P_i^{(k)}(\phi_x, \phi_y, \phi_z)\right)$ where $\rho = \sqrt{\phi_x^2 + \phi_y^2}$, $\theta = \tan^{-1}\left(\frac{\phi_y}{\phi_x}\right)$ to generate cancelable templates. Sudhakar et al. [104]

proposed a multi-instance deep neural network-based cancelable system. First, features are extracted from both the iris images using a proposed CNN architecture which is inspired by pre-trained VGG-19. These features are multiplied with a user-specific random matrix. Then a novel random projection is performed by multiplying the two formed feature vectors to create a cancelable template. Abdellatef et al. [105] developed a multi-modal cancelable scheme where different traits like face, iris, nose, and mouth are extracted from a face image. Features from all the traits are extracted by using a proposed CNN model. Once the features are extracted they are fused to form a single feature vector on which bio-convolution encryption is performed to produce a cancelable template. El-Rahiem et al. [106] developed a multi-modal cancelable system based on iris, fingerprint, and finger vein information. Initially, a proposed CNN model is used to extract features from all of the traits. These features are fused using feature maps, which are then processed by the Deep Dream algorithm to create a cancelable template. Singh et al. [107] presented an integrated template protection strategy for a multi-biometric system., which includes face and electrocardiogram (ECG) biometrics. The technique protects the templates at several phases of biometric fusion by employing deep binarization and secure hashing.

2.2 Bio-Crypto Systems

Biocryptosystems are schemes that use cryptography techniques for protecting biometric data. As illustrated in Figure 1.3, these are classified into two categories.

2.2.1 Key Binding scheme

These are the systems, where we perform a cryptographic operation on the data based on the key provided by the user. Kanade et al. [108] proposed a multimodal biometrics-based cryptographic key renewal mechanism scheme that obtains 183-bit entropy cryptographic key by combining iris and facial features using a weighted feature-level fusion technique. Mai et al. [109] proposed a binary feature fusion approach for multi-biometric cryptosystems. It starts by extracting a collection of weakly dependent feature groups from the various unimodal features, and then each group is combined using a bit mapping that reduces

intra-user variations while increasing inter-user variations. Sreemol et al. [110] proposed a multi-instance cryptosystem scheme that uses a fuzzy vault. This system stores features extracted from the left iris and right iris in a single fuzzy vault and uses feature-level fusion. Lalithamani et al. [111] proposed a multimodal cryptosystem that uses palm and hand veins. Features are extracted from both the traits from which 50 common points are selected. To these selected common points, 20 chaff points are added, which are virtually created by the user. These combined points are used to create a fuzzy vault by using a user-specific key. Amirthalingam et al. [112] proposed a multimodal cryptosystem using face and ear biometrics. First, features are extracted from both the traits from which chaff points are generated using the PSO algorithm. A fuzzy vault is created by using a secret key and the chaff points that are generated. Sujitha et al. [113] proposed a multimodal cryptosystem using fingerprint and palmprint. Features are extracted from fingerprint and palmprint using crossing number and bottom-hat filtering techniques respectively. Once features are extracted, they are combined to form a fused vector from which chaff points are generated. To increase the system's security, pseudo points were incorporated along with the generated points. Using a user secret key, a fuzzy vault is created to secure these points in the database. Dang et al. [114] presented a multimodal cryptosystem that combines cancelability to the system. It uses a periodic transformation to generate a hash by selecting some elements from the feature vector. It also uses a polynomial function for generating points for the fuzzy vault. Chang et al. [115] proposed a fingerprint and iris-based multimodal fusion-level cryptosystem. The feature level fusion is accomplished by merging features from both traits. By combining fuzzy commitment with fuzzy vault, an architecture known as BIOFUSE is created using format-preserving encryption. Ankit Arora et al. [116] proposed a multimodal cryptosystem for user authentication. Initially, features are obtained from the face, hand vein, and finger knuckle by applying different techniques like LOOP, HOG, and Grid-based features respectively. These features are fused and secured by applying Elliptic Curve Cryptography which is optimized by Tay-GW optimization. These features are fed to a CNN for classification. Chanukya et al. [117] proposed a multimodal cryptosystem based on fingerprints and ears. Initially preprocessing is done using a median filter to assist in image cropping. Next, the preprocessed images are used to extract tex-

ture and shape features. These features are then combined and classified using an optimal neural network (ONN), with weights optimized using the firefly algorithm (FF). Kumar et al. [66] proposed a multimodal system by utilizing BCH encoding for parity-code storage and a Hash function for integrity. Two cell-arrays are created: one holds the hash-code and secret key, while the other stores chaff vectors. A regenerative XORCoding shuffles the parity-code for added security. Choudhary et al. [118] proposed a framework that uses face and fingerprint data to authenticate users. It preserves biometric templates by inserting fingerprints in secret spots on the face utilising blind and key-based watermarking methods. Face features are taken from the Discrete Wavelet Transform's approximation subband, which reduces operational complexity.

2.2.2 Key Generation scheme

These are the systems, where the cryptographic key is generated using the biometric trait to perform the cryptographic operation. A. Nagar et al. [119] proposed a multimodal architecture for creating a secure sketch. This architecture uses cryptosystem techniques like Fuzzy vault and fuzzy commitment to create secured templates. First, the features are extracted from the trait on which fuzzy commitment is applied. These feature vectors are combined to form a combined fused vector on which a fuzzy vault is applied to generate secured templates. Talreja et al. [120] proposed a multi-modal templates protection method using face and iris. Here the users' biometric data is processed by the DFB block for creating a fused binarized vector. A unique enrollment key is then generated from a subset of these features. Using this key, a cancelable multimodal template is created by choosing certain values from the feature vector. The template undergoes Forward Error Correction (FEC) decoding to produce the final multimodal sketch. Ma et al. [121] proposed a two-stage multimodal authentication system embedding face features into fingerprint images for data credibility and secondary authentication. It validates patterns using face detection-based strategies for watermark verification, aiding subsequent biometric authentication. The approach preserves fingerprint features by adapting wavelet quantization to distribute watermark energy on significant DWT coefficients of fingerprint images. Chang et al. [122] proposed a multi-

instance iris cryptosystem. First, features are extracted from both traits, where one trait is used to generate a key using a fuzzy extractor. Using this key bit wise encryption is performed on the second trait, which gives us a secured template. The new bit-wise encryption method is employed to reduce the noise generated by bit errors. Zaghouani et al. [123] proposed a secure sketch technique for template protection of ECG. AC/DCT method is used to extract features on which a scalable quantization technique is applied. Then, the quantified ECG template is secured using a safe sketch biometric crypto-system. Ma et al. [124] proposed a multimodal biometric identification method that embeds fingerprint minutiae into facial images. This approach uses a block pyramid based on face region distinctiveness. A first-order statistics QIM approach embeds higher priority numeric watermark bits with greater intensity in the upper pyramid levels, resulting in a balance of watermark robustness, capacity, and accuracy. Chatterjee et al. [57] proposed a biometric authentication system where the templates generated are protected using the secure sketch. Here, several trait instances are combined to form a multisketch that generalizes secure sketches. Kaur et al. [125] proposed a multimodal template system combining iris and dual fingerprint traits. A hash function protects the key, which was created with fuzzy extractors to ensure reliability. To meet the fuzzy extractor's demand for ordered datasets, an approach is developed that converts unordered fingerprint minutiae points into ordered datasets for consistent key creation.

2.3 Hybrid Systems

Hybrid biometric template protection schemes combine cancelable biometrics' transformation capabilities with biometric cryptosystems' cryptographic methods, offering a comprehensive solution for biometric data security. Bousnina et al. [126] developed a multimodal biometrics system that uses a hybrid approach. To preserve privacy and integrity a secure sketch approach is used on fingerprint. The protected fingerprint is then watermarked with the facial image using a mix of Dual-Tree Complex Wavelet Transform (DTCWT) and Discrete Cosine Transform (DCT). To improve overall security, a 3D chaotic-map-based encryption approach is implemented, adding an extra layer of security to the fused bio-

metric data. L Yuan et al. [127] proposed a template protection method for multimodal biometric templates using feature-level fusion, non-invertible transformation, and fuzzy commitment encryption. It shows that multimodal biometric template encryption performs better than unimodal biometric encryption. Nafea et al. [128] proposed a hybrid BTP approach, that embeds fingerprint data into the face image using Watermarking with DWT and SVD. The resulting image is shuffled, XORed with a Hadamard matrix-generated user key, and then encrypted with chaotic maps for enhanced security. Selwal et al. [129] proposed a hybrid BTP technique that combines fingerprint and hand geometry. It begins with bio-hashing to convert feature vectors to binary format, which is then merged with a transformation method to build a single secure template. This template is subjected to an octet indexing approach, to generate secured templates. Chin et al. [130] proposed a multimodal method that uses fingerprints and palmprints to generate a fused vector. Using the user-specified key, a random feature set is constructed by applying Random Tiling to the fused features. This method partitions the feature space into random, non-overlapping tiles. The created random features are then discretized to create the template bit-string, which converts continuous feature values into discrete binary values. Abdul et al. [131] proposed a hybrid Biometric Template Protection (BTP) approach where facial images undergo Discrete Wavelet Transform (DWT) to extract directional sub-bands, where fingerprint features are embedded by quantizing wavelet coefficients' mean values. The inverse DWT (IDWT) reconstructs the watermarked image with encoded fingerprint data. A hyper-chaotic map generates a key stream for encrypting the watermarked image using block-cipher, enhancing security. Zhao et al. [132] presented a hybrid BTP technique that uses face and iris. The traits are processed using deep hashing with two CNN models. Resulting binary codes i.e. face code undergoing a random permutation and Cancelable Feature Extractor module generates a user-specific key from the iris code. Public helper data is produced, and these, along with the key and face code, create a protected template using Cancelable Dual Parallel Encryption for enhanced security and system integrity.

2.4 Homomorphic Encryprion Systems

It is a type of encryption in which certain mathematical operations like addition and multiplication can be performed on encrypted data without first decrypting it. In simpler terms, it enables computations on encrypted data, and the results of these computations will be the same as if they were done on unencrypted data. As shown in Figure. 1.3, these are divided into three types.

2.4.1 Partial homomorphic encryption

These are the systems that supports either additions or multiplications in an encrypted domain but not both.

Mahesh et al. [133] presented a multi-instance iris system. For providing privacy to the templates, they used Elgamal encryption which is a PHE scheme, and for providing integrity, they placed the hash codes of each template in the blockchain. Mahesh et al. [134] developed a multi-instance iris authentication system using Partial homomorohic encryption. It extracts the features from both iris and combines to form a single vector, then compressing it with local random projection for efficiency. Next, the compressed template is encrypted using Paillier Homomorphic Encryption and stored in the cloud for verification Barni et al. [135] uses a Paillier cryptosystem that allows the addition of encrypted data. Here, the probe is encrypted, but the database is not encrypted (which provides no security to the database). Upmanyu et al. [136] proposed RSA-based homomorphic encryption. They are based on a simple client-server architecture, but they use a third-party server for enrollment. Kikuchi et al. [137] proposed additive homomorphic encryption and a cryptographic procedure for demonstrating that a committed value is inside a certain interval without exposing the value itself. The similarity of the vectors is done by using cosine and euclidian based on zero-knowledge proof of range.

2.4.2 Somewhat homomorphic encryption

These are the systems that support additions and multiplications but for a limited number of times. Barni et al. [138] introduced a secure multimodal biometric protocol that combines

iris and face data. Utilizing the Symmetric Homomorphic Encryption (SHE) scheme, they generate both a public key and a shared secret key. These keys facilitate a secured multi-party protocol, ensuring the privacy and integrity of the combined biometric information.

Abidin et al. [139] presented a SHE and ring-LWE-based authentication system. The template is encrypted using SHE, and the matching is done using ring-LWE. The calculation of hamming distance can be done securely as it uses encrypted data.

Cheon et al. [140] proposed an authentication system using SHE. The operations on the data are performed using SHE, whereas matching is done using MAC because SHE is computationally expensive.

Yasuda et al. [141] proposed an authentication system using SHE in which a packing technique for effectively computing multiple hamming distance values on encrypted data was developed.

2.4.3 Fully homomorphic encryption

These are the systems that support additions and multiplications in the encrypted domain any number of times. Gomez et al. (2017) [142] introduced a framework for multi-biometric template protection utilizing Homomorphic Encryption. In this system, all information, whether stored in the database or exchanged between client and server, remains encrypted. The framework is built upon fingerprint and online signature modalities. Features from both traits and fused to generate a unified template. Various models have been presented and evaluated across three fusion levels: feature, score, and decision levels. MK Morampudi et.al [143] proposed a multi-iris authentication system that protects privacy by employing FHE. Rotational invariant templates were created to improve recognition accuracy and eliminates rotational inconsistencies. A batching strategy is used to increase computational efficiency. Sperling et al. [144] introduced a multi-biometric system that integrates voice and face data. Features are gathered from both traits and then encrypted using Fully Homomorphic Encryption (FHE). The encrypted features are merged, and the resulting fused vector undergoes random projection before being normalized to generate the secured template. Salem et al. [145] created a fingerprint and iris-based multi-party

biometric system using Fully Homomorphic Encryption (FHE). A pre-trained deep neural network is used for feature extraction, which includes biometric verification and liveness detection. This technique ensures privacy and scalability because sensitive biometric data does not require training or decryption. Torres et al. [146] developed an FHE-based iris authentication system. The author's major goal is to provide security to the system, which compromises the computational cost. Sperling et al. [144] proposed a multimodal template protection using face and voice. Feature vectors are encrypted using homomorphic encryption and combined to form a single fused encrypted vector. Using an obtained matrix, perform a linear projection to a lower-dimensional space, followed by approximate normalization to build secure templates.

2.5 Summary

This chapter presents a brief literature review of the advancements made in biometric template protection, specifically focusing on multimodal systems. Some of the existing works on cancelable systems, bio cryptosystems, hybrid systems and homomorphic encryption are described. While homomorphic encryption allows computations on encrypted data, it generally comes with high computing costs, which affects overall system performance. Cancelable systems, although enhancing privacy by transforming biometric data, can suffer from information loss, complexity in implementation, and revocability challenges. Bio-crypto systems face challenges in key management, compatibility, and vulnerabilities to attacks such as spoofing. Therfore, the method in chapter 3 solves the rotational inconsistency of iris which improves the performance of the system, it also overcomes the hill-climbing attack and decreases the computational cost using batching scheme. The method in chapter 4 solves the alignment problem of fingerprint, revocabilty issues, it also overcomes various attack. The work in chapter 5 overcomes the rotational and alignment issues along with the key management problem in bio cryptosystem. The method in chapter 6 overcomes various attacks on biometric while providing confidentiality along with integrity to the templates

Chapter 3

Homomorphic encryption-based template protection technique for high-security applications

In this chapter, a multimodal template protection scheme is proposed, utilizing holomorphic encryption to eliminate the requirement for auxiliary data, along with a feature-based random projection that reduces the size of the template.

Chapter Organization: Section 3.1 provides the basics of methods used in the proposed methodology. Section 3.2 explains the proposed methodology, while Section 3.3 presents the experimental results. Section 3.4 offers a comparative analysis, and Section 3.5 discusses the security analysis of the proposed methodology. Finally, Section 3.6 provides a summary of the work.

3.1 Background

3.1.1 Random Projection

Random Projection is a dimensionality reduction technique widely used in biometrics for its ability to efficiently handle high-dimensional data [147]. Random Projection is a simple yet effective method of dealing with various measurements in biometric systems, such as

fingerprint minutiae or face features. By generating a random matrix with lower dimensions than the original data, each data point is projected onto it, keeping the key structure and relationships between points while significantly reducing the computational cost. This technique proves advantageous due to its computational efficiency, ease of implementation, and scalability for large datasets, making it ideal for real-time biometric applications.

Given a feature vector V of size $n \times m$ where n is the number of samples and m is the number of features in each sample, the Random Projection method involves the following steps:

1. **Generate Random Projection Matrix**

   Properties of a Random Matrix R:

   - Element Distribution: The entries of R are typically drawn from a specified probability distribution, such as Gaussian or uniform.
   - Dimensionality: R usually has dimensions that match the transformation needs, e.g., a matrix for dimensionality reduction.
   - Randomness: The elements of R should be independently and identically distributed to ensure randomness.

   Create a random projection matrix R of size $m \times p$, where p is chosen to be less than m. Each element r_{ij} of R is typically drawn independently from a distribution such as Gaussian or uniformly random. The matrix R is represented as:

$$R = \begin{bmatrix} r_{11} & r_{12} & \cdots & r_{1p} \\ r_{21} & r_{22} & \cdots & r_{2p} \\ \vdots & \vdots & \ddots & \vdots \\ r_{m1} & r_{m2} & \cdots & r_{mp} \end{bmatrix}$$

2. **Matrix Multiplication:**

   Multiply the feature vector V with the random projection matrix R to obtain the new matrix V' of size $n \times p$. The multiplication is done as shown in Eq. 3.1

$$V' = V \cdot R \tag{3.1}$$

where V' is the resulting matrix, and each element V'_{ij} is calculated as:

$$V'_{ij} = \sum_{k=1}^{m} V_{ik} \cdot r_{kj}$$

Here, V_{ik} is the element at the ith row and kth column of V, and r_{kj} is the element at the kth row and jth column of R.

3. **New Reduced Feature Matrix**

   The resulting V' matrix represents the transformed feature matrix after random projection. The matrix V' has n rows and p columns. This reduced new matrix V' can be used for further processing.

3.1.2 Homomorphic Encyption

Homomorphic encryption is a type of encryption that enables calculations like addition and multiplication on encrypted data without the need to decrypt it first [148]. This means that data remains encrypted throughout computations, and only the final result, obtained after performing operations on the encrypted data, is decrypted to show the desired outcome.

Operations

- Addition: This operation allows adding two encrypted values without revealing the underlying plaintexts. Given two ciphertexts E(x) and E(y), the addition operation yields a new ciphertext as shown in Eq. 3.2.

$$E(x) + E(y) = E(x + y) \tag{3.2}$$

- Multiplication: This operation allows the multiplication of two encrypted values x and y without decrypting the ciphertexts. Given two ciphertexts E(x) and E(y), the

multiplication operation yields a new ciphertext as shown in Eq. 3.3

$$E(x) \cdot E(y) = E(x \cdot y) \tag{3.3}$$

Functions

- KeyGeneration: This function considers the security parameters and generates three keys namely Public Key(δ_{pk}), Private Key(δ_{sk}), and Evaluation Key(δ_{ek})
- Encryption: This function encrypts the message m using the public key (δ_{pk}) and returns the ciphertext E(X).
- Decryption: This function decrypts the ciphertext E(x) by using the private key (δ_{sk}) and returns the original message m.

3.2 Methodology

Section 1.4.4 provides a brief introduction to homomorphic encryption and discusses the benefits of using it in biometric template protection. The chapter's key contributions are as follows:

- Propose a feature vector-based Random projection technique, i.e., Local Random Projection(LRP), which does not require any key from the user and performs random projection.
- Generates a multimodal cancelable template without any AD, thereby avoiding information leakage.
- To improve the system's accuracy and solve the rotational inconsistency problem, we generate a rotational invariant code.

The proposed authentication system aims to maintain the privacy of templates while enhancing accuracy and reducing computation time. It uses a client-server approach and consists of four modules:

1. Generation of the combined feature vector.
2. Local Random Projection.
3. Encryption and Decryption of templates.
4. Calculation of Hamming Distance.

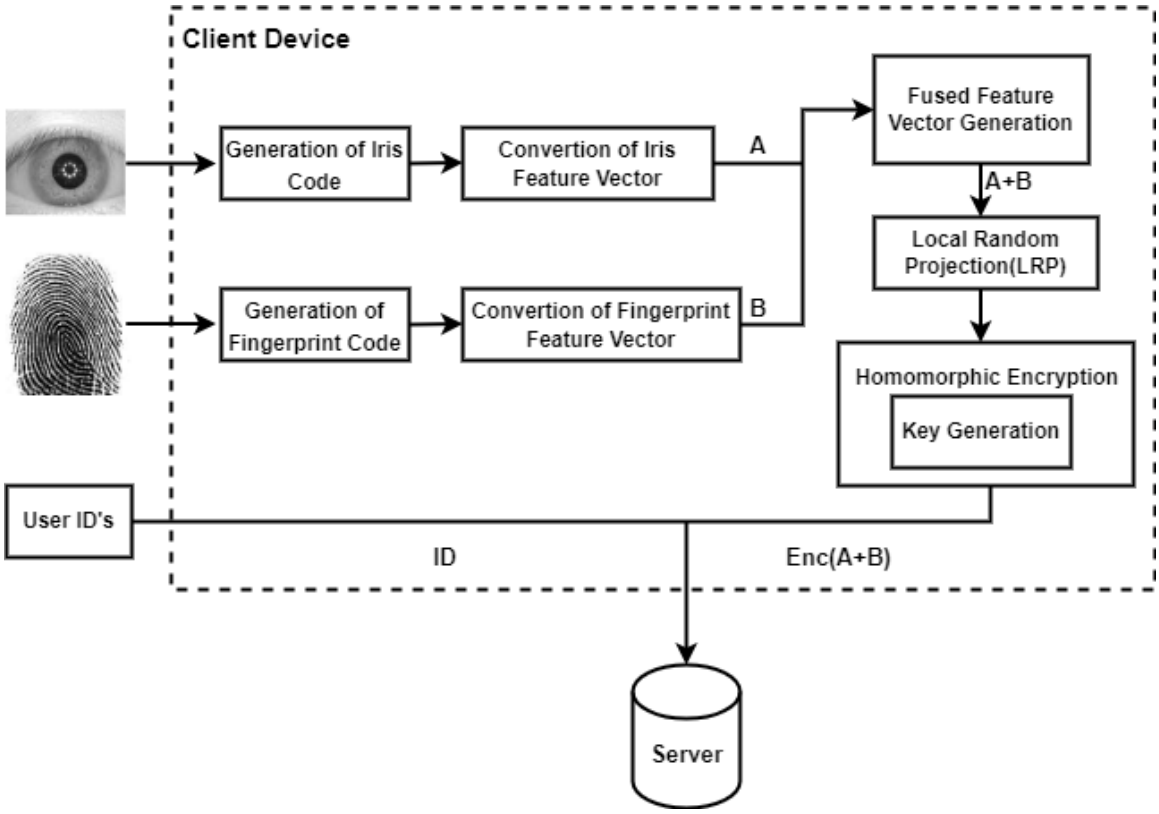


Figure 3.1: Block Diagram for Enrollment phase of proposed system

Figure 3.1 shows the step-wise procedure for the enrollment phase of the proposed method. During this phase, the user gives his biometric traits to the sensors, which are preprocessed, and features are retrieved from the traits. These features are combined to generate a single feature vector for each user. Then local Random Projection (LRP) is applied to this fused feature vector to generate an irreversible template. This irreversible template, which serves as the reference template, is encrypted using a public key. This encrypted template, together with the user ID, is stored on the server. Figure 3.2 shows the step-wise procedure for the verification phase of the proposed method. During verification,

the user presents his traits. Features are extracted from these traits and combined to produce a fused vector, on which LRP is performed. This template is encrypted using the public key to create a probe template. Finally, the server is requested for the reference template using ID. The hamming distance between the reference and probe templates is then determined. The encrypted result is sent to the client device, which decrypts it using the private key. The obtained result is then compared, determining whether the user is real or an imposter.

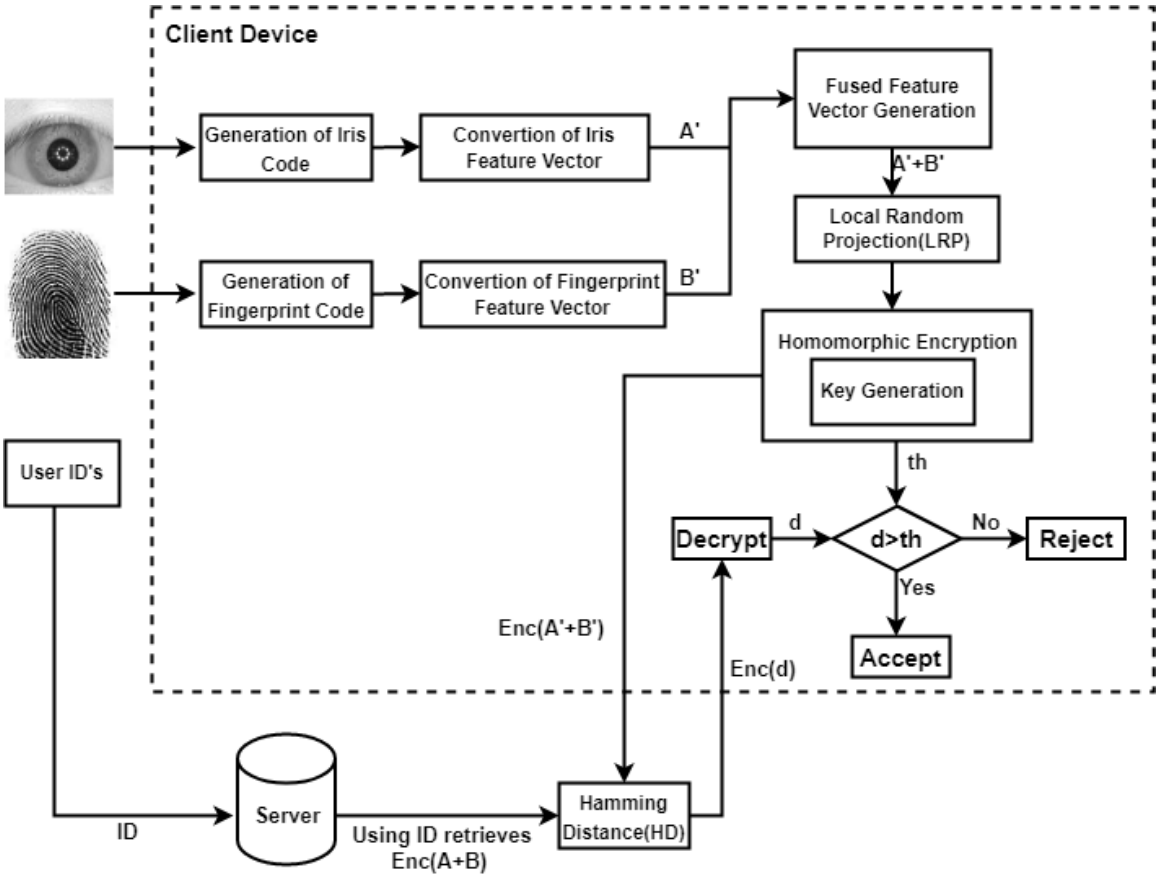


Figure 3.2: Block Diagram for Verification phase of proposed system

3.2.1 Generation of combined feature vector

Extraction of Iris Features

The iris images are first localized to find the boundaries of the iris and the pupil. Next, these localized images are segmented to form normalized images using Weighted Adaptive Hough and Ellipsopolar Transform. Finally, these normalized images are fed to a 1D-log

Gabor filter that extracts the features. These operations are performed using USIT Toolkit [149], which gives us images of size 1x1280, which are greyscaled images shown in Figure 3.3. Next, each bit in this greyscale image is converted to an 8-bit binary format to obtain the 1D feature vector of size 10240.

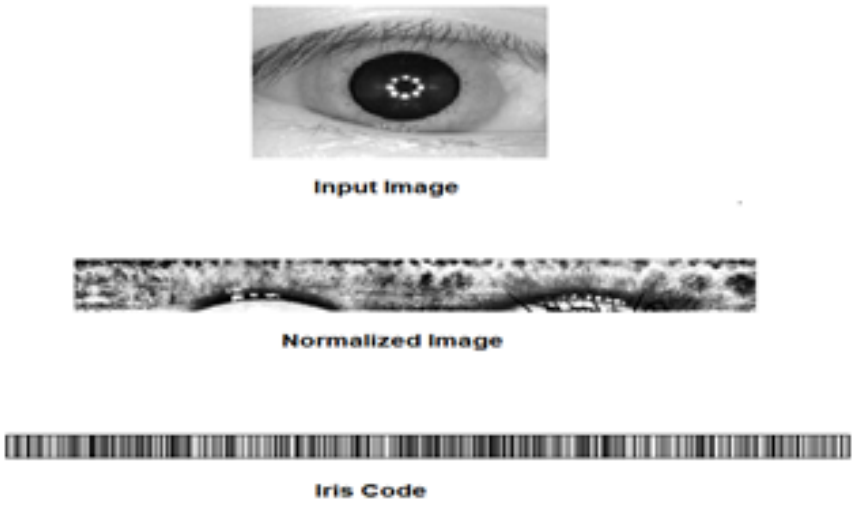


Figure 3.3: Extraction of Iris code

Extraction of Fingerprint features

A fingerprint is a connecting line formed by ridges and valleys. Ridge termination refers to the point at which a ridge abruptly ends. A ridge bifurcation is a point where a ridge separates or diverges into branches. These features together are referred to as minutiae. Each minutia point can be represented using its location, i.e., (x, y) coordinates, and the angle of orientation(θ), i.e., ridge direction. Once the minutiae points have been extracted, these points are mapped onto a 3-D cube. We partition this three-dimensional cube into equal-sized cells($16 \times 16 \times 16$) and assign each minutia point to one of them, as shown in Figure 3.4. If a block contains at least one minutiae point, it is considered as 1; otherwise, it is considered as 0. Once the mapping of all points is done, we generate a feature vector. The feature vector which we generated is of size 4096.

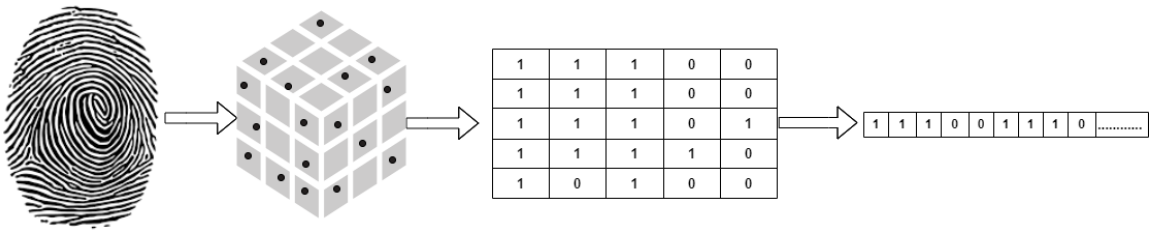


Figure 3.4: Extraction of features from fingerprint

Conversion of feature vectors

After extracting features from both traits, which are of length 10240 and 4096, we need to compress them due to their large size which may affect the computational time. To avoid this, we convert the feature vector by dividing it into equal-sized blocks (b_s), where b_s can take values from multiples of 2, i.e., 2, 4, 8, etc. When it comes to security and noise created during multiplication in homomorphic encryption, block size 4 outperforms all other values of b_s[143]. The smaller the value of b_s, the larger the polynomial modulus is required. The larger the polynomial modulus, the larger the coefficient modulus. A larger coefficient modulus gives rise to more noise. Security is also low when the coefficient modulus is high. Whereas a larger value of b_s can decrease the information present in the fused code. So, we have to choose the value of b_s wisely, which can balance both security and noise. As we choose the value of b_s as 4, the resultant Iris vector will be compressed to 10240/4=2560, and the fingerprint vector will be compressed to 4096/4=1024. Now, the fused vector will be of size 2560+1024=3584. Figure 3.5 shows the conversion of the feature vector and generating fused compressed feature vector.

