Securing Identities Through Fingerprint Template Protection

Ph.D. Thesis

By
VIVEK SINGH BAGHEL

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
INDIAN INSTITUTE OF TECHNOLOGY INDORE

NOVEMBER 2022

Securing Identities Through Fingerprint Template Protection

A Thesis

Submitted in partial fulfillment of the
requirements for the award of the degree
of
Doctor of Philosophy

by

VIVEK SINGH BAGHEL

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
INDIAN INSTITUTE OF TECHNOLOGY INDORE

NOVEMBER 2022

INDIAN INSTITUTE OF TECHNOLOGY INDORE

I hereby certify that the work which is being presented in the thesis entitled **Securing Identities Through Fingerprint Template Protection** in the partial fulfillment of the requirements for the award of the degree of **Doctor of Philosophy** and submitted in the **Department of Computer Science and Engineering**, **Indian Institute of Technology Indore**, is an authentic record of my own work carried out during the time period from **December 2018** to **November 2022** under the supervision of **Dr. Surya Prakash, Associate Professor, Department of Computer Science and Engineering, Indian Institute of Technology Indore**.

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

21/11/2022
Signature of the student with date

(Vivek Singh Baghel)

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

21-Nov-2022
Signature of Thesis Supervisor with date

(Dr. Surya Prakash)

Vivek Singh Baghel has successfully given his Ph.D. Oral Examination held on **March 9, 2023**.

9-March-2023
Signature of Thesis Supervisor with date

(Dr. Surya Prakash)

ACKNOWLEDGEMENTS

I would like to take this opportunity to thank a number of persons who in one or the other way contributed by making this time as learnable, enjoyable, and bearable as possible. First, I would like to express my heartfelt gratitude to my supervisor **Dr. Surya Prakash**, who has been a constant source of inspiration during my work. Without his constant guidance and research directions, this research work wouldn't have been possible. His continuous support and encouragement have always motivated me to remain streamlined in my research work. In addition, I am also grateful to him for extending all necessary support during his tenure as Head of the Department of Computer Science & Engineering.

I am thankful to **Dr. Puneet Gupta** and **Dr. Vivek Kanhangad**, my research progress committee members, for taking time out of their busy schedules to evaluate my progress all these years. Their valuable comments and suggestions have helped me to improve my work at various stages.

I am also grateful to **Dr. Somnath Dey**, Head of the Department of Computer Science & Engineering, for extending all necessary support to me. My sincere acknowledgement and respect to **Prof. Suhas Joshi**, Director, Indian Institute of Technology Indore, for providing me the opportunity to explore my research capabilities at the Indian Institute of Technology Indore.

I would also like to thank my labmate Syed Sadaf Ali for providing the suggestions during my research work and hearty thanks to other labmates Iyappan, Akhilesh, Piyush, Afeeza, Ratna, Anagha, and Prasad for their cooperation during the course of my research work. I would appreciate the fine company of my dearest colleagues and friends, especially, Yeeshu, Chandan, Sheetal, Anuj, Vikas, Rahul, Alok, and Rituraj.

I would like to express my heartfelt respect to my parents for their love, care, and support they have provided to me throughout my life. Especially, I would like to thank my mother for her constant love, support, and encouragement.

Finally, I am thankful to *Almighty Lord Krishna*, the most gracious and merciful, and all his creatures who directly or indirectly contributed, helped, and supported me.

Vivek Singh Baghel

Dedicated

to

My Parents and Teachers

ABSTRACT

Biometric authentication systems have been extensively used in numerous applications of different fields in order to provide secure access to different resources. These systems recognize an individual by means of physiological traits such as fingerprint, face, iris, ear, etc., or behavioral traits such as gait, signature, voice, etc. These traits possess unique and permanent features and are capable of distinguishing the identity of an individual from others in a biometric system. Biometric authentication systems have several advantages over the conventional authentication systems which mainly rely on passwords and tokens. In conventional authentication systems, there is an ample number of possibilities where a password or token can be stolen by an adversary. In addition, the user has to always remember the password or token or carry the card for authentication purposes. In contrast, as biometric traits are an integral part of the human body, there is no need to remember anything as well as make any special efforts to carry them along for the purpose of using them in the biometric authentication system.

Among all of these biometric traits, the fingerprint is one of the extensively used biometric traits for authentication. This is due to several advantages, such as permanence, easy to capture, uniqueness, etc., that it offers. In a fingerprint-based biometric system, information of minutiae points is commonly utilized to compute the user template. The template is further stored in the database for future authentication purposes. Although fingerprint biometrics provides numerous advantages over the other biometric traits, it suffers from security and privacy issues of the stored user template. It has been discussed in the literature that the reconstruction of the fingerprint image is feasible by means of a compromised fingerprint based user template that basically contains the information of the minutiae points. Consequently, this can cause a permanent identity loss to an individual as the fingerprint biometrics is unchangeable if it is compromised. Therefore, it is crucial to protect the fingerprint based user template in such a way that even if it is compromised, it is infeasible for an adversary to reconstruct the original fingerprint image or features from it.

By keeping these issues in mind, we propose four different techniques to protect the fingerprint based user template consisting of information of the minutiae points. The proposed

techniques are mainly based on a fuzzy vault scheme and non-invertible transformation. The first work in the thesis proposes a template protection technique based on fuzzy vault and a mechanism for selecting strong minutiae points during matching. In this work, we also propose a method based on Principal Component Analysis (PCA) to align the fingerprint images. In the second work, we propose a non-invertible transformation based technique to protect the fingerprint based user template. In the technique, a user keyset is used as a transformation parameter, and a PCA-based technique is utilized for the alignment purpose. In the third work, transformed pair-polar structures of the minutiae are adopted to compute an alignment-free, non-invertible, and singular point independent secure user template. In this work, the secure template is obtained in binary form by mapping the transformed pair-polar coordinates to a 3D grid and then permuting the binary strings. In the fourth work, we directly make use of pair-polar coordinates without transformation and map them to a 3D grid. Thereafter, Discrete Fourier Transform (DFT) followed by permutation is used to perform the non-invertible transformation. The technique provides a secure fingerprint template and also significantly improves the overall recognition performance as compared to previous techniques.

The user templates computed by means of the proposed work possess all the required properties, $viz.$, revocability, diversity, security, and performance, of a secure template. We have analyzed the proposed techniques by considering various attack scenarios and have found them robust and secure against different attacks. The experimental analysis of the proposed techniques is performed on the publicly available fingerprint databases obtained from various Fingerprint Verification Competitions (FVC), $i.e.$, FVC2000, FVC2002, and FVC2004. The experimentation shows highly promising results as compared to state-of-the-art techniques and demonstrates the effectiveness of the proposed template protection techniques.

LIST OF PUBLICATIONS

(A) From Ph.D. thesis work:

A1. Journal Articles:

J1. **V. S. Baghel**, S. Prakash, and I. Agrawal, *An enhanced fuzzy vault to secure the fingerprint templates*, **Multimedia Tools and Applications**, 80, 33055–33073 (2021). DOI: 10.1007/s11042-021-11325-w (Impact Factor: 2.577)

J2. **V. S. Baghel**, S. S. Ali, and S. Prakash, *A non-invertible transformation based technique to protect a fingerprint template*, **IET Image Processing**, 1–15 (2021). DOI: 10.1049/ipr2.12130 (Impact Factor: 1.773)

J3. **V. S. Baghel**, S. S. Ali, and S. Prakash, *Adaptation of pair-polar structure to protect the fingerprint template*, **IEEE Transactions on Industrial Informatics**, 19(2), 1947-1956 (2022). DOI: 10.1109/TII.2022.3195938 (Impact Factor: 11.648)

J4. **V. S. Baghel**, A. Ali, and S. Prakash, *A robust and secure singular point independent fingerprint shell*, **Applied Intelligence**, 1-15 (2022). DOI: 10.1007/s10489-022-04038-6 (Impact Factor: 5.086)

J5. **V. S. Baghel** and S. Prakash, *Generation of secure fingerprint template using DFT for consumer electronics devices*, **IEEE Transactions on Consumer Electronics**, 1-10 (2022). (Early Access), DOI: 10.1109/TCE.2022.3217234 (Impact Factor: 4.414)

A2. Book Chapter:

Ch1. **V. S. Baghel** and S. Prakash, *Securing Identities through Biometric Template Security*, Multimedia security: Tools, Techniques and Applications, AAP CRC Press, 2021 (Accepted).

(B) Other publications during Ph.D.:

B1. Journal Articles:

Published/Accepted:

J1. S. S. Ali, **V. S. Baghel**, I. I. Ganapathi, S. Prakash, N. Son Vu, and N. Werghi, *A novel technique for fingerprint based secure user authentication*, **IEEE Transactions on Emerging Topics in Computing**, 10(4), 1918-1931 (2021). DOI: 10.1109/TETC.2021.3130126 (Impact Factor: 6.595)

J2. S. S. Ali, **V. S. Baghel**, I. I. Ganapathi, and S. Prakash, *Robust biometric authentication system with a secure user template*, **Image & Vision Computing**, 104, 1-15 (2021). DOI: 10.1016/j.imavis.2020.104004 (Impact Factor: 3.86)

J3. A. Ali, **V. S. Baghel**, and S. Prakash, *Enhanced minutiae triplet based alignment-free fingerprint template protection technique*, **The Visual Computer**, 1-15 (2022). DOI: 10.1007/s00371-022-02726-5 (Impact Factor: 2.835)

Under Review/Revision:

J4. A. Ali, **V. S. Baghel**, and S. Prakash, *A robust and effective fingerprint template protection based on k-NNs and Delaunay triangulation*, communicated to **IEEE Transactions on Dependable and Secure Computing**. [Manuscript No.: TDSC-2022-09-0793, Submitted on 9th September 2022] (Impact Factor: 6.791)

B2. Conference Articles:

C1. **V. S. Baghel**, S. Prakash, A. Banala, and A. Ravikumar, *Secure Fingerprint Authentication using a Robust and Effective Biometric Cryptosystem*, In Proceedings of International Conference on Smart Systems and Advanced Computing, (**SysCom 2022**), Macau, China, Dec 30-31, Virtual, 2022. (Accepted)

C2. **V. S. Baghel**, S. Patel, S. Prakash, and A. M. Srivastava, *A Deep Learning based Approach to Perform Fingerprint Matching*, In Proceedings of the International Conference on Cyber Security, Privacy and Networking (**ICSPN 2022**), Virtual, Sep 9-11, 2022. DOI: 10.1007/978-3-031-22018-0_22

C3. S. S. Ali, **V. S. Baghel**, G. I. Iyappan, S. Prakash, N. Son Vu, and N. Werghi, *Toe Prints: An Application Study for Biometric Verification in Adults*, In Proceedings of

the IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (**CVPRW 2021**), 1418-1424, 2021. DOI: 10.1109/CVPRW53098.2021.00157

C4. A. Ali, **V. S. Baghel**, and S. Prakash, *An alignment-free fingerprint template protection technique based on minutiae triplets*, In Proceedings of International Conference on Recent Trends in Image Processing & Pattern Recognition, (**RTIP2R 2021**), University of Malta, Msida, Malta, Dec 8-10, Virtual, 2021. DOI: 10.1007/978-3-031-07005-1_16

C5. **V. S. Baghel**, A. M. Srivastava, and S. Prakash, *Minutiae points extraction using Faster RCNN*, In Proceedings of International Conference on Advanced Computing, Networking, and Informatics, (**ICACNI 2019**), IIIT Kalyani, India, Dec 20-21, 2019. DOI: 10.1007/978-981-15-8610-1_1

Contents

List of Figures

List of Tables

List of Abbreviations

FRR	False Rejection Rate
FAR	False Acceptance Rate
EER	Equal Error Rate
GAR	Genuine Acceptance Rate
KS	Kolmogorov-Smirnov
FVC	Fingerprint Verification Competition
FNMR	False Non-Match Rate
FMR	False Match Rate
FCMR	False Cross Match Rate
FNCMR	False Non-Cross Match Rate
BiPS	Binarized Phase Spectrum
FCS	Fuzzy Commitment Scheme
RDQT	Randomized Dynamic Quantization Transformation
MVD	Minutia Vicinity Decomposition
k**-NNs**	k-Nearest Neighbors
PCA	Principal Component Analysis
PIN	Personal Identification Number
XOR	Exclusive-OR operation
DFT	Discrete Fourier Transform
DWT	Discrete Wavelet Transform
ARM	Attack via Record Multiplicity
MLC	Multi-Line Code
RGHE	Randomized Graph-Based Hamming Embedding
DITOM	Densely Infinite-To-One Mapping
MCC	Minutia Cylinder-Code
LSB	Least Significant Bit
MSB	Most Significant Bit
CASIA	Chinese Academy of Sciences' Institute of Automation

Chapter 1

Introduction

Establishing a person's identity is a crucial task to provide security against illegitimate access to different resources and applications. The identity recognition of a person can be done by utilizing the three different kinds of information as discussed in [11, 12], and these are (i) the knowledge, (ii) the possession, and (iii) the person's physiological and behavioral characteristics. In the first category, a person knows some confidential information such as password, key, PIN, etc., through which the identification process is done. In the second category, a person is identified with the help of a physical token such as smart card, driving license, etc. In the last category, the identification of a person is made using the physiological and behavioral traits (characteristics) of a person, and these characteristics are known as biometrics. The recognition systems that are based on biometrics have many leverages over the knowledge-based and possession-based recognition systems. The biometric information of a person is non-changeable, non-shareable, and impossible to steal, making it a highly reliable way to identify a person as compared to knowledge-based and possession-based recognition systems.

Biometric authentication systems establish the identity of a person based on his/her physiological and behavioral biometric traits. The physiological biometric traits include

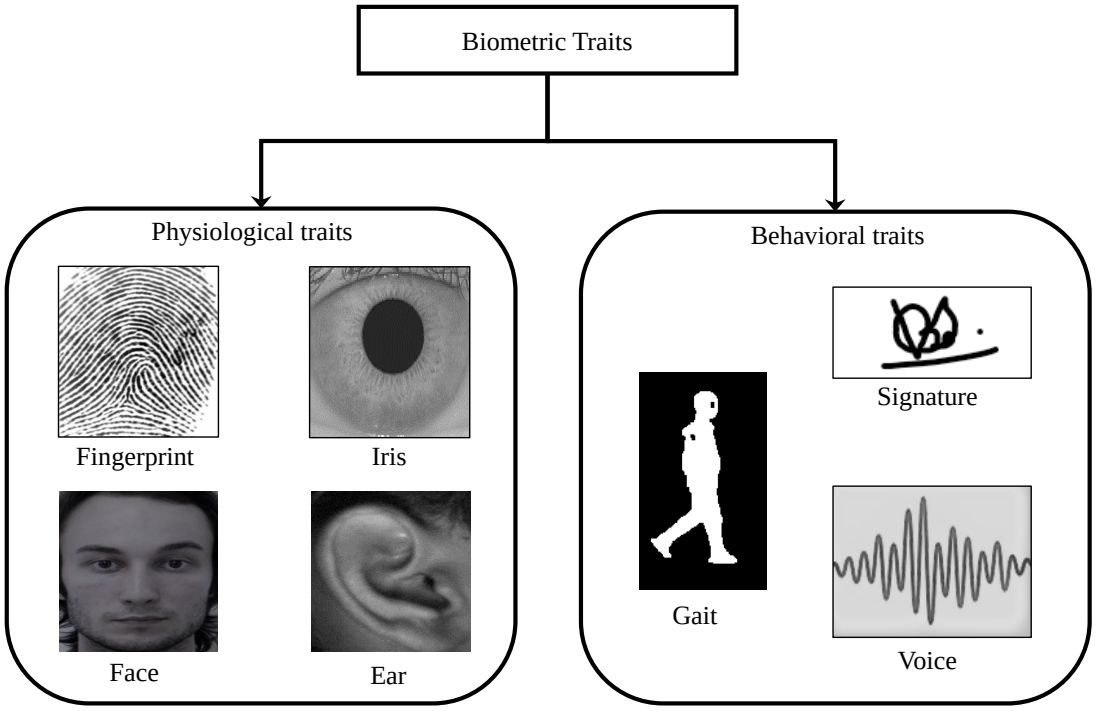
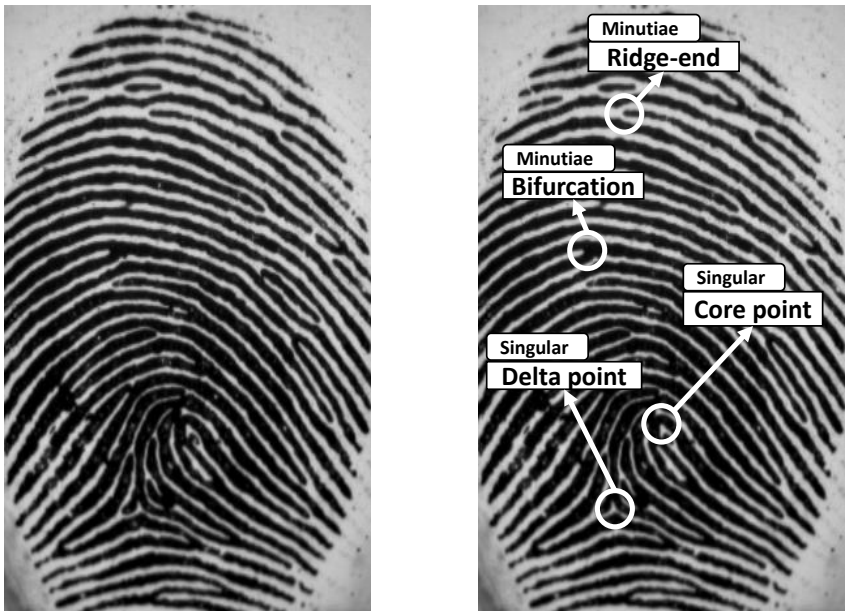