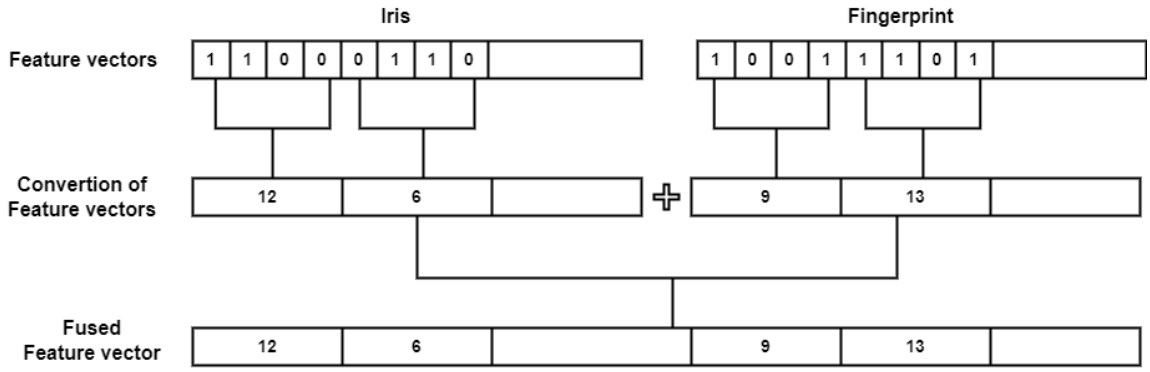


Figure 3.5: Generation of Fused compressed Feature vector

3.2.2 Local Random Projection (LRP)

Random projection is performed on the fused compressed template. We improve the traditional random projection by generating the projection matrices from the feature vector, which creates an irreversible template. Let the feature vector f_v = [15,0,0,10,2,1,5,0.....,9] of length l. The random projection is performed by using a user-specific random matrix R_m. The traditional random projection is performed as shown in Eq. (3.1).

Our objective in this work is to improve security by considering the projection matrix from the features and reducing the size of the template. Now we will go through the details of local feature projection. The compressed fused feature vector f_v is divided into m slots, each of which has b_s elements (here, $m*b_s = l$), represented as $f_v = f_1||...||f_i||...||f_m$. The i^{th} slot of f_v is represented as f_i = $[f_{i\_1}, f_{i\_2}, ..., f_{i\_b_s}]$, where $i \in [1, m]$. By considering the vector f_i and the slot number i, we are going to generate the local random projection matrix R_{lrp} as shown in Eq. (3.4), which is of size $b_s \times j$ where $j < b_s$, i.e.

$$\boldsymbol{R_{lrp}} = rand(\boldsymbol{f_i}, i) \tag{3.4}$$

To generate the random projection matrix, we use any random generator function rand(.), which is a well-known linear congruential generator [150]. This linear congruential generator is generated by using a recurrence relation as shown in Eq. 3.5.

$$X_n + 1 = (a_0 * X_n + c)\ mod\ g \tag{3.5}$$

Here, g is the modulus, X_n is the seed value, and a_0 and c are constants. This generator is utilized to create the random projection matrix R_{lrp}, as shown in Equation (3.4).

Once the random projection matrix R_{lrp} is generated, we multiply each slot of feature vector f_v with R'_m, which gives us the modified projected vector(f_{lrp}) as shown in Eq. (3.6).

$$\boldsymbol{f_{lrp}} = \boldsymbol{f_i} * \boldsymbol{R_{lrp}} \tag{3.6}$$

Algorithm 3.1 shows the step-by-step procedure of local random projection. After generating the local random projected feature vector f_{lrp}, it is encrypted and stored in a database

for matching purposes.

Algorithm 3.1 Local Random Projection

Input: Feature Vector f_v, block size b_s

Output: Local Random Projected vector f_{lrp}

$m \leftarrow \text{length}(f_v)/b_s$

$f_i \leftarrow \text{split\_into\_subarrays}(f_v, m)$ ▷ Spliting the array into m slots

$i \leftarrow \text{random.randint}(0, m-1)$ ▷ randomly selecting a slot as in Eq 3.4

$R_{lrp} \leftarrow []$

for each element X in f_i **do**

    $y \leftarrow \text{LCG}(X, g)$

    append y to R_{lrp} ▷ Generating Random projection matrix as in Eq 3.5

$f_{lrp} \leftarrow []$

for each subarray f_i in f_v **do**

    $f_{lrp} \leftarrow (f_i \cdot R_{lrp})$ ▷ Random projection as in Eq 3.6

return f_{lrp}

3.2.3 Encryption and decryption

The encoding is done using the Simple Encrypted Arithmetic Library (SEAL) HE library, which is maintained by the Cryptography Research Group at Microsoft Research. PySEAL is a Python wrapper version for the SEAL library which supports batching [151]. Batching is a powerful encoding method that decreases the number of operations. Let N denote the degree of the polynomial modulus, and P' denotes a big prime integer that is a plaintext modulus. SEAL allows batching if P' is a prime number and is congruent to 1 modulo 2*N. The plaintext is stored in this approach as matrices of size $2 \times (N/2)$, where an integer modulo of P' is performed on each element. In general, homomorphic operations are performed element by element between two encrypted matrices, allowing the user to speed up vector calculations. It is done in two ways 1) rotating the rows in a cyclic and 2) rotating columns by exchanging the rows. All of these actions need the use of a particular key, known as a Galois key or an evaluation key.

Fully Homomorphic Encryption

FHE permits to do any number of operations on the encrypted data. $R_a = Z_a[x']/(x'_n + 1)$ is a polynomial with coefficients smaller than modulo a and a maximum degree of N. The [.]a sign denotes any number that is decreased in the interval $[-a/2, a/2)$ by performing a modulo operation. $\lfloor a \rfloor$ represents the closest number which is larger than or equal to a. $\lceil a \rceil$ represents the closest number which is smaller than or equal to a. $\lfloor a \rceil$ represents the number which is nearest to a.

The encryption scheme used in our method is the Brakerski-Fan Vercuteran (BFV) Scheme. Unlike traditional cryptographic techniques such as DES, AES, etc, BFV uses a fully homomorphic encryption. It allows us to perform both the additions and multiplications on the encrypted data itself without having to decrypt it. RSA is a partial homomorphic encryption, which allows us to perform only multiplications on the encrypted data. On the other hand, partial HE (PHE) schemes such as Paillier, ElGamal, RSA, etc face problems shortly due to Quantum computers [152]. The security of the BFV scheme depends on the hardness of the Ring Learning with Errors (RLWE) problem, which is also difficult to break in the quantum era.

Fan-Vercauteren Scheme[153]: A number must be encoded in ring format R_a if it is to be encrypted using a fully homomorphic encryption technique.

Parameters: The security parameter is denoted by λ, while the number base is denoted by ω. c' is defined as the number of terms created while decomposing P' while maintaining the base as ω, where P' is a huge prime used as modulus. The formula for c' is $[log_\omega P']$. FHE is represented with the following operations.

Key Generation: The key generation method generates three keys: (i)public key (δ_{pk}), (ii) private (or) secret key (δ_{sk}), (iii)evaluation key (δ_{ek})

- Public Key (δ_{pk}): For encryption, a public key is used, which is calculated as follows: x' is sampled from R_q, e is taken from χ, s' is randomly picked from R_2, and coefficients are chosen from 0 to 1.
  δ_{pk} = $([-(s'x' + e)]_{P'}, x')$

- Private Key (δ_{sk}): For decryption, a private key is used, which is taken from R_2

- Evaluation Key (δ_{ek}): The evaluation key is used to minimize the growth of noise or ciphertext expansion, particularly during homomorphic multiplication. It is calculated as follows: x'_i is sampled from R_q, y_i is sampled from χ, and j takes the values from 0 to c

  δ_{ek} = $([-(x'_i\delta_{pk} + y_i) + \omega^i\delta^2_{pk}]_{P'}, x'_i)$

Encryption

It encrypts a message (M) using the public key (δ_{pk}) and generates the ciphertext (Enc). It is calculated as follows: u is taken from R_2, and e_1, e_2 are taken from χ.

$Enc\_0 = \Delta M + \delta_{pk}[0] * u + e_1$

$Enc\_1 = [\delta_{pk}[1] * u + e_2]_{P'}$

$Enc = [Enc\_0, Enc\_1]$

Addition

The addition of two ciphertexts in the encrypted domain is performed as

$Enc_0 = (\Delta M1 + \delta_{pk}[0] * u + e_1, \delta_{pk}[1] * u + e_2)$

$Enc_1 = (\Delta M2 + \delta_{pk}[0] * u + e_1, \delta_{pk}[1] * u + e_2)$

$Enc[0] = Enc_0[0] + Enc_1[0]$

$Enc[1] = Enc_0[1] + Enc_1[1]$

$Add = (Enc[0], Enc[1])$

Multiplication

As the depth of multiplication increases, the size of the ciphertext also increases. If the first ciphertext has a size of n_1 and the second ciphertext has a size of n_2, the result of homomorphic multiplication should have a size of $n_1 + n_2 - 1$ to keep the noise under control. The multiplication of two ciphertexts in the encrypted domain is performed as

$Mul_1 = [\lfloor (Enc_0[0] * Enc_1[0]) * (a/P') \rceil]_{P'}$,

$Mul_2 = [\lfloor ((Enc_0[0] * Enc_1[1]) + (Enc_0[1] * Enc_1[0])) * (a/P') \rceil]_{P'}$,

$Mul_3 = [\lfloor (Enc_0[1] * Enc_1[1]) * (a/P') \rceil]_{P'}$.

$Mul = [Mul_1, Mul_2, Mul_3]$

Decryption

With the use of a secret key (δ_{sk}), the ciphertext is decrypted, and message (M) is obtained as the output.

Original message(M) = $[\lfloor (Enc[0] + (Enc[1] * \delta_{sk})) * (a/P') \rfloor]$

3.2.4 Calculation of Hamming Distance

The Hamming Distance is the count of positions where corresponding bits differ between two binary vectors of equal length. HD is calculated between the probe and reference template, which are in encrypted form as shown in Eq. (3.7). The resulting distance obtained is also in encrypted form, which is decrypted using a private key(δ_{sk}) during verification.

$$HD(d) = Enc(P) * c_1 + Enc(Q) * c_2 \tag{3.7}$$

Where $P = A + B$, $Q = A' + B'$(A,B are reference template and A',B' are probe templates) and the polynomial constants c_1 and c_2 are represented as $c_1 = -(x_1 + x_2 + x_3 + ... + x_n)$ and $c_2 = (x_0 + x_1 + x_2 + x_3 + ... + x_{n-1})$, It takes two multiplications and one addition in encrypted form for HD calculation. The HD is calculated on the server side, which is sent to the client in encrypted form. The client decrypts it using a private key, and polynomial coefficients are retrieved. These coefficients are the difference in compressed code between the reference and probe templates. This group of coefficients now forms a large vector $m(x) \rightarrow [m(\alpha_0), m(\alpha_1), .., m(\alpha_{n-1})]$ of integers that are converted to binary, and the number of ones in the binary vector is recorded as R. As shown in Eq. (3.8) if the number of ones in R does not exceed a certain threshold(T), then the user is considered as genuine; otherwise, the user is considered as an imposter.

$$Verification = \begin{cases} Genuine, & if R < T \\ Imposter, & Otherwise \end{cases} \tag{3.8}$$

3.3 Experimental Results

This section provides a description of the datasets used to assess the proposed model, as well as the system's performance on those datasets. The qualitative and quantitative results

of the proposed model are then compared with the existing models in section 3.4.

3.3.1 Datasets

In the experiments, we used the publicly available multimodal biometric dataset known as CMBD to evaluate the proposed method. The CMBD comprises images of children and has been curated by students in kindergarten classes. Iris images were obtained using a Cross-Match iris scanner, capturing both left and right iris samples simultaneously. Fingerprint images were captured using a Cross Match L-Scan slap fingerprint scanner with a resolution of 500 ppi. Five samples were recorded for each user's left hand, right hand, and two thumbs, respectively. We selected 5 samples from 108 users for both iris and fingerprint modalities. These 5 samples were labeled from 0 to 4.

3.3.2 Evaluation

Table 3.1 demonstrates the significance of the proposed LRP-HE on both unimodal and multimodal systems. The unimodal systems include iris and fingerprint systems, while the multimodal systems consist of individual and fused template systems. Initially, the LRP-HE is implemented on an iris unimodal system, resulting in a decrease in the compressed template size from 2560 to 2240 and an EER% of 3.8545. Subsequently, when the LRP-HE is applied to a fingerprint unimodal system, the compressed template size decreases from 1024 to 896, with an EER% of 4.4686. Later, the LRP-HE is utilized on individual templates of the iris and fingerprint multimodal system, resulting in a template size of 3136 and a notable reduction in EER% to 2.6213%. Furthermore, when the proposed LRP-HE method is applied to a fused template multimodal system, the EER% is further reduced to 0.0214%, indicating an enhancement in the system's efficiency. This illustrates that the proposed LRP-HE method effectively reduces the size of templates without compromising the system's accuracy. Consequently, the application of the LRP-HE method to the fused template multimodal system demonstrates its accuracy and efficiency in addressing challenges related to high security and poor recognition.

In Table 3.1, EER values are presented, highlighting LRP-HE's effectiveness. LRP-

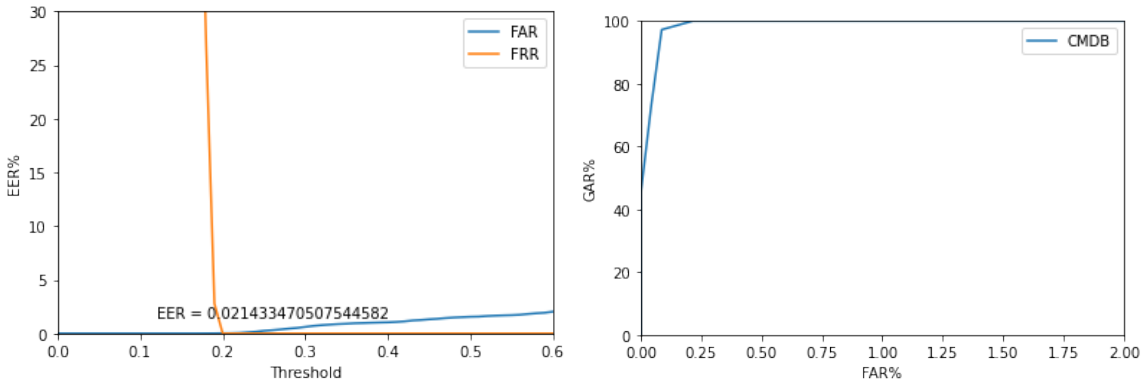
Table 3.1: Comparison of EER% for unimodal and multimodal with and without LRP

Template	**Size**	**EER**
LRP-HE on Iris	2240	3.854581
LRP-HE on Fingerprint	896	4.468671
LRP-HE on individual templates	2240+896=3136	2.621343
Proposed Method(LRP-HE on Fused Template)	2240+896=3136	0.021433

HE on fused templates achieves a low EER of 0.0214%, enhancing system accuracy. On the other hand, an EER of 2.6213% is obtained when LRP-HE is applied to individual templates.

To further analyze the performance of LRP-HE, EER curves are plotted using FAR (False Acceptance Rate) on the x-axis and FRR (False Rejection Rate) on the y-axis. Figure 3.6a and Figure 3.7a illustrate these curves for LRP-HE applied to the fused template and individual template, respectively. These curves depict how error rates change with different threshold values, providing an overview of the system's behavior and performance.

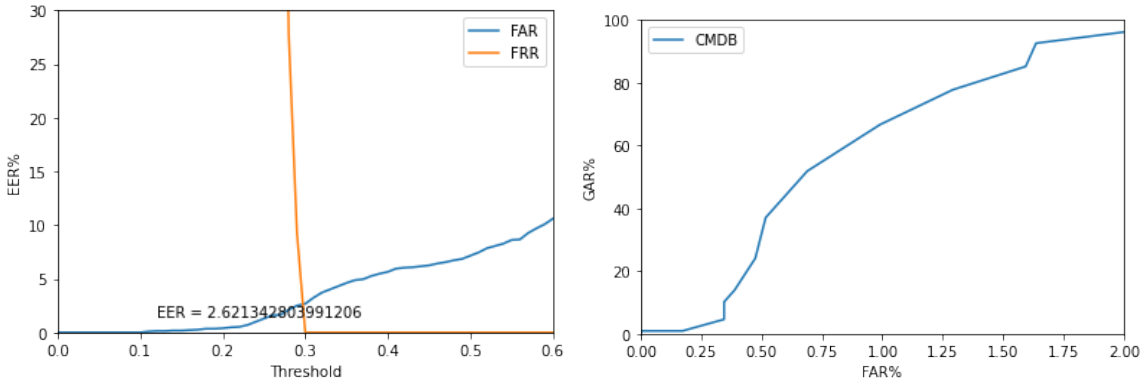
Moreover, ROC (Receiver Operating Characteristic) curves are plotted to evaluate the trade-off between FAR and GAR (Genuine Acceptance Rate). Figure 3.6b and Figure 3.7b display the ROC curves for LRP-HE on the fused template and individual template, respectively. These curves illustrate the system's ability to distinguish between genuine and impostor samples across varying thresholds, providing valuable information for system optimization and performance evaluation.



(a) (b)

Figure 3.6: a)EER Curve b)ROC Curve for LRP-HE on fused template

Additionally, Figure 3.8 presents a comparative analysis of the ROC curves for LRP-



(a) (b)

Figure 3.7: EER and ROC Curves for LRP-HE on individual templates

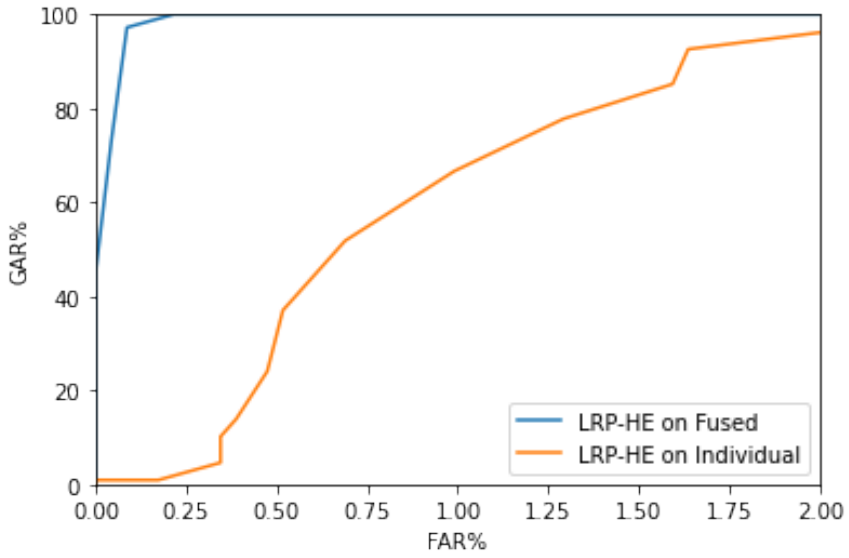


Figure 3.8: Comparison of ROC curve for LRP-HE on the fused template and LRP-HE on individual templates

HE applied to fused and individual templates. This comparison clearly demonstrates the superior performance of the LRP-HE on the fused template method, as indicated by its consistently higher GAR values across different FAR levels. This superiority demonstrates the effectiveness of combining multimodal information through template fusion, resulting in enhanced recognition accuracy.

3.4 Comparative Analysis

In Table 3.2, a comprehensive comparison of the EER% values obtained by our proposed technique and existing methods utilizing Homomorphic Encryption (HE) on different databases is presented. The comparison analysis gives information on the performance of different biometric recognition systems. Firstly, Gomez-Barrero et al. [142] conducted their study on the BiosecurID multimodal database, employing online signature and fingerprint traits. Their method achieved an EER% of 0.12, indicating the level of accuracy attained by their approach. Similarly, Mahesh et al. [143] evaluated their technique on the CASIA-V 1.0 database, utilizing left and right iris traits. Their method yielded an EER% of 0.19, demonstrating its performance in iris-based biometric authentication. In contrast, our proposed method was assessed on the Children Multimodal Biometric Database [154], which includes iris and fingerprint traits. However, our approach achieved a significantly lower EER% of 0.02143, outperforming previous methods on the mentioned features. This analysis highlights the superiority of our proposed method in terms of EER% performance when compared to existing techniques.

Table 3.2: Comparison of EER% of our proposed technique with existing techniques on different databases

Method	**Database**	**Traits used**	**EER%**
Gomez-Barrero et al. [142]	BiosecurID multimodal database	Online signature and Fingerprint	0.12
Mahesh et al. [143]	CASIA-V 1.0	Left iris and right iris	0.19
Proposed method	Children Multimodal Biometric Database [154]	Iris and Fingerprint	0.021433

Moreover, the significance of the proposed method has been shown in Table. 3.3 by comparing it with the existing methods on Children Multimodal Biometric Database [154], where the proposed method with an EER% of 0.02143 outperforms the existing methods such as Gomez-Barrero et al. [142] and Mahesh et al. [143] with an EER% of 0.128 and 0.2621 respectively. Here, the lower the EER value, the higher the performance of the system.

Table 3.3: Comparison of EER% of our method with existing methods on Children Multimodal Biometric Database

Method	**Database**	**EER%**
Gomez-Barrero et al. [142]	Children Multimodal Biometric Database [154]	0.128008193
Mahesh et al. [143]		0.26213428
Proposed method		0.021433

3.5 Security Analysis

3.5.1 Irreversibility Analysis

First, a fused feature vector is produced to calculate the distance between two templates, and then LRP and encryption are performed, returning $Enc(P)$. Similarly, the server receives the encrypted template using the query traits A' and B', yielding $Enc(Q)$. These encrypted templates are then sent to the server for distance calculations. Using Eq. 3.6, the server generates an encrypted result denoted as $HD(d)$. If the user is genuine, they possess the private key (δ_{sk}) necessary for decryption. By utilizing the private key, the user can decrypt the computed result and obtain the actual distance value between the biometric templates.

The encryption of the templates ensures that they remain secure and confidential during transmission and processing by the server. Moreover, the utilization of encryption techniques makes it computationally difficult for unauthorized users to decipher the templates without having the corresponding private key (δ_{sk}). This property of encryption meets the irreversibility requirement criterion, as it ensures that the biometric data remains protected and irreversible to unauthorized access or manipulation. Thus, the use of encryption techniques enhances the overall security and privacy of the biometric authentication system.

3.5.2 Unlinkability

In our approach, unlinkability is maintained by calculating the distance metric, as shown in Eq. 3.6. This calculation compares the similarities between encrypted reference and probing templates. Importantly, our encryption scheme uses randomness during the generation of the public key (δ_{pk}). Specifically, a random value s' is selected from a predefined

set R_2. This randomization ensures that templates from the same user can produce various ciphertexts, irrespective of whether the same or different encryption keys are used.

Furthermore, the use of Fully Homomorphic Encryption (FHE) in our scheme provides additional security against potential attacks, including chosen-plaintext attacks [155]. FHE ensures that no meaningful information can be extracted from the encrypted template, thereby preventing any attempt to link the encrypted data back to the original template. As a result, comparing or analyzing protected templates within an unprotected domain is no longer possible.

Overall, the combination of randomness in encryption and the security guarantees offered by FHE ensures that the unlinkability of the biometric data is maintained throughout the authentication process. This protection against unauthorized correlation of biometric information improves the overall security and privacy of the authentication system.

3.5.3 Revocability

Revocability ensures that if a template is compromised, then it should be canceled, and a new template is generated based on the same biometric data. Our approach uses Local Random Projection (LRP), which divides the feature vector (f_v) into an equal number of slots (m). During the random projection, a slot is selected randomly, introducing variability and enhancing the security of the generated templates. In the case of a template compromise, our system provides a solution by modifying the slot index (i) used for random projection and creating a new feature vector (f_{lrp}) using Eq. 3.5. This technique effectively invalidates the compromised template, resulting in a new template for the biometric data.

Furthermore, since our templates are encrypted, recovering relevant information from hacked ones is impossible due to their irreversible nature. Even if an attacker obtains some information from the compromised template, our encryption approach assures that the data is secure. In such a case, the compromised template can be re-encrypted using a different encryption key, enhancing its security and preventing unauthorized use.

Overall, the combination of Local Random Projection and encryption techniques provides strong revocability capabilities, allowing for the immediate cancellation and regen-

eration of compromised templates while ensuring the biometric authentication system's security. This guarantees that hacked templates do not pose a threat to the overall security of the system and can be quickly changed with new templates to protect user privacy.

3.5.4 Hill Climbing (or) Inverse Biometric Attack

One potential threat to biometric authentication systems is the hill-climbing attack, which includes iteratively improving an attacker's assumption of the original biometric template based on feedback acquired from comparing various reference templates. However, our proposed method effectively reduces the risk of a hill-climbing attack.

In our biometric authentication system, the similarity between two encrypted templates, represented by the Hamming Distance ($HD(d)$), is computed and encrypted. Only the client possesses the secret key (δ_{sk}) required for decryption, ensuring that the decrypted similarity score remains confidential and accessible only to authorized users.

The inherent security features of our encryption scheme prevent attackers from accessing meaningful feedback information required for constructing an original template. Since the similarity score between encrypted templates is calculated and maintained in encrypted form, attackers lack the necessary feedback information to iteratively refine their guesses and construct an original template.

Overall, the combination of encryption techniques and the lack of feedback information in encrypted similarity scores effectively reduces the risk of hill-climbing attacks in our proposed biometric authentication system.

3.5.5 Lost-key scenario

In our biometric authentication system, all templates in the database are encrypted using the same encryption key, which presents a potential vulnerability. If this key is lost or stolen, it could lead to unauthorized access to the user's data, compromising their privacy and security. However, our proposed technique addresses this issue by applying Local Random Projection (LRP) to the fused template (f_v).

LRP introduces an additional layer of security by incorporating randomness into the

projection process. Even if an attacker steals the encryption key (δ_{pk}), they can only access the local randomly projected feature vector (f_{lrp}), not the original template (f_v). This is because LRP modifies the projection matrix (R_{lrp}) based on local slots (i) of the feature vector, ensuring that the resulting templates are unique.

Overall, the implementation of LRP improves the security of our biometric authentication system by reducing the risks of stolen key attacks and unauthorized access to sensitive user information.

3.6 Summary

In this chapter, multimodal template protection was designed using local random projection and Homomorphic encryption. To address the challenge of rotational inconsistency in biometric data, rotational invariant templates are developed, ensuring consistent and accurate recognition across varying orientations. The fusion of iris and fingerprint templates is achieved to enhance recognition accuracy and robustness. Local Random Projection (LRP) is then used to create a pseudo template that takes advantage of randomization to improve security. These templates are then secured with Fully Homomorphic Encryption (FHE), which ensures that sensitive biometric information is protected during transmission and processing. To reduce computational costs related to FHE operations, a batching approach is used, which allows several multiplications to be executed in encrypted form with a single operation. This optimization method significantly reduces computing overhead while ensuring the confidentiality and privacy of biometric information. The primary objective of using homomorphic encryption is to allow operations on user data to be performed in an encrypted domain, resulting in a similarity score that is encrypted throughout the process. Overall, the proposed methodology offers a comprehensive solution for safeguarding multimodal biometric templates, addressing challenges related to security, privacy, and computational efficiency. By combining LRP with HE, the system protects sensitive biometric data while providing accurate and secure user authentication.

Chapter 4

An alignment-free cancelable template protection technique

This chapter introduces a cancelable template protection mechanism to address the issue of trait alignment during acquisition. This method involves generating a 2-D shell from a fingerprint, which is then combined with iris features to create a 3-D shell.

Chapter Organization: Section 4.1 explains the proposed methodology, while Section 4.2 provides the experimental results. Section 4.3 presents the comparative analysis, and Section 4.4 discusses security analysis of the proposed methodology. Finally, Section 4.5 provides a summary of the work.

4.1 Methodology

During the enrolling process, iris and fingerprint codes are first produced. After code generation, the fingerprint codes are used to construct a 2-D shell, which is then combined with iris codes to generate a 3-D shell. These shells, along with the user ID, are saved in the database as reference shells and used during the verification process. Figure 4.1 shows a flow diagram of the enrollment process. During the verification process, the user provides both traits and codes are generated for each trait. The generated codes are then converted into 3-D shells known as probe shells. The reference template is obtained from the server using the user ID, and the reference and probe shells are compared using Hamming Dis-

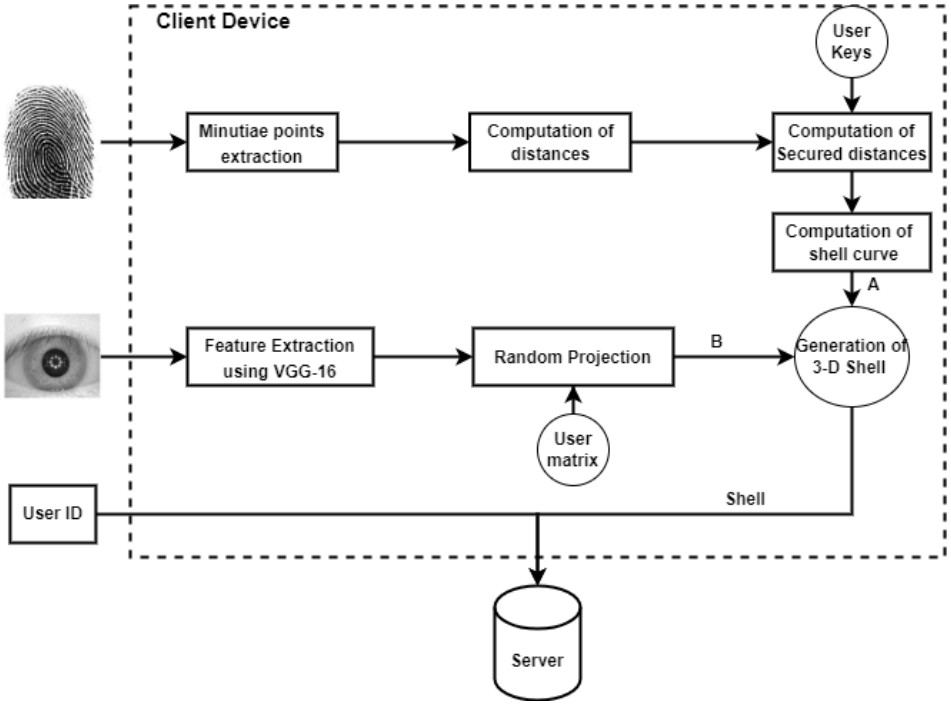


Figure 4.1: Enrollment process of the proposed method

tance (HD). The HD uses a specified threshold to verify whether the user is genuine or an imposter. Figure 4.2 depicts the verification process flow diagram. Our proposed method-

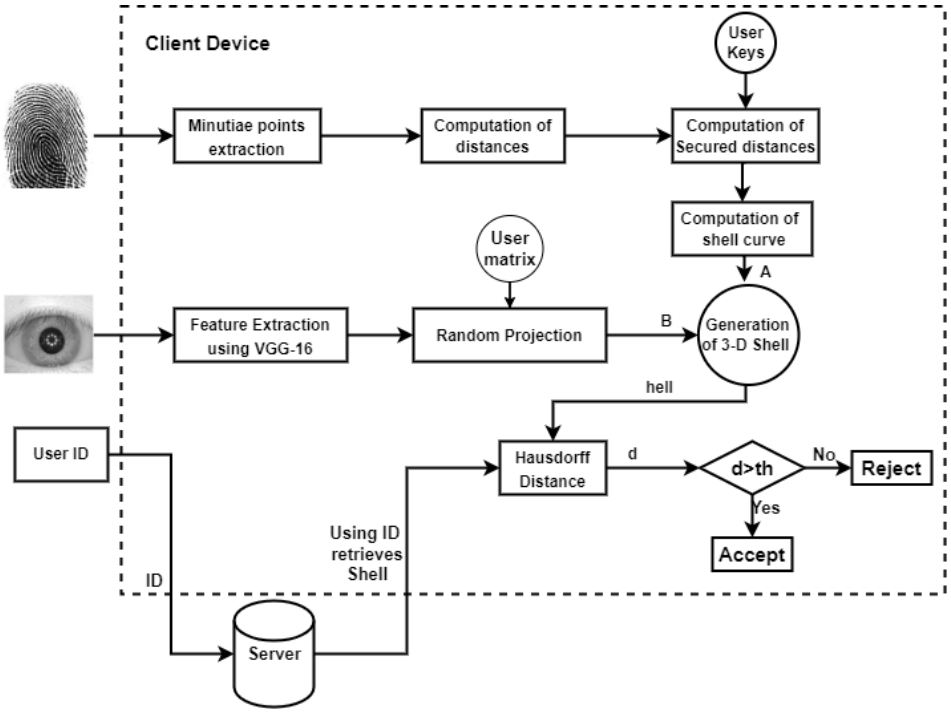


Figure 4.2: Verification process of the proposed method

ology uses a two-entity model with a client and a server. It is divided into four modules, as shown below:

- Generation of fingerprint shell
- Extraction of Iris features
- Generation of 3-D shell
- Matching

4.1.1 Generation of fingerprint shell

First, the provided fingerprint image undergoes preprocessing to enhance its quality. Subsequently, the image is analyzed to identify the locations of valleys and ridges, which are characteristic features of fingerprint patterns. These ridges are further examined to pinpoint specific points known as minutiae. These minutiae points serve as key reference points for fingerprint recognition. Figure 4.3 shows how minutiae points are derived from a fingerprint image.

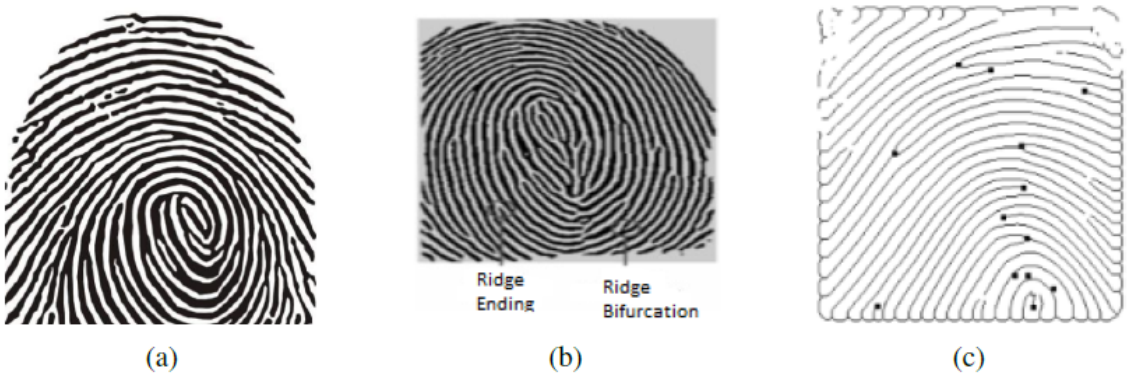


Figure 4.3: Fingerprint images a) Fingerprint b)Ridge Ending and Bifurcation c)Minutiae point

Measuring Distances

After extracting fingerprint features, each minutia point is represented as a triplet (x, y, θ), where (x, y) specifies the minutia point's coordinates and θ represents the orientation angle

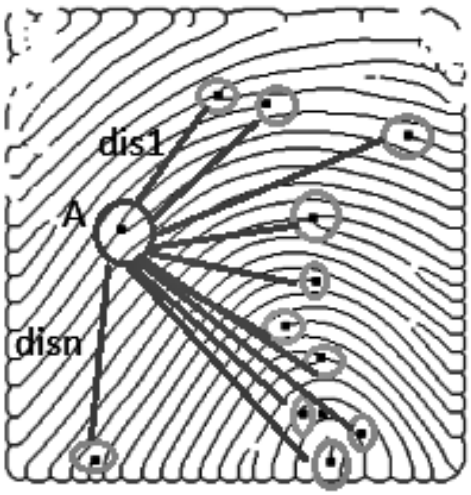


Figure 4.4: Calculating distances from point A to all other minutiae points

of the ridge at that location. Then, using each minutia point as a reference, we calculate the distances to all other minutiae points in the fingerprint. This procedure entails determining the Euclidean distance between each pair of points as shown in Figure 4.4.

The Euclidean distance between two minutiae points one as a reference having coordinates (x_0, y_0) and some minutiae point (x_i, y_i) is calculated as shown in Eq. 4.1.

$$dis_i = \sqrt{(x_i - x_0)^2 + (y_i - y_0)^2} \tag{4.1}$$

Securing Distances

Protecting the original features is essential for protecting user privacy. To address this concern, instead of directly storing the distances $dis_1, dis_2, ..., dis_n$ between minutia points, we adopt a security-enhanced approach by employing secured distances $sdis_1, sdis_2, ..., sdis_n$. These secured distances are computed by including user-specific keys, denoted as $p_0 \in \{1, 100\}$ and $q_0 \in \{1, 100\}$, as shown in Eq. 4.2. This approach ensures that even if the original features are compromised, the sensitive information remains protected, preserving privacy.

$$sdis_i = \sqrt{dis_i^2 + q_0^2 + 2(dis_i \times q_0 \times cos(\theta_i - p_0))} \tag{4.2}$$

Spiral Curve Generation

All these calculated distances, which are computed among the minutiae points, are arranged in ascending order. A user key r_0 is added to all of these distances. Now the distance set becomes $r + sdis_0, r + sdis_1, ..., r + sdis_n$. A spiral curve is generated using this distance set, where the secured distance forms right contiguous triangles. The procedure for constructing the shell is shown in Figure 4.5. The spiral curve generated using Algorithm 4.2 is shown in Figure 4.6.

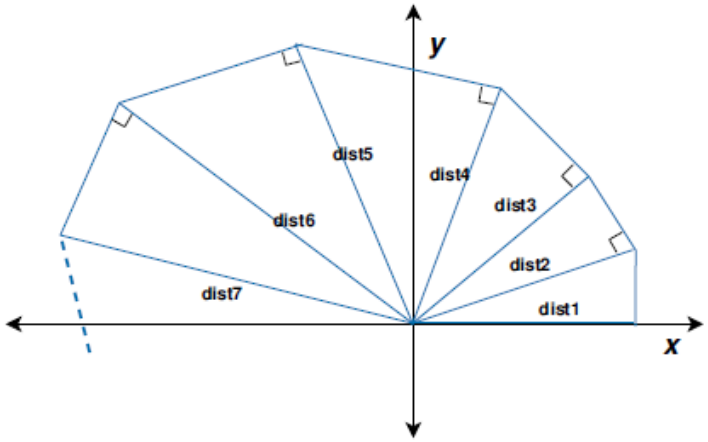


Figure 4.5: Sample curve construction

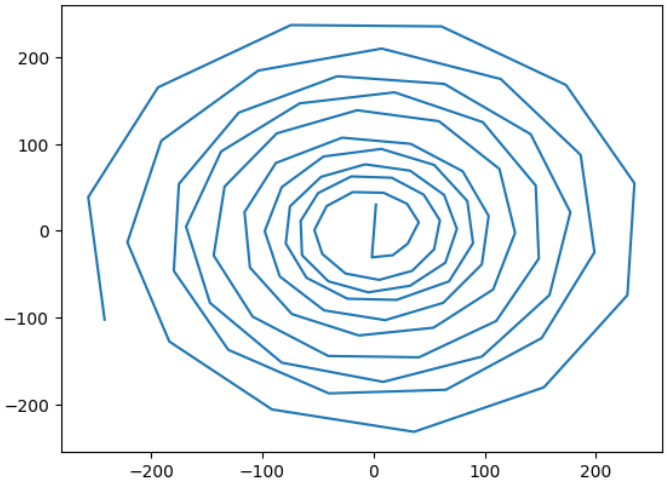


Figure 4.6: 2-Dimensional spiral curve

Algorithm 4.2 Fingerprint Shell Algorithm

Input: Minutiae points, key-set(p_0,q_0,r_0)
Output: 2D Spiral curve

for i = 1 to **n do** ▷ Computing the distances
  for j = 1 to **n do**
    $dis_{ij} = \sqrt{(x_i - x_j)^2 + (y_i - y_j)^2}$
▷ Securing the distances
for i = 1 to **n do**
  for j = 1 to **n do**
    $sdis_{ij} = \sqrt{dis_{ij}^2 + q_0^2 + 2(dis_{ij} \times q_0 \times cos(\theta_j - p_0))}$
sort the secured distances
for i = 1 to **n do** ▷ Hypotenuses of right angle triangles
  for j = 1 to **n do**
    $sdis_{ij} = sdis_{ij} + r_0$
    if i==1 **then**
      $\hat{x}_{ij} = r_0$
      $\hat{y}_{ij} = \sqrt{sdis_{ij}^2 - r_0^2}$
      $\phi_{ij} = \tan^{-1}(\hat{y}_{ij}/\hat{x}_{ij})$
    else
      $\phi_{ij} = \phi_{ij-1} + \cos(sdis_{ij-1}/sdis_{ij})$
      $\hat{x}_{ij} = sdis_{ij} \times \cos(\phi_{ij})$
      $\hat{y}_{ij} = sdis_{ij} \times \sin(\phi_{ij})$
$Curve_i = (x_i, y_i)|i = 1\ to\ n$

Quantization

Quantization is a multi-step procedure that converts the information in each shell into binary vectors of equal size. Initially, we determine the highest and lowest values of each row and column using $\hat{x}_{ij}$ and $\hat{y}_{ij}$. Next, we compute the normalized values of $\hat{x}_{ij}$ and $\hat{y}_{ij}$. Finally, we use a tuning parameter (T_p) to determine the dimensions of the quantized array. Algorithm 4.3 explains various steps involved in the quantization process.

4.1.2 Extraction of Iris features

For the feature extraction of iris images, a pre-trained VGG-16 model is used, which has been trained on a vast dataset comprising of 2.6 million images belonging to 2.6 thousand individuals. As the VGG-16 model requires a 224×224 image as input, all input images

Algorithm 4.3 Quantization

Input : Fingerprint 2D matrix of size m×n(finarr), Tuning parameter(T_p)
Output : Quantized array(quantarr)

for i=0 to m **do**
    for i=0 to n **do**
        Find the minimum and maximum value of each row and column
row$_{max}$=max($\hat{x}_{ij}$) - min($\hat{x}_{ij}$)
col$_{max}$=max($\hat{y}_{ij}$) - min($\hat{y}_{ij}$)
Set some tuning parameter T_p
Initialise quantarr of size (r=row$_{max}$/T_p)X (c=col$_{max}$/T_p)
for i=0 to r **do**
    for j=0 to c **do**
        quantarr[(finarr[i][j][0]/T_p)][(finarr[i][j][1]/T_p)]=1

are preprocessed to obtain the appropriate dimensions. The pre-trained VGG-16 model is then modified to guarantee that it produces a feature vector with a size of 2048. The proposed model uses 13 convolutional kernels with a size of 3×3 and a stride of 1, as well as 2×2 pooling layers with a stride of 2. The convolutional layers produce a vector of size 25,088 (7×7×512). In addition, these convolution layers are connected to three fully connected layers, each consisting of 4096, 4096, and 2048 neurons, respectively, thereby resulting in a vector (f_{ir}) of size 2048. Finally, random projection is performed on the vectors (f_{ir}) produced by the VGG-16 model, as shown in Eq. 4.3. This random projection is done using a matrix (R_p) which is an average of user matrix and feature matrix of size 2048×1000, thereby resulting in the iris feature vector (f'_{ir}) with dimensions of 1×1000. The architecture used for iris feature extraction via the pre-trained VGG-16 model is illustrated in Figure 4.7.

$$\boldsymbol{f'_{ir}} = \boldsymbol{f_{ir}} * \boldsymbol{R_p} \tag{4.3}$$

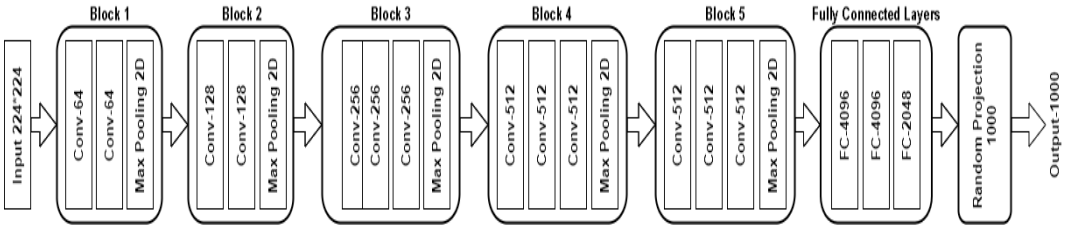


Figure 4.7: Block diagram of VGG-16 architecture for feature extraction

4.1.3 Generation of 3-D shell

Once the 2-D shell of the fingerprint and the feature vector of the iris are generated, feature-level fusion is performed to construct a 3-D shell. Firstly, the iris feature vector (f'_{ir}) of length l is divided into m slots, each containing b_s elements, where $m \times b_s = l$. The iris vector is then represented as $f'_{ir} = f_1||...||f_i||...||f_m$, with each slot f_i containing b_s elements. Each slot f_i is then converted into a decimal number, resulting in a decimal vector z_i with length b_s. After that, the user key t_0 is produced from the keys p_0, q_0, r_0, and s_0, yielding a 32-bit integer. To generate t_0 the first eight bits are retrieved from p_0, the next eight bits from q_0, the next eight bits from r_0, and the last eight bits from s_0. Finally, the 3-D shell is created by combining the 2-D curve information of the fingerprint, the user keys, and the iris decimal vector (z_i). Figure 4.8 shows the 3-D shell produced by this method, as described in Algorithm 4.4.

Algorithm 4.4 3-D Shell Algorithm

Input :*iris feature vector* f'_{ir} *of length l , key-set*(p_0,q_0,r_0,s_0)*, block size*(b_s)

Output : *3-D Spiral curve*

1: m = l/b_s

2: $f'_{ir} = f_1||...||f_i||...||f_m$ where f_i = $[f_{i\_1}, f_{i\_2}, ..., f_{i\_b_s}]$

3: **for** i = **1** to **j do**

4: $z_i = decimal(f_i)$

5: t = $\lfloor p_0 \rfloor$ + 256*$\lfloor q_0 \rfloor$ + 65536*$\lfloor r_0 \rfloor$ + 16777216*$\lfloor s_0 \rfloor$

6: **for** i = **1** to **n do**

7: $\begin{pmatrix} x_i & y_i & z_i \end{pmatrix} = \begin{pmatrix} x_i & y_i & z_i \end{pmatrix} \times \begin{pmatrix} cos(q_0) & sin(q_0) & 0 \\ -sin(q_0) & cos(q_0) & 0 \\ 0 & 0 & 1 \end{pmatrix} \times \begin{pmatrix} cos(r_0) & 0 & -sin(r_0) \\ 0 & 1 & 0 \\ sin(r_0) & 0 & cos(r_0) \end{pmatrix}$

8: $\begin{pmatrix} x_i & y_i & z_i \end{pmatrix} = \begin{pmatrix} x_i & y_i & z_i \end{pmatrix} + \begin{pmatrix} t_0 \times sin(r_0) \times sin(q_0) & t_0 \times cos(r_0) & t_0 \times sin(r_0) \times cos(q_0) \end{pmatrix}$

9: Curve = $\left\{ \begin{pmatrix} x_i & y_i & z_i \end{pmatrix} | i = 1 \; to \; n \right\}$

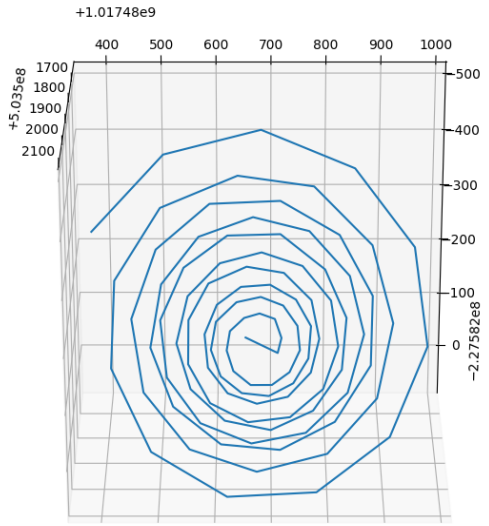


Figure 4.8: 3-D spiral curve for secured template

4.1.4 Matching

During the authentication process, a 3-D curve is generated for the probe images. The reference curve is then retrieved from the database by using the user ID of the individual for matching purposes. Hausdorff Distance (HUD) is used as the metric to calculate the degree of similarity between these curves because it is the best matching technique for comparing shapes. The HUD of two sets, denoted as P and Q, is calculated according to Eq. 4.4. This calculated score is then evaluated against a predefined threshold value to determine whether the user is genuine or an imposter.

$$HUD(P,Q) = max[h_d(P,Q), h_d(P,Q)] \tag{4.4}$$

$$h_d(P,Q) = max(min(D_m(p,q))), p \subset P \& q \subset Q$$

where D_m(P, Q) denotes the distance measures like Euclidean, Manhattan, etc.

4.2 Experimental Results

4.2.1 Datasets

The proposed work is evaluated using three publicly available databases. The performance is calculated using the Children Multimodal Biometric Database [154], which is represented as DB-3 in our work. Other databases like Casia-V1 [156] & FVC2004 [157] and Casia-V3 [158] & FVC2006 [159] were also used to evaluate the proposed method, which are represented as DB-1 and DB-2, respectively. These databases serve as comprehensive benchmarks for evaluating the effectiveness of the proposed method, as shown in Table 4.1.

Table 4.1: Databases used for experimentation

Database	Iris	Fingerprint
DB1	CASIA V1	FVC 2004
DB2	CASIA V3	FVC 2006
DB3	Children Multimodal Biometric Database	

4.2.2 Evaluation

The proposed method uses key set p_0,q_0,r_0 and the tuning parameter T_p for generating a fingerprint shell, and user matrix M, slot(i) and block size(b_s) for generating an iris feature vector. Table 4.2 provides a comparison of the EER%, d', and ks-test values for three different databases: DB1, DB2, and DB3.

For DB1, the EER% is 0.032, indicating a relatively low error rate. The d' and KS test values are 3.0037 and 0.93 which indicates a strong ability to discriminate between genuine and imposter distributions. In the case of DB2, although the EER% is slightly higher at 0.09 compared to DB1, it still demonstrates a relatively low error rate. The d' and ks-test values remains high at 2.9610 and 0.89, indicating good separability between genuine and imposter scores. Among the three databases, DB3 has the lowest EER% of 0.015, indicating the lowest error rate. The highest d' and ks-test values across the three datasets were at 3.1046 and 0.94, respectively, indicating excellent separability between

real and imposter scores.

Overall, the analysis reveals that lower EER% values are associated with higher d' values and ks-test values, indicating better differentiation between genuine and imposter scores. This suggests that the lower the EER%, the more effectively the system distinguishes between genuine and imposter attempts, highlighting the discriminative power of the biometric authentication system.

Table 4.2: Comaprison of EER%, d' and ks-test of DB1,DB2,DB3

Database	**EER%**	d'	**ks-test**
DB1	0.032	2.9610	0.93
DB2	0.09	3.0037	0.89
DB3	0.015	3.1046	0.94

The EER (Equal Error Rate) curves, depicted in Figure 4.9, illustrate the relationship between the False Acceptance Rate (FAR) and False Rejection Rate (FRR) across different datasets, namely DB-1, DB-2, and DB-3. DB-1 exhibits a low error rate of 0.032, indicating high accuracy in distinguishing genuine and imposter attempts. DB-2 shows a slightly higher error rate at 0.09, whereas DB-3 has the lowest error rate of 0.015, indicating superior performance in authentication. These error rates provide information about system accuracy, which can be used to optimize biometric authentication for increased security.

The ROC curve shows how well a system performs in terms of true and false positives. Figure 4.10 shows an analysis of ROC curves plotted using FAR and GAR on three datasets such as DB-1, DB-2, and DB-3. Here, DB-1, DB-2, and DB-3 have a wider area under the curve, indicating the effectiveness of the proposed approach.

The distribution of test scores for various datasets DB-1, DB-2, and DB-3 are shown in Figure 4.11, demonstrating that impostor and genuine scores are well distinguished.

To determine the separability of genuine and impostor scores, d' and ks-test values are computed. Figure 4.12 depicts EER, d', and ks-test values for CASIA-V1 & FVC-2004, CASIA-V3 & FVC-2006 and CMBD databases. It can be seen that the d' is inversely related to EER. Here, the genuine and impostor scores are clearly distinguished by the higher d' value. Similarly, the genuine and impostor scores are clearly distinguished if the ks-test value(ranges between 0 and 1) is closer to 1.

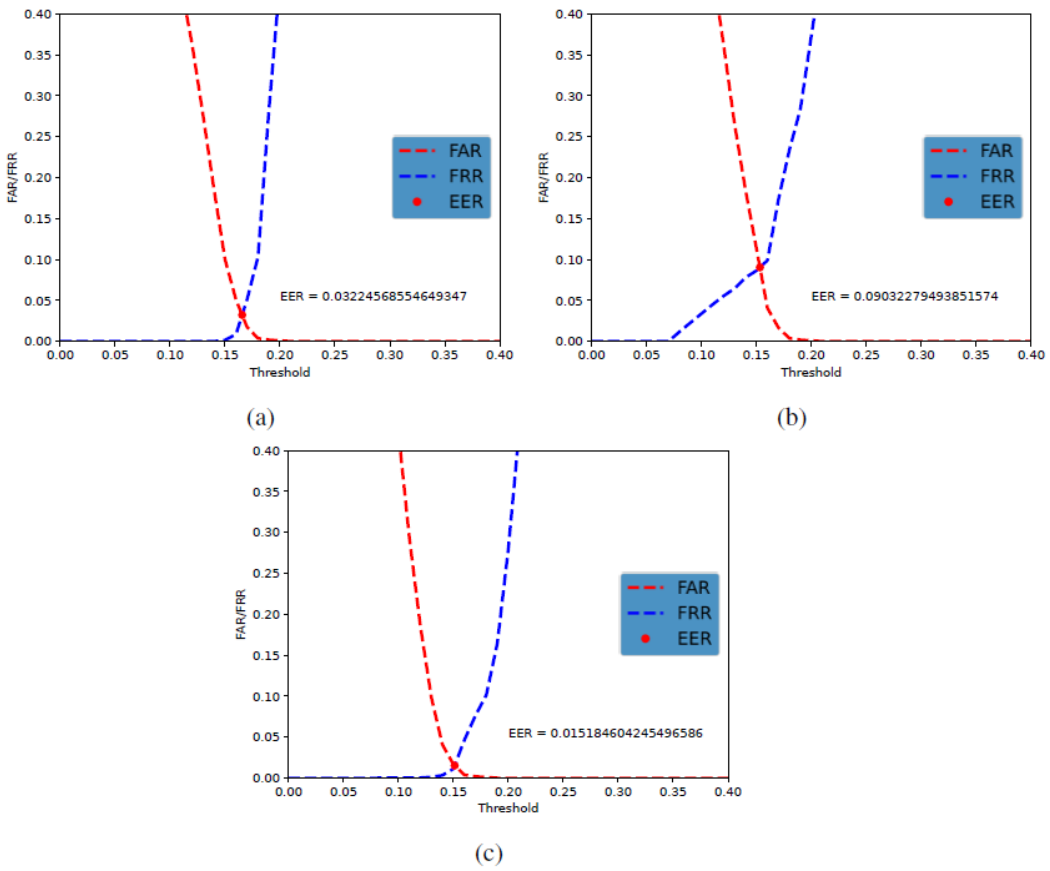


Figure 4.9: EER curves for a)DB1 b)DB2 c)DB3

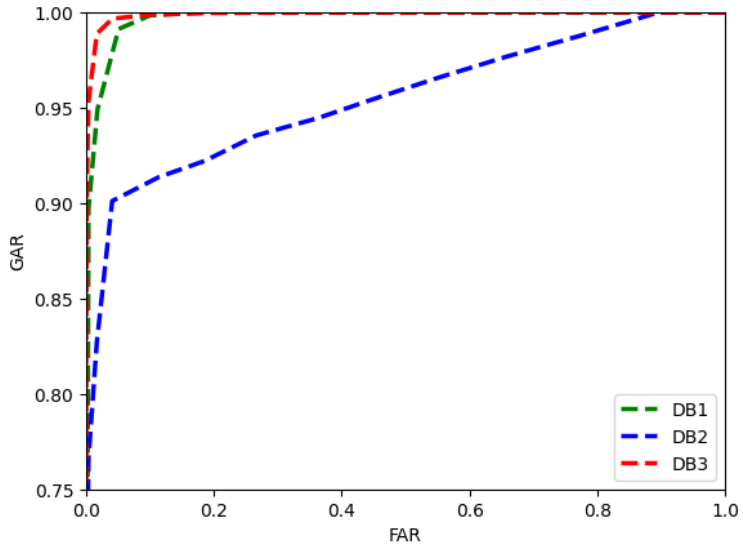


Figure 4.10: ROC curves for DB1, DB2, DB3

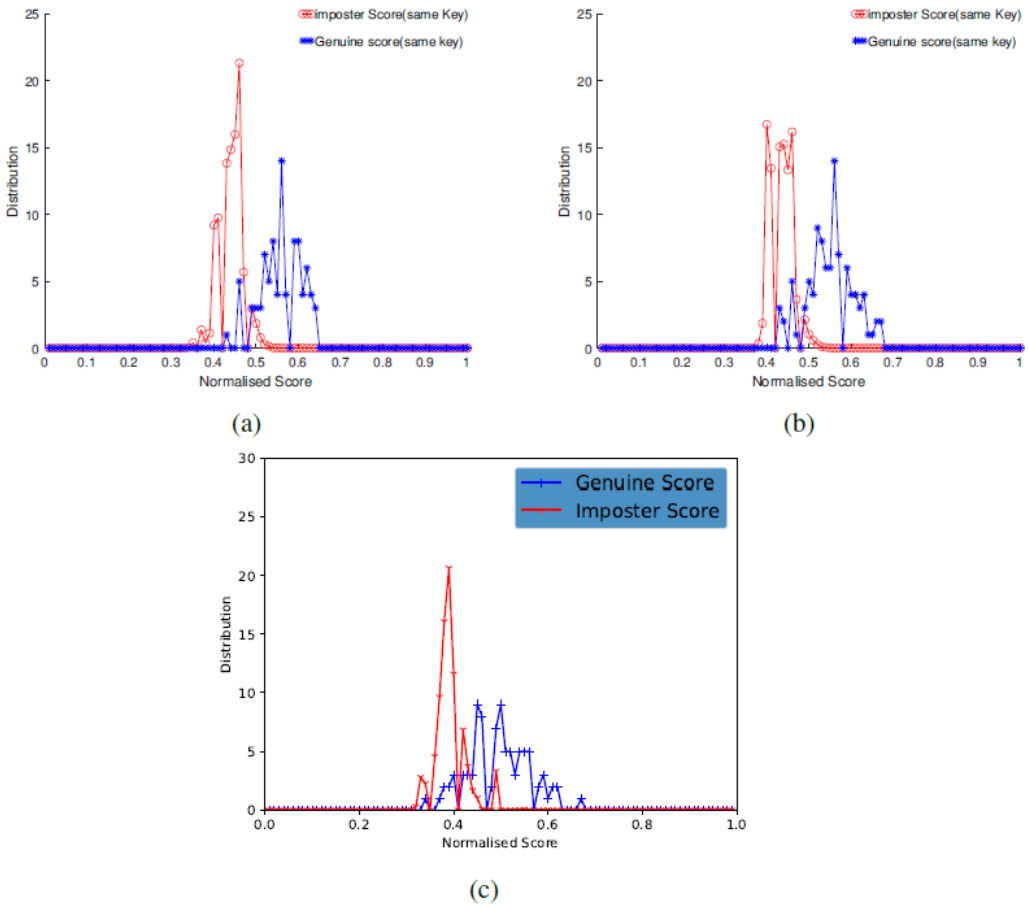


Figure 4.11: Genuine/Imposter Distributions for a)DB1 b)DB2 c)DB3

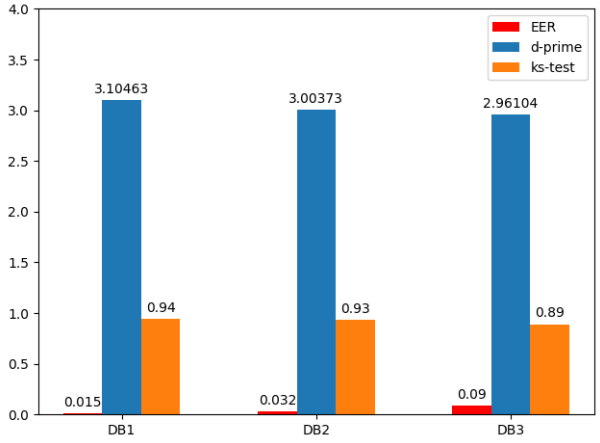


Figure 4.12: EER,d' & ks-test measures for DB1, DB2, DB3

4.3 Comparative Analysis

The comparison between the proposed method and existing techniques across various datasets, including CASIA-V1 & FVC-2004(DB1), CASIA-V3 & FVC-2006(DB2), and Children Multimodal Biometric Database(DB3), is presented in Table 4.3. For DB1 dataset, the proposed method exhibits a low Equal Error Rate (EER) of 0.032%, demonstrating its superior performance compared to existing methods. Benaliouche et al. [160] and Mustafa et al. [161] obtained EER values of 0.038% and 1.9%, respectively, highlighting the effectiveness of the proposed approach. Similarly, on the DB2 dataset, the proposed method maintains its superiority with an EER of 0.09%, outperforming existing methods such as Walia et al. [102] and Rajasekar et al. [162], which report EERs of 2.35% and 0.18%, respectively.