Figure 1.1: A few examples of physiological and behavioral biometric traits/characteristics (Biometric samples are taken from FVC2002 fingerprint database [1], CASIA Iris database [2], FEI Face database [3], and IITD Ear database [4], these images are used throughout the chapter for representation purposes).

face, fingerprint, ear, iris, palm print, etc., whereas the behavioral biometric traits consist of signature, gait, keystroke dynamics, voice, etc. A few examples of various biometric traits, both physiological as well as behavioral, have been depicted in Figure 1.1. Among different biometric traits, the fingerprint is one of the extensively used physiological biometric traits due to its permanence, uniqueness, and easiness of acquisition. A fingerprint contains a continuous pattern of ridges and valleys that exhibit some unique features/characteristics utilized to differentiate the identity of a person from others. These unique features are called minutiae points, which are named as ridge end and ridge bifurcation. The point where a ridge abruptly ends is called a ridge end, whereas the bifurcation is the point where a ridge bifurcates into two different ridges. An example of a fingerprint image along with different features marked on it is shown in Figure 1.2. In a fingerprint-based authentication



(a) (b)

Figure 1.2: An example of (a) fingerprint image [1] and (b) the representation of minutiae and singular points.

system, during enrollment, these distinctive features are extracted from the input fingerprint image (it is known as the gallery image) and stored in the database. During the verification stage, the features are again extracted from the fingerprint image acquired from the user at that time (it is known as the probe image) and are matched with that of the stored gallery template in the database to compute a matching score. This score is further used to decide if the verification was successful or not. Similarly, a probe template is computed and matched with all the stored templates in the database to recognize a person's identity during the identification stage. An overview of a fingerprint biometric system is shown in Figure 1.3. Although fingerprint-based biometric systems have several advantages over traditional systems (for example, passwords/token-based systems), they face some challenges. Among them, identity theft is a very important one, which causes a permanent loss of a person's fingerprint data. To prevent the identity theft of a person, different fingerprint template protection techniques have been proposed in the literature. The following sections discuss

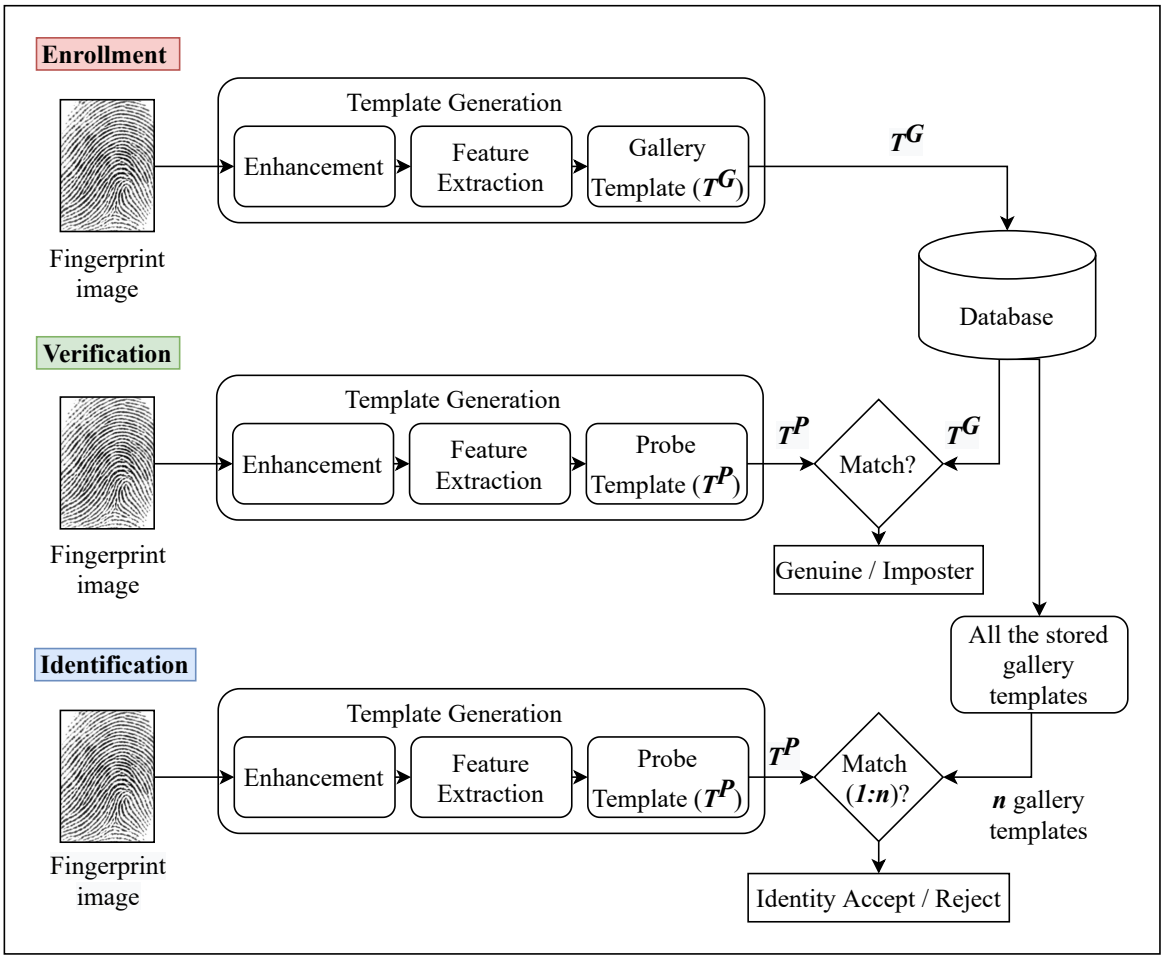


Figure 1.3: Overview of a fingerprint biometric system.

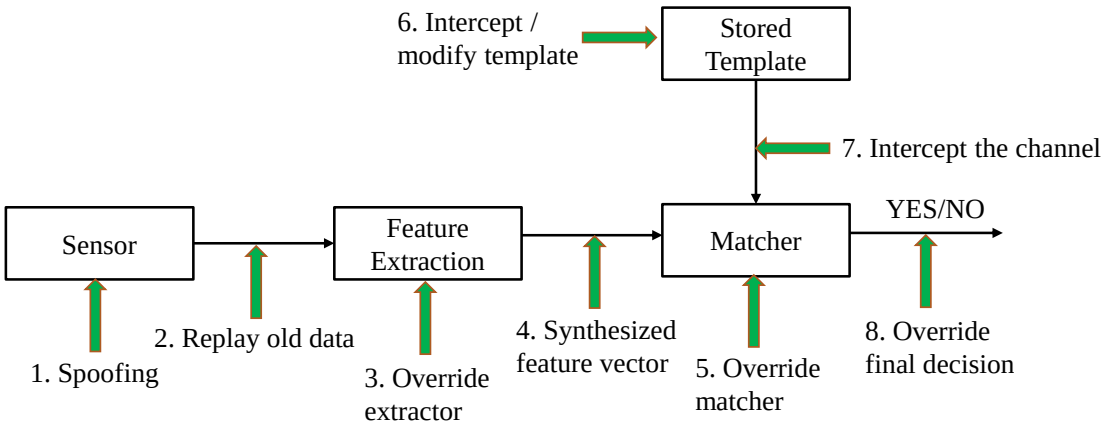


Figure 1.4: Different kinds of attacks at various points of a biometric system [5].

fingerprint template protection in detail.

1.1 Fingerprint Template Protection

Biometric systems provide high-level security to different resources and applications of various fields. However, these systems themselves have some security issues, which have been discussed in detail in [5]. Figure 1.4 presents different kinds of attack scenarios which are possible at various points in a biometric system and the same is very true for a fingerprint based biometric systems as well. At point#6, the figure shows the possibility of intercepting the biometric template stored in the database by an adversary. In the event of an attack, if the adversary inspects the database and gets the original fingerprint template, it causes a permanent identity loss of the person as the fingerprint information, or the biometric data in general is immutable in nature. These acquired templates can be used to get illegitimate access to the biometric system by an adversary. Further, in the case of an attack, these can also be modified, which will restrict the access of the legitimate user to the biometric system. In addition, it has been discussed in the literature [13, 14, 15, 16, 17] that the original fingerprint information can be reconstructed from the fingerprint user template stored in the database. A fingerprint template protection technique secures the user template stored in the database and protects it against various attacks.

In order to secure the stored fingerprint template in the database, several techniques known as fingerprint template protection/security techniques, have been discussed in the literature. The primary concept behind these techniques is to store a non-invertible transformed/encrypted fingerprint template instead of the original fingerprint template; hence, if an attack occurs in the database, an adversary will be unable to recover the original information of the fingerprint image from the template. According to the literature, the fingerprint template protection technique can be mainly categorized into two types, namely, biometric cryptosystems [9, 18], and cancelable biometrics [5, 19]. There are a few other techniques

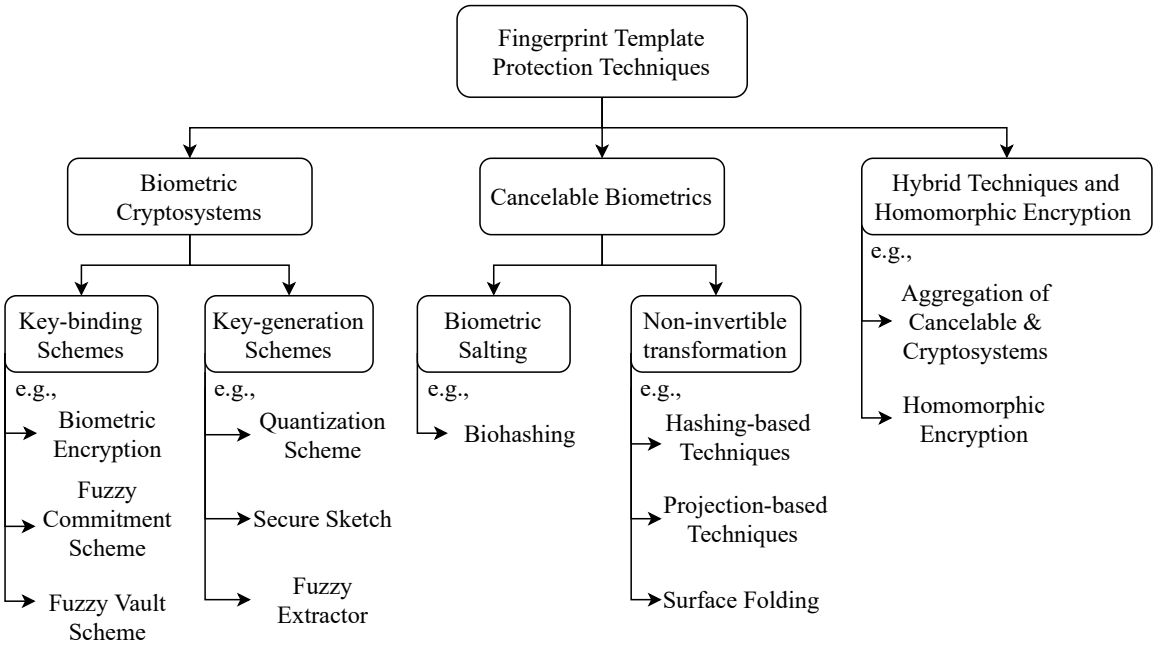


Figure 1.5: Classification of fingerprint template protection techniques.

of user template protection which are hybrid approaches (combination of cancelable approaches and cryptosystems or different cryptosystems) or based on homomorphic encryption. In Figure 1.5, different types of fingerprint template protection techniques are shown in a hierarchical manner. Various techniques depicted in the figure are further discussed in a concise manner in the next chapter under the literature review. As discussed in [20], a template protection technique should possess four essential properties, which are revocability, diversity, security, and performance. These properties along with various frameworks used to analyze them, are discussed in detail in the following section.

1.2 Essential Properties of a Fingerprint Template Protection Technique

A fingerprint template protection technique should meet some important requirements, such as revocability, diversity, security, and performance [20]. The following is a discussion

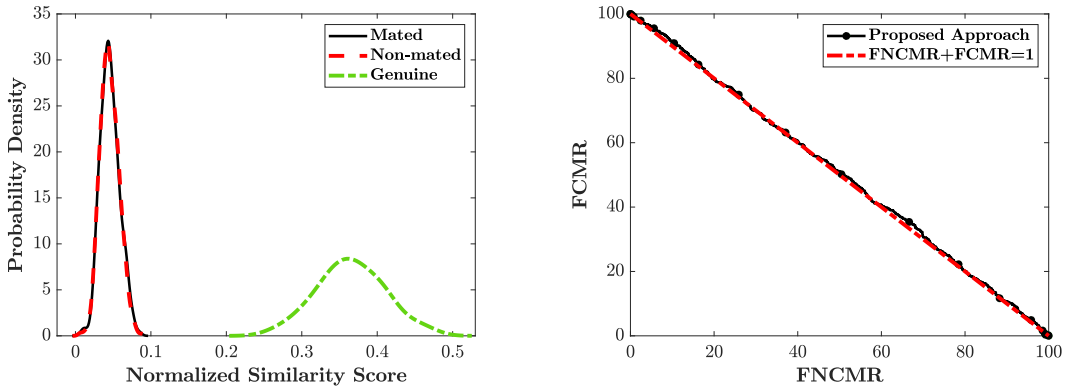
on these critical properties of a template protection technique.

1.2.1 Revocability

The capacity to replace a stored secure template (compromised template) in the database with a totally new secure template that is generated using the same biometric data but different keys/parameters for altering the previous biometric template is termed as revocability. Although these two secure templates, the one which got compromised and another newly generated template, are generated using the same biometric data, they will not have any significant similarities with each other. In order to verify the notion that a template protection technique exhibits revocability property some frameworks, such as [21, 22], have been studied in the literature.

An attack scenario has been introduced in [21] to assess the revocability of an approach. This attack scenario is known as a revoked template attack, and it involves attacking a biometric system using a revoked template in two separate scenarios. In the first case, known as a Type-I attack, the revoked template is matched with the replaced new template, which is generated using the same fingerprint impression but different transformation keys/parameters. In the second case, known as a Type-II attack, a revoked template is matched with the replaced new template, which is constructed using another fingerprint impression of the same finger but different transformation keys/parameters. The results of the Type-I and Type-II attack scenarios determine the effectiveness of a template protection technique in terms of the revocability property. If the percentage of successful matches is close to zero, the secure templates are considered revocable, and the technique is said to meet the criteria of revocability.

In addition, a framework has been discussed in [22] to analyze the revocable capability of secure templates in the case of iris biometric data. In this framework, the mean and



(a) (b)

Figure 1.6: Representation of outcomes to assess the unlinkability of a Biometric Template Protection (BTP) technique using two different frameworks [6, 7].

variance of genuine, imposter, and pseudo-imposter scores are calculated. The pseudo-imposter scores are calculated by matching the two secure templates that are constructed using the same image but different transformation keys. According to [22], if the mean and variance values of pseudo-imposter scores are distinct from that of genuine scores and are close to imposter scores, then the user templates are considered revocable, and the template protection technique is considered adhering to the revocability property.

1.2.2 Diversity

According to the property of diversity (also known as unlinkability), the secure templates that are generated using a template protection technique for the same biometric impression and using different keys/parameters of transformation should be unlikable to each other. In other words, there should be no similarity between the secure templates computed using the same biometric data. In such cases, a template stored in the database can be easily replaced with a completely new and different template in the event of an attack on the database. To demonstrate unlinkability or diversity property, a few frameworks such as proposed in [6, 7] have been discussed in the literature.

In [6], Gomez-Barrero et al. have introduced a new generalized framework to analyze template protection in the light of unlinkability. The framework computes two matching score distributions, namely, mated and non-mated matching score distributions. The mated score distribution is computed after matching the templates obtained from the same impression of a finger and by using different keys/parameters of the transformation function. On the other hand, non-mated score distribution is computed by matching the templates obtained from different impressions of the different fingers and different keys/parameters of the transformation function. If these two distributions overlap, as shown in Figure 1.6(a), a template protection technique is said to exhibit the unlinkability property and the templates are considered unlinkable.

Another framework to analyze the unlinkability property is being discussed in [7]. By considering the given template protection technique, the two different rates, $i.e.$, False Cross Match Rate (FCMR) and False Non-Cross Match Rate (FNCMR), are computed. Here, FCMR denotes the rate of successful matching between non-mated samples (as discussed in [6]), whereas FNCMR denotes the rate of unsuccessful matching between mated samples. As shown in Figure 1.6(b), the values of FNCMR and FCMR for various thresholds are plotted against each other. According to the framework discussed in [7], if the plot of FNCMR-*Vs*-FCMR nearly overlaps with the plot of FCMR+FNCMR=1, then the given biometric template protection technique adheres to unlinkability.

1.2.3 Security

According to this property, the biometric template protection technique must be capable of preventing data breaches and unauthorized access to the biometric system. To ensure the privacy of the original biometric data, the encrypted/transformed template must adhere to the non-invertibility property. This assures that an intruder cannot recover the original

biometric data ($e.g.$, fingerprint impression) from a compromised template.

In an attack scenario, known as a brute force attack, an attacker may attempt to guess the original template from the compromised template by attempting all conceivable permutations. To secure the user template from such an attempt, the transformed user template should be constructed in such a way that an intruder finds it computationally impossible to predict the original biometric data by performing the brute force attack.

Furthermore, if an intruder has prior knowledge of matching score calculation as well as the minimum necessary matching score to get access, he/she may be able to get illegitimate access to the biometric system by applying the false accept attack. In this attack scenario, an intruder tries to guess the combination in such a way that the final matching score is close to the minimum necessary matching score, thus reducing the number of available combinations as compared to a brute force attack. To handle this attack scenario, a transformed user template should be built in such a manner that guessing the original template becomes computationally impossible, even if the number of alternatives to try are lower than that required in a brute force attack.

Now, assume that an intruder obtains multiple templates that are calculated using the same biometric data. In that case, it is possible that the intruder may try to link these templates to get the knowledge about the original biometric data, which may then be used to gain access to a biometric system. This attack scenario is known as an Attack via Record Multiplicity (ARM) scenario. To handle this attack, the created transformed templates should not have any linking between themselves which may reveal information about the original biometric data.

1.2.4 Performance

This is one of the most crucial requirements of a template protection technique. The recognition performance of a biometric system may suffer due to the encryption/transformation performed on the original biometric information in order to provide protection against the identity theft. Therefore, encryption/transformation should be used in such a way that the performance of a biometric system should not be compromised in order to develop a robust and effective template protection technique. There are a few metrics that have been widely used in the literature to measure the performance of a biometric system. These performance metrics are Genuine Acceptance Rate (GAR), False Acceptance Rate (FAR), False Rejection Rate (FRR), and Equal Error Rate (EER).

- **Genuine Acceptance Rate (GAR):** GAR depicts the capability of a biometric system to correctly accept a genuine user. It is computed as the ratio of the truly accepted genuine users and the total number of genuine comparisons.

- **False Acceptance Rate (FAR):** FAR represents the rate at which a biometric system falsely accepts an imposter. It is computed as the ratio of the falsely accepted imposters and the total number of imposter comparisons. FAR is sometimes denoted as False Match Rate (FMR).

- **False Rejection Rate (FRR):** FRR represents the rate at which a biometric system falsely rejects a genuine user. It is computed as the ratio of the falsely rejected genuine user and the total number of genuine comparisons. The FRR is sometimes denoted as False Non-Match Rate (FNMR). The GAR and the FRR are related by the following formulae, FRR $= 1 -$ GAR.

- **Equal Error Rate (EER):** EER denotes the rate at which the value of FAR and FRR

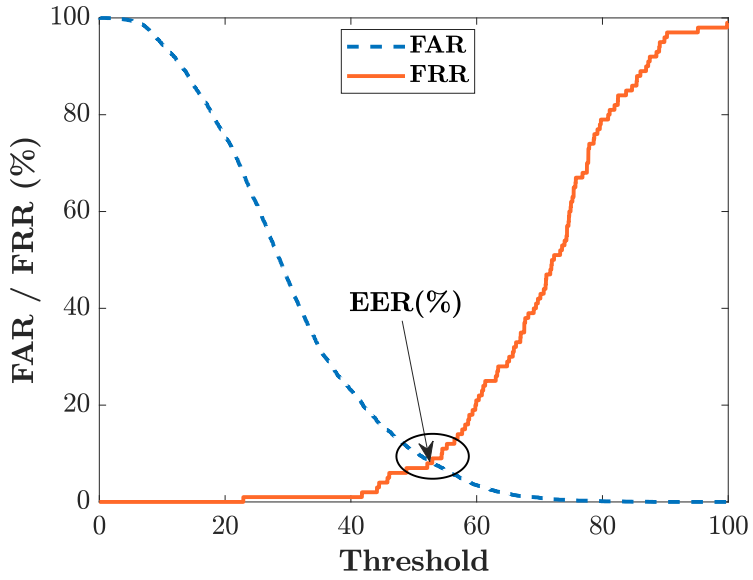


Figure 1.7: The threshold Vs. FAR/FRR plots where the intersection of FAR and FRR represents the value of EER.

becomes equal, as depicted in Figure 1.7. The value of EER close to zero represents a highly robust and effective biometric system in terms of the performance.

In addition, there are a few statistical analysis based metrics, which are utilized to assess the performance of a biometric system. These metrics are used to depict the significant distinctiveness between the genuine and imposter score distributions. In the case of template protection, these metrics dictate the effectiveness of the considered template protection technique. A brief discussion on two statistical metrics is provided below.

- **Kolmogorov-Smirnov (KS) test** [23]**:** It is a non-parametric and distribution-free statistical test to find out the difference between the two sets of samples. The value of the KS-test varies in the range of [0, 1], where a lower value shows that the two sets are completely similar to each other whereas a higher value shows that the two sets are significantly different from each other. In the analysis of a biometric system, genuine and imposter scores are used as the two input sets to the KS-test. Therefore,

if the value of KS-test is close to 1, it shows that the genuine and imposter score distributions are significantly different from each other for the biometric system and the approach is efficient in terms of the performance.

- **Student's t-test** [24]**:** It is a statistical hypothesis test used to show the significant difference between two sets of observations. In the case of a biometric system, these two sets are genuine and imposter scores. In the t-test, if the value of $|t - stat|$ is greater than the value of $t - critical$, then the null hypothesis is rejected and it represents that the input samples are significantly different from each other. This substantiates that the genuine and imposter distributions are well-separated from each other and the biometric system is efficient in terms of the performance.

1.3 Motivation and Objectives

Fingerprint biometrics is most extensively used among various physiological biometric traits as it is convenient to capture, easy to process, and is found to be persistent. Fingerprint-based authentication systems [20] mainly rely on the information of minutiae and singular points. In a typical fingerprint-based authentication system, the information of minutiae (*i.e.,* location and orientation values of a minutia point) is usually stored in the database to authenticate a person. In such systems, when an attack happens on the database and the stored information is compromised, it is possible to reconstruct the original fingerprint image using the compromised fingerprint user template [13, 15, 16, 17]. Further, in [14], a method describes that even an original fingerprint can be computed by using a minutiae template of ISO standard. This vulnerability may cause a permanent identity loss for an individual as the fingerprint information is unique and unchangeable for a person, if it is compromised. Further, the compromised template may be used to get illegitimate access to

a fingerprint system. Due to these security and privacy concerns, it is crucial to construct the fingerprint user template in such a way that it is infeasible to reconstruct the fingerprint image from the compromised template. This is the primary motivation of this thesis and it has aimed at developing fingerprint template protection techniques to prevent the issue of identity theft and permanent identity loss.

Most of the fingerprint template protection techniques proposed in the literature provide reasonable security to the users' data. Nevertheless, they have limitations in terms of non-invertibility and revocability issues, challenges in aligning the gallery and probe fingerprint images while matching, loss of discriminative features of fingerprints due to transformations, singular point dependency, etc. The thesis deals with all these issues and proposes techniques to handle them. A few works presented in this thesis utilize the location of the singular point of the fingerprint image for alignment purposes; however, this dependency has been eliminated in the other techniques presented in the later part of the thesis. The proposed techniques are based on fuzzy vault scheme ($i.e.$, the part of biometric cryptosystems) and non-invertible transformation ($i.e.$, the part of cancelable biometrics), and have been analyzed in terms of the four essential properties, namely, revocability, diversity, security, and performance. In the techniques, matching is performed in the transformed (encrypted) domain which ensures the security of the original fingerprint features. Multiple unique secure templates can be constructed by means of the same fingerprint image and by using different user-specific keys. This allows diversity in the generated secure user templates stored in various fingerprint systems as well as enables the capability of revoking the compromised templates. The secure templates are computed in such a way that the reconstruction of original fingerprint information from a compromised template is infeasible by an adversary. In addition, predicting the final secure template to get illegitimate access is also computationally infeasible in the proposed techniques. Although the fingerprint matching in the

Table 1.1: The information of various fingerprint databases

Databases	**Sensors**	**Image size**	Subjects × Samples	**Resolution**
FVC2000 DB2	Low-cost capacitive	256×364	$100 \times 8 = 800$	500 dpi
FVC2002 DB1	Optical	388×374	$100 \times 8 = 800$	500 dpi
FVC2002 DB2	Optical	296×560	$100 \times 8 = 800$	569 dpi
FVC2002 DB3	Capacitive	300×300	$100 \times 8 = 800$	500 dpi
FVC2002 DB4	SFinGe v2.51	288×384	$100 \times 8 = 800$	≈500 dpi
FVC2004 DB1	Optical	640×480	$100 \times 8 = 800$	500 dpi
FVC2004 DB2	Optical	328×364	$100 \times 8 = 800$	500 dpi

proposed techniques is performed in the transformed domain, the recognition performances of the techniques are not compromised due to the applied transformations.

1.4 Various Fingerprint Databases and Evaluation Protocols

1.4.1 Databases used for evaluation

The seven publicly available fingerprint databases, $viz.$, FVC2000 DB2 [25], FVC2002 (DB1, DB2, DB3, DB4) [1], and FVC2004 (DB1, DB2) [26] have been utilized to evaluate the performance of the proposed techniques in this thesis. These databases are the part of first, second, and third Fingerprint Verification Competitions (FVCs). Each of these databases contains 800 fingerprint images acquired from 100 subjects where for each subject, there are 8 samples present in the database. The summary of these databases is provided in Table 1.1. Minutiae extraction from the fingerprint images is performed using Verifinger-SDK (Demo version) [27]. The technique proposed in [28] is being utilized to find the locations of the singular points in a fingerprint image. As this technique is not efficient in detecting the location of singular points in arch-type fingerprint images, the technique proposed in [29] is utilized to locate the singular points in such images.

1.4.2 Evaluation protocols

In order to compute the values of various performance measures discussed in Section 1.2.4, two standard evaluation protocols, namely, 1-vs-1 and FVC protocols, have been utilized in the proposed techniques. A brief description of these protocols is provided in this section. In the case of 1-vs-1 protocol, the percentage value of FRR and genuine score distribution are computed by matching the first sample of each subject to the second sample of the same subject in a database. In contrast, every sample of each subject is matched with all the remaining samples of the same subject (excluding duplicate pairs) to compute the FRR and genuine score distribution in the case of the FVC protocol. In order to compute FAR, the first sample of each subject is matched with the first sample of all the remaining subjects in the database and it is the same for both protocols. Each database used in the experimentation contains the fingerprint images of 100 subjects, where each subject is having 8 samples. Therefore, the total number of genuine comparisons would be 100 and 2800 ($i.e.$, $\frac{8\times7}{2} \times 100$) for 1-vs-1 and FVC protocols, respectively, whereas 4950 ($i.e.$, $\frac{100\times99}{2}$) imposter comparisons would be carried out in the case of both 1-vs-1 and FVC protocols. All the proposed techniques are evaluated by means of the aforementioned protocols and databases on a machine having Intel® Core(TM) i5-7500 CPU @ 3.40GHz 3.41GHz and 8GB RAM. The implementation of the proposed techniques has been done using MATLAB® R2019a.

1.5 Thesis Contributions

The thesis proposes four fingerprint template protection techniques. Out of these, one technique falls under the biometric cryptosystems category whereas the rest of them belong to the cancelable biometrics category. The techniques offer revocability, unlinkability, and security of the biometric template without compromising the recognition performance of

the system. Further, the infeasibility of reconstructing the original fingerprint information from a compromised template is ensured in the proposed techniques and they are capable of efficiently handling different types of attacks on a fingerprint based biometric system. The four contributions of the thesis are briefly discussed below.