Moreover, when evaluated on the Children Multimodal Biometric Database, the proposed method continues to demonstrate its effectiveness, achieving an impressive EER of 0.015%. In contrast, existing methods like Gomez-Barrero et al. [163], Mahesh et al. [163], Vallabhadas et al. [163], and Mahesh et al. [164] yield EERs of 0.128%, 0.262%, 0.021% and 0.160% respectively, further highlighting the superior performance of the proposed approach across various datasets. These results indicates the consistency and efficacy of the proposed method in achieving low error rates and affirm its potential for real-world biometric authentication applications.

Table 4.3: EER% of the proposed method vs existing methods on various datasets

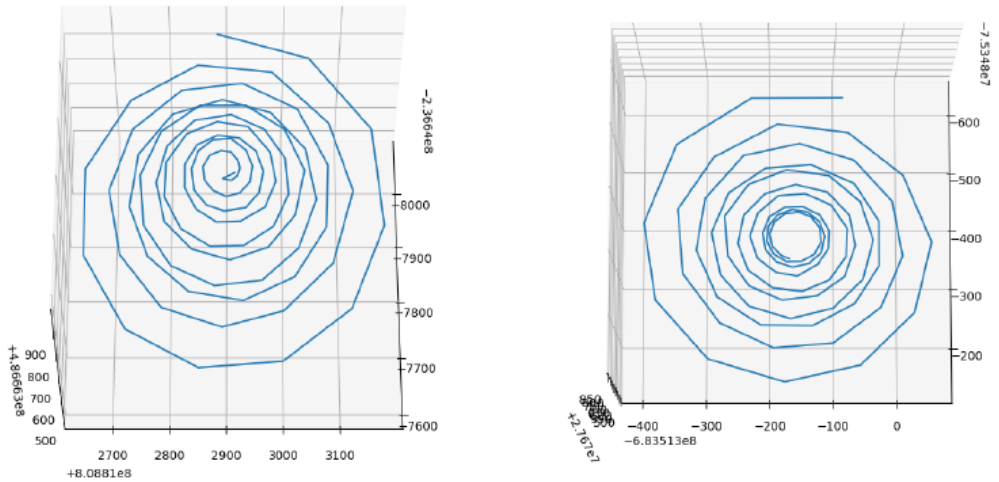
Method	**Database**	**EER%**
Benaliouche et al. [160]	CASIA-V1 & FVC2004	0.038
Mustafa et al. [161]		1.9
Proposed method		0.032
Walia et al. [102]	CASIA-V3 & FVC2006	2.35
Rajasekar et al. [162]		0.18
Proposed method		0.09
Gomez-Barrero et al. [163]	Children Multimodal Biometric Database	0.128
Mahesh et al. [163]		0.262
Vallabhadas et al. [163]		0.021
Mahesh et al. [164]		0.160
Proposed method		0.015

4.4 Security Analysis

Once the templates are created from the features, the BTP approach should preserve the templates' privacy and security. To assure them, the templates produced should be revocable, irreversible, and unlikable.

4.4.1 Revocability

If any biometric authentication system is hacked, we must be able to construct another template from the same recorded information such that there is no link between those two templates. The proposed technique achieves this by allowing the creation of distinct user templates using the user key-set p_0,q_0,r_0,s_0 for fingerprint data, and slot (i), block size(b_s) for iris data. This approach ensures that even if a template is compromised, a new one can be generated without any link to the compromised template. The effectiveness of this revocability feature is clearly illustrated in Figure 4.13, where two distinct curves are generated from the same biometric data using different key-sets p_0,q_0,r_0,s_0. Despite using the same biometric information, these curves are entirely different from each other, highlighting the system's ability to revoke compromised templates and generate new, unlinkable ones.



(a) (b)

Figure 4.13: Comparison of 2 Shells generated from same data

4.4.2 Diversity

In biometric template protection, diversity is a crucial aspect that ensures the resilience and security of the system. It ensures the ability to generate multiple templates for a single individual such that each template is unique and not linked to any other template, particularly if a template is compromised in one application. In our proposed approach, diversity is achieved through the generation of multiple templates using different sets of parameters. By altering the key set and slot(i), which represents specific parameters or identifiers within the biometric data, we create distinct templates for the same user. This means that a person can have several templates derived from the same biometric source, each with its own set of parameters, ensuring diversity and preventing the linkage between compromised and newly generated templates. The ability to adjust parameters enables the utilization of these diverse templates across various applications, further enhancing the versatility and applicability of the biometric system. Figure 4.13 shows how our approach creates numerous templates with different parameters, ensuring diversity and robustness against template compromise.

Cross Matching Attack:

If an attacker obtains the templates generated in one application, the same information can be used to bypass the system in other applications. Cross-matching attacks are not allowed using our method since we vary the parameters key-set and the slot(i) for different applications, resulting in distinct templates for the same person. For example, if we use a key set in the interval [1,100] in one application, we use a key set in the interval [100,200] in the second application. This results in unique curves in each application that cannot be cross-matched.

4.4.3 Irreversibility

Any biometric authentication technique, when transforming the original biometric template using some transformation technique, it must be ensured that the original template cannot be derived from the changed template. As the features are permanently associated with the

identity of a person, which compromises the privacy of the user. In our proposed method to generate a fingerprint shell, we use a key set that changes the orientation of the minutiae point, and neither minutiae point coordinates nor the orientation is saved. Additionally, the random projection used in the process reduces the size of the template by discarding certain bits, thereby hiding the original template. These measures ensure that no direct information about the user's biometric features is retained, preserving the user's privacy. So this will never leak any information of the user, and the generated 3-D shell is irreversible.

Brute-force Attack:

As the generated template is irreversible, the attacker can obtain the initial feature vector through an extensive guessing approach known as brute force. Consider the worst-case situation in which the adversary has access to the 3-D shell and knows how to reconstruct the feature vector. For instance, in the case of a fingerprint with n minutiae points, each minutia point has approximately 360 possibilities for placing a point around it. Consequently, the total number of combinations required to cover all possible cases in the fingerprint is 360^n. Similarly, for an iris with a length of m, each bit in the iris vector provides two possible states. Hence, the total number of combinations needed to cover all possibilities in the iris is 2^m. When considering both the fingerprint and iris together, the total number of guesses required to determine the original feature vector is $360^n * 2^m$. This exponential growth in the number of combinations made the task of brute forcing the initial feature vector extremely difficult and computationally costly, making it almost impossible to complete.

4.4.4 Record Multiplicity Attack:

In this type of attack, the attacker has access to multiple instances of a user's templates and attempts to link all of these transformed templates to find the solution for generating the original template. The random matrix in our proposed technique is computed using the user matrix and the feature vector slot. The user matrix is erased after each random projection; therefore, it is inaccessible. Moreover, projection matrix's construction primarily relies on the feature slot(i). As a result, it is impossible for the attacker to find the projection

matrix without the original feature vector, which makes our system free from ARM. By implementing these security features, our approach effectively mitigates the risk of ARM attacks while also protecting the privacy and integrity of the user's biometric information against unauthorized access.

4.5 Summary

In this chapter, an alignment-free multimodal cancelable scheme is developed that combines fingerprint features with iris features at feature-level fusion. First, the fingerprint minutiae points are safeguarded, and a secure shell is constructed in the form of a 2D curve that does not require a singularity point, resulting in improved accuracy. Then quantization on the fingerprint shell is performed which makes the modality more secure. Later, iris features are extracted using a pre-trained CNN model on which feature-based random projection is performed to make it irreversible. Finally, the fingerprint quantized array and iris feature vector are combined to generate a 3-D shell that is secured. Our experimental results showcase the efficiency and effectiveness of our proposed method when compared to existing techniques across three diverse datasets. This demonstrates the potential of our approach to significantly enhance the performance and security of biometric authentication systems.

Chapter 5

A cancelable technique that uses deep CNN for enhanced security and performance

In this chapter, a multimodal cancelable technique was presented which uses deep CNN for feature extraction and feature-hashed random projection for enhancing security and performance.

Chapter Organization: Section 5.1 provides the basics of methods used in the proposed methodology. Section 5.2 explains the proposed methodology, while Section 5.3 provides the experimental results. Section 5.4 presents the comparative analysis, and Section 5.5 discusses security analysis of the proposed methodology. Finally, Section 5.6 provides a summary of the work.

5.1 Background

5.1.1 Transfer Learning

Transfer learning is a machine learning technique in which a pre-trained model that was originally constructed for one task is reused and applied for a different similar task [165]. Instead of starting model training from scratch, transfer learning takes the knowledge ob-

tained from solving a previous problem and applies it to a new problem. This strategy is particularly useful when the new task has limited data available, because the pre-trained model uses the learned patterns and features from the previous work, improving the model's capacity to generalize and perform well on the new task. Transfer learning can be implemented using fine-tuning, which involves changing the pre-trained model's parameters to fit the new data in which previous layers of the model are frozen and only the last layers are trained on the new dataset. Transfer learning reduces the training time, improves model efficiency, and improves the overall performance of the models.

5.1.2 VGG-16 Model

VGG-16 is a deep convolutional neural network architecture developed by the Visual Geometry Group (VGG) at the University of Oxford [166]. It is named VGG-16 because it consists of 16 layers which includes 13 convolutional layers and 3 fully connected layers. The key characteristic of the VGG-16 architecture is its simplicity and uniformity, where the convolutional layers all have a small 3×3 filter size, and the max-pooling layers have a 2×2 window with a stride of 2. The architecture is known for its deep stack of convolutional layers, which allows it to learn detailed patterns and features from images.

Architecture Overview

Figure 5.1 illustrates the design of the VGG-16 model, which includes various layers as discussed below.

- **Input Layer:** The VGG-16 model takes a fixed-size image of 224 × 224 pixels.
- **Convolutional Blocks:** The VGG-16 architecture is made up of 13 convolutional layers, each with a 3x3 filter size and followed by a Rectified Linear Unit (ReLU) activation function for nonlinearity. The convolutional layers are intended to capture low-level features including edges, textures, and patterns.
- **Max Pooling Layers:** Following the convolutional layers in each block a max-pooling layer is placed with a stride of two and a window size of 2 by 2. Max

pooling decreases the spatial dimensions of feature maps while preserving the most essential information.

- **Fully Connected Layers:** Three fully connected layers are placed at the end of the network. A ReLU activation function, except the last one, follows each fully linked layer.

- **Output Layer:** The last Fully connected layer is a softmax activation layer that calculates the probabilities for each class in a classification problem. For classification, the output size of the layer is proportional to the number of classes in the dataset.

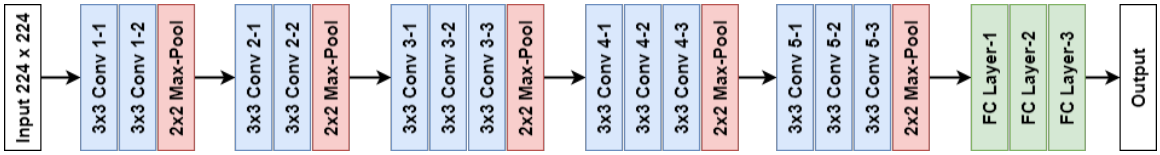


Figure 5.1: VGG-16 Architecture

5.2 Methodology

The proposed multimodal cancelable system is divided into three modules.

- Feature Extraction Module (FEM)
- Cancelable Template Creation Module (CTCM)
- Matching Module (MM)

The proposed secure multi-biometric system's overall architecture is shown in Figure 5.2. During enrollment, the user provides his iris and fingerprint, which are given to the FEM block, which extracts the features, binarizes, fuses, and performs ARX operation on them to generate a fused feature vector. This vector is then passed through the CTM block, where feature-hashed random projection is performed to generate cancelable templates which are called reference templates. These secured templates are then stored in the database for verification. During verification, the user presents both of his traits. These

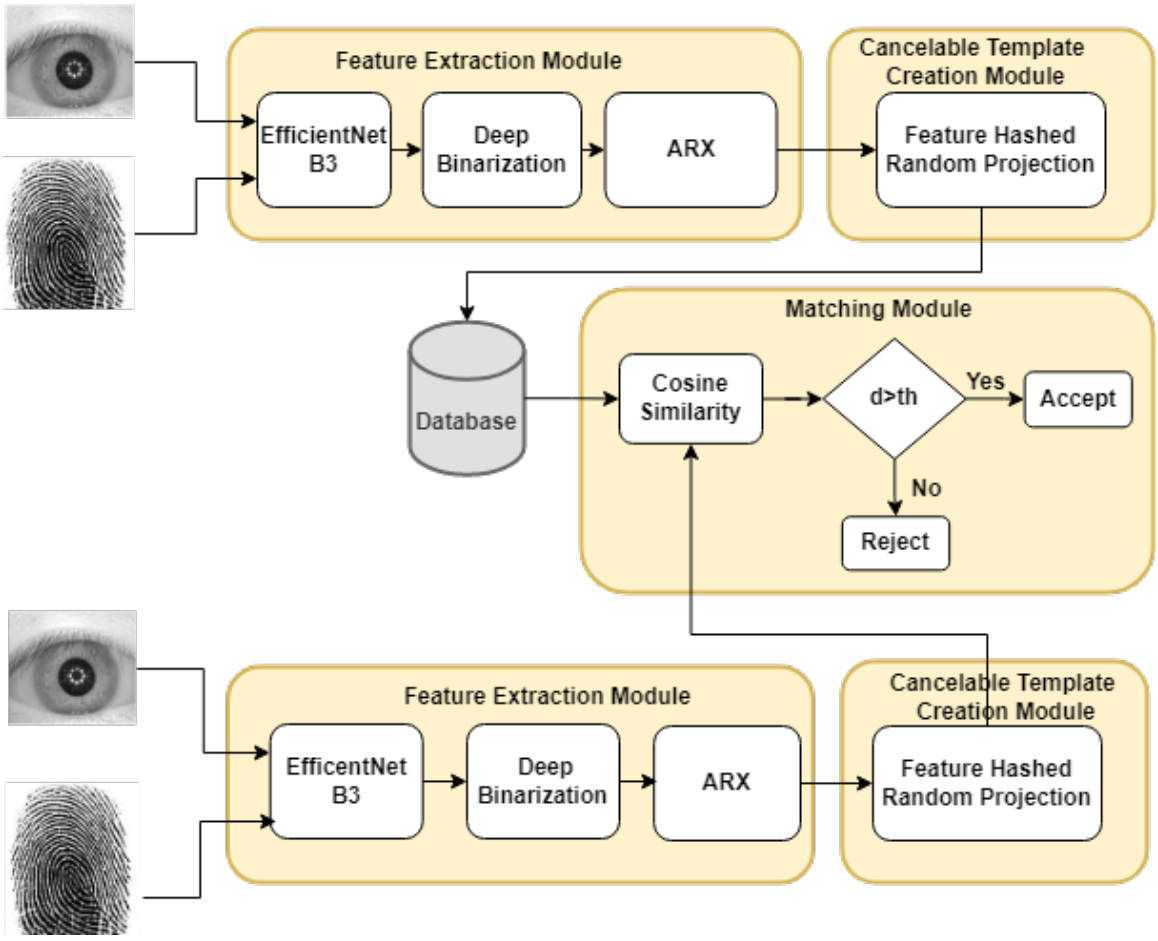


Figure 5.2: Block Diagram for Proposed System Architecture

traits are provided as input to the FEM block, which generates a fused vector. This fused vector is then processed using the CTM block to produce cancelable probe templates. Finally, these probe templates are compared to the reference templates in the database, and the user is classified as genuine or an imposter based on the similarity score.

5.2.1 Feature Extraction Module:

The FEM block is responsible for extracting features from the iris and fingerprint. It contains a CNN model which is formed by using trait-related layers, a hashing layer, fused FC layer, and a ARX layer.

1. **Trait-related layers:** In the proposed method a pre-trained model named VGG-16 is used as a trait-specific network, which is a deep neural network designed for

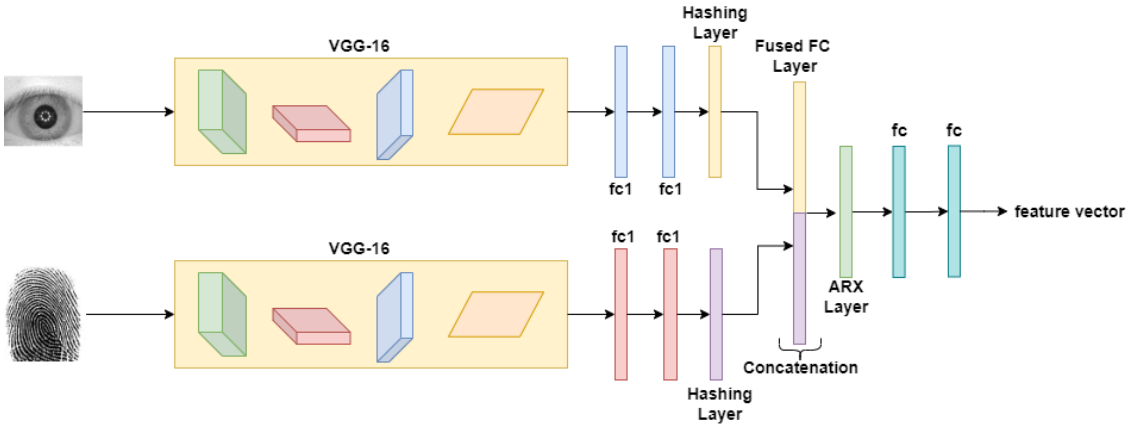


Figure 5.3: Feature extraction using Concatenation(Method1)

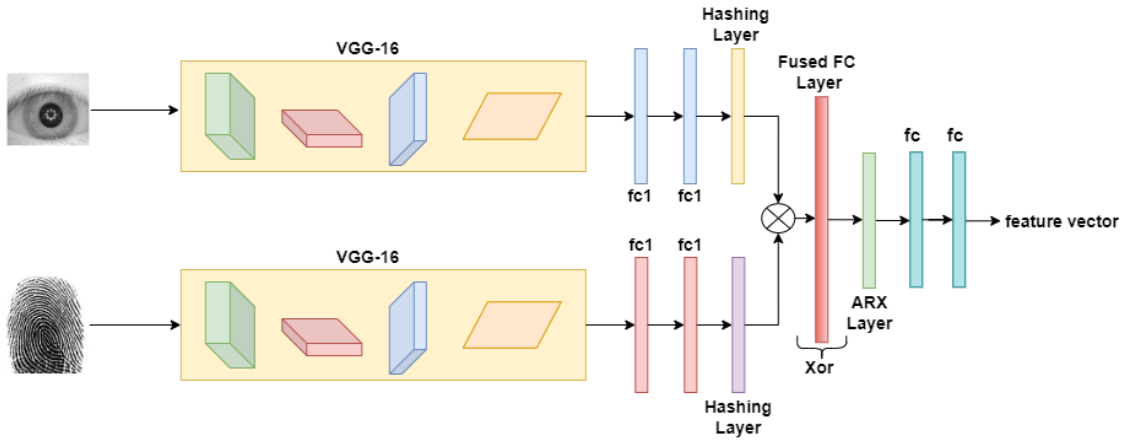


Figure 5.4: Feature extraction using Xor(Method2)

efficient and accurate image classification. The VGG-16 network takes the iris and fingerprint images as input and learns discriminative features from them. The output of the VGG-16 network is then passed through two fully connected layers for fine-tuning the model and then to a hashing layer to get binary features.

2. **Hashing layer:** The hashing layer transforms the extracted features into a binary representation. It employs a hash function that converts the continuous-valued features into binary codes and intra-class variations are added by applying random permutations. This binary representation enables efficient storage and comparison of the templates while preserving privacy. The output of the hashing layer for both the iris and fingerprint traits are combined to form a fused layer.

3. **Fused FC layer:** This layer takes binary features from both traits and combines them to form a fused fully connected (FC) layer. In this proposed method the FC layer is implemented using two different architectures a) Concatenated architecture and b) Xor architecture.

   Figure 5.3 represents the concatenation architecture in which the binary features of the iris and fingerprint are concatenated to form a single fused vector. This fused vector is passed through a fully connected layer which combines both the features and also reduces the size of the feature vector. In this architecture, the fused layer is made up of the concatenation layer and a fully connected layer.

   Figure 5.4 represents the Xor architecture in which the binary features of the iris and fingerprint are Xor-ed to form a single fused vector. This Xor-ed vector is passed through a fully connected layer to generate combined features. In this architecture, the fused layer is made up of the Xor-ed layer and a fully connected layer.

4. **ARX Layer:** The output produced by the fused FC layer i.e. fused vector is given as input to the ARX layer. The steps involved in this technique are as follows.

   (a) **Block Division:** The fused vector(f_v) is divided into n blocks of equal size, where n is determined by the desired block size which is represented as $f_v = f_1||f_2||...||f_n$. Each block f_i contains a subset of features from the fused vector i.e. $f_i = [f_{i1}, f_{i2}, ..., f_{in}]$.

   (b) **Matrix Arrangement:** As shown in Eq. 5.1, the n blocks of the fused vector, $f_1, f_2, ..., f_n$ are arranged in a matrix structure of dimension $n \times n$. The matrix format makes it easier to extract certain parts, such as rows, columns, and diagonals, which will be used to construct the key.

$$\begin{pmatrix} f_{11} & f_{12} & \cdots & f_{1n} \\ f_{21} & f_{22} & \cdots & f_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ f_{n1} & f_{n2} & \cdots & f_{nn} \end{pmatrix} \tag{5.1}$$

(c) **Key Generation:** For key generation, we consider the primary diagonal (pd) and secondary diagonal (sd) of the above-formed matrix. The primary diagonal consists of elements that have the same row and column index (i.e., (1, 1), (2, 2), ..., (n, n)). The secondary diagonal consists of elements that have row and column indices that sum up to n+1 (i.e., (1, n), (2, n-1), ..., (n, 1)). The elements from these two diagonals are combined using a bitwise AND operation to generate a key as shown in Eq. 5.2.

$$Key = AND(pd, sd) \tag{5.2}$$

(d) **ARX Operation:** Using the generated key, each block in the initial fused vector is XORed with the key by bitwise XORing the corresponding elements of the block and the key. The outcome of this operation is a modified block, which is then concatenated to form the ARX fused vector as shown in Eq. 5.3.

$$f'_v = Concatenation(f_1 \oplus key, f_2 \oplus key, \ldots, f_n \oplus key) \tag{5.3}$$

Algorithm 5.5 explains the steps used for ARX operation. This Xor-ed feature vector(f'_v) is passed through a pair of FC layers and a softmax layer to generate a modified feature vector(f''_v)

Algorithm 5.5 ARX Transformation

Input: feature vector(f_v)

Output: ARX feature vector(f'_v)

$f'_v \leftarrow [\,]$
for $i \leftarrow 0$ to length$(f_v) - 1$ **do**
    $x \leftarrow$ sqrt(length($f_v[0]$))
    $new\_arr \leftarrow$ reshape $f_v[i]$ into a 2D array of size (m, m)
    $pd \leftarrow$ primary diagonal elements of new_arr
    $sd \leftarrow$ secondary diagonal elements of new_arr
    $key \leftarrow$ bitwise-XOR(pd,sd)
    $result \leftarrow$ bitwise-XOR(key,new_arr)
    $f'_v \leftarrow$ flatten $result$ into a 1D array
return f'_v

5.2.2 Cancelable Template Creation Module

This module creates a cancelable template by applying feature-hashed random projection(FHRP). The input to the FHRP method is the feature vector(f''_v) received from the Feature extraction module. The steps involved in FHRP are as follows

1. **Block Division:** The fused vector is divided into *m* blocks of b_s elements in each block as shown in Eq. 5.4. From these *m* blocks, one block is selected randomly. This random block serves as the feature seed for generating the hash value which is used for forming the random projection matrix.

$$f''_v = f''_1||f''_2||....||f''_m \tag{5.4}$$

2. **Matrix Formation:** Figure 5.5 shows the generation of a matrix for the feature-hashed random projection. First, a block is selected from the feature vector known as the feature seed block is converted into a hash value using the SHA3-512 hashing algorithm. The SHA3-512 algorithm takes the feature seed as input and produces a

fixed-length hash value. The resulting hash value is arranged as a matrix called as feature matrix (F_m) of size $p \times q$, where p represents the number of rows and q represents the number of columns. The user provides a user seed as additional input. This user seed, along with the SHA3-512 algorithm, is used to generate another matrix called as user matrix (U_m) of size $p \times q$. The matrix formed from the feature seed and the matrix formed from the user seed is averaged element-wise to form a random projection matrix (R_p) as shown in Eq. 5.5. Element-wise averaging ensures that the resulting matrix contains a combination of characteristics from both the feature seed and the user seed, thus introducing randomness and further enhancing cancelability.

$$R_p = Avg(F_m, U_m) \tag{5.5}$$

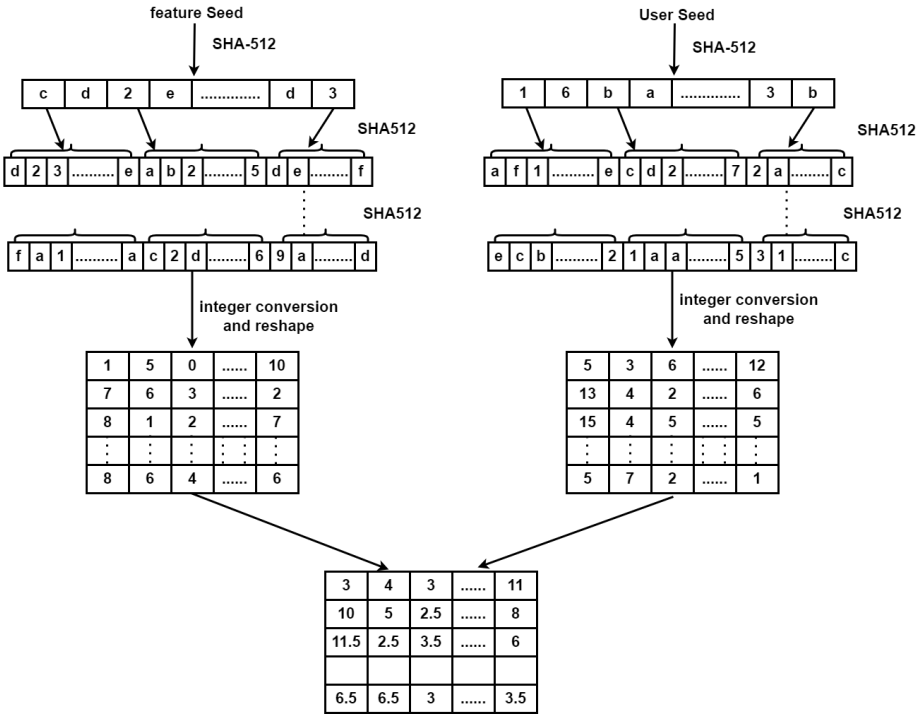


Figure 5.5: Feature hashed projection matrix generation

3. **Random Projection:** The random projection matrix (R_p) obtained from the averaging step is multiplied by the modified feature vector (f_v''). This matrix multiplication operation applies a linear transformation to the blocks, projecting them into a lower-dimensional space. The result is a feature-hashed random projected vector.

The feature hashed random projected vectors obtained from the previous step, which correspond to each block in the initial vector, are concatenated to form the final cancelable template (f_t) as shown in Eq. 5.6. This cancelable template maintains the matching properties of the original features while incorporating feature hashing and random projection to enhance cancelability, privacy, and dimensionality reduction. The step-by-step procedure of feature-hashed random projection is explained in Algorithm 5.6.

$$f_t = f_v'' * R_p \tag{5.6}$$

Algorithm 5.6 Cancelable Template Generation

Input: ARX vector f_v'', block size b_s, user_seed, size of R_p(p $\times$ q)

Output: Cancelable Template f_t

$m \leftarrow \frac{\text{len}(f_v'')}{b_s}$ ▷ Step 1: Divide into blocks

$random\_block \leftarrow$ random.randint$(0, m-1)$

for $i \leftarrow 0$ to length$(f_v'') - 1$ **do**

  $feature\_seed \leftarrow$ blocks$[random_block]$ ▷ Step 2: Generate feature matrix

  sha $\leftarrow$ hashlib.sha256$(feature_seed$.encode$())$

  $hash\_hex \leftarrow$ sha.hexdigest()

  $hash\_bytes \leftarrow$ bytes.fromhex$(hash_hex)$

  $F_m \leftarrow$ np.frombuffer$(hash_bytes,$ dtype $=$ np.uint8$)$

  $F_m \leftarrow$ reshape F_m into a 2D array of size (p, q)

  sha $\leftarrow$ hashlib.sha256$(user_seed$.encode$())$ ▷ Step 3: Generate User matrix

  $hash\_hex \leftarrow$ sha.hexdigest()

  $hash\_bytes \leftarrow$ bytes.fromhex$(hash_hex)$

  $U_m \leftarrow$ np.frombuffer$(hash_bytes,$ dtype $=$ np.uint8$)$

  $U_m \leftarrow$ reshape U_m into a 2D array of size (p, q)

  $R_p \leftarrow \frac{F_m + U_m}{2}$ ▷ Step 4: Generate Random projection matrix

  $f_t \leftarrow \text{f}_v'' * R_p$

return f_t

5.2.3 Matching Module:

Let P be the template that is stored in the database. Then, the user provides both traits for verification which is converted to probe template Q. The matching score between reference template P and query template Q is performed by using the cosine similarity as shown in the Eq. 5.7.

$$CS = \frac{\sum_{i=1}^{n} P_i Q_i}{\sqrt{\sum_{i=1}^{n} {P_i}^2} \sqrt{\sum_{i=1}^{n} {Q_i}^2}} \tag{5.7}$$

5.3 Experimental Results

5.3.1 Datasets

The performance of the proposed method is evaluated on various Databases as shown in Table 5.1. The effectiveness of the proposed model is evaluated based on the metrics given in section 1.7.