1.5.1 Securing a fingerprint template using fuzzy vault

In this work, a technique which is motivated from the fingerprint fuzzy vault implementation [30], is presented to secure the fingerprint template. In the technique, well-separated and filtered minutiae are used in order to generate a fuzzy vault. Further, an efficient approach is adapted to filter out the genuine minutiae during vault decoding phase by means of the relative distances of minutiae from the singular point. It is observed that the alignment of fingerprints is one of the critical issues encountered during the matching stage in a fingerprint based biometric system. To handle this, a Principal Component Analysis (PCA) based alignment approach is proposed in order to align the galley and probe fingerprint images during matching as shown in Figure 1.8. The obtained results show that the proposed PCA based approach performs quite well as compared to other existing approaches such as [30]. In the proposed PCA based alignment approach, principal components are computed for a thinned fingerprint image ($i.e.$, gallery or probe fingerprint images) considering the locations of the pixels as the input distribution. Subsequently, the minutiae points of the image are projected along the directions of the principal components to achieve a unique representation. The same procedure is adopted for both gallery and probe fingerprint images before encoding and decoding of the fuzzy vault. The advantage of the proposed PCA based alignment is that there is no need to store any auxiliary information in the database in order to align the fingerprint images during verification, unlike the curvature point based approach proposed in [30]. The obtained values of FAR(%) and FRR(%) are also improved as

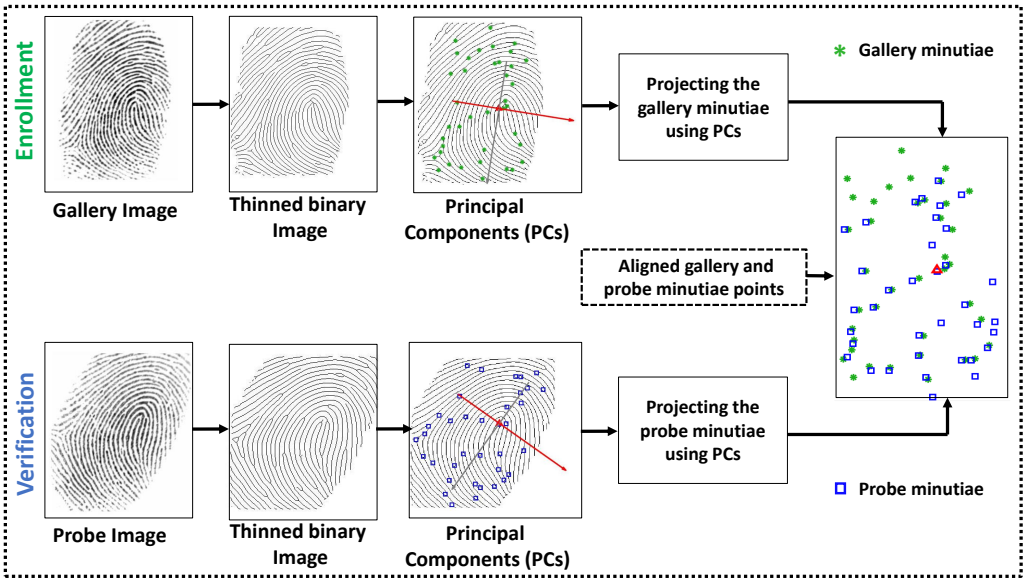


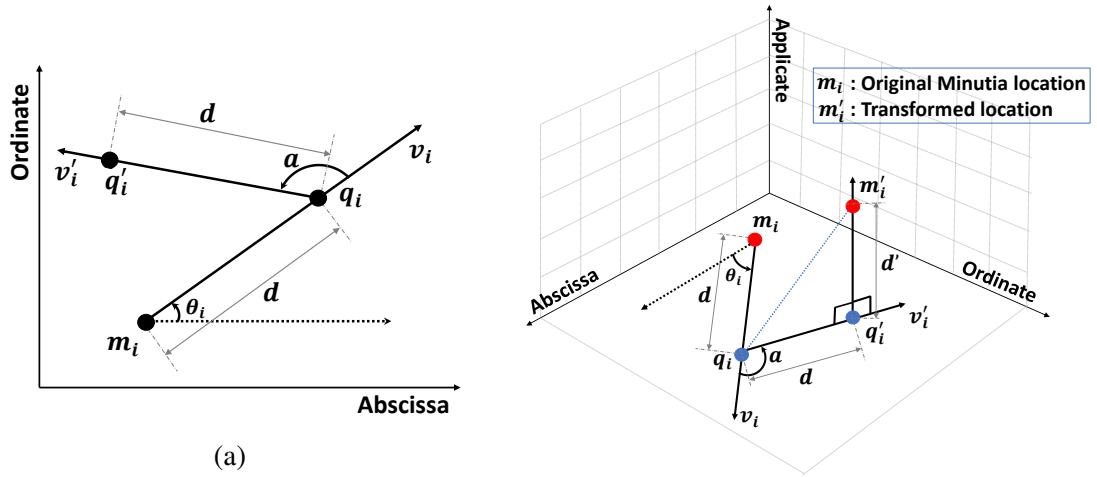
Figure 1.8: Different steps followed to align the fingerprint images using PCA.

compared to a few of the existing techniques based on the biometric cryptosystems, which shows the effectiveness of the proposed technique.

1.5.2 A non-invertible transformation based technique to protect a fingerprint template

The previously presented technique based on fuzzy vault has performed pretty well as compared to the existing techniques based on biometric cryptosystems. However, it lags in terms of the performance when we compare it with the other existing techniques which are based on cancelable biometrics. In addition, the templates produced are also found to be not very diverse in the previous technique. Keeping these points in mind, this work proposes a fingerprint template protection technique based on the non-invertible transformation that is a sub-category of the cancelable biometrics. The non-invertible transformation is performed on the original set of minutiae $M = \{(x_i, y_i, \theta_i), i = 1, 2, ..., n\}$ using a user-specific keyset $\{d, \alpha, d'\}$ as depicted in Figure 1.9. In this technique, before performing the non-invertible transformation, fingerprint images are aligned using a PCA based procedure which is sim-

ilar to the one used in the previous technique. Further, in the technique, the transformed locations of n minutiae are stored in the database as a secure user template.



(a) (b)

Figure 1.9: Computation of transformed location of minutia point m_i.

The proposed technique ensures that even if the stored template is compromised, it is infeasible to reconstruct the original fingerprint information from the template. The technique also proposes an approach to securely store the keyset in the system. In order to do that, the XOR operation is being performed between the binary equivalent of the keyset and a user-specific PIN, which would not be stored in the database. Due to this, only a legitimate user can extract the original keyset values during the verification. The experimental analysis has been performed in terms of revocability, unlinkability/diversity, security, and performance. The obtained results show the effectiveness of the proposed technique as compared to the existing techniques.

1.5.3 Adaptation of pair-polar structure to generate a secure fingerprint template

The technique discussed in the previous section is completely secure and effective; however, the computed secure template is not an alignment-free template. In the technique, it

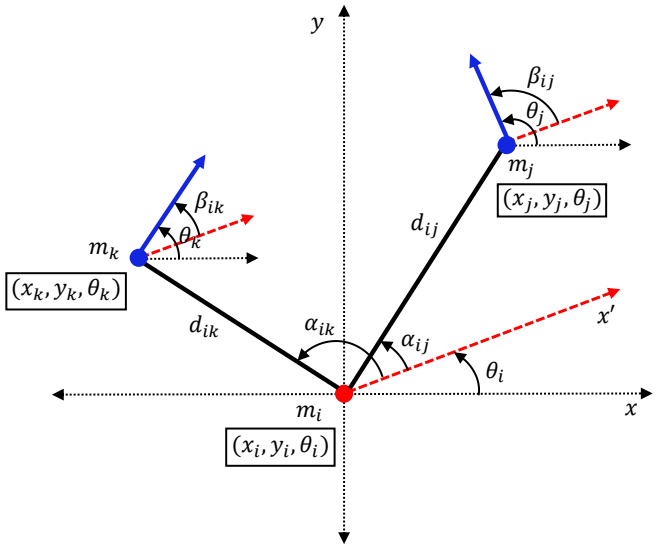


Figure 1.10: Representation of pair-polar minutiae structure with respect to a minutiae m_i.

is necessary to align the gallery and probe fingerprint images to be matched perfectly. This adds an extra step in the technique and even sometimes decreases the performance. To overcome this, an alignment-free fingerprint template protection technique is proposed in this work, which generates a rotation and translation-invariant secure template. The presented technique utilizes the pair-polar structure of the minutiae and computes a secure binary template by mapping the transformed pair-polar coordinates to a 3D grid with respect to each minutia. An example of a pair-polar structure with respect to a minutia m_i is shown in Figure 1.10. Further, the 3D grids obtained corresponding to each minutia are sequentially unfolded and stored in the database after performing a random permutation. The transformation of pair-polar coordinates is non-invertible, preventing the reconstruction of original fingerprint images from the transformed pair-polar structures. An example depicting the non-invertible transformation of pair-polar coordinates is shown in Figure 1.11.

The proposed technique has been tested on six publicly available fingerprint databases under the stolen-key attack and plain-key verification scenarios. It is seen that the technique attains 0% EER for all the databases under the plain-key verification scenarios. Further,

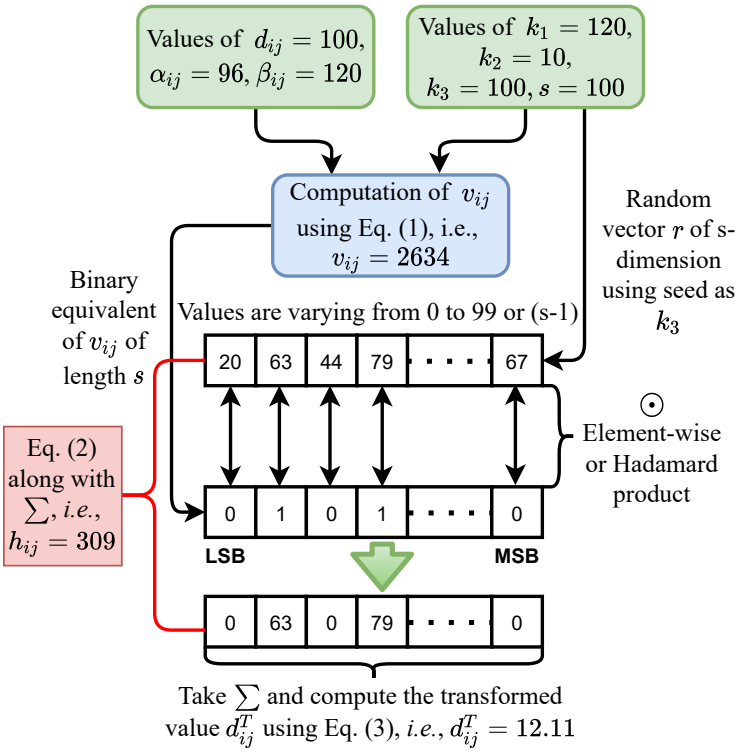


Figure 1.11: An example representing the transformation of pair-polar minutiae coordinates.

the percentage values of EER under the stolen-key attack scenario are also found to be superior to the same obtained in the existing techniques on different databases. The results are analyzed in terms of the aforementioned four essential requirements, and the analysis clearly demonstrates the efficacy of the proposed technique.

1.5.4 Generation of secure fingerprint template using pair-polar structure of minutiae and DFT

In the aforementioned proposed technique, the non-invertible transformation is performed on the original pair-polar structures before mapping them into a 3D grid. In the technique, performance degrades a bit due to the transformation of the original features. However, if the non-invertible transformation is applied on the binary template obtained by mapping of original features directly into the 3D grid, performance is found to improve in

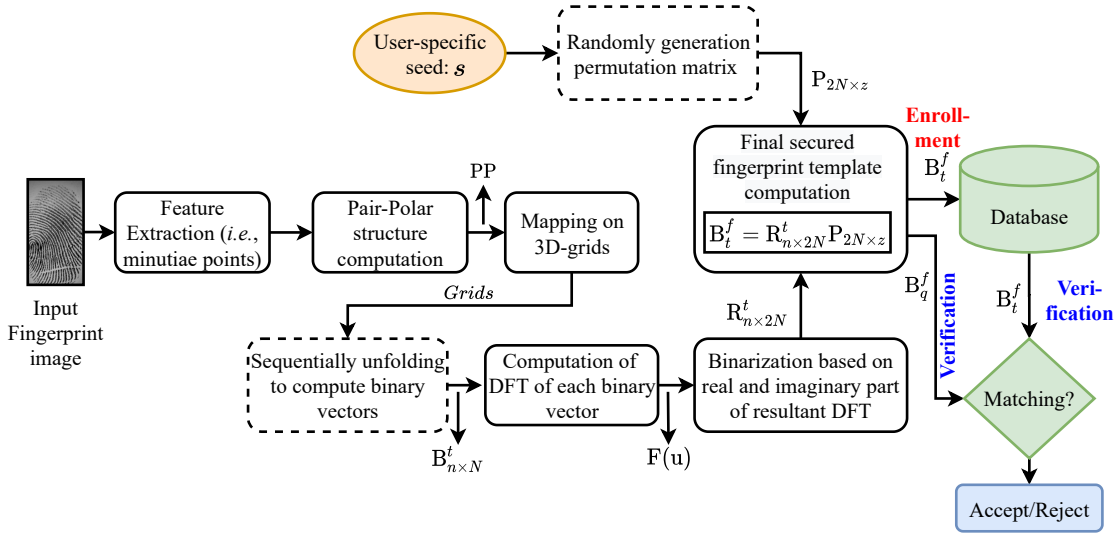


Figure 1.12: A block diagram representing the various steps involved in the generation of secure fingerprint template using pair-polar structure and DFT.

comparison to the same obtained when a transformation is performed on the original features. This has been demonstrated in the technique proposed in this section with the help of a Discrete Fourier Transform (DFT) based non-invertible transformation. In the process, the N-point DFT of the binary template is computed and further binarized by means of the real and imaginary parts of the DFT. It can be clearly seen that the reconstruction of the original binary string from the binarized Fourier spectrum is infeasible as there can be infinite possibilities to do that. In the technique, the secure binary strings ($i.e.$, binarized Fourier spectrum) corresponding to n minutiae are stored in the database as a user template after performing a random permutation on each secure binary string. The proposed technique has been tested on four publicly available fingerprint databases under the stolen-key attack and the plain-key verification scenarios. The technique attains 0% EER on all the databases under the plain-key verification scenario. Further, the EER values obtained under the stolen-key attack scenario are also found to be superior as compared to the existing techniques. The results are analyzed in terms of the aforementioned four essential requirements, and the analysis clearly demonstrates the efficacy of the proposed technique.

1.6 Thesis Organization

The rest of the thesis is organized as follows. In **Chapter 2**, a discussion on various existing techniques related to the biometric template protection has been presented. These existing approaches have been discussed by considering the categorization of biometric template protection, such as biometric cryptosystems, cancelable biometrics, etc.

In **Chapter 3**, a fingerprint template protection technique based on the fingerprint fuzzy vault implementation is proposed. The work also proposes a PCA based fingerprint alignment technique to perform efficient matching of the fingerprints during verification.

In **Chapter 4**, a non-invertible transformation based cancelable fingerprint template generation technique has been proposed, which also utilizes the PCA based alignment approach. The performance under the stolen-key attack scenario and in the 1-vs-1 protocol is improved in this technique.

In **Chapter 5**, an alignment-free non-invertible transformation based technique is proposed which utilizes the pair-polar structures of minutiae points. In this work, the performance is improved to quite an extent not only in the stolen-key and 1-vs-1 protocol scenarios but also under the FVC protocol.

In **Chapter 6**, a template protection technique is proposed which further improves the performance by utilizing a non-invertible transformation of binary template based on DFT. The said binary template is computed by utilizing the original pair-polar structure of the minutiae points instead of the transformed structures, unlike the work presented in the previous chapter.

In **Chapter 7**, the contributions of the thesis are summarized and a few possible future directions have been presented.

Chapter 2

Literature Review

In biometrics, the fingerprint is one of the extensively used biometric traits in order to provide the secure authentication system for applications of various fields. Although fingerprint based authentication systems provide secure access control systems they suffer with a critical issue of identity theft. It has been presented in the literature [13, 15, 16, 17] that the reconstruction of the original fingerprint image is feasible by means of the compromised user template by an adversary. Therefore, it is crucial to secure the original fingerprint template before storing it in the database. In order to secure the original fingerprint template, many fingerprint template protection techniques have been discussed in the literature. The work available in the literature related to the area of fingerprint template protection can be broadly classified into two categories which are biometric cryptosystems [9, 18], and cancelable biometrics [5, 19]. Further, there are a few more techniques discussed in the literature, which are basically homomorphic encryption and hybrid approaches (a combination of cancelable and cryptosystems or different cryptosystems). In Figure 1.5, various categories of fingerprint template protection techniques are shown in a hierarchical manner. Further, in this chapter, the existing template protection techniques corresponding to various categories from the literature are discussed.

2.1 Biometric Cryptosystems

Biometric cryptosystems [8, 9, 31] provide a way to secure the template by means of combining the cryptographic key with the biometric data or directly generating it from the biometric data during verification. In order to bind a key with the biometric data or to directly retrieve it from the biometric data, a piece of public information is stored in the database, which is called helper data [32]. The helper data is basically derived from the biometric data and doesn't disclose any fruitful information about the original biometric in the event of an attack on the database. Hence, an encrypted form of biometric is involved in the key-release process instead of the original biometric here and this makes the biometric cryptosystems a secure biometric template protection technique.

Biometric cryptosystems provide a replacement to conventional (password-based) key-release, where biometric data of an individual is utilized to release the key. This makes biometric cryptosystems more secure than the password-based key-release as biometric data is difficult to steal, forge, and share as compared to passwords. In conventional biometric systems, the decision of accept or reject during the verification is taken based on the matching score and a threshold value, which is a kind of fuzzy decision. On the other hand, in the biometric cryptosystems, the decision is always binary and depends on the successful release of the key. Biometric cryptosystems are mainly classified into two categories, $i.e.$, key-binding schemes [8, 9, 18] and key-generation schemes [31]. In key-binding schemes, a key is combined with the original biometrics of a user, and the constructed encrypted information is stored in the database. The stored information is later used as helper data for the release of the key during verification. In contrast, a key is generated directly from the biometric data itself instead of using a separate key in the case of key-generation schemes. These schemes are further discussed in the following sections.

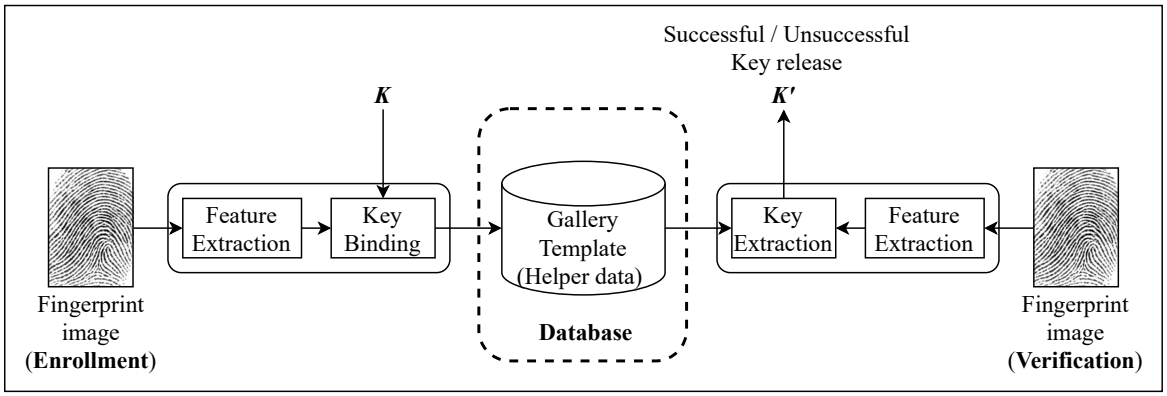


Figure 2.1: A schematic block diagram representing the working of the key-binding scheme.

2.1.1 Key-binding schemes

Key-binding schemes are one of the categories of biometric cryptosystems, which are defined in terms of the generation of helper data. In the key-binding scheme, the helper data is generated by combining a key with the original gallery biometric template, then stored in the database during the enrollment stage. The generated helper data would not reveal any information about the original biometric template if it is stolen through an attack. During the verification stage, the stored helper data and the probe biometric template is used to compute the key, and if the key is successfully released, then the probe template would be accepted; otherwise, it would be rejected. The working of key-binding scheme has been depicted in Figure 2.1. Further, the key-binding schemes can be mainly divided into two categories, which are fuzzy commitment scheme [8] and fuzzy vault scheme [9]. These schemes have been discussed in the following subsections.

2.1.1.1 Fuzzy commitment scheme

Fuzzy commitment scheme is one of the examples of biometric cryptosystems based on the key-binding strategy. This scheme combines the error-correcting codeword with cryptography to secure the original biometric data of a user. It has been introduced by Juels and Wattenberg in [8]. For proposing the scheme, the authors have taken an inspiration from

the conventional bit commitment and have shown the application of it for secure biometric authentication. In order to provide template security, the fuzzy commitment scheme utilizes the binary form of the user's biometric data. A brief description of the working of a fuzzy commitment scheme considering both the enrollment and verification stages of a biometric system is given below.

In order to implement the fuzzy commitment scheme, commitment function F is computed in such a way that $F(c, x) = (h(c), \delta)$. Here, x is an $n - bits$ binary string, which is basically representing the witness (biometric data). Further, $c \in C$ is a codeword of length $n - bits$, which is generated using an error correction codeword, $h(c)$ is the cryptographic hash ($e.g.$, SHA-1) of codeword c, and δ represents the difference between witness x and codeword c. Hence, the difference δ can be written as $\delta = x - c$. Now, the commitment $F(c, x)$ is stored in the database at the stage of enrollment. It is clear from the above discussion that just by knowing the $h(c)$ and δ, it is infeasible to get back the original witness (biometric data) x. Further, at the stage of verification, the value of the codeword c' is computed by taking the difference between a query biometric data x' of length $n - bits$ and the stored binary vector δ, which is given as $c' = x' - \delta$. Hence, if the query witness x' closely resembles enrolled x (or belong to the genuine subject), then the hash of codeword c' ($h(c')$) would be equal to the stored hash value $h(c)$, showing the successful verification otherwise, the verification would be considered unsuccessful. A block diagram representing the working of the fuzzy commitment scheme is shown in Figure 2.2.

In the literature, there are many techniques proposed to secure the original templates of different biometric traits, which are basically inspired by the general framework of fuzzy commitment scheme [8]. In this section, we have included a brief description of a few prominent works related to the fuzzy commitment scheme.

Teoh and Kim [18] have proposed an approach to generate the binary equivalent from

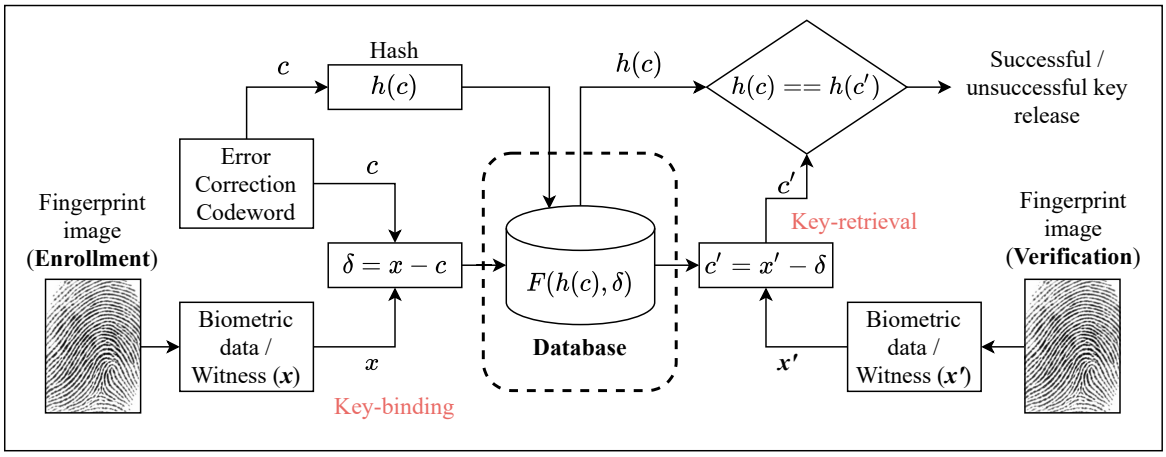


Figure 2.2: A schematic block diagram representing the general working of the fuzzy commitment scheme [8].

the fingerprint features. This approach is known as Randomized Dynamic Quantization Transformation (RDQT), which has used finger-code [33] as an input feature of the fingerprint biometric. RDQT consists of three steps, *viz.*, random projection, quantization, and condensation. First, features are randomly projected onto a vector by using an underdetermined linear system of equations. This is followed by quantization to generate the binary equivalent of the feature vector. Finally, condensation is performed which eliminates the perturbations in binary strings, if they exist. Further, the obtained binary vector is secured by using the fuzzy commitment scheme, where a concatenated codewords, *viz.*, Hadamard and Reed-Solomon codes are used. In [34], a theoretical analysis has been discussed for choosing the best suitable error correction codeword to secure different types of biometric data by means of a fuzzy commitment scheme. In this work, the authors have discussed about the upper bound of the error-correcting capacity of a codeword along with the min-sum decoding algorithm for an error correction codeword. In the end, the authors have tested the theoretical findings on fingerprint and iris biometric databases to establish the empirical proof of the theoretical study.

In [35], a cryptosystem based on fuzzy commitment has been proposed to secure the

fingerprint template. In order to accomplish it, first, minutiae information ($i.e.$, locations and orientation values) is extracted and represented in the form of a delta function. Subsequently, the Fourier spectrum corresponding to the delta function is computed. Further, the obtained Fourier spectrum is quantized using the polar logarithmic grid to compute the binary representation, called as Binarized Phase Spectrum (BiPS). In this work, a method to extract reliable bits has also been proposed. This reliable binary vector is secured by using the fuzzy commitment scheme, which utilizes turbo codes as an error correction codeword. A new approach to calculate the binary vector from the fingerprint features has been discussed in [36]. In this work, minutiae triplet has been utilized to compute the binary vector. In the process of generating binary string from minutiae triplets, more than one fingerprint image is used for a single user. In addition, the generation of the binary vector is inspired by the concept of user-specific questions, which is discussed in [37]. Further, in order to secure the binary template using fuzzy commitment scheme, three different error correction codewords, $viz.$, BCH codes, Two-layer concatenated codes (BCH and Reed-Solomon codes), and LDPC codes are used. Yadigar et al. in [38] have proposed a biometric cryptosystem by combining the texture-based features of fingerprint images. These features include finger code [33], Local Binary Pattern (LBP) [39], and Local Directional Pattern (LDP) [40]. All of these features provide a binary vector as output obtained using the reliability-based binarization method. Further, the binary vector has been secured by using the fuzzy commitment scheme with the BCH and LDPC codes as error correction codewords in this work. In addition, the fusion of binary vectors generated from three different texture-based features has also been performed in this work.

A fuzzy commitment scheme based fingerprint cryptosystem is proposed by Bentahar et al. [41] to protect the information transmitted in the Internet of Things (IoT) applications. In the technique, Discrete Wavelet Transform (DWT) is used to extract the binary vector from

a fingerprint image. This produces a binary vector of length 96-bits, which is generated after computing the DWT of 64×64 block of the fingerprint image around the core point. For computing the commitment, a key of 48-bits is randomly generated and converted into the 96-bits long codeword using Hamming codes. This obtained codeword is further combined with the binary biometric data. Due to this implementation, the transmission would take place through an encrypted channel between the smart connected things, owner, and remote server. In [42], authors have proposed a technique to provide the security to multi-server-based E-healthcare systems by using biometrics. In order to protect the biometric data, a fuzzy commitment scheme is used in this work. This scheme provides the error correction capability to handle the intra-class variations which exist in the biometrics. Also, the cancelable biometric templates are generated, which enables the revocable nature of biometric templates. Shi et al. in [43] have proposed an approach to protect the fingerprint template, which is used in the secure transmission of data in cloud-based IoT systems. The authors have utilized fuzzy commitment schemes and BCH codes as an error correction codeword to protect the original fingerprint data of the user. In order to extract the binary feature vector from a fingerprint image, sector encoding has been used around the singular (core) point of the fingerprint image in this technique.

2.1.1.2 Fuzzy vault scheme

Fuzzy vault is one of the biometric cryptosystems, which is based on the key-binding approach. It is also one of the popular cryptosystems to secure the original biometric template of a user. It is first introduced by Juels and Sudan in [9]. In the fuzzy vault scheme, the biometric features, which can be in any order, are mapped to a polynomial, and these mapped points along with a large number of chaff points are stored in the database as a vault. The polynomial is generated by utilizing an error correction codeword and a cryptographic

key. The query biometric features, which mostly overlap with the template biometric features, can only successfully unlock the vault; otherwise, it is infeasible to unlock the vault. Moreover, if the information stored in the vault is compromised, then the reconstruction of the original biometric data is infeasible from the vault information. It ensures the privacy of users' biometric data. Further, according to [9], the working of a fuzzy vault based biometric cryptosystem is discussed below.

At the enrollment stage, the polynomial p is generated by using a secret key k in such a way that the coefficients of the polynomial are derived from the key k, which can be represented as $p \leftarrow k$. Now, the biometric data A (it can be unordered as well) is mapped to the polynomial p, $i.e.$, $p(A)$. Further, chaff points are added to hide the original points, and the number of chaff points is always much greater ($\gg$) than the number of points in A. Chaff points are the points in the two-dimensional space, where the y-axis value should not be lying on the polynomial p. Finally, the collection of $\{A, p(A)\}$ and chaff points called as vault V_A are stored in the database. Here, the key idea is to generate a codeword for generic error correction codeword to hide the secret key k, where the codeword is generated by utilizing the biometric data A. Thus, during the verification stage, if biometric data B sufficiently overlaps with A, then most of the genuine points can be filtered out from all the vault points V_A ($\{A, p(A)\}$ and chaff points). Now, the polynomial p' can be reconstructed from these filtered genuine points using the error correction codeword. Further, secret key k can be retrieved using the reconstructed polynomial p'; thus, the vault would be unlocked. In contrast, if set B does not largely overlap with set A ($i.e.$, the case of imposter), then the secret key k would not be released successfully, and verification/authentication would be unsuccessful. A block diagram representing the working of the fuzzy vault scheme is shown in Figure 2.3. A few of the existing techniques related to the fuzzy vault scheme to protect the original fingerprint template are discussed below.

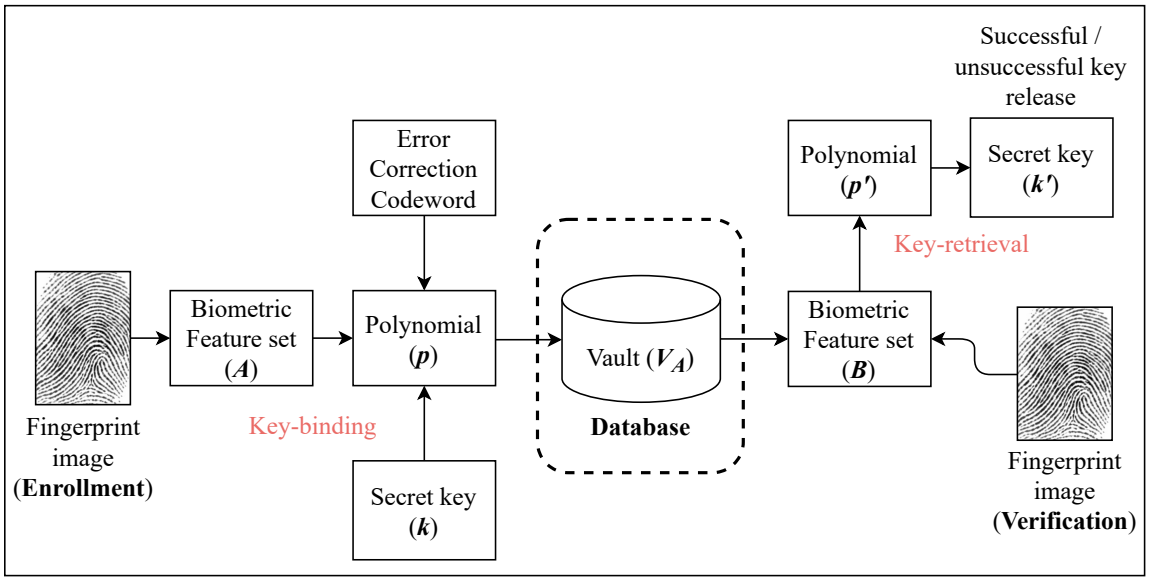


Figure 2.3: A schematic block diagram representing the general working of the fuzzy vault scheme [9].

In [44], a fingerprint template protection technique based on fuzzy vault and Cyclic Redundancy Check (CRC) has been proposed. In this work, the binary equivalents of locations of minutiae are used to compute a set of integers, which are to be mapped in the polynomial. The authors have utilized the alignment approach based on Iterative Closest Point (ICP) and Lagrange polynomial interpolation to reconstruct the polynomial at the time of authentication. Nandkumar et al. have extended this work in [30] and have proposed a new approach to filter the minutiae locations from the vault at the time of authentication, which they have called coarse-filtering. In this work, the locations of minutiae points and orientation values are utilized and are mapped on the polynomial during the construction of the vault. This work has also utilized an alignment approach based on the ICP and high curvature points present in the fingerprint image. In [45], Nandkumar et al. have addressed the issues with respect to a fuzzy vault scheme and developed the fuzzy vault by means of transformed minutiae information (by using a password), making the approach revocable in nature. They utilized CRC codes to check the error of extracted key during the authentication.