Table 5.1: Databases used for experimentation

Database	Iris	Fingerprint
DB1	Children Multimodal Biometric Database	
DB2	CASIA V1	FVC 2004
DB3	CASIA V3	FVC 2006

5.3.2 Evaluation

A biometric template protection approach should safeguard the user's privacy while maintaining the performance of the system. In this evaluation, we assess the efficacy of our proposed multimodal system across three datasets: CMBD (108 users), CASIA-V1 & FVC-2004 (100 users), and CASIA-V3 & FVC-2006 (100 users), each comprising 5 samples per user. Table 5.2 showcases the importance of template protection through a comparison of EER% and separability measures (d' and ks-test) between protected and unprotected templates. Protected templates are the ones to which FHRP is applied and Unprotected templates are the ones without FHRP.

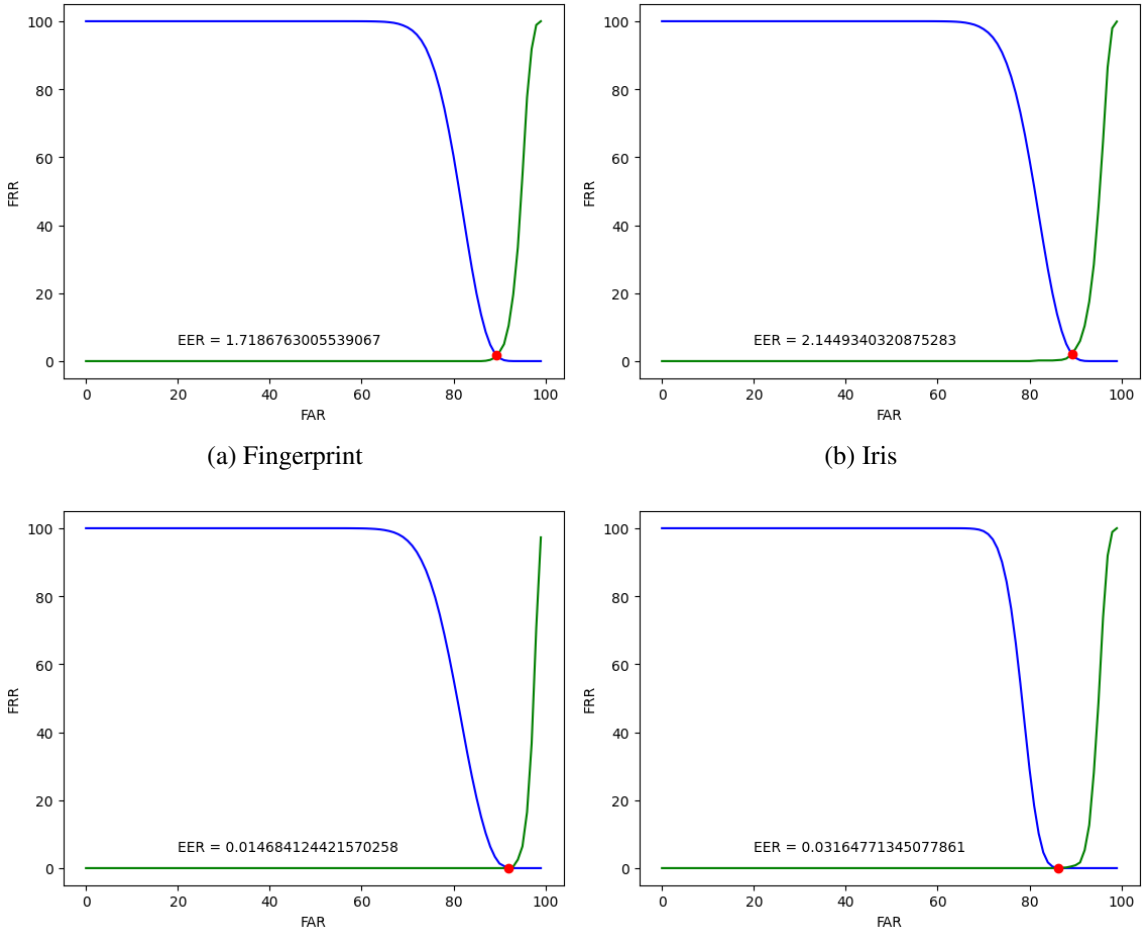
For the DB1 dataset, which consists of unimodal (iris and fingerprint) and multimodal (concatenated and Xor-ed iris-fingerprint) templates, the proposed Method 1 outperforms all others. It achieves an impressively low EER% of 0.014, coupled with a high d' value of 6.428 and a ks-test value of 0.96.

For DB2, Method 1 demonstrates an EER% of 0.029 with a d' value of 6.379 and a ks-test value of 0.96, showcasing its robustness in protecting templates while maintaining system performance. Similarly, on the DB3 dataset, Method 1 showcases a low EER% of 0.033 with a d' value of 5.257 and a ks-test value of 0.95, indicating its effectiveness in preserving user privacy. The d' and ks-test values of the protected templates across all datasets (DB1, DB2, and DB3) are consistently higher compared to the unprotected ones, indicating significantly enhanced security. The results from Table 5.2 demonstrates the effectiveness of the proposed Method 1 in achieving the balance between template security and system performance across various datasets.

Table 5.2: Comparison of EER and d' for unimodal and multimodal systems

Database	Template	Protected			Unprotected		
		EER%	d'	ks-test	EER%	d'	ks-test
DB1	Iris	1.710	2.995	0.87	2.534	0.892	0.39
	Fingerprint	2.144	2.705	0.81	3.128	0.703	0.3
	Method1	0.014	6.428	0.96	0.443	3.192	0.89
	Method2	0.031	6.087	0.95	1.668	2.627	0.8
DB2	Iris	1.860	2.797	0.82	2.110	0.866	0.37
	Fingerprint	2.644	2.699	0.8	3.970	0.817	0.35
	Method1	0.029	6.379	0.96	1.370	2.612	0.81
	Method2	0.053	4.135	0.91	1.597	2.970	0.84
DB3	Iris	1.865	2.722	0.81	2.978	1.372	0.49
	Fingerprint	3.105	2.255	0.75	4.655	1.177	0.45
	Method1	0.033	5.257	0.95	0.768	2.995	0.87
	Method2	0.275	3.868	0.90	2.048	2.950	0.83

The Equal Error Rate (EER) curves illustrate the trade-off between False Acceptance Rate (FAR) and False Rejection Rate (FRR) at different threshold values, providing useful insights into the performance of unimodal and multimodal systems across three datasets: DB1, DB2, and DB3. Figures 5.6a and 5.6b illustrate the EER curves of the unimodal systems for DB1. Figures 5.7a and 5.7b show the EER curves for unimodal systems in DB2. Figures 5.8a and 5.8b shows the EER curves of unimodal systems for DB3, demonstrating the performance of fingerprint and iris modalities.



(a) Fingerprint

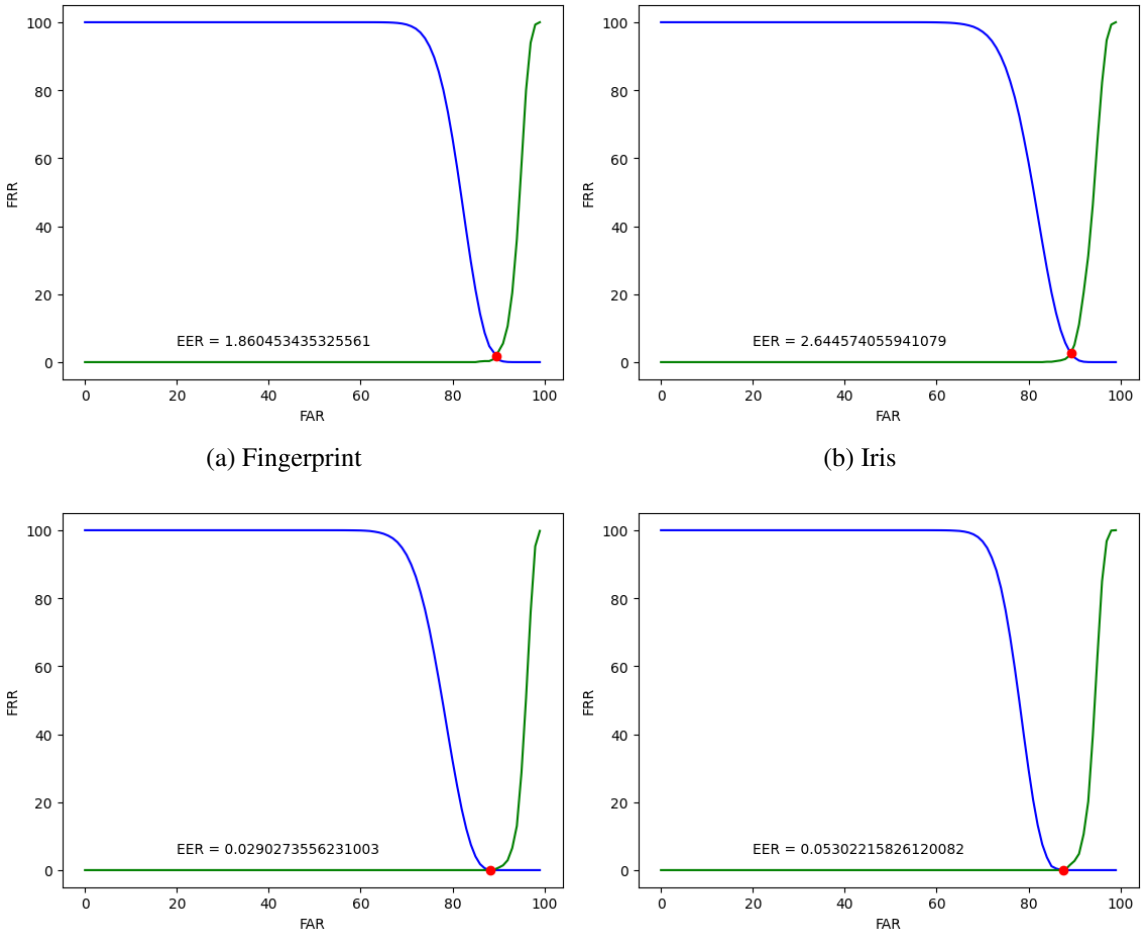
(b) Iris

(c) Fusion using Concatenation

(d) Fusion using Xor

Figure 5.6: EER Curves of unimodal and multimodal systems for DB1

To evaluate multimodal systems, Figures 5.6c and 5.6d show the EER curves for DB1. These figures represents the fusion techniques applied, namely Concatenation and Xor, demonstrating the effectiveness of combining iris and fingerprint modalities using these methods. Similarly, Figures 5.7c and 5.7d illustrate the EER curves of multimodal systems for DB2. Finally, Figures 5.8c and 5.8d illustrate the EER curves of multimodal systems for DB3.



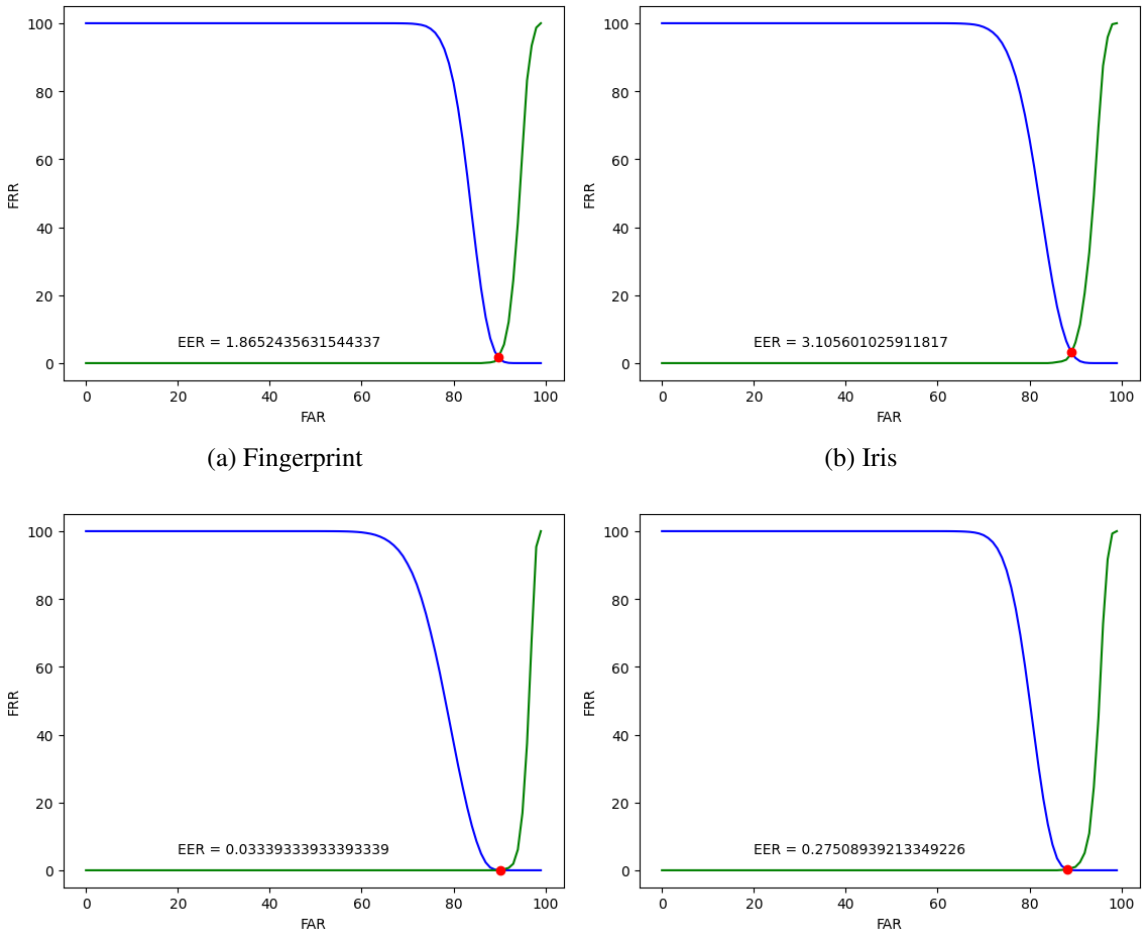
(a) Fingerprint

(b) Iris

(c) Fusion using Concatenation

(d) Fusion using Xor

Figure 5.7: EER Curves of unimodal and multimodal systems for DB2



(a) Fingerprint

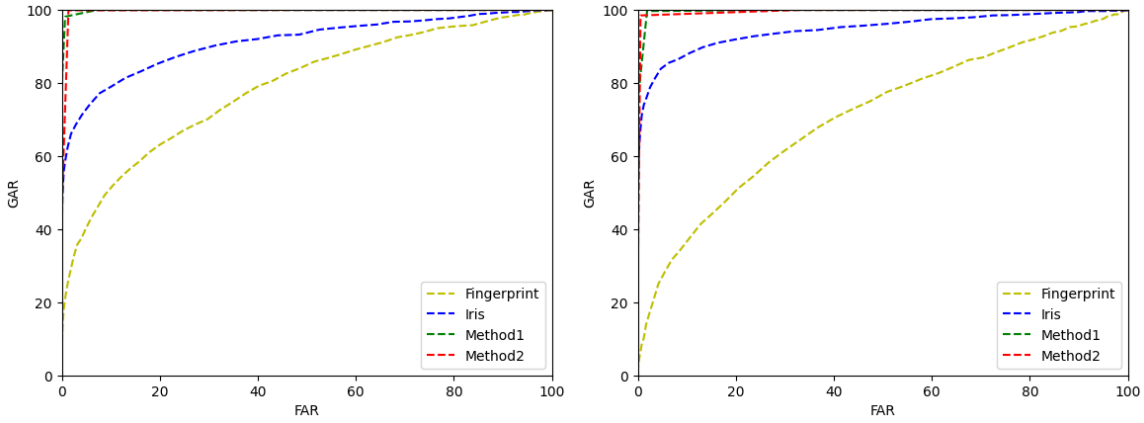
(b) Iris

(c) Fusion using Concatenation

(d) Fusion using Xor

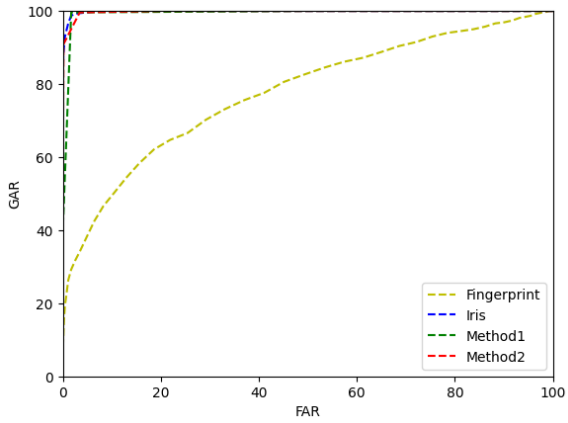
Figure 5.8: EER Curves of unimodal and multimodal systems for DB3

The Receiver Operating Characteristic (ROC) curves play an important role in evaluating biometric systems as they represent the relationship between the Genuine Acceptance Rate (GAR) and the False Acceptance Rate (FAR) at different threshold levels. A large area under the ROC curve in a biometric authentication system indicates that the system has strong discriminatory power, effectively distinguishing between genuine users and impostors. Figures 5.9a, 5.9b, and 5.9c visualise ROC comparisons for unimodal and multimodal systems in the DB1, DB2, and DB3 datasets, respectively.



(a) DB1

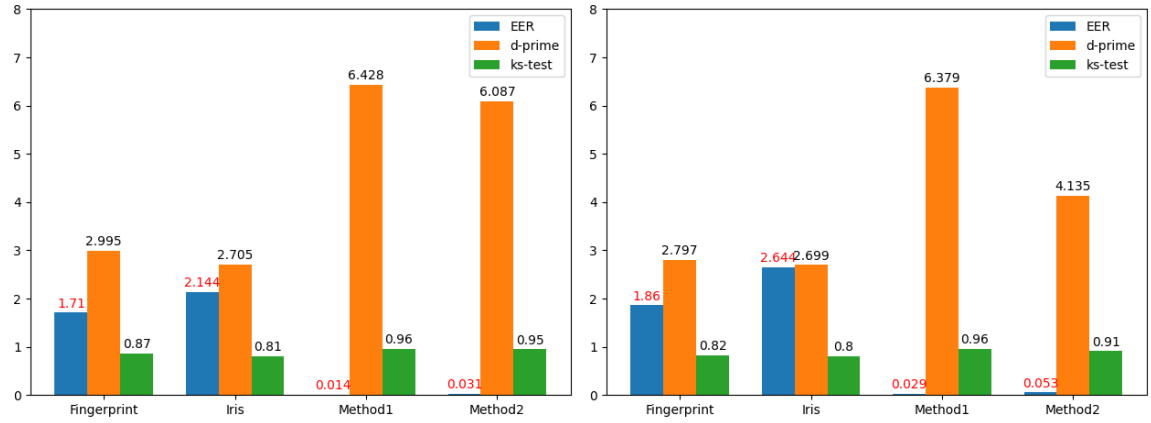
(b) DB2



(c) DB3

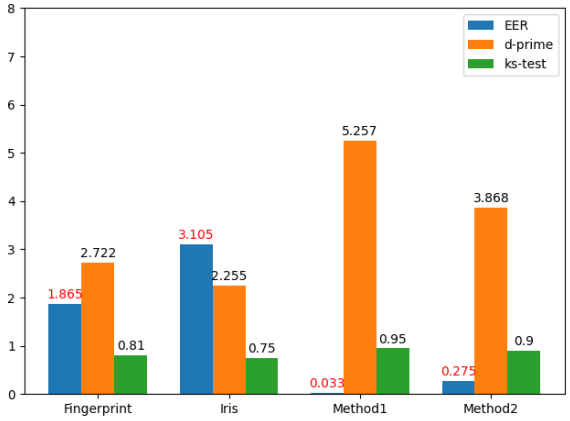
Figure 5.9: Comparison of ROC curves for unimodal and multimodal systems

Figure 5.10 depicts a comparison of unimodal and multimodal systems in terms of EER% and separability measures(d' and ks-test) values. Figure 5.10a, 5.10b and 5.10c shows the comparison of these metrics for DB1, DB2 and DB3 respectively. As we can observe higher separability measure values are related to lower system error rates. This indicates an inverse relation between separability measures and EER.



(a) DB1

(b) DB2



(c) DB3

Figure 5.10: Comparison of EER, d' and ks-test values for unimodal and multimodal systems

5.4 Comparative Analysis

Table 5.3 provides a comprehensive comparison of the proposed biometric template protection techniques with existing methods across various datasets. Our proposed method1 performs efficiently, with a low EER% of 0.014 on DB1, outperforming all existing techniques listed. This is significantly better than Gomez et al.'s method [142] on the BiosecurID multimodal database, Mahesh et al.'s approach [143] on CASIA-V 1.0, A. Singh et al.'s method [107] on Multi-PIE & PTB database, Sudhakar et al.'s technique [104] on FV-USM database, and Talreja et al.'s method [120] on WVU multimodal database. Fur-

thermore, when compared to other approaches on DB2 and DB3, our proposed method1 maintains its superiority with impressively low EER% values of 0.029 and 0.033, respectively. When evaluating our proposed method2, it also performs competitively with an EER% of 0.031 on DB1, 0.059 on DB2, and 0.275 on DB3. These results indicate the robustness and effectiveness of our proposed techniques in protecting biometric templates.

Table 5.3: EER% of the proposed approach vs existing methods on various databases

Method	Database	Traits	EER%
Gomez et al. [142]	BiosecurID multimodal database	Online signature & Fingerprint	0.12
Mahesh et al. [143]	CASIA-V 1.0	Left & right iris	0.19
Vallabhadas et al. [163]	Children Multimodal Biometric Database	Iris & Fingerprint	0.021
A. Singh et al. [107]	Multi-PIE & PTB database	Face & ECG	0.14
Sudhakar et al. [104]	FV-USM database	index & middle fingervein	0.05
Talreja et al. [120]	WVU multimodal database	face & iris	1.45
Proposed method1	DB1	Iris & Fingerprint	0.014
Proposed method2	DB1	Iris & Fingerprint	0.031
Proposed method1	DB2	Iris & Fingerprint	0.029
Proposed method2	DB2	Iris & Fingerprint	0.059
Proposed method1	DB3	Iris & Fingerprint	0.033
Proposed method2	DB3	Iris & Fingerprint	0.275

Table 5.4 compares the proposed methods to the existing methods on three datasets DB1, DB2 and DB3, where the proposed method with an EER% of 0.014 outperform the existing methods such as Gomez et al. [142], Mahesh et al. [143], Vallabhadas et al. [163], and Mahesh et al. [164] with EER% of 0.128, 0.262, 0.021, and 0.16, respectively. However, the proposed method2 achieves an EER% of 0.031 which is higher than Vallabhadas et al. [163] for DB1. For DB2 the proposed method with an EER% of 0.029 outperform the existing methods such as Benaliouche et al. [160] and Mustafa et al. [161], with EER% of 0.038 and 1.9, respectively. However, the proposed method2 achieves an EER% of 0.053 which is higher than Benaliouche et al. [160]. For DB3 the proposed method with an EER% of 0.033 outperform the existing methods such as Walia et al. [102] and Rajasekar et al. [162], with EER% of 2.35 and 0.18, respectively. However, the proposed method2

achieves an EER% of 0.275 which is higher than Rajasekar et al. [162]. Our proposed method1(concatenation of iris and fingerprint) outperforms all the other existing methods whereas the method2(Xor of iris and fingerprints) fails in some cases.

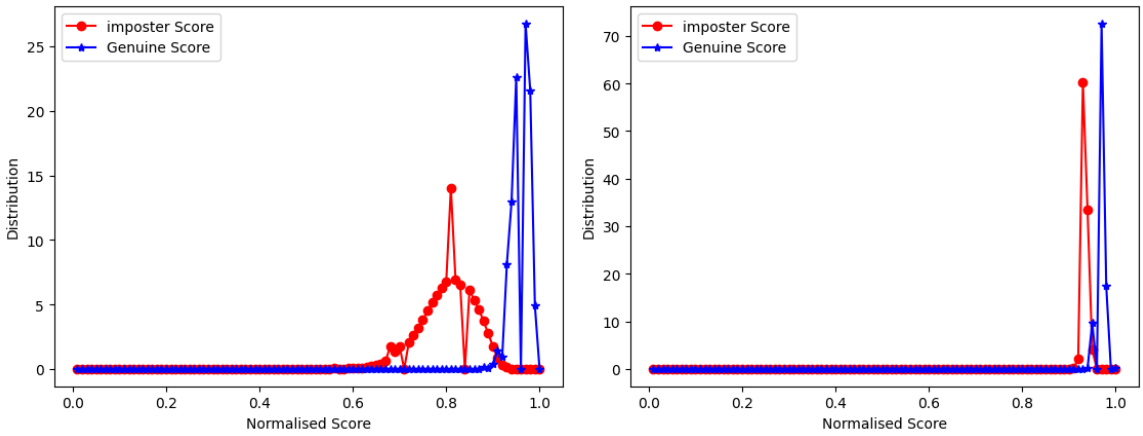
Table 5.4: EER% of the proposed method vs existing methods on various datasets

Method	**Database**	**EER%**
Gomez-Barrero et al. [163]	DB1	0.128
Mahesh et al. [163]		0.262
Vallabhadas et al. [163]		0.021
Mahesh et al. [164]		0.16
Proposed method1		0.014
Proposed method2		0.031
Benaliouche et al. [160]	DB2	0.038
Mustafa et al. [161]		1.9
Proposed method1		0.029
Proposed method2		0.053
Walia et al. [102]	DB3	2.35
Rajasekar et al. [162]		0.18
Proposed method1		0.033
Proposed method2		0.275

5.5 Security Analysis

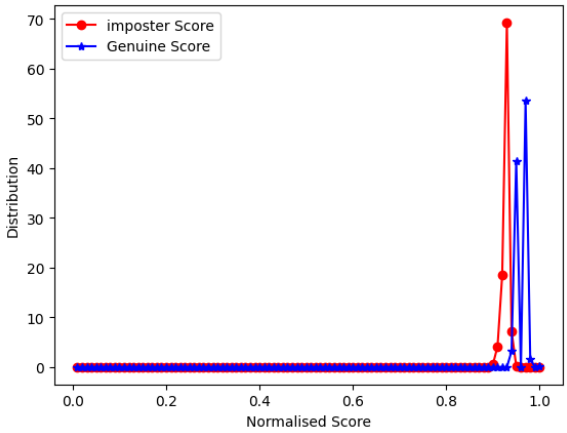
5.5.1 Revocability

Revocability ensures that in the event of a compromised template, it must be revoked, and a new template should be created using the same biometric data. In our system, we employ FHRP, which splits the feature vectors (f_v) into p equal parts and randomly selects one of them for random projection. If a template is corrupted, we can alter the slot (i) and construct a fresh template. Additionally, during feature extraction, we utilize ARX, and in case of template compromise, we can modify the key by considering different rows and columns, rather than using primary and secondary diagonals. As we can see in Figure 5.11 the distributions of genuine and imposter are well separated which indicates that the system differentiates between the genuine and imposter effectively.

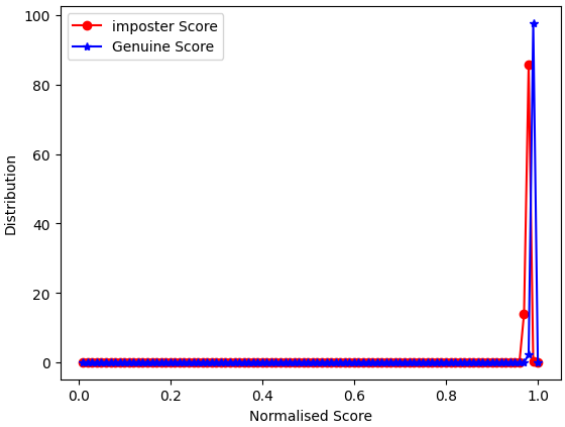


(a) Method1 for DB1

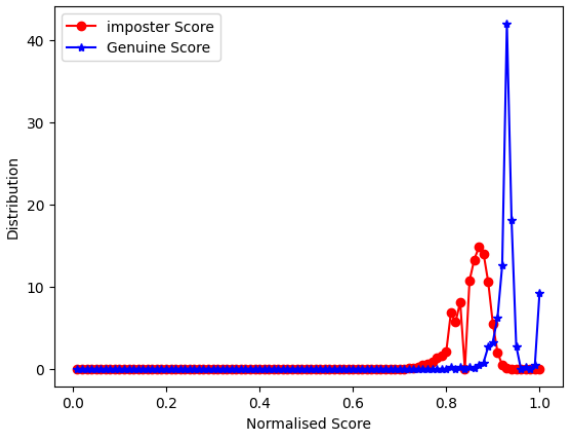
(b) Method2 for DB1



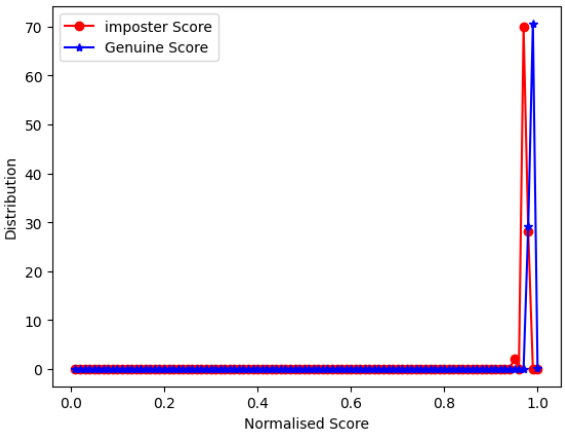
(c) Method1 for DB2



(d) Method2 for DB2



(e) Method1 for DB3



(f) Method2 for DB3

Figure 5.11: Revocability test using Genuine and Imposter distributions

5.5.2 Unlinkability Analysis

It is possible to build various templates for a single user by altering the key used in the ARX operation, by considering different rows and columns. Additionally, different templates for a single user can be constructed by changing the block size (p) and feature slot (i) in feature-hashed random projection. This illustrates how the cancelable transformation allows us to generate diverse parameter sets in various applications.

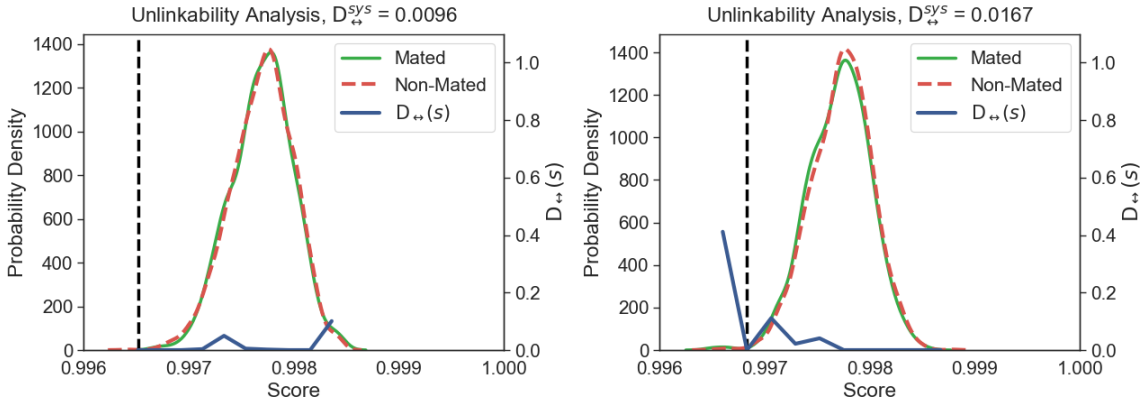
Cross matching attack:

If an attacker acquires the template used in one application, the same template can be used to bypass the system in another application. However, a cross-matching attack is not possible on our technique. Our proposed approach varies parameters such as the key for the ARX operation, block size (p), and feature slot (i) for random projection in different applications, generating distinct templates for the same user.

Gomez et al. [142] developed a framework to assess a system's unlinkability, which includes two measurements: local linkability (D↔(s)) and global linkability ($D_{\leftrightarrow}^{sys}$). Both measurements are in the range of 0 to 1 i.e. [0, 1]. A value of 0 indicates that the templates are completely linkable, whereas a value of 1 indicates that the templates are completely unlikable. To evaluate our proposed methods, we utilized 10 user keys. Using these keys and the first sample from each user, we generated 972 mated scores and 1026 non-mated scores. These scores were then plotted on the graph, as shown in Figure 5.12. Both of our proposed approaches have highly overlapping curves; however, method 1 on DB1 provides the lowest $D_{\leftrightarrow}^{sys}$ value, almost approaching zero with a minimum of 0.009. This indicates that the proposed system achieves a high level of unlinkability, making it nearly impossible to link templates together.

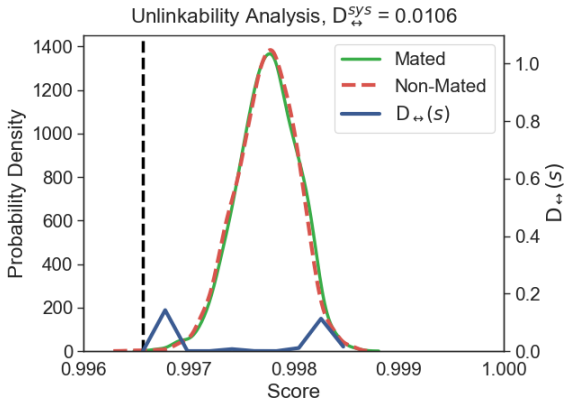
5.5.3 Irreversibility Analysis

As the features from the fused vector are extracted after performing ARX operation, the attacker need to know the key for obtaining the original data. Furthermore, these extracted features are converted to a template using feature hashed random projected for which the

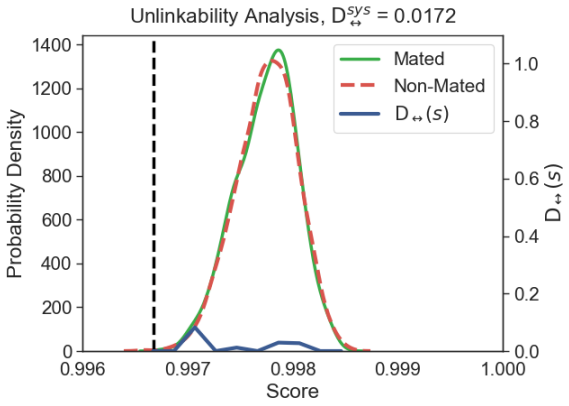


(a) Method1 for DB1

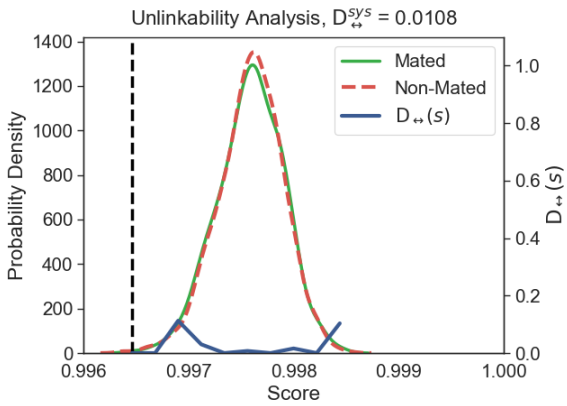
(b) Method2 for DB1



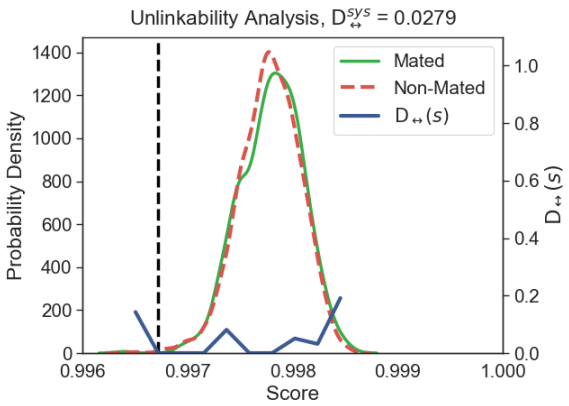
(c) Method1 for DB2



(d) Method2 for DB2



(e) Method1 for DB3



(f) Method2 for DB3

Figure 5.12: Unlinkability Analysis using Genuine and Imposter distributions

random projection matrix is generated using user matrix and feature slot generated matrix. It is important to note that even if the attacker obtains the templates, he will not be able

to generate a feature vector. This is because the user matrix (U_m), which contains critical information to create the projection matrix (R_m), is deleted and unavailable to the attacker. As a result, the process remains secure against attempts to reconstruct the original feature vector from the templates.

5.5.4 Record Multiplicity attacks

In this attack, the attacker uses multiple compromised templates, to construct an equation for the system to find a solution. However, the proposed feature-hashed random projection method generates the matrix using the feature slot and user seed. The projection matrix is discarded following each random projection and is not available. As a result, the attacker cannot obtain the features without knowledge of original trait and the key used for the ARX operation. This ensures the security and privacy of the biometric system.

5.5.5 Lost key scenario

In the worst-case situation, if the attacker possesses both the template and the user seed, he can apply an extensive guessing strategy to extract the initial feature vector from the created template. The ARX operation uses a key produced from a 64 $\times$ 64 matrix. This matrix provides $\binom{130}{2}$ potential ways i.e. 8385 possibilities to build a key by choosing two vectors from either rows (64), columns (64), or diagonals (2). In addition, the feature vector is split into different slots, let us assume slot size as 8, yielding 128 slots, one of which is randomly chosen. It is therefore very difficult for the attacker to compute because it requires 8385 * 128 = 1,073,280 ($\approx$1.07M) guesses in total to acquire the original feature vector.

5.6 Summary

This work presents a BTP technique based on feature-level fusion that combines Deep binarization and feature-hashed random projection. Initially, features are extracted from iris and fingerprint images using VGG-16, which are then binarized and merged to create a fused vector. The obtained fused vector is further processed through ARX and FC layers to obtain

a modified vector. Later, the modified vector passes through a cancelable template module where feature-hashed random projection is performed resulting in secured templates. The proposed technique is evaluated using two fusion techniques such as concatenation and Xor, on the three datasets. The experimental results illustrates the efficacy of the method by achieving an EER of 0.014%, 0.029%, and 0.0219%, and a d' value of 6.428, 6.379 and 5.257 respectively for method1 when compared to existing methods. These results show the efficiency and performance of the proposed method while preserving privacy.

Chapter 6

A hybrid template protection technique that provides confidentiality and integrity

In this chapter, a multimodal cancelable technique was presented which uses deep CNN and Block-Xor operation for feature extraction and signcryption using a hyperelliptic curve cryptosystem for enhancing security and performance.

Chapter Organization: Section 6.1 provides the basics of methods used in the proposed methodology. Section 6.2 explains the proposed methodology, while Section 6.3 provides the experimental results. Section 6.4 presents the comparative analysis, and Section 6.5 discusses a security analysis of the proposed methodology. Finally, Section 6.6 provides a summary of the work.

6.1 Background

6.1.1 Signcryption

Signcryption is a cryptographic technique that combines the functionalities of digital signature and encryption into a single operation [167]. Signcryption allows a sender to encrypt a message using the recipient's public key for confidentiality and sign it with their private

key for authentication in a single step. This assures that only the intended receiver can decode and read the message, while also validating the sender's identity and integrity of the message. Signcryption simplifies cryptographic processes by reducing computational overhead and communication costs, making it efficient for secure messaging and data sharing.

Procedure

Input:

- Sender has a message M, Sender private key K_s and Recipient's public key K_r.

Signcryption Operation:

- The sender performs the signcryption operation on the message M using their private key K_s and the recipient's public key K_r. The signcrypted message $SC(M)$ consists of both the encrypted message and the digital signature.

$$SC(M) = \text{Signcrypt}(M, K_s, K_r) = (E(M, K_r), \text{Sign}(M, K_s))$$

  Here, $E(M, K_r)$ represents the encryption of message M using the recipient's public key K_r, and $\text{Sign}(M, K_s)$ represents the digital signature of M using the sender's private key K_s.

Sending:

- The sender sends the signcrypted message $SC(M)$ to the recipient over a secure channel.

Receiving:

- The recipient receives the signcrypted message $SC(M)$.

Decryption and Verification:

- The recipient performs the following steps to decrypt and verify the signcrypted message $SC(M)$.

  Decryption:

  – Decrypt the encrypted message part $E(M, K_r)$ using the recipient's private key K_r^{-1}. This yields the original message M' sent by the sender.

$$M' = D(E(M, K_r), K_r^{-1})$$

  Verification:

  – Verify the digital signature Sign(M, K_s) using the sender's public key K_s. If the verification is successful, the recipient knows that the message M' is from the sender and has not been altered.

$$\text{Verify}(\text{Sign}(M, K_s), M', K_s)$$

6.2 Methodology

The proposed multimodal cancelable system is divided into three modules.

- Feature Extraction Module (FEM)
- Template Creation Module (TCM)
- Matching Module (MM)

Figure 6.1 illustrates the overall architecture of the proposed secure multi-biometric system. During the enrollment process, the user provides his iris and fingerprint, which are then passed to the Feature Extraction Module (FEM) block. Within the FEM block, the features are extracted, binarized, fused, and subjected to Block-Xor operations, resulting in a fused feature vector. This vector is then given to the Template Creation Module

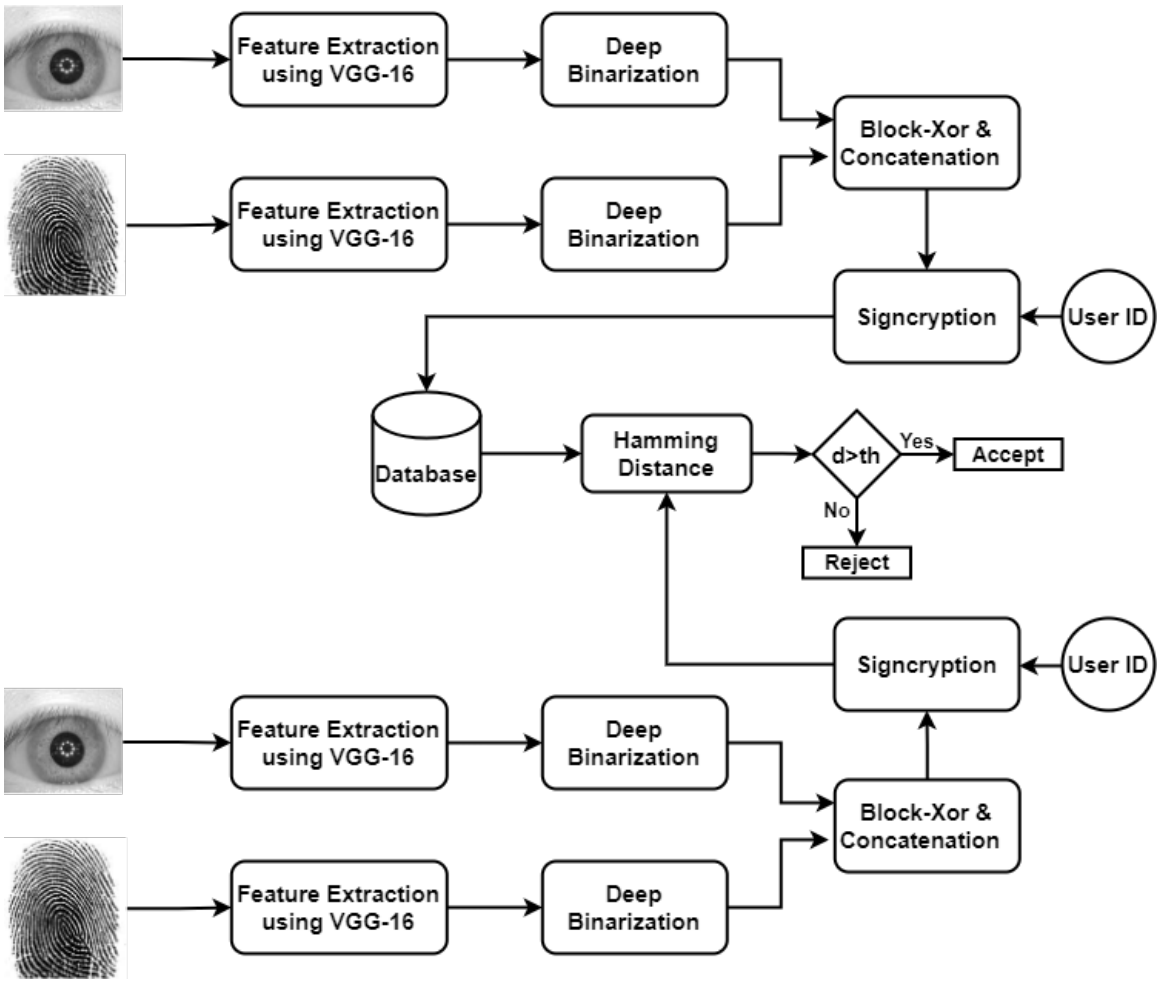


Figure 6.1: Block Diagram for Proposed System Architecture

(TCM), where Signcryption is applied to produce cancelable templates known as reference templates. These secured reference templates are then stored in the database for later verification. During the verification phase, the user presents both of his biometric traits. These traits are fed into the FEM block to generate a fused vector, which is further processed through the TCM block to produce cancelable probe templates. These probe templates are then compared against the reference templates stored in the database. The system determines the user's authenticity based on the similarity score derived from this comparison.

6.2.1 Feature Extraction Module:

The overall architecture of the FEM is illustrated in Figure 6.2. The FEM block extracts features from both the iris and the fingerprints. This block has a Convolutional Neural

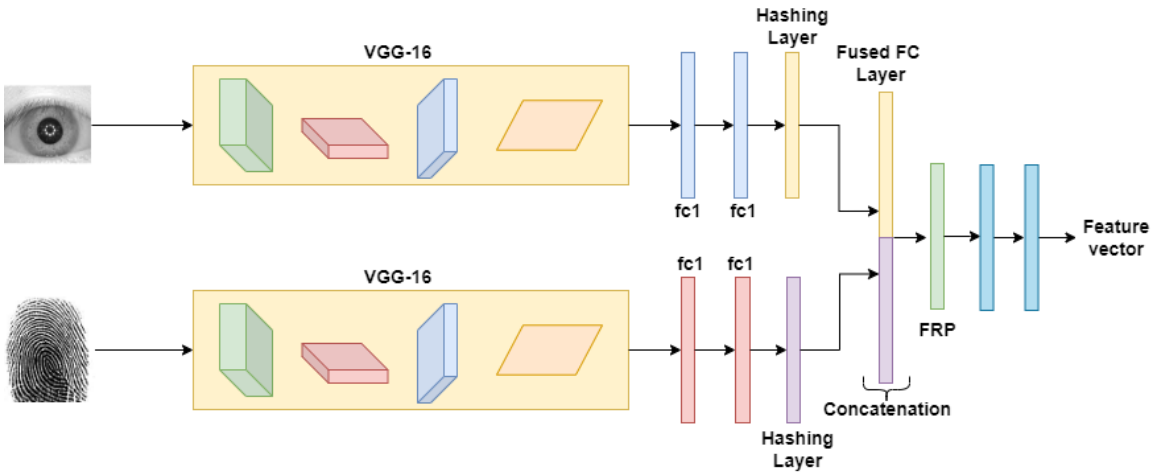


Figure 6.2: Feature extraction using Concatenation

Network (CNN) model with trait-related layers, a hashing layer, a Block-Xor layer, and a pair of FC layers.

1. **Trait-related layers:** The Trait-Specific Layer of the feature extraction module uses a modified VGG-16 model explicitly designed for extracting features from the iris and fingerprint traits. This modified model maintains the fundamental architecture of the VGG-16 network while adding two more fully connected layers. The model is fine-tuned to capture detailed patterns and distinguishing properties unique to iris and fingerprint data. This layer effectively extracts the trait-specific features required for accurate biometric identification using the VGG-16 architecture's inherent capabilities.

2. **Hashing layer:** The Hashing Layer in the feature extraction module is crucial for transforming the extracted features into a binary format. The hashing layer uses a hash function to modify the output of the modified VGG-16 model, which consists of continuous-valued features. A random permutation is used for the binary codes to introduce intra-class variances. The layer turns the derived characteristics into binary values by performing a binarisation process, allowing for efficient storage, processing, and privacy. This binary encoding protects sensitive biometric data while keeping the integrity of the original features.

3. **Block-Xor layer:** The output generated by the hashing layer for iris and fingerprint,

serves as the input to the Block-Xor layer. This approach involves the following steps:

- Block Division: The Block-Xor technique begins with the division of the iris feature vector (f_{ir}) and fingerprint feature vector (f_{fp}) into a specified number of blocks, denoted as *m* with each block contains b_s number of elements.
- Key Generation: Following block division, a unique key is generated from these blocks to perform the XOR operation. The key generation process includes selecting a slot *i* from both the iris feature vector (f_{ir}) and fingerprint feature vector (f_{fp}) and combining them using an AND operation as shown in Eq. 6.1.

$$key = AND_s(f_{ir}^i, f_{fp}^i) \tag{6.1}$$

- Block-Xor: Using the generated key, the Block-Xor operation is performed on the initial feature vectors to create a modified feature vector. This procedure involves performing an XOR operation on each block of the feature vectors f_{ir} and f_{fp} with the generated key as shown in Eq's. 6.2 and 6.3. The modified feature vectors f'_{ir} and f'_{fp} are then concatenated to generate the final modified feature vector as shown in Eq. 6.4.

$$f'_{ir} = Concatenation(f_{ir\_1} \oplus key, f_{ir\_2} \oplus key, \ldots, f_{ir\_m} \oplus key) \tag{6.2}$$

$$f'_{fp} = Concatenation(f_{fp\_1} \oplus key, f_{fp\_2} \oplus key, \ldots, f_{fp\_m} \oplus key) \tag{6.3}$$

$$f_v = Concatenation(f'_{ir}, f'_{fp}) \tag{6.4}$$

Algorithm 6.7 illustrates the Block-Xor procedure. This feature vector (f_v) is processed through two FC layers to generate a modified feature vector (f'_v).

Algorithm 6.7 Block-Xor Algorithm

Input: Iris vector f_{ir}, Fingerprint vector f_{fp}, block size b_s, slot i

Output: Feature vector f_v

▷ **Step 1: Block Division**

$blocks \leftarrow [\,]$

$m \leftarrow f_{ir}/b_s \; or \; m \leftarrow f_{fp}/b_s$

for i in range(m) **do**

    $block_i \leftarrow f_{ir}[i \cdot p : (i+1) \cdot b_s]$

    $block_p \leftarrow f_{fp}[i \cdot p : (i+1) \cdot b_s]$

▷ **Step 2: Key Generation**

$f_{ir}^i \leftarrow rand(block_i)$

$f_{fp}^i \leftarrow rand(block_p)$

$key \leftarrow AND_s(f_{ir}^i, f_{fp}^i)$

▷ **Step 3: Block-Xor**

for i in range(m) **do**

    $modified\_block_i \leftarrow blocks_i \oplus key$

    $modified\_block_p \leftarrow blocks_p \oplus key$

$f'_{ir} \leftarrow$ **concatenate**($modified\_blocks_i$, **axis**$= 0$)

$f'_{fp} \leftarrow$ **concatenate**($modified\_blocks_p$, **axis**$= 0$)

$f'_v \leftarrow$ **concatenate**(f'_{ir}, f'_{fp})

6.2.2 Template Creation Module

This module uses signcryption to create a cancelable template using hyperelliptic curve cryptography(HECC). This module takes as input the feature vector (f'_v) acquired by the Feature Extraction module which is signcrypted and stored in the database for verification. The signcryption scheme consists of four essential algorithms for each sender and receiver, where K denotes the key space, M denotes the message, and S denotes the signcryption. They are described as follows:

- Setup: This phase is used to initialize the parameters required for the scheme. For a

finite field F, let y^2 = f(x) represent the hyperelliptic curve, where f(x) is a polynomial of degree n. The hyperelliptic curve is defined over a finite field F, and its size is given by a prime number P'. To generate the public and private keys, let us consider a base point B_p on the curve along with a divisor D.

- Key Generation: This phase is used to generate keys for both sender and receiver.
  - Sender Keys:
    - Select a private key δ^s_{sk} for the sender from the range [1, P'-1].
    - Calculate the corresponding public key by computing δ^s_{pk}= δ^s_{sk} × B_p.
  - Receiver Keys:
    - Select a private key δ^r_{sk} for the recipient from the range [1, P'-1].
    - Calculate the corresponding public key by computing δ^r_{pk}= δ^r_{sk} × B_p.
- Signcryption:
  - Compute the scalar multiplication L=k * δ^r_{pk}, where k is randomly chosen from the range [1, P'-1].
  - Compute (K_1, K_2)=h(ϕ(L)), where ϕ is the mapping to the elliptic curve and h is the hash function.
  - Encrypt the message M using K_2 to obtain c = E_{k_2}(m).
  - Compute r = h(K_1 || User_ID).
  - Compute s=(k*r+δ^s_{sk}) mod$q$
  - Compute R = r*D
  - The signcrypted message is (c, R, s).
- Unsigncryption:
  - Compute (K_1, K_2) = h(ϕ(s*δ^r_{sk} (δ^s_{pk} + R)))
  - Compute r = h(K_1 || User_ID).
  - Decrypt the message M using K_2 to obtain M = D_{k_2}(c).
  - Verify if r*D=R, accept the message; otherwise, reject

6.2.3 Matching Module:

Let P be the template stored in the database. Then, the user provides both traits for verification which is converted to probe template Q. The matching score between reference template P and query template Q is performed by using the hamming distance similarity as shown in the Eq. 6.5.

$$HD = \sum_{i=1}^{n} (p_i \oplus q_i) \tag{6.5}$$

6.3 Experimental Results

6.3.1 Datasets

The performance of the proposed method is evaluated on various Databases as shown in Table 6.1. The effectiveness of the proposed model is evaluated based on the metrics given in section 1.7.

Table 6.1: Databases used for experimentation

Database	Iris	Fingerprint
DB1	Children Multimodal Biometric Database	
DB2	CASIA V1	FVC 2004
DB3	CASIA V3	FVC 2006

6.3.2 Evaluation

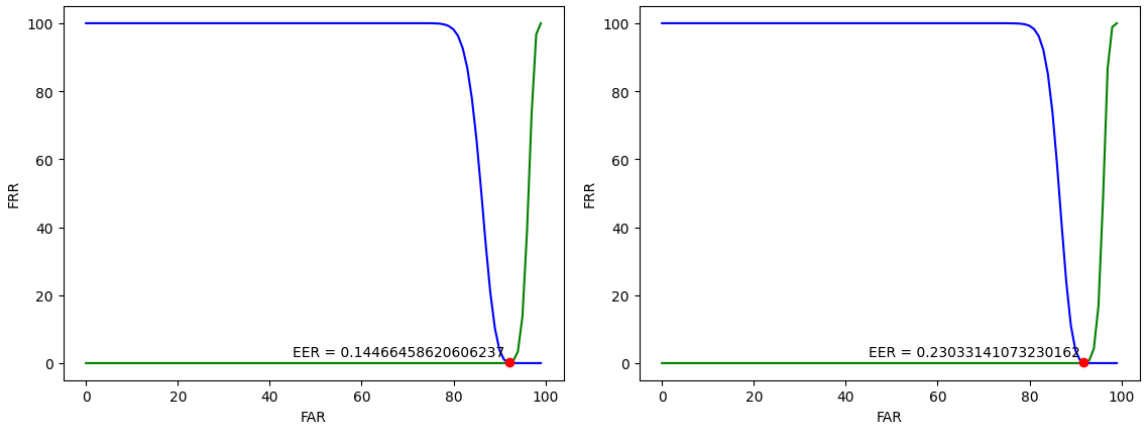
The primary goal of a biometric template protection technique is to maintain the privacy of the user's information while maintaining the system's performance standards. In this study, we examine the efficiency of the proposed multimodal system utilizing three different datasets: CMBD (108 users), CASIA-V1 & FVC-2004 (100 users), and CASIA-V3 & FVC-2006 (100 users), each with five samples per user. Table 6.2 shows the importance of template protection by comparing EER%, d', and ks-test values for templates with and without encryption. Protected templates are those that have been signcrypted, whereas unprotected templates do not have this extra layer of security.

For DB1, which comprises iris, fingerprint, and concatenated iris-fingerprint templates, the proposed method performs well with an incredibly low EER% of 0.020, a high d' of 3.672, and a ks-test value of 0.91. This demonstrates the method's effectiveness in balancing template protection and system efficiency. Furthermore, on DB2 the proposed approach continues to perform nicely with an EER% of 0.044, a d' of 3.541, and a ks-test value of 0.91, demonstrating its strength in safeguarding templates. On DB3, the proposed technique remains effective, with an EER% of 0.093, a d' of 3.525, and the ks-test value of 0.90, indicating constant performance in safeguarding user privacy. The d' and ks-test values of protected templates are significantly higher than those of unprotected templates across all datasets, indicating a significant security improvement. These results highlight how well the proposed approach works across various datasets to achieve a balance between template security and system performance.

Table 6.2: Comparison of EER and d' for unimodal and multimodal systems

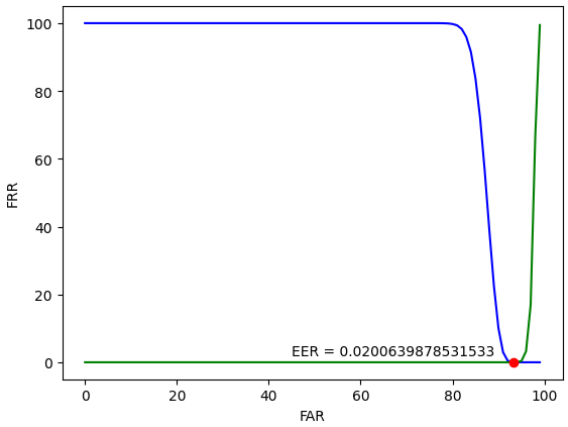
Database	Template	Protected			Unprotected		
		EER%	d'	ks-test	EER%	d'	ks-test
DB1	Iris	0.144	3.452	0.89	2.245	0.899	0.47
	Fingerprint	0.230	3.306	0.87	2.932	0.866	0.46
	Proposed	0.020	3.672	0.91	1.721	1.312	0.49
DB2	Iris	0.206	3.374	0.88	2.654	0.876	0.47
	Fingerprint	0.235	3.301	0.87	3.124	0.865	0.45
	Proposed	0.044	3.541	0.91	1.992	1.176	0.48
DB3	Iris	0.298	3.261	0.86	3.212	0.791	0.44
	Fingerprint	0.349	2.920	0.86	3.530	0.765	0.40
	Proposed	0.093	3.525	0.90	2.145	1.064	0.48

Equal Error Rate (EER) curves were plotted using False Acceptance Rate (FAR) and False Rejection Rate (FRR) to assess the system's performance by providing a visual representation of the performance trade-offs between FAR and FRR. These curves indicate the points at which the FAR and FRR are equal, which represents the EER for each modality. Figures 6.3a and 6.3b illustrate the EER curves for fingerprint and iris modalities in DB1's unimodal systems, while Figure 6.3c demonstrate the performance of multimodal systems. These figures yield EER values of 0.144, 0.230, and 0.020 for the fingerprint, iris, and combination modalities, respectively.



(a) Fingerprint

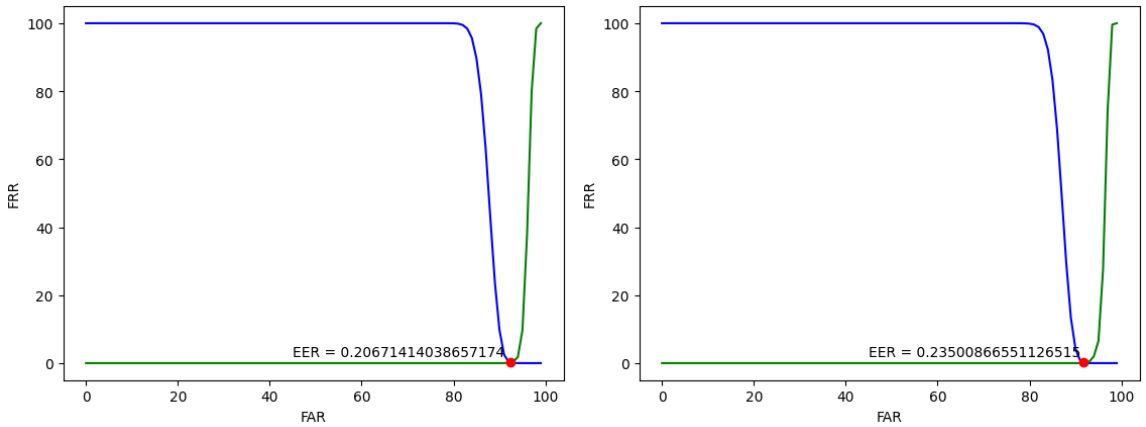
(b) Iris



(c) Fusion using Concatenation

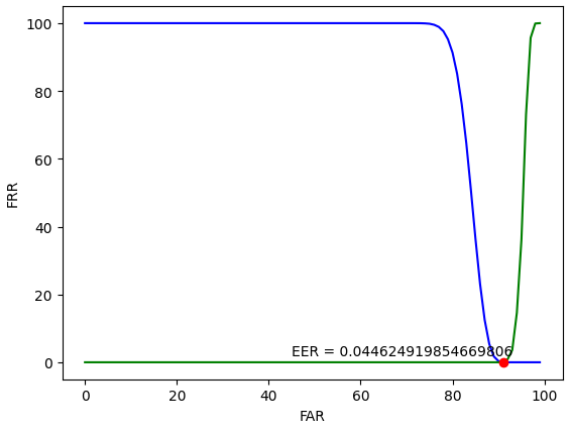
Figure 6.3: EER Curves of unimodal and multimodal systems for DB1

Similarly, Figures 6.4a and 6.4b depict the EER curves for the unimodal systems in DB2, while Figure 6.4c demonstrate the EER curves for the multimodal system. These figures yield EER values of 0.206, 0.235, and 0.044 for the fingerprint, iris, and combination modalities, respectively.