Zhou et al. in [46], have presented a fingerprint fuzzy vault technique in which an extra user-specific password is used to randomly compute the artificial minutiae that are combined with the genuine minutiae to form the vault. In addition, the user-specific password has also been utilized in this approach to calculate the hash of the secret key, which is used to encode the polynomial. In [47], Yang et al. have proposed a technique based on bio-cryptosystem and the modified version of the Voronoi Neighborhood Structure (VNS). The technique is an alignment-free technique as it utilizes the VNS local structures of minutiae. In [48], the authors have presented an approach that transforms the pair-wise minutiae features using the user-specific password. Further, these features have been secured by utilizing the fuzzy vault scheme. In [49], a detailed security analysis of minutiae-based fuzzy vault has been given, and the minutiae locations centered on a hexagonal grid have been used to eliminate the chances of cross-matching attack. Li and Hu have proposed a fuzzy vault based template protection technique in [50] by utilizing the pair-polar structure of minutiae points. In this technique, the number of the fuzzy vault for a fingerprint impression is equal to the total number of minutiae because each minutia is considered as a reference point to compute the pair-polar minutiae structures.

Neu et al. in [51], have presented an improvement in the fuzzy vault scheme by means of minutia angles to eliminate the chances of correlation attack. In this work, authors have also addressed a new attack scenario, which is the angle correlation attack and is occurred due to the use of minutia angles. Mai et al. have discussed a biometric cryptosystem based technique in [52] to protect a fused multi-modal biometric template. In the technique, a dependency reductive method for bit-grouping and discriminative within the group for a fusion of multi-modal biometrics have been utilized to construct the binary template. In [53], Bobkowska et al. have discussed an approach for protecting the e-passport system by utilizing a fuzzy vault scheme. In order to do that, the authors have integrated different

biometric traits such as fingerprint, iris, and face biometrics.

2.1.2 Key-generation schemes

Key-generation schemes are also part of the umbrella term biometric cryptosystems, which can be defined by the way of generating the helper data and the key. In the key-generation scheme, a separate secret key is not required as the key is directly generated from the biometric data itself or from the helper data (which is also derived using the biometric data). The helper data does not need to be always stored in the database as some of the approaches do not use any kind of helper data to generate the key during authentication. However, if any attack happens then, there is no chance of revocability in such approaches. Further, a few approaches store the helper data in the database to generate the key during the verification/identification stage. The generic working of the key-generation scheme has been depicted in Figure 2.4. Key-generation schemes have the advantage of generating keys directly from the biometric data; however, the performance of biometric systems suffers due to the less discriminability. Nevertheless, this issue can be addressed by analyzing the key stability and key entropy of the approach which is based on the key-generation scheme. Quantization schemes, fuzzy extractors, and secure sketches are examples of the key generation schemes discussed in the literature.

Quantization is a procedure of converting a large set of input values to a smaller number of values, which contains concrete information about the input data. Similarly, the quantization scheme [54] has been used to generate a key directly from biometric data. In a quantization scheme, multiple biometric samples of a subject are used to find out the intervals of each feature parameter of input biometric data. Further, this information is stored in the database as helper data to compute the key during the verification stage. At the time of verification, the key is released directly from the query biometric data by using the interval

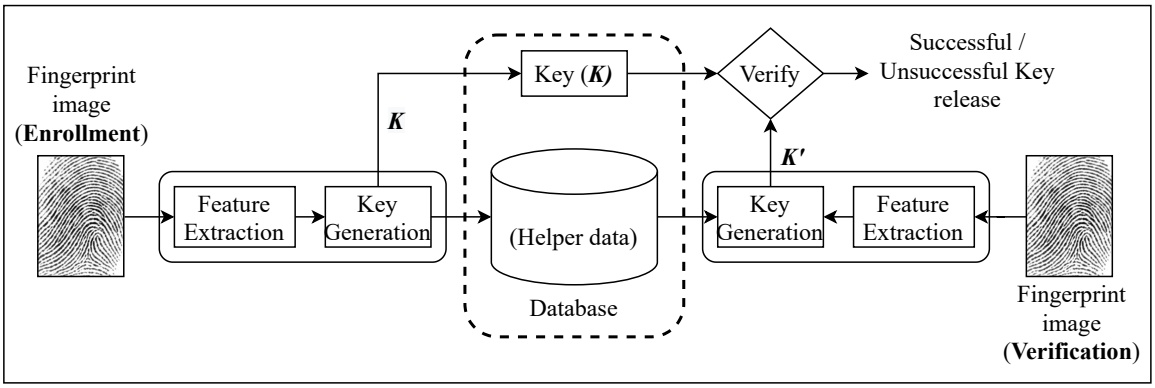


Figure 2.4: A schematic block diagram representing the working of a key-generation scheme.

information stored in the database. A fuzzy extractor and secure sketch are also examples of key-generation schemes. These techniques have been introduced by Dodis et al.[55]. The fuzzy extractor fetches the random secret key from the input biometric data. It is an error-tolerant primitive, which means the same random key would be generated even if the input changes a little bit (for example, different samples of the same subject). The secure sketch generates a public information, P_{info}, from an input biometric data I_1 and P_{info} does not reveal any idea about the input I_1; however, at the time of verification, I_1 can be retrieved from P_{info} if another input, I_2 is available, which largely overlaps with the input I_1. A brief description of the approaches related to the key generation scheme is given below.

Dodis et al. in [55] have introduced the concepts of the fuzzy extractor and secure sketch primitives. These both techniques are proposed to protect any kind of biometric and noisy data. In this work, authors have also shown the closely optimal constructions of these primitives by means of Hamming distance, edit distance, and set difference closeness measures. In [56], two approaches are proposed to show the application of biometric data for mutual authentication or key exchange over an insecure channel. These approaches are inspired by the fuzzy extractor, and secure sketch [55]. Sutcu et al. [57] have discussed about the issues related to the practical implementation of secure sketch theory. A generalized frame-

work has also been proposed in this work to implement and analyze the secure sketch for face biometric data. In [58] and [59], authors have shown the implementation of the fuzzy extractor and the secure sketch, respectively, for fingerprint biometric data. In [60], Sutcu et al. have shown the implementation of the secure sketch for the multi-model biometric system, which utilizes face and fingerprint biometrics. In [61], the definition of security and correctness for the fuzzy extractor has been extended. In this work, a generic construction of fuzzy extractor has been proposed, which works for both discrete and continuous noisy data. Tian et al. discussed about the solution for leakage-attack in remote authentication by using the fuzzy extractor in [62]. The generic framework that is proposed in this work allows a user to securely authenticate to the remote server by using his/her biometric data.

2.2 Cancelable Biometrics

Cancelable biometrics is one of the extensively used template protection techniques. In cancelable biometrics, transformed biometric features are stored in the database instead of original features in order to cater the privacy of the user's biometric data. The transformation of biometric data is performed in such a way that if an attacker steals the transformed biometric features (stored in the database), then it is not feasible for the attacker to reconstruct the original biometric template from the transformed one. As the transformed features are stored in the database, the matching is also performed in the transformed domain during the verification/identification stage. A schematic diagram representing the general working of cancelable biometrics is shown in Figure 2.5. In [5], various types of attacks on a biometric system have been discussed as depicted in Figure 1.4, and also the principle of cancelable biometrics has been introduced. Further, cancelable biometrics can be categorized into two major categories, which are salting and non-invertible transformations [32]. In the salting based techniques, the biometric features are transformed by utilizing a transformation func-

tion and the user-defined keys/parameters. These keys or parameters of the transformation function need to be secured due to the invertible behavior of transformation to a large extent in the salting techniques. In contrast, the template protection techniques based on the non-invertible transformation utilize a transformation function, which is non-invertible in nature. Hence, even if the transformation parameters/keys are compromised by an attacker, it is infeasible to reconstruct the original biometric features from the transformed template. We have incorporated a brief review of various techniques here that are presented in the literature and are related to the salting and non-invertible cancelable biometrics.

2.2.1 Salting techniques

In the literature, there is less number of salting techniques proposed as compared to the non-invertible transformation based techniques. A brief overview of a few prominent existing salting approaches is as follows. In one of the first works, Connie et al. [63] have proposed a technique to compute the revocable template by utilizing biometric salting. To compute the secured and revocable palmprint template, they have used Fisher Discriminant Analysis (FDA) for feature extraction, and binary discretization for computing the hash code called palm hash. These palm hash codes are stored in the smart card or chip for verification purposes. Teoh et al. [64] have proposed a new technique to secure the fingerprint template, and they have called their formulation as BioPhasor. Actually, the BioPhasor is a binary code, which is computed by combining the pseudo-random numbers (user-specific) with fingerprint features in an iterative manner. In [65], a new approach which is called Minutia Vicinity Decomposition (MVD), has been proposed. In this approach, the template has been computed using salting on geometrically invariant features, which are extracted from minutiae triplets. In this technique, the decomposition of minutia vicinity into minutiae triplets is performed, and geometrically invariant features are extracted using these triplets.

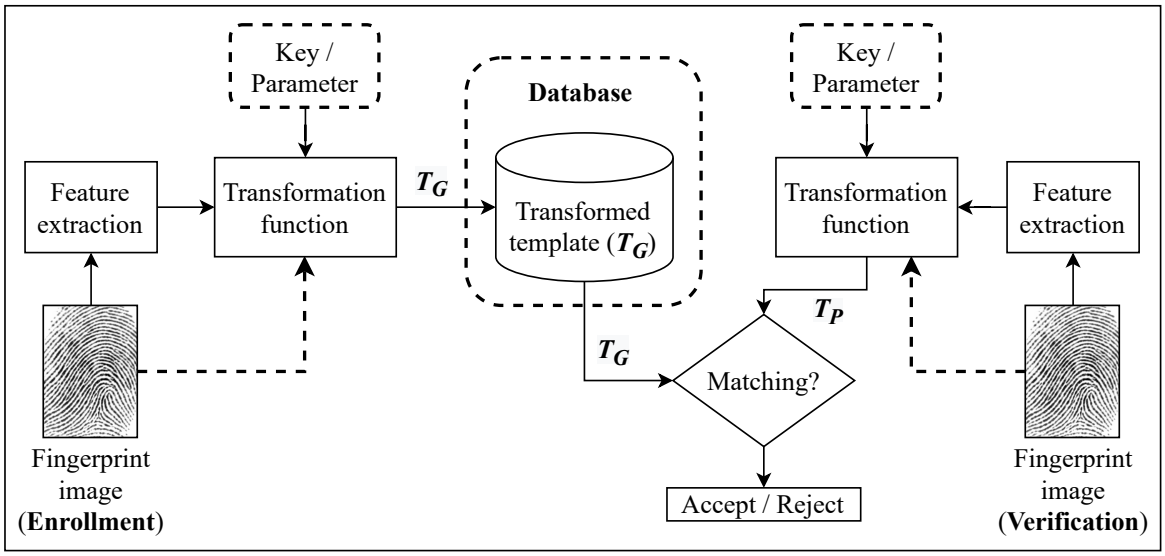


Figure 2.5: A schematic block diagram representing the generic working of the cancelable biometrics.

The template is generated using these features and salting (random offset).

2.2.2 Non-invertible transformation based techniques

In the non-invertible transformation, the biometric template is highly secure as it is infeasible to reconstruct the original biometric data from a transformed template even if an intruder acquires the transformation keys/parameters, unlike salting techniques. In the literature, several techniques based on non-invertible transformation have been proposed to protect the fingerprint template of an individual. In this section, we have incorporated a brief summary of a few of the existing prominent works. In [19], various approaches to generate a cancelable fingerprint template have been proposed. In this work, the templates have been constructed using three different ways, which include the transformation of the locations of minutiae in Cartesian and polar space, and surface folding. In the case of transformation in Cartesian space, minutiae locations are transformed in the Cartesian space, whereas in the case of polar space, the transformation is performed by utilizing the polar coordinates of minutiae. In the case of functional, surface folding has been used to transform the fingerprint

features. An alignment-free template protection technique based on the patches of minutia points has been proposed in [66]. The technique has generated the signature from patches of minutiae, and these signatures are transformed by using a key. In [67], a fingerprint template protection technique has been proposed based on non-invertible transformation. In the technique, pairs of minutiae have been projected on a circle around them, and by using bin-based quantization, a user template is generated. Lee et al. [68] have proposed an alignment-free technique to protect a fingerprint based user template. In this work, a binary string has been computed by using the minutiae locations, which are calculated after rotating the minutiae with respect to a reference minutia point. These locations are mapped into a 3-Dimensional array to generate the binary string, and the permutation of this binary string using a user key is used as a secured user template. In [69], Ahmed et al. have discussed a technique, which is based on pair-polar coordinates of minutiae. In this work, many-to-one mapping is used to map the pair-polar coordinates of minutiae into the different sectors around the reference minutia point, which is used to compute the pair-polar coordinate. Similarly, in [70], authors have made use of an infinite-to-one mapping scheme to secure the fingerprint template. Also, the proposed template protection technique is alignment-free in this work. The infinite-to-one mapping technique has been called Densely Infinite-To-One Mapping (DITOM) in [70].

In [71], Boult et al. have proposed a new technique in which they have used public-key encryption for both invertible and non-invertible transformations. In this technique, the transformed fingerprint user template is called a bio-token. In the technique, bio-token is stored in the database as a secured user template. Symmetric polynomials of different degrees have been used in [72] to compute the hash of minutiae points of a fingerprint image which is used as a user template. The intra-subject variations present in the fingerprint images make a significant difference between the hash values of fingerprint impressions of the

same subject and hence, pose a challenge in maintaining a stable performance in this technique. Ahn et al. [73] have proposed a non-invertible transformation based template protection technique that is alignment-free and utilizes the geometrical information of minutiae triplet to generate a secure user template. Kumar et al. [74] have proposed a technique to compute the secure template as an aggregation of symmetric hash functions calculated for multiple k-plets of minutiae points of a fingerprint image. Though this approach is capable of protecting a fingerprint based user template from different attacks, the performance of the system is seen reduced in this approach. Cappelli et al. [75] have introduced a new alignment-free minutiae representation to compute a cancelable fingerprint template, which is called Minutia Cylinder-Code (MCC). MCC is basically computed with respect to the spatial and directional contribution of minutiae points around a reference minutia point in a fingerprint image. Although the performance is significantly better as compared to other techniques, it suffers from the invertibility issue. Ferrara et al. [76] have extended the technique proposed in [75]. In their work, the generated templates are completely secure and non-invertible in nature. Though this technique computes non-invertible templates and has shown good performance, it lacks in terms of revocability. Ferrara et al. have proposed another technique based on MCC [75] in [21], which eliminates the major problems of MCC [75, 76] with respect to invertibility and non-revocability.

In [77], 3-tuple quantization based approach has been proposed to generate a bit string from the set of minutiae points. In this technique, a set of minutiae points have been computed by dividing the overall fingerprint image in the form of a polar grid. In [78], Multi-Line Code (MLC) has been used to compute the secure fingerprint template. The accuracy of the system is reduced due to the binary code in this technique, and in order to overcome it, a new similarity measure has also been introduced. In [79], authors have incorporated a Randomized Graph-Based Hamming Embedding (RGHE), which makes use of graphs

to generate the secured fingerprint template. In order to compute the fingerprint features, Minutia Vicinity Decomposition (MVD) has been used along with the randomized projection approach. In [80], authors have discussed a fingerprint template protection technique by using the k-Nearest Neighborhood Structure (k-NNS) of minutiae. To compute the cancelable template, k-NNS structures are computed by considering each minutia as a reference point and are mapped on a 2D grid. This information is further used to form a binary string. These binary strings are then converted into the final cancelable template using DFT and non-invertible transformation. In [81], in order to compute the secured fingerprint template, features are generated using the Delaunay triangulation of minutiae points. These Delaunay triangulation based features are further transformed by using the non-invertible transformation in order to compute the final cancelable template.