(a) Fingerprint

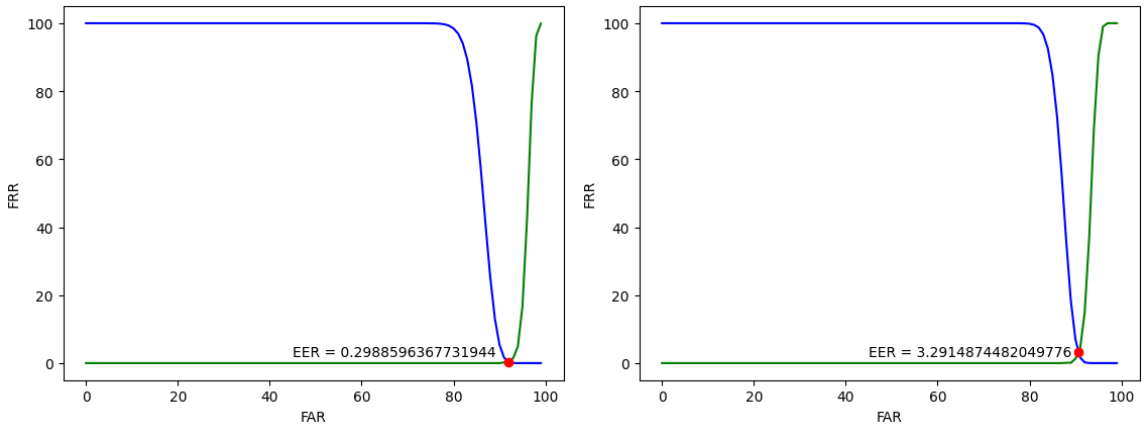
(b) Iris



(c) Fusion using Concatenation

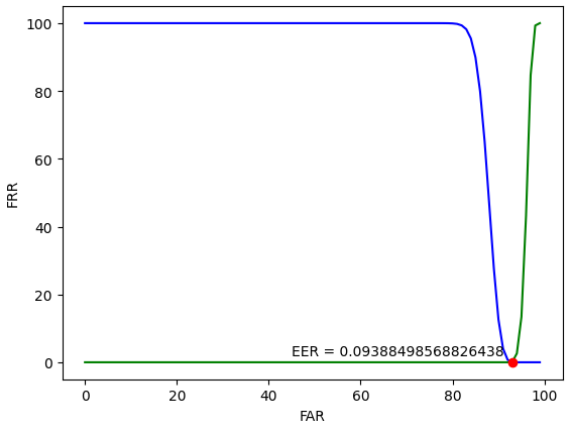
Figure 6.4: EER Curves of unimodal and multimodal systems for DB2

Similarly, Figures 6.5a and 6.5b depict the EER curves for the unimodal systems in DB3, while Figure 6.5c demonstrate the EER curves for the multimodal system. These figures yield EER values of 0.298, 0.349, and 0.093 for the fingerprint, iris, and combination modalities, respectively. The lower EER value of the multimodal system suggests improved performance compared to the individual unimodal systems which indicates that, fusion enhances authentication accuracy.



(a) Fingerprint

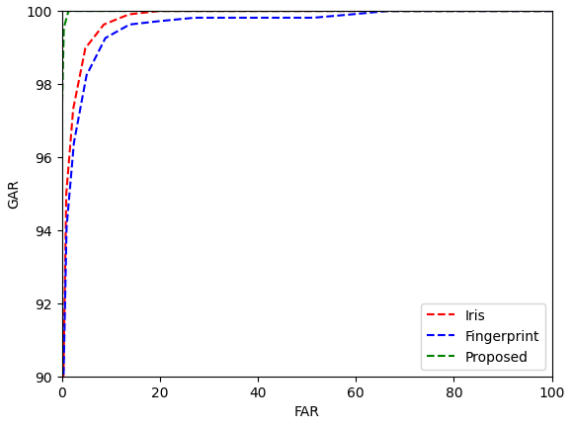
(b) Iris



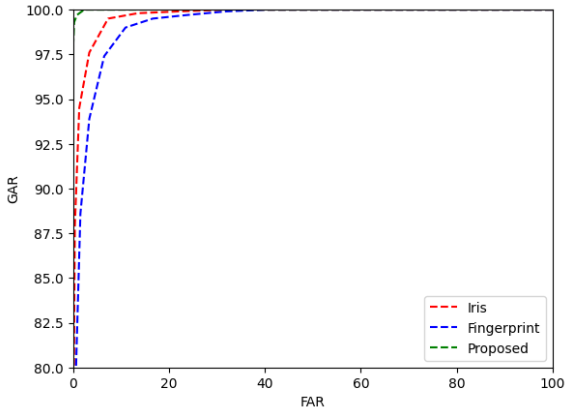
(c) Fusion using Concatenation

Figure 6.5: EER Curves of unimodal and multimodal systems for DB3

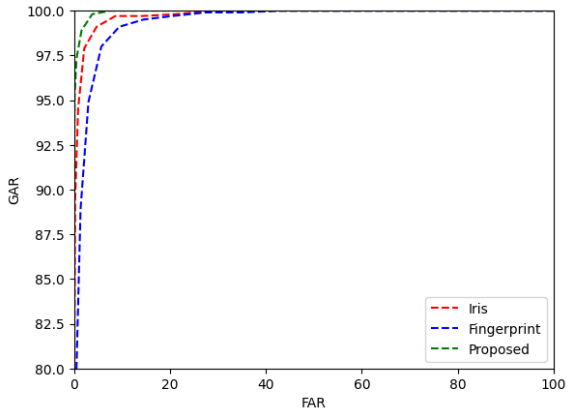
Receiver operating characteristic (ROC) curves were plotted to provide a comprehensive view of the system's performance in terms of FAR and GAR. Figures 6.6a, 6.6b, and 6.6c show the ROC comparisons between unimodal and multimodal systems for DB1, DB2, and DB3, respectively. These ROC curves offer a detailed analysis of the trade-offs between FAR and GAR for various threshold values across the different databases.



(a) DB1



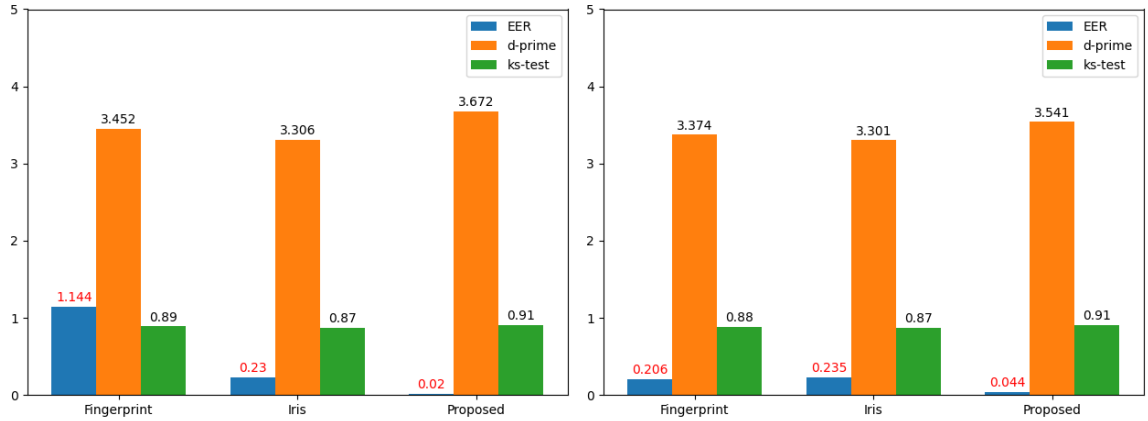
(b) DB2



(c) DB3

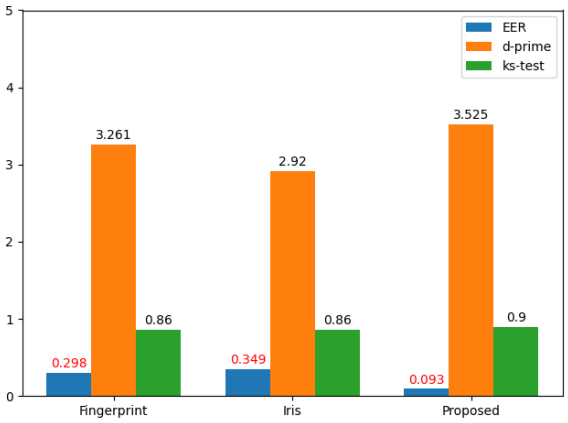
Figure 6.6: Comparison of ROC curves for unimodal and multimodal systems

A detailed comparison of unimodal and multimodal systems is shown in Figure 6.7, wherein the Equal Error Rate (EER%) and the values of separability measures (d' and ks-test) are examined for three different databases: DB1, DB2, and DB3. In Figures 6.7a, 6.7b, and 6.7c, the graphical representation clearly demonstrates the relationship between these metrics. Notably, higher values of separability measures correspond to lower error rates within the systems. This inverse correlation between separability and EER indicates that systems exhibiting stronger separability tend to have reduced error rates.



(a) DB1

(b) DB2



(c) DB3

Figure 6.7: Comparison of EER, d', and ks-test values for unimodal and multimodal systems

6.4 Comaparative Analysis

Table 6.3 provides a comprehensive comparison between the proposed technique and existing methods across various datasets, demonstrating the effectiveness of the proposed method. The proposed approach demonstrates superior efficiency for multimodal biometric authentication, displaying a significantly low Equal Error Rate (EER%) of 0.0201 on DB1, 0.044 on DB2, and 0.093 on DB3. Considering that Gomez et al.'s [142] method using the BiosecurID multimodal database achieved an EER% of 0.12 by employing online signature and fingerprint features, Mahesh et al. [143] on the CASIA-V 1.0 dataset,

which attained an EER% of 0.19 with left and right iris traits. Furthermore, Vallabhadas et al.'s [163] method, concentrating on the CMBD with iris and fingerprint traits, achieved an EER% of 0.021and A. Singh et al.'s [107] work on the Multi-PIE & PTB database, involving face and ECG features, resulted in an EER% of 0.14. Additionally, Sudhakar et al.'s [104] strategy on the FV-USM database, concentrating on index and middle finger-vein traits, acquired an EER% of 0.05 and Talreja et al.'s [120] method on the WVU multimodal database, utilizing face and iris traits, reported a greater EER% of 1.45. The consistently low EER% values demonstrate the robustness and reliability of the proposed approach.

Table 6.3: EER% of the proposed approach vs existing methods on various databases

Method	Database	Traits	EER%
Gomez et al. [142]	BiosecurID multimodal database	Online signature and Fingerprint	0.12
Mahesh et al. [143]	CASIA-V 1.0	Left iris and right iris	0.19
Vallabhadas et al. [163]	Children Multimodal Biometric Database	Iris and Fingerprint	0.021
A. Singh et al. [107]	Multi-PIE & PTB database	Face and ECG	0.14
Sudhakar et al. [104]	FV-USM database	index and middle fingervein	0.05
Talreja et al. [120]	WVU multimodal database	face and iris	1.45
Proposed method	DB1	Iris and Fingerprint	0.0201
Proposed method	DB2	Iris and Fingerprint	0.044
Proposed method	DB3	Iris and Fingerprint	0.093

Table 6.4 compares the proposed method with existing methods across three datasets. (DB1, DB2, and DB3). The proposed method demonstrates superior performance with an Equal Error Rate (EER) of 0.0201 on DB1, outperforming Gomez et al. [142] (EER: 0.128), Mahesh et al. [143] (EER: 0.262), Vallabhadas et al. [163] (EER: 0.021), and Mahesh et al. [164] (EER: 0.16). On DB2, the proposed method achieves an EER of 0.044, surpassing Mustafa et al. [161] (EER: 1.9), but falls short compared to Benaliouche et al. [160] (EER: 0.038). On DB3, the proposed method outperforms Walia et al. [102] (EER: 2.35) and Rajasekar et al. [162] (EER: 0.18) with an EER of 0.093. Importantly, our method outperforms existing methods in terms of both privacy and integrity.

Table 6.4: EER% of the proposed method vs existing methods on various datasets

Method	**Database**	**EER%**
Gomez-Barrero et al. [142]	DB1	0.128
Mahesh et al. [143]		0.262
Vallabhadas et al. [163]		0.021
Mahesh et al. [164]		0.16
Proposed method		0.0201
Benaliouche et al. [160]	DB2	0.038
Mustafa et al. [161]		1.9
Proposed method		0.044
Walia et al. [102]	DB3	2.35
Rajasekar et al. [162]		0.18
Proposed method2		0.093

6.5 Security Analysis

6.5.1 Irreversibility Analysis

As the Block-Xor operation is performed after the features are retrieved, the attacker must know the key for Block-Xor operation to obtain the original data. Furthermore, signcryption is used to convert these extracted features into a template. The keys for this process are produced using a user ID not kept in the database. Additionally, an attacker could not create a feature vector even if they were to gain access to the templates and user ID. This is due to the random generation of keys, determined by points on a curve. As a result, the system maintains its security integrity, effectively preventing any efforts to reconstruct the original feature vector from the obtained templates.

6.5.2 Unlinkability Analysis

By changing the slot (i) utilized in the key generation for the Block-Xor operation, multiple templates can be created for a single user. Considering different values of i for both the iris and fingerprint feature vectors enables the formation of distinct keys. Moreover, the alteration of the block size (b_s) and the curve E used in the signcryption process allows for the construction of different templates for a single user. This illustrates the flexibility of cancelable transformations in the proposed method, enabling the generation of diverse

parameter sets suitable for various applications.

Cross matching attack: When an attacker gains access to a template from one application, the concern arises that this template could potentially be exploited to circumvent security in other applications as well. To avoid such risks, our proposed technique introduces dynamic variations in key parameters like the block size (b_s) and feature slot (i) during the Block-Xor operation. Furthermore, each user is assigned unique sets of private keys (δ_{sk}) and public keys (δ_{pk}) across different applications. This multi-layered approach ensures that even for the same user, distinct templates are generated, significantly enhancing the system's resistance against cross-matching attacks.

6.5.3 Revocability

Revocability guarantees that in the event of a corrupted template, it must be canceled, and a fresh template is constructed with the same biometric data. In our system, we use Block-Xor, which splits the feature vectors (f_{ir}) and f_{fp} into m blocks of size b_s and randomly selects one of them to generate the key. If a template is corrupted, we can adjust the slot (i) and block size (b_s) to create a new one. Additionally, during the signcryption process, private keys (δ_{sk}) and public keys (δ_{pk}) are generated randomly by considering points on a curve. In the event of a compromised template, we can improve security by changing the key and selecting various points on the curve, thereby enhancing the system's overall security.

6.5.4 Record Multiplicity attacks

In this attack scenario, the attacker attempts to solve for the system's solution by constructing an equation from many hacked templates. Our system's Block-xor operation creates the key based on the feature slot (i) and block size (b_s) of the feature vectors f_{ir} and f_{fp}. As a result, without knowledge of the original trait and the exact parameter set used for the Block-Xor operation, the attacker is unable to obtain the features. This approach improves the security and privacy of the biometric system.

6.5.5 Lost key scenario:

In the worst-case scenario, if the attacker has both the template and the keys, they may use extensive guessing to extract the first feature vector from the template. However, the attacker faces enormous complexity because the Block-Xor approach produces keys based on slot (i) and block size (b_s). The selection of slot (i) provides 4l+4 options, where l indicates the length of f_{ir} divided by p or f_{fp} divided by b_s. Additionally, the attacker must predict the block size, b_s. For example, considering rows, columns, or diagonals from a matrix of size n$\times$n needs 2n+2 possibilities. This complex key generation procedure makes it difficult for the attacker to recover the original features from the compromised template.

6.6 Summary

This chapter presents a biometric template protection (BTP) strategy based on feature-level fusion, which combines Block-Xor with signcryption. Features from iris and fingerprint images are initially extracted using VGG-16, then binarized and combined using Block-Xor to create a fused vector. The resulting fused vector is then processed through fully connected (FC) layers to produce a modified vector. This modified vector is then passed to a template creation module, where signcryption is applied to produce secure templates. The effectiveness of the proposed method is assessed using three publicly available datasets. Experimental findings show the method's efficiency, with EER values of 0.0201%, 0.044%, and 0.093%, and d' values of 3.672, 3.541, and 3.542, respectively, compared to existing approaches. These findings highlight the suggested method's high efficiency and privacy preservation.

Chapter 7

Conclusion and Future Scope

This chapter presents the summary of the contributions of this thesis, the conclusion of each objective and the future scope of research for further direction of this thesis is presented.

7.1 Conclusions

This study aims to tackle challenges associated with biometric template protection techniques. By investigating diverse feature extraction methods, incorporating advanced techniques, exploring different types of template protections, and optimizing computational resources, the research aims to provide adaptable solutions suitable for various applications. The ultimate objective is to develop an efficient biometric template protection technique capable of safeguarding templates against various attacks without compromising system performance.

In chapter 3, multimodal template protection was designed using local random projection and Homomorphic encryption. Rotational invariant templates are developed to overcome the problem of rotational inconsistency and increase the system's accuracy. Local random projection is used to reduce the template size and to generate a pseudo template. These templates are encrypted using a fully homomorphic encryption. To minimize the computational cost, a batching scheme is used, which performs several multiplications in encrypted form using a single operation. The main objective of using homomorphic encryption is that operations on user data can be performed in an encrypted domain that

produces a similarity score which is also encrypted. The client device decrypts the score using a private key to verify whether the user is genuine or an imposter.

In chapter 4, an alignment-free multimodal cancelable scheme is developed that combines fingerprint features with iris features at feature-level fusion. First, the fingerprint minutiae points are protected, and a secure shell is constructed in the form of a 2D curve that does not require a singularity point. The fingerprint shell is then quantized to improve the security of the modality. Later, iris characteristics are extracted using a pre-trained CNN model, and feature-based random projection is used to make them irreversible. Finally, the fingerprint quantized array and the iris feature vector combine to generate a secure 3-D shell.

In chapter 5, a biometric template protection technique was developed that combines Deep binarization and feature-hashed random projection. Initially, features are extracted from iris and fingerprint images using VGG-16, which are then binarized and merged to create a fused vector. The obtained fused vector is further processed through AXR and FC layers to obtain a modified vector. Later, the modified vector passes through a cancelable template module where feature-hashed random projection is performed resulting in secured templates. The proposed method is evaluated using two fusion techniques such as concatenation and Xor, on the three datasets.

In chapter 6, a biometric template protection (BTP) strategy based on feature-level fusion, which combines Block-Xor with signcryption. Features from iris and fingerprint images are initially extracted using VGG-16, then binarized and combined using Block-Xor to create a fused vector. The resulting fused vector is then processed through fully connected (FC) layers to produce a modified vector. This modified vector is then passed to a template creation module, where signcryption using hyperelliptic curve cryptography is applied to produce secure templates.

7.2 Future Scope

Future scope for the proposed multimodal template protection schemes can focus on several directions:

- Further research and development efforts should focus on exploring and developing fully homomorphic encryption techniques that offer enhanced security and reduced execution time.

- Research into various fusion techniques, feature extraction methods, and matching algorithms can lead to the discovery of more diverse and effective template protection techniques. This exploration should encompass all biometric traits to ensure comprehensive security.

- The development of hybrid template protection methods, combining the advantages of homomorphic encryption, cancelable and crypto systems. These techniques should enable computations on encrypted data while maintaining high performance and secure transmission and storage of data, ensuring robust template protection.

- Template protection schemes should be evaluated on large-scale databases to validate their effectiveness and significance in real-world scenarios. Conducting evaluations on extensive datasets will provide insights into the scalability and reliability of these techniques.

- Future research should focus on enhancing the security of biometric template protection techniques by implementing dynamic key generation mechanisms. Generating dynamic key sets for each user based on their feature vectors would increase resilience against attacks, particularly brute-force attempts to access template data.

- Incorporating additional biometric traits into the template protection system can enhance its performance and overall security. Research into the compatibility and effectiveness of combining multiple biometric modalities can lead to stronger authentication systems.

- Future developments should aim to create template protection techniques that are resilient against advanced attacks such as machine learning-based attacks, adversarial attacks, quantum attacks and model inversion attacks. Enhancing the robustness of these techniques will ensure long-term security and reliability.

Bibliography

[1] A. Jain, R. Bolle, and S. Pankanti, *Introduction to Biometrics*. Springer, 1996.

[2] L. O'Gorman, "Comparing Passwords, Tokens, and Biometrics for User Authentication," *Proceedings of the IEEE*, vol. 91, no. 12, pp. 2021–2040, 2003.

[3] S. Prabhakar, S. Pankanti, and A. K. Jain, "Biometric Recognition: Security and Privacy Concerns," *IEEE security & privacy*, vol. 1, no. 2, pp. 33–42, 2003.

[4] A. K. Jain, A. Ross, and S. Prabhakar, "An Introduction to Biometric Recognition," *IEEE Transactions on circuits and systems for video technology*, vol. 14, no. 1, pp. 4–20, 2004.

[5] A. K. Jain, R. Bolle, and S. Pankanti, *Biometrics: Personal Identification in Networked Society*. Springer Science & Business Media, 2006.

[6] S. Prabhakar, S. Pankanti, and A. K. Jain, "Biometric Recognition: Security and Privacy Concerns," *IEEE security & privacy*, vol. 1, no. 2, pp. 33–42, 2003.

[7] J. L. Wayman, "Fundamentals of Biometric Authentication Technologies," *International Journal of Image and Graphics*, vol. 1, no. 01, pp. 93–113, 2001.

[8] S. Liu and M. Silverman, "A Practical Guide to Biometric Security Technology," *IT Professional*, vol. 3, no. 1, pp. 27–32, 2001.

[9] R. W. Frischholz and U. Dieckmann, "BiolD: a Multimodal Biometric Identification System," *Computer*, vol. 33, no. 2, pp. 64–68, 2000.

[10] N. K. Ratha, J. H. Connell, and R. M. Bolle, "Enhancing Security and Privacy in Biometrics-Based Authentication Systems," *IBM systems Journal*, vol. 40, no. 3, pp. 614–634, 2001.

[11] S. Kumar, S. Singh, and J. Kumar, "A Comparative Study on Face Spoofing Attacks," in *2017 International Conference on Computing, Communication and Automation (ICCCA)*, pp. 1104–1108, IEEE, 2017.

[12] T. Matsumoto, H. Matsumoto, K. Yamada, and S. Hoshino, "Impact of Artificial "Gummy" Fingers on Fingerprint Systems," in *Optical security and counterfeit deterrence techniques IV*, vol. 4677, pp. 275–289, SPIE, 2002.

[13] A. Antonelli, R. Cappelli, D. Maio, and D. Maltoni, "Fake Finger Detection by Skin Distortion Analysis," *IEEE Transactions on Information Forensics and Security*, vol. 1, no. 3, pp. 360–373, 2006.

[14] R. Agarwal and A. S. Jalal, "Presentation Attack Detection System for Fake Iris: a Review," *Multimedia Tools and Applications*, vol. 80, pp. 15193–15214, 2021.

[15] R. Tolosana, R. Vera-Rodriguez, J. Fierrez, A. Morales, and J. Ortega-Garcia, "Deepfakes and Beyond: A Survey of Face Manipulation and Fake Detection," *Information Fusion*, vol. 64, pp. 131–148, 2020.

[16] A. K. Jain, A. Ross, and U. Uludag, "Biometric Template Security: Challenges and Solutions," in *2005 13th European signal processing conference*, pp. 1–4, IEEE, 2005.

[17] P. Campisi, "Security and Privacy in Biometrics: Towards a Holistic Approach," in *Security and privacy in biometrics*, pp. 1–23, Springer, 2013.

[18] N. Riaz, A. Riaz, and S. A. Khan, "Biometric Template Security: An Overview," *Sensor Review*, vol. 38, no. 1, pp. 120–127, 2018.

[19] A. Nagar, K. Nandakumar, and A. K. Jain, "Biometric Template Transformation: A Security Analysis," in *Media Forensics and Security II*, vol. 7541, pp. 237–251, SPIE, 2010.

[20] E. Chandra and K. Kanagalakshmi, "Cancelable Biometric Template Generation and Protection Schemes: A Review," in *2011 3rd International Conference on Electronics Computer Technology*, vol. 5, pp. 15–20, IEEE, 2011.

[21] 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, 2014.

[22] M. Sandhya and M. V. Prasad, "Biometric Template Protection: A Systematic Literature Review of Approaches and Modalities," *Biometric security and privacy*, pp. 323–370, 2017.

[23] I. Secretary, "Information Technology–Security Techniques–Biometric Information Protection," *International Organization for Standardization, Standard ISO/IEC*, vol. 24745, p. 2011, 2011.

[24] 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.

[25] V. M. Patel, N. K. Ratha, and R. Chellappa, "Cancelable Biometrics: A Review," *IEEE signal processing magazine*, vol. 32, no. 5, pp. 54–65, 2015.

[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] A. B. Teoh, A. Goh, and D. C. Ngo, "Random Multispace Quantization as an Analytic Mechanism for Biohashing of Biometric and Random Identity Inputs," *IEEE transactions on pattern analysis and machine intelligence*, vol. 28, no. 12, pp. 1892–1901, 2006.

[28] A. B. J. Teoh and C. T. Yuang, "Cancelable Biometrics Realization with Multispace Random Projections," *IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics)*, vol. 37, no. 5, pp. 1096–1106, 2007.

[29] S. Hirata and K. Takahashi, "Cancelable Biometrics with Perfect Secrecy for Correlation-Based Matching," in *Advances in Biometrics: Third International Conference, ICB 2009, Alghero, Italy, June 2-5, 2009. Proceedings 3*, pp. 868–878, Springer, 2009.

[30] O. Ouda, N. Tsumura, and T. Nakaguchi, "Tokenless Cancelable Biometrics Scheme for Protecting Iris Codes," in *2010 20th international conference on pattern recognition*, pp. 882–885, IEEE, 2010.

[31] K. H. Cheung, A. Kong, J. You, and D. Zhang, "An Analysis on Invertibility of Cancelable Biometrics based on BioHashing.," in *2005 International Conference on Imaging Science, Systems, and Technology: Computer Graphics, CISST'05*, pp. 40–45, 2005.

[32] 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.

[33] J. Hämmerle-Uhl, E. Pschernig, and A. Uhl, "Cancelable Iris Biometrics using Block Re-Mapping and Image Warping," in *International conference on information security*, pp. 135–142, Springer, 2009.

[34] E. Maiorana, P. Campisi, J. Fierrez, J. Ortega-Garcia, and A. Neri, "Cancelable Templates for Sequence-Based Biometrics with Application to OnLine Signature Recognition," *IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans*, vol. 40, no. 3, pp. 525–538, 2010.

[35] L. Nanni, E. Maiorana, A. Lumini, and P. Campisi, "Cancelable Templates for Sequence-Based Biometrics with Application to Online Signature Recognition," *Expert Systems with Applications*, vol. 37, no. 5, pp. 3676–3684, 2010.

[36] S. Z. Li and A. Jain, *Encyclopedia of Biometrics*. Springer Publishing Company, Incorporated, 2015.

[37] U. Uludag, S. Pankanti, S. Prabhakar, and A. K. Jain, "Biometric Cryptosystems: Issues and Challenges," *Proceedings of the IEEE*, vol. 92, no. 6, pp. 948–960, 2004.

[38] A. Juels and M. Sudan, "A Fuzzy Vault Scheme," *Designs, Codes and Cryptography*, vol. 38, pp. 237–257, 2006.

[39] 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.

[40] Y. J. Lee, K. R. Park, S. J. Lee, K. Bae, and J. Kim, "A New Method for Generating an Invariant Iris Private Key Based on the Fuzzy Vault System," *IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics)*, vol. 38, no. 5, pp. 1302–1313, 2008.

[41] T. H. Nguyen, Y. Wang, Y. Ha, and R. Li, "Performance and Security-Enhanced Fuzzy Vault Scheme Based on Ridge Features for Distorted Fingerprints," *IET Biometrics*, vol. 4, no. 1, pp. 29–39, 2015.

[42] C. Feng, M. Fang, X.-Y. Liu, *et al.*, "The Neurobiological Pathogenesis of Poststroke Depression," *The Scientific World Journal*, vol. 2014, 2014.

[43] A. Juels, "Encryption Basics," *Handbook of Information Security: threats, vulnerabilities, prevention, detection, and management*, vol. 2, pp. 469–478, 2006.

[44] C. Soutar, D. Roberge, A. Stoianov, R. Gilroy, and B. V. Kumar, "Biometric Encryption using Image Processing," in *Optical Security and Counterfeit Deterrence Techniques II*, vol. 3314, pp. 178–188, SPIE, 1998.

[45] F. Hao, R. Anderson, and J. Daugman, "Combining Crypto with Biometrics Effectively," *IEEE transactions on computers*, vol. 55, no. 9, pp. 1081–1088, 2006.

[46] M. Haghighat, S. Zonouz, and M. Abdel-Mottaleb, "Identification using Encrypted Biometrics," in *Computer Analysis of Images and Patterns: 15th International Conference, CAIP 2013, York, UK, August 27-29, 2013, Proceedings, Part II 15*, pp. 440–448, Springer, 2013.

[47] V. Kakkad, M. Patel, and M. Shah, "Biometric Authentication and Image Encryption for Image Security in Cloud Framework," *Multiscale and Multidisciplinary Modeling, Experiments and Design*, vol. 2, no. 4, pp. 233–248, 2019.

[48] A. Juels and M. Wattenberg, "A Fuzzy Commitment Scheme," in *Proceedings of the 6th ACM conference on Computer and communications security*, pp. 28–36, 1999.

[49] A. B. J. Teoh and J. Kim, "Secure Biometric Template Protection in Fuzzy Commitment Scheme," *IEICE Electronics Express*, vol. 4, no. 23, pp. 724–730, 2007.

[50] E. Maiorana, P. Campisi, and A. Neri, "User Adaptive Fuzzy Commitment for Signature Template Protection and Renewability," *Journal of Electronic Imaging*, vol. 17, no. 1, pp. 011011–011011, 2008.

[51] C. Rathgeb and A. Uhl, "Systematic Construction of Iris-Based Fuzzy Commitment Schemes," in *International Conference on Biometrics*, pp. 940–949, Springer, 2009.

[52] E. Maiorana and P. Campisi, "Fuzzy Commitment for Function Based Signature Template Protection," *IEEE signal processing letters*, vol. 17, no. 3, pp. 249–252, 2009.

[53] C. Rathgeb and A. Uhl, "A Survey on Biometric Cryptosystems and Cancelable Biometrics," *EURASIP journal on information security*, vol. 2011, no. 1, pp. 1–25, 2011.

[54] 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.

[55] C. Fang, Q. Li, and E.-C. Chang, "Secure Sketch for Multiple Secrets," in *Applied Cryptography and Network Security: 8th International Conference, ACNS 2010, Beijing, China, June 22-25, 2010. Proceedings 8*, pp. 367–383, Springer, 2010.

[56] Y. Sutcu, Q. Li, and N. Memon, "Protecting Biometric Templates with Sketch: Theory and Practice," *IEEE Transactions on Information Forensics and Security*, vol. 2, no. 3, pp. 503–512, 2007.

[57] R. Chatterjee, M. S. Riazi, T. Chowdhury, E. Marasco, F. Koushanfar, and A. Juels, "Multisketches: Practical Secure Sketches using off-the-shelf Biometric Matching Algorithms," in *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, pp. 1171–1186, 2019.

[58] 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.

[59] W. Yang, J. Hu, S. Wang, and M. Stojmenovic, "An Alignment-Free Fingerprint Bio-Cryptosystem based on Modified Voronoi Neighbor Structures," *Pattern Recognition*, vol. 47, no. 3, pp. 1309–1320, 2014.

[60] R. Ranjan and S. K. Singh, "Improved and Innovative Key Generation Algorithms for Biometric Cryptosystems," in *2013 3rd IEEE International Advance Computing Conference (IACC)*, pp. 943–946, IEEE, 2013.

[61] L. Wu, X. Liu, S. Yuan, and P. Xiao, "A Novel Key Generation Cryptosystem based on Face Features," in *IEEE 10th International Conference on Signal Processing Proceedings*, pp. 1675–1678, IEEE, 2010.

[62] S. Hoque, M. Fairhurst, and G. Howells, "Evaluating Biometric Encryption Key Generation using Handwritten Signatures," in *2008 Bio-inspired, Learning and Intelligent Systems for Security*, pp. 17–22, IEEE, 2008.

[63] Y. C. Feng, P. C. Yuen, and A. K. Jain, "A Hybrid Approach for Generating Secure and Discriminating Face Template," *IEEE transactions on information forensics and security*, vol. 5, no. 1, pp. 103–117, 2009.

[64] A. Nagar, K. Nandakumar, and A. K. Jain, "A Hybrid Biometric Cryptosystem for Securing Fingerprint Minutiae Templates," *Pattern recognition letters*, vol. 31, no. 8, pp. 733–741, 2010.

[65] H. Liu, D. Sun, K. Xiong, and Z. Qiu, "A Hybrid Approach to Protect Palmprint Templates," *The Scientific World Journal*, vol. 2014, no. 1, p. 686754, 2014.

[66] A. Kumar and A. Kumar, "A Cell-Array-Based Multibiometric Cryptosystem," *IEEE access*, vol. 4, pp. 15–25, 2015.

[67] M. Sandhya and M. V. Prasad, "Cancelable Fingerprint Cryptosystem based on Convolution Coding," in *Advances in Signal Processing and Intelligent Recognition Systems: Proceedings of Second International Symposium on Signal Processing and Intelligent Recognition Systems (SIRS-2015) December 16-19, 2015, Trivandrum, India*, pp. 145–157, Springer, 2016.

[68] Z. Jin, A. B. J. Teoh, B.-M. Goi, and Y.-H. Tay, "Biometric Cryptosystems: A new Biometric Key Binding and its Implementation for Fingerprint Minutiae-Based Representation," *Pattern Recognition*, vol. 56, pp. 50–62, 2016.

[69] C. Fontaine and F. Galand, "A Survey of Homomorphic Encryption for Nonspecialists," *EURASIP Journal on Information Security*, vol. 2007, pp. 1–10, 2007.

[70] P. V. Parmar, S. B. Padhar, S. N. Patel, N. I. Bhatt, and R. H. Jhaveri, "Survey of various Homomorphic Encryption Algorithms and Schemes," *International Journal of Computer Applications*, vol. 91, no. 8, 2014.

[71] A. Acar, H. Aksu, A. S. Uluagac, and M. Conti, "A Survey on Homomorphic Encryption Schemes: Theory and Implementation," *ACM Computing Surveys (Csur)*, vol. 51, no. 4, pp. 1–35, 2018.

[72] W. Diffie and M. E. Hellman, "New Directions in Cryptography," in *Democratizing Cryptography: The Work of Whitfield Diffie and Martin Hellman*, pp. 365–390, 2022.

[73] T. ElGamal, "A Public Key Cryptosystem and a Signature Scheme based on Discrete Logarithms," *IEEE transactions on information theory*, vol. 31, no. 4, pp. 469–472, 1985.

[74] S. D. Galbraith, "Elliptic Curve Paillier Schemes," *Journal of Cryptology*, vol. 15, pp. 129–138, 2002.

[75] T. Okamoto and S. Uchiyama, "A new Public-Key Cryptosystem as Secure as Factoring," in *Advances in Cryptology—EUROCRYPT'98: International Conference on the Theory and Application of Cryptographic Techniques Espoo, Finland, May 31–June 4, 1998 Proceedings 17*, pp. 308–318, Springer, 1998.

[76] A. C. Yao, "Protocols for Secure Computations," in *23rd annual symposium on foundations of computer science (sfcs 1982)*, pp. 160–164, IEEE, 1982.

[77] T. Sander, A. Young, and M. Yung, "Non-Interactive Cryptocomputing for NC/SUP 1," in *40th Annual Symposium on Foundations of Computer Science (Cat. No. 99CB37039)*, pp. 554–566, IEEE, 1999.

[78] D. Boneh, E.-J. Goh, and K. Nissim, "Evaluating 2-DNF Formulas on Ciphertexts," in *Theory of Cryptography: Second Theory of Cryptography Conference, TCC 2005, Cambridge, MA, USA, February 10-12, 2005. Proceedings 2*, pp. 325–341, Springer, 2005.

[79] Y. Ishai and A. Paskin, "Evaluating Branching Programs on Encrypted Data," in *Theory of Cryptography Conference*, pp. 575–594, Springer, 2007.

[80] W. A. A. Torres, N. Bhattacharjee, and B. Srinivasan, "Effectiveness of Fully Homomorphic Encryption to Preserve the Privacy of Biometric Data," in *Proceedings of the 16th International Conference on Information Integration and Web-based Applications & Services*, pp. 152–158, 2014.

[81] W. A. Alberto Torres, N. Bhattacharjee, and B. Srinivasan, "Privacy-Preserving Biometrics Authentication Systems using Fully Homomorphic Encryption," *International Journal of Pervasive Computing and Communications*, vol. 11, no. 2, pp. 151–168, 2015.

[82] A. K. Jindal, I. Shaik, V. Vasudha, S. R. Chalamala, R. Ma, and S. Lodha, "Secure and Privacy Preserving Method for Biometric Template Protection using Fully Homomorphic Encryption," in *2020 IEEE 19th international conference on trust, security and privacy in computing and communications (TrustCom)*, pp. 1127–1134, IEEE, 2020.

[83] V. N. Boddeti, "Secure Face Matching using Fully Homomorphic Encryption," in *2018 IEEE 9th international conference on biometrics theory, applications and systems (BTAS)*, pp. 1–10, IEEE, 2018.

[84] K. Delac and M. Grgic, "A Survey of Biometric Recognition Methods," in *Proceedings. Elmar-2004. 46th International Symposium on Electronics in Marine*, pp. 184–193, IEEE, 2004.

[85] M. Gudavalli, S. V. Raju, A. V. Babu, and D. S. Kumar, "Multimodal Biometrics–Sources, Architecture and Fusion Techniques: An Overview," in *2012 International Symposium on Biometrics and Security Technologies*, pp. 27–34, IEEE, 2012.

[86] J. Fiérrez-Aguilar, J. Ortega-Garcia, D. Garcia-Romero, and J. Gonzalez-Rodriguez, "A comparative evaluation of fusion strategies for multimodal biometric verification," in *Audio-and Video-Based Biometric Person Authentication: 4th International Conference, AVBPA 2003 Guildford, UK, June 9–11, 2003 Proceedings 4*, pp. 830–837, Springer, 2003.

[87] A. Aftab, F. A. Khan, M. K. Khan, H. Abbas, W. Iqbal, and F. Riaz, "Hand-based multibiometric systems: State-of-the-art and future challenges," *PeerJ Computer Science*, vol. 7, p. e707, 2021.

[88] J. Fierrez-Aguilar, Y. Chen, J. Ortega-Garcia, and A. K. Jain, "Incorporating Image Quality in Multi-Algorithm Fingerprint Verification," in *International Conference on Biometrics*, pp. 213–220, Springer, 2006.

[89] M. Sandhya, Y. Sreenivasa Rao, S. Biswajeet, V. Dilip Kumar, and M. Anup Kumar, "A Score-Level Fusion Method for Protecting Fingerprint and Palmprint Templates," in *Security and Privacy*, pp. 1–11, Springer, 2021.

[90] P. Punyani, R. Gupta, and A. Kumar, "A Multimodal Biometric System using Match Score and Decision Level Fusion," *International Journal of Information Technology*, vol. 14, no. 2, pp. 725–730, 2022.

[91] A. K. Jain, P. Flynn, and A. A. Ross, *Handbook of Biometrics*. Springer Science & Business Media, 2007.

[92] B. Abd El-Rahiem, F. E. Abd El Samie, and M. Amin, "Efficient Cancellable Multi-Biometric Recognition System based on Deep Learning and Bio-Hashing," *Applied Intelligence*, vol. 53, no. 2, pp. 1792–1806, 2023.

[93] Z. H. Goh, Y. Wang, L. Leng, S.-N. Liang, Z. Jin, Y.-L. Lai, and X. Wang, "A Framework for Multimodal Biometric Authentication Systems with Template Protection," *IEEE Access*, vol. 10, pp. 96388–96402, 2022.

[94] F. Bedad, N. Bousahba, and I. Bennadji, "Protection of Multi-Biometric Data based on Deep Learning and BioHashing," in *2023 International Conference on Electrical Engineering and Advanced Technology (ICEEAT)*, vol. 1, pp. 1–6, IEEE, 2023.

[95] M. Khurshid and A. Selwal, "A Novel Block Hashing-Based Template Security Scheme for Multimodal Biometric System," *Decision Analytics Applications in Industry*, pp. 173–183, 2020.

[96] D. Zhong, H. Shao, and X. Du, "A Hand-based Multi-Biometrics via Deep Hashing Network and Biometric Graph Matching," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 12, pp. 3140–3150, 2019.

[97] R.-H. Jeng and W.-S. Chen, "Two Feature-Level Fusion Methods with Feature Scaling and Hashing for Multimodal Biometrics," *IETE Technical Review*, vol. 34, no. 1, pp. 91–101, 2017.

[98] C. Rathgeb and C. Busch, "Cancelable Multi-Biometrics: Mixing Iris-Codes based on Adaptive Bloom Filters," *Computers & Security*, vol. 42, pp. 1–12, 2014.

[99] R. Dwivedi and S. Dey, "A Novel Hybrid Score Level and Decision Level Fusion Scheme for Cancelable Multi-Biometric Verification," *Applied Intelligence*, vol. 49, no. 3, pp. 1016–1035, 2019.

[100] W. Yang, S. Wang, J. Hu, G. Zheng, and C. Valli, "A Fingerprint and Finger-Vein Based Cancelable Multi-Biometric System," *Pattern Recognition*, vol. 78, pp. 242–251, 2018.

[101] S. Ghouzali, O. Nafea, A. Wadood, and M. Hussain, "Cancelable Multimodal Biometrics based on Chaotic Maps," *Applied Sciences*, vol. 11, no. 18, p. 8573, 2021.

[102] G. S. Walia, G. Jain, N. Bansal, and K. Singh, "Adaptive weighted graph approach to generate multimodal cancelable biometric templates," *IEEE transactions on information forensics and security*, vol. 15, pp. 1945–1958, 2019.

[103] K. Gupta, G. S. Walia, and K. Sharma, "Novel Approach for Multimodal Feature Fusion to Generate Cancelable Biometric," *The Visual Computer*, vol. 37, no. 6, pp. 1401–1413, 2021.

[104] T. Sudhakar and M. Gavrilova, "Deep Learning for Multi-Instance Biometric Privacy," *ACM Transactions on Management Information Systems (TMIS)*, vol. 12, no. 1, pp. 1–23, 2020.

[105] E. Abdellatef, N. A. Ismail, S. E. S. Abd Elrahman, K. N. Ismail, M. Rihan, and F. E. Abd El-Samie, "Cancelable Multi-Biometric Recognition System based on Deep Learning," *The Visual Computer*, vol. 36, pp. 1097–1109, 2020.

[106] B. A. El-Rahiem, M. Amin, A. Sedik, F. E. A. E. Samie, and A. M. Iliyasu, "An Efficient Multi-Biometric Cancellable Biometric Scheme based on Deep Fusion and Deep Dream," *Journal of Ambient Intelligence and Humanized Computing*, pp. 1–13, 2021.

[107] A. Singh and Y. N. Singh, "Cancelable Multibiometrics Template Security using Deep Binarization and Secure Hashing," *International Journal of Pattern Recognition and Artificial Intelligence*, vol. 37, no. 05, p. 2356007, 2023.

[108] S. Kanade, D. Petrovska-Delacrétaz, and B. Dorizzi, "Obtaining Cryptographic Keys using Feature Level Fusion of Iris And Face Biometrics for Secure User Authentication," in *2010 IEEE Computer Society Conference on Computer Vision and Pattern Recognition-Workshops*, pp. 138–145, IEEE, 2010.

[109] G. Mai, M.-H. Lim, and P. C. Yuen, "Binary feature fusion for discriminative and secure multi-biometric cryptosystems," *Image and Vision Computing*, vol. 58, pp. 254–265, 2017.

[110] R. Sreemol, M. S. Kumar, and A. Sreekumar, "Improvement of Security in Multi-Biometric Cryptosystem by Modulus Fuzzy Vault Algorithm," in *2021 International Conference on Advances in Computing and Communications (ICACC)*, pp. 1–7, IEEE, 2021.

[111] N. Lalithamani and M. Sabrigiriraj, "Palm and Hand Vein-Based Fuzzy Vault Generation Scheme for Multibiometric Cryptosystem," *The Imaging Science Journal*, vol. 63, no. 2, pp. 111–118, 2015.

[112] G. Amirthalingam and G. Radhamani, "New chaff point based fuzzy vault for multimodal biometric cryptosystem uusing particle swarm optimization," *Journal of King Saud University-Computer and Information Sciences*, vol. 28, no. 4, pp. 381–394, 2016.

[113] V. Sujitha and D. Chitra, "A Novel Technique for Multi Biometric Cryptosystem using Fuzzy Vault," *Journal of medical systems*, vol. 43, no. 5, pp. 1–9, 2019.

[114] T. K. Dang, Q. C. Truong, T. T. B. Le, and H. Truong, "Cancellable Fuzzy Vault with Periodic Transformation for Biometric Template Protection," *IET Biometrics*, vol. 5, no. 3, pp. 229–235, 2016.

[115] D. Chang, S. Garg, M. Ghosh, and M. Hasan, "BIOFUSE: A Framework for Multi-Biometric Fusion on Biocryptosystem Level," *Information Sciences*, vol. 546, pp. 481–511, 2021.

[116] A. Arora and R. Miri, "Cryptography and Tay-Grey Wolf Optimization based Multimodal Biometrics for Effective Security," *Multimedia Tools and Applications*, pp. 1–23, 2022.

[117] P. S. Chanukya and T. Thivakaran, "Multimodal Biometric Cryptosystem for Human Authentication using Fingerprint and Ear," *Multimedia Tools and Applications*, vol. 79, no. 1, pp. 659–673, 2020.

[118] S. K. Choudhary and A. K. Naik, "Multimodal Biometric-based Authentication with Secured Templates," *International Journal of Image and Graphics*, vol. 21, no. 02, p. 2150018, 2021.

[119] 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, 2011.

[120] V. Talreja, M. C. Valenti, and N. M. Nasrabadi, "Deep Hashing for Secure Multimodal Biometrics," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 1306–1321, 2020.

[121] B. Ma, Y. Wang, C. Li, Z. Zhang, and D. Huang, "Secure Multimodal Biometric Authentication with Wavelet Quantization Based Fingerprint Watermarking," *Multimedia tools and applications*, vol. 72, pp. 637–666, 2014.

[122] D. Chang, S. Garg, M. Hasan, and S. Mishra, "Cancelable Multi-Biometric Approach using Fuzzy Extractor and Novel Bit-Wise Encryption," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 3152–3167, 2020.

[123] E. K. Zaghouani, A. Benzina, and R. Attia, "ECG Biometric Template Protection based on Secure Sketch Scheme," in *2017 25th International Conference on Software, Telecommunications and Computer Networks (SoftCOM)*, pp. 1–5, IEEE, 2017.

[124] B. Ma, C. Li, Y. Wang, Z. Zhang, and Y. Wang, "Block Pyramid based Adaptive Quantization Watermarking for Multimodal Biometric Authentication," in *2010 20th International Conference on Pattern Recognition*, pp. 1277–1280, IEEE, 2010.

[125] T. Kaur and M. Kaur, "Cryptographic Key Generation from Multimodal Template using Fuzzy Extractor," in *2017 Tenth International Conference on Contemporary Computing (IC3)*, pp. 1–6, IEEE, 2017.

[126] N. Bousnina, S. Ghouzali, M. Mikram, M. Lafkih, O. Nafea, M. Al-Razgan, and W. Abdul, "Hybrid Multimodal Biometric Template Protection," *Intell. Autom. Soft Comput*, vol. 27, no. 1, pp. 35–51, 2021.

[127] L. Yuan, "Multimodal Cryptosystem based on Fuzzy Commitment," in *2014 IEEE 17th International Conference on Computational Science and Engineering*, pp. 1545–1549, IEEE, 2014.

[128] O. Nafea, S. Ghouzali, W. Abdul, and E.-u.-H. Qazi, "Hybrid Multi-Biometric Template Protection using Watermarking," *The Computer Journal*, vol. 59, no. 9, pp. 1392–1407, 2016.

[129] A. Selwal, S. K. Gupta, and Surender, "Low Overhead Octet Indexed Template Security Scheme for Multi-Modal Biometric System," *Journal of Intelligent & Fuzzy Systems*, vol. 32, no. 5, pp. 3325–3337, 2017.

[130] Y. J. Chin, T. S. Ong, A. B. J. Teoh, and K. Goh, "Integrated Biometrics Template Protection Technique Based on Fingerprint and Palmprint Feature-Level Fusion," *Information Fusion*, vol. 18, pp. 161–174, 2014.

[131] W. Abdul, O. Nafea, and S. Ghouzali, "Combining Watermarking and Hyper-Chaotic Map to Enhance the Security of Stored Biometric Templates," *The Computer Journal*, vol. 63, no. 3, pp. 479–493, 2020.

[132] G. Zhao, Q. Jiang, D. Wang, X. Ma, and X. Li, "Deep Hashing based Cancelable Multi-biometric Template Protection," *IEEE Transactions on Dependable and Secure Computing*, 2023.

[133] M. Mahesh Kumar, M. V. Prasad, and U. Raju, "BMIAE: Blockchain-based Multi-Instance Iris Authentication using Additive Elgamal Homomorphic Encryption," *IET Biometrics*, vol. 9, no. 4, pp. 165–177, 2020.

[134] M. K. Morampudi, N. Gonthina, S. Bojjagani, N. K. Sharma, and D. Veeraiah, "Reliable and Privacy-Preserving Multi-Instance Iris Verification using Paillier Homomorphic Encryption and One-Digit Checksum," *Signal, Image and Video Processing*, pp. 1–13, 2024.

[135] M. Barni *et al.*, "A Privacy-Compliant Fingerprint Recognition System based on Homomorphic Encryption and Fingercode Templates," in *2010 Fourth IEEE International Conference on Biometrics: Theory, Applications and Systems (BTAS)*, pp. 1–7, IEEE, 2010.

[136] M. Upmanyu, A. M. Namboodiri, K. Srinathan, and C. Jawahar, "Blind Authentication: A Secure Crypto-Biometric Verification Protocol," *IEEE transactions on information forensics and security*, vol. 5, no. 2, pp. 255–268, 2010.

[137] H. Kikuchi, K. Nagai, W. Ogata, and M. Nishigaki, "Privacy-Preserving Similarity Evaluation and Application to Remote Biometrics Authentication," *Soft computing*, vol. 14, no. 5, pp. 529–536, 2010.

[138] M. Barni, G. Droandi, R. Lazzeretti, and T. Pignata, "SEMBA: Secure Multi-Biometric Authentication," *IET Biometrics*, vol. 8, no. 6, pp. 411–421, 2019.

[139] A. Abidin and A. Mitrokotsa, "Security Aspects of Privacy-Preserving Biometric Authentication based on Ideal Lattices and Ring-LWE," in *2014 IEEE International Workshop on Information Forensics and Security (WIFS)*, pp. 60–65, IEEE, 2014.

[140] J. H. Cheon, H. Chung, M. Kim, and K.-W. Lee, "Ghostshell: Secure Biometric Authentication using Integrity-based Homomorphic Evaluations," *Cryptology ePrint Archive*, 2016.

[141] M. Yasuda, T. Shimoyama, J. Kogure, K. Yokoyama, and T. Koshiba, "Secure Pattern Matching using Somewhat Homomorphic Encryption," in *Proceedings of the 2013 ACM workshop on Cloud computing security workshop*, pp. 65–76, 2013.

[142] M. Gomez-Barrero, E. Maiorana, J. Galbally, P. Campisi, and J. Fierrez, "Multi-Biometric Template Protection based on Homomorphic Encryption," *Pattern Recognition*, vol. 67, pp. 149–163, 2017.

[143] M. K. Morampudi, M. V. Prasad, and U. Raju, "Privacy-Preserving Iris Authentication using Fully Homomorphic Encryption," *Multimedia Tools and Applications*, vol. 79, no. 27, pp. 19215–19237, 2020.

[144] L. Sperling, N. Ratha, A. Ross, and V. N. Boddeti, "HEFT: Homomorphically Encrypted Fusion of Biometric Templates," in *2022 IEEE International Joint Conference on Biometrics (IJCB)*, pp. 1–10, IEEE, 2022.

[145] M. Salem, S. Taheri, and J.-S. Yuan, "Utilizing Transfer Learning and Homomorphic Encryption in a Privacy Preserving and Secure Biometric Recognition System," *Computers*, vol. 8, no. 1, p. 3, 2018.

[146] W. A. A. Torres, N. Bhattacharjee, and B. Srinivasan, "Privacy-Preserving Biometrics Authentication Systems using Fully Homomorphic Encryption," *International Journal of Pervasive Computing and Communications*, 2015.

[147] E. Bingham and H. Mannila, "Random Projection in Dimensionality Reduction: Applications to Image and Text Dataa," in *Proceedings of the seventh ACM SIGKDD international conference on Knowledge discovery and data mining*, pp. 245–250, 2001.

[148] N. P. Smart and F. Vercauteren, "Fully Homomorphic Encryption with Relatively Small Key and Ciphertext Sizes," in *International Workshop on Public Key Cryptography*, pp. 420–443, Springer, 2010.

[149] C. Rathgeb, F. Struck, and C. Busch, "Efficient BSIF-based Near-Infrared Iris Recognition," in *Proceedings of International Conference on Image Processing Theory, Tools and Applications (IPTA'16)*, 2016.

[150] P. L'ecuyer, "Tables of Linear Congruential Generators of Different Sizes and Good Lattice Structure," *Mathematics of Computation*, vol. 68, no. 225, pp. 249–260, 1999.

[151] A. J. Titus, S. Kishore, T. Stavish, S. M. Rogers, and K. Ni, "Pyseal: A Python Wrapper Implementation of the SEAL Homomorphic Encryption Library," *arXiv preprint arXiv:1803.01891*, 2018.

[152] M. Mosca, "Cybersecurity in an Era with Quantum Computers: will we be ready?," *IEEE Security & Privacy*, vol. 16, no. 5, pp. 38–41, 2018.

[153] J. Fan and F. Vercauteren, "Somewhat Practical Fully Homomorphic Encryption." Cryptology ePrint Archive, Report 2012/144, 2012.

[154] P. Basak, S. De, M. Agarwal, A. Malhotra, M. Vatsa, and R. Singh, "Multimodal Biometric Recognition for Toddlers and Pre-School Children," in *2017 IEEE International Joint Conference on Biometrics (IJCB)*, pp. 627–633, IEEE, 2017.

[155] J. Kim and A. Yun, "Secure Fully Homomorphic Authenticated Encryption," *IEEE Access*, vol. 9, pp. 107279–107297, 2021.

[156] "Chinese Academy of Science—Institute of Automation, CASIA Iris Image Database Version 1.0 (CASIA-IrisV1)." http://biometrics.idealtest.org/. Accessed: 03-13-2024.

[157] "FVC2004: Third Fingerprint Verification Competition, author=Maio, Dario and Maltoni, Davide and Cappelli, Raffaele and Wayman, Jim L and Jain, Anil K, booktitle=International conference on biometric authentication, pages=1–7, year=2004, organization=Springer,"

[158] "Chinese Academy of Science—Institute of Automation, CASIA Iris Image Database Version 3.0 (CASIA-IrisV3)." http://biometrics.idealtest.org/#/datasetDetail/3. Accessed: 03-13-2024.

[159] R. Cappelli, M. Ferrara, A. Franco, and D. Maltoni, "Fingerprint Verification Competition 2006," *Biometric Technology Today*, vol. 15, no. 7-8, pp. 7–9, 2007.

[160] H. Benaliouche and M. Touahria, "Comparative Study of Multimodal Biometric Recognition by Fusion of Iris and Fingerprint," *The Scientific World Journal*, vol. 2014, 2014.

[161] A. S. Mustafa, A. J. Abdulelah, and A. K. Ahmed, "Multimodal Biometric System Iris and Fingerprint Recognition based on Fusion Technique," *International Journal of Advanced Science and Technology*, vol. 29, pp. 7423–7432, 2020.

[162] V. Rajasekar, B. Predić, M. Saracevic, M. Elhoseny, D. Karabasevic, D. Stanujkic, and P. Jayapaul, "Enhanced Multimodal Biometric Recognition Approach for Smart Cities Based on an Optimized Fuzzy Genetic Algorithm," *Scientific Reports*, vol. 12, no. 1, pp. 1–11, 2022.

[163] D. K. Vallabhadas and M. Sandhya, "Securing Multimodal Biometric Template using Local Random Projection and Homomorphic Encryption," *Journal of Information Security and Applications*, vol. 70, p. 103339, 2022.

[164] M. K. Morampudi, M. Sandhya, and M. Dileep, "Privacy-Preserving Bimodal Authentication System using Fan-Vercauteren Scheme," *Optik*, vol. 274, p. 170515, 2023.

[165] L. Torrey and J. Shavlik, "Transfer Learning," in *Handbook of research on machine learning applications and trends: algorithms, methods, and techniques*, pp. 242–264, IGI global, 2010.

[166] K. Simonyan and A. Zisserman, "Very Deep Convolutional Networks for Large-Scale Image Recognition," *arXiv preprint arXiv:1409.1556*, 2014.

[167] M. Yung, *Practical Signcryption*. Springer Science & Business Media, 2010.

List of Publications

Publications from the Thesis

Journal papers:

1. **D. K. Vallabhadas** and M. Sandhya, “Securing Multimodal Biometric Template using Local Random Projection and Homomorphic Encryption,” *Journal of Information Security and Applications*, vol. 70, p. 103339, 2022. (**Published**, Indexing: SCIE, IF: 5.6, Publisher: Elsevier)

2. **D. K. Vallabhadas** and M. Sandhya, “Cancelable Bimodal Shell using Fingerprint and Iris,” *Journal of Electronic Imaging*, vol. 32, no. 6, p. 063027–063027, 2023. (Published, Indexing: SCIE, IF: 1.1, Publisher: SPIE).

3. **D. K. Vallabhadas**, and M. Sandhya. "Multimodal Template Protection using Deep Binarization and Feature-Hashed Random Projection." *Signal, Image and Video Processing*. (**Under review**, Indexing: SCIE, IF: 2.3, Publisher: Springer).

4. **D. K. Vallabhadas**, and M. Sandhya. "Securing Multimodal Templates with Block-Xor and Signcryption" *Multimedia Tools and Applications*. (**Submitted**, Indexing: SCIE, IF: 3.0, Publisher: Springer)

Other publications related to Thesis

Journal papers:

5. **D. K. Vallabhadas**, M. Sandhya, S. D. Reddy, D. Satwika, and G. L. Prashanth, “Biometric template protection based on a cancelable convolutional neural network over iris and fingerprint,” *Biomedical Signal Processing and Control*, vol. 91, p. 106006, 2024. (**Published**, Indexing: SCIE, IF: 5.1, Publisher: Elsevier)

6. **D. K. Vallabhadas**, M. K. Morampudi, M. Sandhya, P. Maheshwari, and M. Kadyan, “Cancelable Bimodal Shell using Fingerprint and Iris,” *Journal of Electronic Imaging*, vol. 32, no. 1, p. 013027-013027, 2023. (Published, Indexing: SCIE, IF: 1.1, Publisher: SPIE).

7. M. Sandhya, **D. K. Vallabhadas**, and S. Rathod, “Revocable iris templates using partial sort and randomised look-up table mapping,” *International Journal of Biometrics*, vol. 15, no. 1, p. 21-39, 2023. (**Published**, Indexing: ESCI, IF: 0.81, Publisher: INDERSCIENCE).

Conference papers:

8. **V. Dilip Kumar**, M. Sandhya, S. Sarkar, and Y. Rupesh Chandra, "Multimodal Biometric Authentication Using Fully Homomorphic Encryption," in *2023 2nd International Conference on Paradigm Shifts in Communications Embedded Systems, Machine Learning and Signal Processing (PCEMS)*, pp. 1–6, IEEE, 2023. (**Published**)

9. M. Sandhya, U. Rudani, **V. Dilip Kumar**, M. Dileep, S. Bojjagani, S. Pallantla, and P. D. S. S. Lakshmi Kumari, "Deep Neural Networks with Multi-class SVM for Recognition of Cross-Spectral Iris Images," in *Machine Learning and Metaheuristics Algorithms, and Applications: Second Symposium, SoMMA 2020, Chennai, India, October 14–17, 2020, Revised Selected Papers 2*, pp. 29–41, Springer Singapore, 2021. (**Published**)

10. M. Sandhya, Y. Sreenivasa Rao, S. Biswajeet, **V. Dilip Kumar**, and M. Anup Kumar, “A Score-Level Fusion Method for Protecting Fingerprint and Palmprint Templates,” in Security and Privacy, pp. 1–11, Springer, 2021. (**Published**)

11. M. Sandhya, T. Dhopavkar, **V. Dilip Kumar**, J. Palla, M. Dileep, and S. Bojjagani, "Leukocyte Subtyping Using Convolutional Neural Networks for Enhanced Disease Prediction," in *Advanced Machine Intelligence and Signal Processing*, pp. 1–17, Springer Nature Singapore, 2022. (**Published**)