Jin et al. [82] have used a kernelized PCA based approach to construct a fixed-length structure utilizing the minutiae points in a fingerprint image and have used multiple samples of a subject at the time of enrollment. In [83], in order to compute the cancelable fingerprint template, a blind system identification technique has been introduced. In this work, the authors have made use of a quantized minutiae pair vector in order to build the blind system identification. Sandhya et al. in [84], have proposed a technique to construct the non-invertible fingerprint template. To compute the non-invertible template, authors have utilized a different set of features from the Delaunay triangulation structure of minutiae points. These sets of features are mapped into a 3D grid to construct a binary vector, which is eventually used as a template after computing the transformation. In [85], Khodadoust and Khodadoust have implemented indexing of fingerprints by utilizing extended Delaunay triangulation along with the k-means clustering for retrieval of fingerprints. According to this work, the proposed indexing approach can be used to improve the efficiency of Automatic Fingerprint Identification Systems (AFISs). Sandhya and Prasad [86] have utilized

fused feature structures to compute a secure fingerprint template. In this work, the authors have computed two types of features from minutiae points, namely local and distant features. These features are further converted into bit-strings, and the fusion of bit-strings is used to compute the cancelable template.

In [87], Wang et al. have used partial Hadamard transform to obtain a secure user template. In their technique, the transformation has been performed on the DFT of binary string computed from the fingerprint features to construct the cancelable user template. A new approach has been proposed in [88], which is called dense registration of a fingerprint, to eliminate the intra-subject variations like distortions that arise due to the elasticity of the skin. To design a secure partial fingerprint authentication system, Lee et al. in [89] have proposed a technique based on minutiae points along with a new feature, called the ridge shape feature. Wang et al. in [90] have utilized the local minutiae structure by extraction of zoned minutiae pairs and have performed a non-invertible transform based on DFT to construct a cancelable user template. Moujahdi et al. [91] have introduced a fingerprint template protection technique, which is known as Fingerprint Shell. In this work, the authors have utilized the distances of minutiae points from a singular point to compute the spiral curve, and Hausdorff distance has been employed to perform the matching between spiral curves. Jain and Prasad in [92] have further used the fingerprint shell along with a clustering technique to index fingerprints. There is a major limitation of the template constructed using fingerprint shell [91]. In the case of an attack on the database, the distances, which are used to compute the user template (spiral curve), can be easily computed from the spiral curve. To eliminate this shortcoming of the fingerprint shell, Ali and Prakash have proposed an enhanced form of fingerprint shell in [93, 94], which is further improved in [95, 96]. In [97], a translation/rotation independent technique has been proposed where locations of minutiae points are transformed by using a non-invertible transformation and

user-specific key/parameters to secure the original fingerprint template. This technique has been further improved in [98]. Trivedi et al. [99] have proposed a non-invertible fingerprint template generation approach by means of minutiae triplets. The Delaunay triangulation has been used as triplets and the geometrical features are extracted to compute the template. The computed template seems secure in this work; however, the proper analysis hasn't been provided and the performance is degraded as compared to the state-of-the-art techniques. Yang et al. [100] have proposed a multi-biometric system based on fingerprint and finger-vein. Geometric features of minutiae pairs from fingerprint and image features from finger-vein are used to compute the fused multi-biometric template. This work has also been tested for fingerprint biometrics alone and the performance is not significant as compared to existing approaches. However, the presented approach has performed pretty well for the multi-biometric scenario. In [101], Ali et al. have proposed a framework based on polynomial curves, which is known as Polynomial Vault. In this work, the polynomial curve is generated using the transformed distances of minutiae points from a singular point. In [102], a Delaunay triangulation-based template protection approach has been discussed. This approach utilizes the internal angles of Delaunay triangles and orientation values of minutiae to construct the feature vector, which is transformed by means of user-specific keys. In [103], Tetrahedron structures are computed using the combination of four minutia points. Further, the extracted features from these structures are transformed to compute the secure template. Although the generated templates through the presented approach are shown to be secured, there is a possibility of the missing minutiae problem since the performance deteriorates for low-quality fingerprint images. The minutia points in [104] have been divided into four groups around the singular point. The transformed minutiae information has then been calculated using the user-specific keys unique to each group. In this work, although the template is non-invertible, the recognition performance is shown to be

very low. A feature-adaptive projection based approach has been proposed in [105] to protect the minutiae-pair features of fingerprint images. In this work, a new projection scheme has been adopted; however, the performance is not good and has not been evaluated on challenging protocols. A two-stage feature transformation approach has been presented in [106] to secure the fingerprint template. Although the performance is better than the existing works, the technique uses more than one sample to compute the secure template.

2.3 Hybrid and Homomorphic Encryption based Techniques

In the literature, a few more techniques based on hybrid and homomorphic encryption have been proposed to protect the fingerprint template. Hybrid techniques combine the functionality of different template protection techniques from cancelable biometrics and biometric cryptosystems. By using these kinds of combinations, the overall security of the biometric systems is shown to increase significantly, along with providing a higher recognition rate. Nagar et al. [107, 108] have developed a hybrid technique to secure the fingerprint template. In this work, a fuzzy commitment scheme is utilized to encrypt the polynomial, which is evaluated using a fuzzy vault scheme. The authors have used a minutiae descriptor, which constitutes orientation values and ridge count around a minutia's neighborhood. It is shown that the combination of two different biometric cryptosystems in this work has improved security significantly. In a recent work, Ouda et al. [109] have presented a hybrid approach, which is named as a cancelable biometric vault. This approach combines the functionality of cancelable biometrics in order to compute the secure features and encodes them by means of a cryptographic key.

Homomorphic encryption is an encryption scheme that allows performing the compu-

tation on encrypted data. This encryption scheme is adapted in some of the works for encrypting the biometric data in order to protect the original template. The concept of homomorphic encryption resembles with the cancelable biometrics as the matching is performed in the encrypted domain in this case as well. Some of the works related to the application of homomorphic encryption for biometric security are discussed here. In [110], a protocol has been proposed by Upmanyu et al. to provide secure authentication using hand geometry. Here, the biometric data is encrypted by means of an asymmetric encryption approach, and the generic Support Vector Machine (SVM) is used for verification in a client-server based architecture. Marta et al. in [111] have proposed a multi-modal biometric system for fingerprint and online signature based on a homomorphic probabilistic encryption approach. In this work, the proposed encryption based technique has been analyzed for three different types of fusions, namely, feature-level fusion, score-level fusion, and decision-level fusion. In [112], a fully homomorphic encryption based technique has been proposed by Morampudi et al. to protect the iris biometric data. In this work, Hamming distance measure is used during the verification stage.

Chapter 3

Securing a Fingerprint Template using Fuzzy Vault

In this chapter, a fuzzy vault based technique is proposed to prevent identity theft and secure the fingerprint information (essentially, minutiae points) stored in the database. A block diagram representing various steps involved in a fuzzy vault scheme is shown in Figure 3.1. Furthermore, we propose a novel technique to filter the genuine vault points from a combination of genuine and chaff points used in the fuzzy vault technique during the verification stage. Since minutiae points are used to construct the vault, it is a challenging task to align the probe and the gallery fingerprint images during verification. In order to do that, a Principal Component Analysis (PCA) based alignment technique is proposed to align the gallery and probe templates. The proposed technique is evaluated on three different Fingerprint Verification Competition (FVC) databases that come under the FVC2002 and FVC2004. Subsequently, the obtained results are compared with that of the recent existing techniques in the literature and are found to be superior in terms of the Genuine Acceptance Rate (GAR), False Acceptance Rate (FAR), and Equal Error Rate (EER). Further, the

The work presented in this chapter has been published in the paper: "*An enhanced fuzzy vault to secure the fingerprint templates*", Multimedia Tools and Applications, 80, 33055–33073 (2021). DOI: 10.1007/s11042-021-11325-w

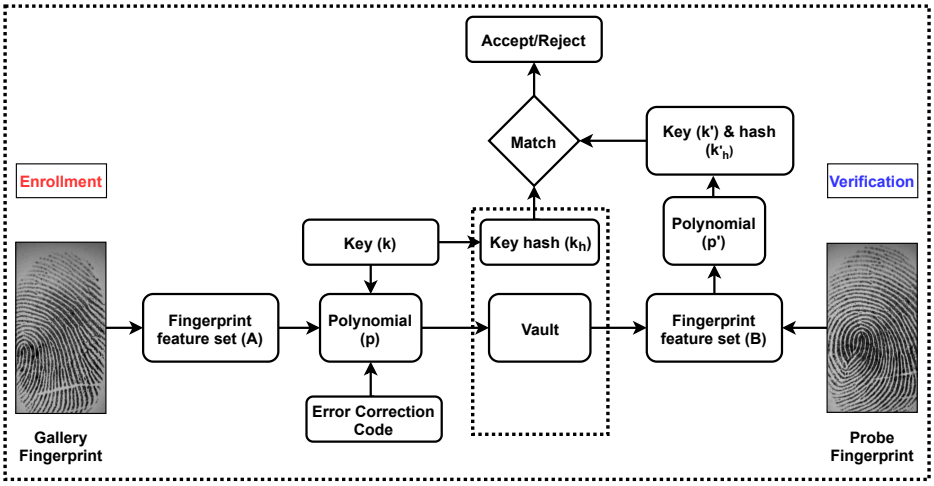


Figure 3.1: Block diagram representing the basic operations of fuzzy vault scheme.

proposed technique and the experimental analysis are also discussed in the chapter.

3.1 Proposed Technique

In fingerprint biometrics, minutiae points are the prominent features, which are mostly used along with the singular points ($i.e.$, core and delta points) for human recognition. An example of a fingerprint image with minutiae marked on it is shown in Figure 3.2. In fingerprint-based biometric systems, attributes of minutiae points, $i.e.$, minutiae locations and orientation values, are commonly stored in the database as a user template; however, this information is sensitive and can lead to identity theft and unauthorized access, if gets compromised. Hence, the security of the user template is of great concern.

In the literature, fuzzy vault [9] is one of the biometric cryptosystems that has been used to provide security to the fingerprint-based user template. Our proposed fingerprint template protection technique relies on fuzzy vault and is inspired by the implementation of fingerprint fuzzy vault proposed in [30]. In our technique, first, minutiae points are extracted from a fingerprint and from them, a set of minutiae points that are well-separated is determined. Subsequently, these minutiae points, known as the locking set, are aligned

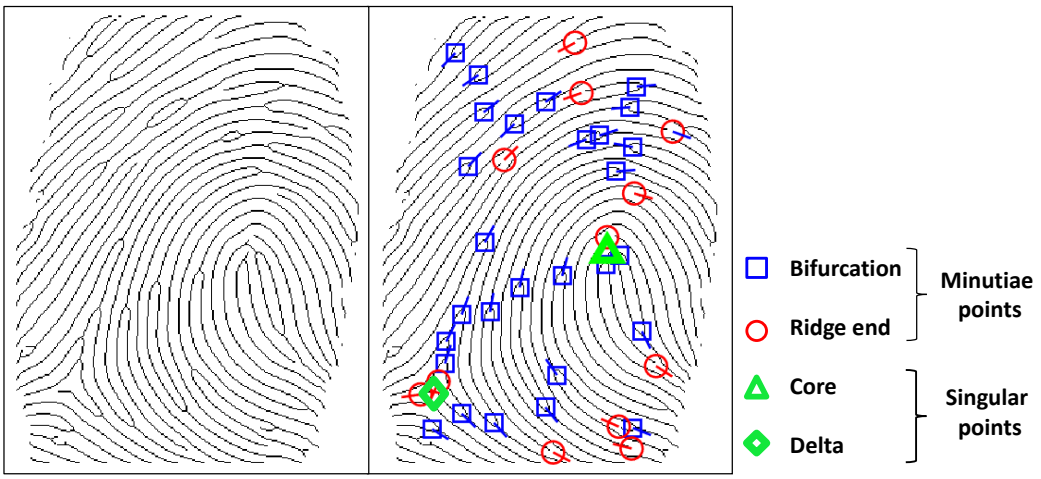


Figure 3.2: Representing original thinned fingerprint image (left) along with the extracted feature points (right).

using PCA. The obtained points are further encoded into a fuzzy vault which is stored in the database while performing the enrollment of a user with the biometric system. As the distortion in a fingerprint impression increases when one moves towards the boundary of the fingerprint from the center, instead of considering all the well-separated minutiae points of the fingerprint, only the well-separated minutiae points close to the center (that is, the singular point) of the fingerprint, known as unlocking set, are considered from the probe template at the time of verification. During the decoding process, probe minutiae points are first aligned using PCA before being used to decode the vault for authentication purposes. A block diagram depicting the different steps of the proposed technique, for both enrollment and verification, is shown in Figure 3.3. The following discussion provides a detailed description of the proposed technique.

3.1.1 Feature extraction and representation

A minutia point in a fingerprint image is represented using its location and orientation information. As it has been shown in [30], the intra-class variation in the orientation value is found to be more as compared to the variation in the location of the minutiae points.

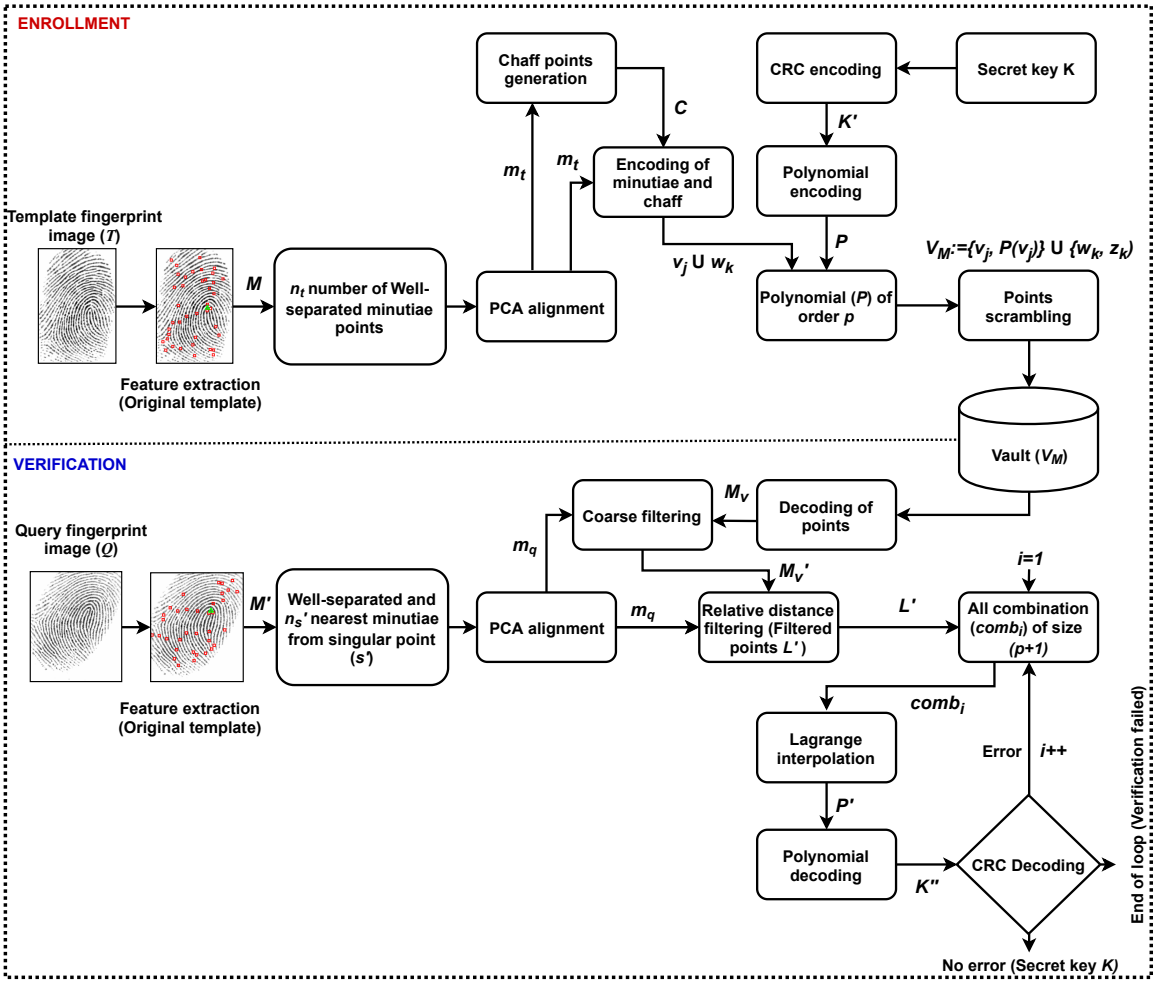


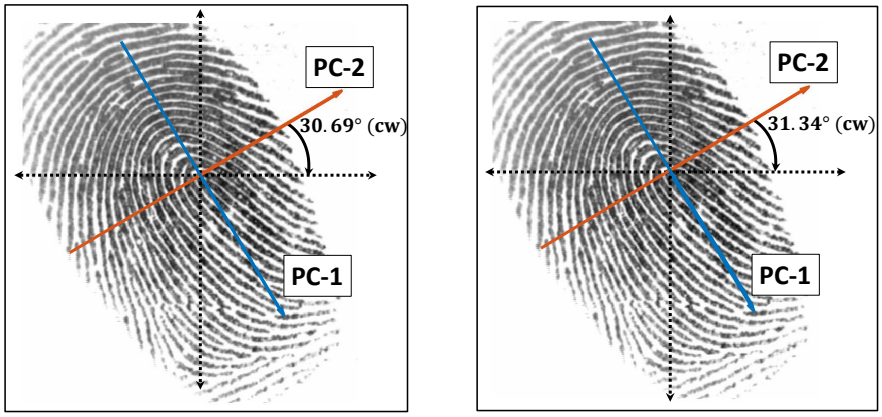
Figure 3.3: Block diagram representing the different steps followed during enrollment and verification in the proposed technique.

Hence, we consider only the location information of minutiae points to represent them in the proposed technique. Let $M = \{(x_i, y_i),\ i = 1, 2, ..., n\}$ be the set of minutiae points present in a fingerprint image, where $(x_i,\ y_i)$ denotes the location of i^{th} minutia point and n denotes the total number of minutiae points present in the fingerprint image. Further, let (s_x, s_y) be the location of the singular point S in the fingerprint. Out of n minutiae points available in a fingerprint, we select n_t well-separated minutiae points from the set M, before encoding the vault. We use the Euclidean distance based criterion to identify well-separated minutiae points where a minutia point is selected if its distance from all other minutiae points is greater than a predetermined threshold t_1. If the value of n_t is less than u_{min},

where u_{min} is the minimum number of minutiae that should be matched to unlock the vault, the fingerprint is rejected and is not considered for encoding. The selected n_t minutiae points of the fingerprint are further used to encode the vault after performing the necessary alignment as discussed in the next section.

3.1.2 Alignment of fingerprint templates

In a fingerprint-based biometric system, alignment of the fingerprint images is essential at the time of matching. In [30], an alignment technique is being proposed which utilizes high curvature points of ridges as helper data and uses it for alignment. During the enrollment phase, helper data is stored in the database along with minutiae attributes and is used in the matching of two fingerprints at the time of authentication. However, in this approach, there is a need to store a piece of extra auxiliary information (that is, helper data) in the database to perform the alignment. Moreover, this information can be attacked by an adversary. Hence, we propose a technique to align two fingerprint images for matching them without storing any auxiliary information in the database. The technique is based on PCA [10]. In [10], PCA has been demonstrated to align different types of images such as MRI scans of brain, images of MNIST dataset [113], and fingerprint images. For performing alignment in this work, coordinates of all the pixels of fingerprint impression (including ridges and valleys) are used as an input to PCA. However, the use of coordinates of all the pixels makes the computation of principle components very slow in PCA. To overcome this, we propose the use of only coordinates of pixels of thinned ridges. This drastically reduces the computational cost of alignment without compromising the correctness of the alignment. Figure 3.4 shows the comparison of alignment obtained by our technique with that of [10]. We observe that the principal component directions in both the cases are very similar. This is to be noted that the PCA analysis is carried out using the pixel coordi-



(a) (b)

Figure 3.4: Principle components obtained using (a) Proposed technique, (b) Technique given in [10].

nates of thinned fingerprint ridges, whereas obtained principal components are used to align the original fingerprint template which mainly contains minutiae location and orientation values. Alignment of the minutiae points of a fingerprint image by using the principal component, as discussed here, makes the original fingerprint template rotation invariant. The complete procedure followed in the alignment is described below.

In the technique, to align minutiae points of the gallery and probe fingerprint images before vault encoding and decoding, thinned images of these fingerprints are used. To get the thinned image of a fingerprint in the proposed technique, the fingerprint image is first enhanced using the techniques proposed in [114, 115]. Next, the binary equivalent of the enhanced image is converted into a thinned binary image by utilizing morphological operations for thinning. From the obtained thinned image, the coordinates of pixels (representing thinned ridges) are extracted, and principal components of the distribution of these pixels are obtained using PCA. To align the minutiae points of gallery and probe fingerprint images, these points are projected along with the directions of obtained principal components from their respective thinned images. Figures 3.5 and 3.6 show the various steps involved during alignment and an example of aligned gallery and probe minutiae sets, respectively.

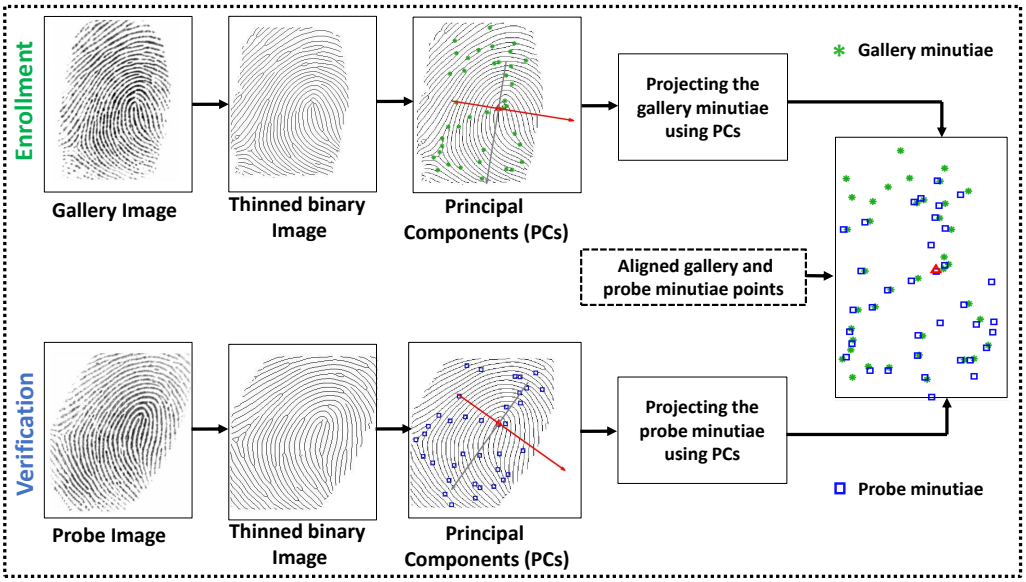


Figure 3.5: Different steps followed to align the fingerprint images using PCA.

Let there be q pixels in a thinned fingerprint image. Further, let matrix $\mathbf{A}$ of size $q \times 2$ contains coordinates of all such pixels and is defined as below where a_i and b_i represent the X and Y coordinates of i^{th} pixel in the thinned image, respectively.

$$\mathbf{A} = \begin{bmatrix} a_1 & b_1 \\ a_2 & b_2 \\ \vdots & \vdots \\ a_q & b_q \end{bmatrix} \tag{3.1}$$

The matrix $\mathbf{A}$ is analyzed using PCA to get the principal components. As we know that the shape of a fingerprint impression is generally elliptical, the PCA gives two principal components directed along the major and minor axes of the ellipse bounding the fingerprint image. To compute the principal components in the PCA, first, the covariance matrix is calculated and subsequently, it is followed by the Eigen decomposition of the covariance matrix. To compute the principle components of the data represented by $\mathbf{A}$, its covariance matrix $\mathbf{C}$ of size 2×2 is computed as follows after centering the ridge points around the mean (m_a,m_b).

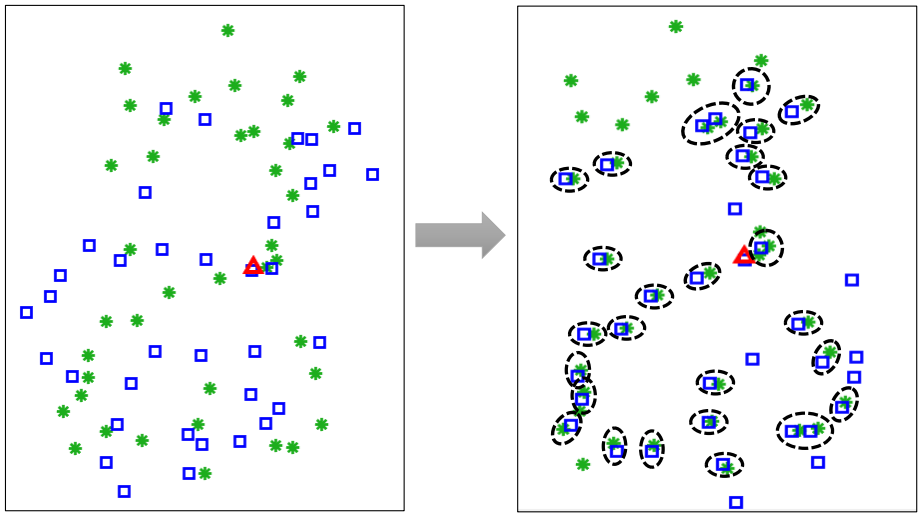


Figure 3.6: Minutiae points of the gallery (green stars) and probe (blue squares) fingerprint images before and after the alignment. Here, red triangle and circular black signs represent the singular point, and matched gallery and probe minutiae, respectively.

$$\mathbf{A} = \begin{bmatrix} a_j - m_a & b_j - m_b \end{bmatrix}, \text{where } j = 1, 2, ...p \tag{3.2}$$

$$\mathbf{C} = \frac{1}{(p-1)} \times \mathbf{A}^T\mathbf{A} \tag{3.3}$$

Principal components are computed by performing the singular value decomposition of the covariance matrix **C** using Equation 3.4. In the equation, **U** and **V** are two orthogonal matrices whereas **S** is a diagonal matrix. The matrix **S** contains Eigenvalues in decreasing order where the first diagonal element contains the largest value. In matrix **U**, each column contains an Eigenvector corresponding to an Eigenvalue in **S**. The Eigenvector obtained with respect to the largest Eigenvalue (*i.e.*, the first column of **U**) corresponds to the first principal component in PCA.

$$\mathbf{C} = \mathbf{USV}^T \tag{3.4}$$

$$\mathbf{U} = \begin{bmatrix} u_{11} & u_{12} \\ u_{21} & u_{22} \end{bmatrix} \tag{3.5}$$

In the matrix **U**, the first and second columns represent the first and second principal components respectively, which are computed corresponding to the first and the second largest Eigenvalues respectively. To align a set of minutiae points of a fingerprint image, the points are multiplied by matrix **U** obtained from the respective thinned image. It is believed that if the gallery and probe images that are being matched belong to the same subject, their principal components obtained from the respective thinned images will be oriented in the same direction with respect to the image data. Due to this, when minutiae points of gallery and probe images are projected along with their respective principal components, they indirectly get aligned. This process makes the orientation of the distributions of minutiae points of the gallery and probe fingerprints aligned with each other; however, there might exist a translation between them. In order to remove the translation component as well, minutiae points are first translated in such a way that they get centered around a singular point before projecting them using principal components. The final oriented minutiae points can be given as follow.

$$\begin{bmatrix} x_i & y_i \end{bmatrix} = \begin{bmatrix} x_i - s_x & y_i - s_y \end{bmatrix} \times \begin{bmatrix} u_{11} & u_{12} \\ u_{21} & u_{22} \end{bmatrix} \tag{3.6}$$

Further, these resultant locations of minutiae points are used to encode the fingerprint vault in the case of a gallery fingerprint image during the enrollment. In contrast, during the verification stage, these aligned minutiae locations of a probe fingerprint image are used to unlock the fingerprint vault.

3.1.3 Fingerprint fuzzy vault encoding

The well-separated and aligned minutiae points of the fingerprint are encoded into a fuzzy vault to secure them. Let $\{(m_t)_i\}_{i=1}^{n_t}$, where $n_t >= u_{min}$ be the set containing well-separated aligned minutiae points. To initiate the encoding process, a set of chaff points $C = \{(m_c)_i\}_{i=1}^{n_c}$ are generated in such a way that the minimum distance of each chaff point to all the points in $\{(m_t)_i\}_{i=1}^{n_t} \cup \{(m_c)_i\}_{i=1}^{n_c}$ is greater than the threshold t_1. The number of chaff points is kept quite large as compared to the number of minutiae points (that is, $n_c >> n_t$) in vault generation. Further, let the coordinates (x, y) of a minutiae point be represented in terms of an 8-bit long binary string, denoted as B_x and B_y respectively. The binary strings B_x and B_y are concatenated to form a 16-bit long binary string $[B_x + B_y]$ which is further converted to a decimal equivalent. The same process is followed to compute the decimal equivalents for all the minutiae as well as the chaff points. These sets of encoded minutiae and chaff points are represented as $EM^t = (v_j)_{j=1}^{n_t}$ and $EC = (w_k)_{k=1}^{n_c}$ respectively. Once encoding of the minutiae and the chaff points is available, a $16 \times p$ bits long secret key K is generated to construct an encoding polynomial of degree p. Further, a 16-bit long CRC code is appended to the key K using the generator polynomial of CRC given in Equation(3.7), resulting in a new secret key K' of length $16 \times (p + 1)$. Now, the key K' is partitioned into 16-bit long $(p + 1)$ strings and the decimal equivalents of these strings are used as the coefficients of the encoding polynomial P of degree p. Let this polynomial has coefficients *i.e.* $c_0, c_1, c_2...., c_p$, then the polynomial can be given by Equation(3.8).

$$G(r) = r^{16} + r^{15} + r^2 + 1 \tag{3.7}$$

$$P = c_p x^p + c_{p-1} x^{p-1} + ... + c_0 \tag{3.8}$$

The values of encoded minutiae set EM^t are mapped onto the polynomial P giving rise to a new set $P(EM^t) = \{P(v_j)\}_{j=1}^{j=n_t}$ along with locking set $lm = \{v_j, P(v_j)\}_{j=1}^{n_t}$. For the encoded chaff points EC, corresponding z_k values denoted as $cp = (w_k, z_k)_{k=1}^{n_c}$, are chosen in such a way that the value of z_k must not lie on the polynomial. The union of sets lm and cp is computed and is further shuffled to get the final encoded vault V_M, referred as a fuzzy vault, for the fingerprint. This vault V_M is stored as a template in the database for the corresponding fingerprint which is being encoded. It can be noted that along with the vault, there is no other auxiliary information being stored in the database in the proposed technique unlike done in [30].

3.1.4 Fingerprint fuzzy vault decoding

At the time of authentication, a probe fingerprint image is considered authenticated or verified if it successfully decodes the vault. The decoding process goes as follows.

- Let the set of minutiae points extracted from the probe fingerprint image be M'. From the set M', let n_q well-separated minutiae points are obtained following the similar criterion used during the encoding or enrollment process discussed in Section 3.1.1. When the set M' is used to filter the chaff points from the vault, the filtered genuine points are usually more which makes the decoding process of vault very slow. Hence, out of n_q minutiae points present in M', only n'_s minutiae points which are closest to the singular point S' of the probe fingerprint image are considered in the decoding process and other minutiae points of the probe image are ignored. This is due to the fact that, due to moisture in the finger, skin elasticity, and pressure applied during fingerprint capture, distortion occurs and it is more in the ridges present towards the corners of the fingerprint image [116, 20]. Further, these selected minutiae points are aligned using PCA as discussed in Section 3.1.2. If $n_q < n'_s$ then all minutiae

points are selected in the encoding process; however, the value of n_q should always be greater than or equal to the value of u_{min}. Let the final set of selected and aligned minutiae points of the probe image used in the decoding process be $\{(m_q)_i\}_{i=1}^{n'_s}$, where $n'_s \geq u_{min}$.

- In order to unlock the vault, the value of x-coordinate of each vault point (V_M) is converted to a 16-bit long bit string which is further partitioned into two 8-bit binary strings B_x and B_y respectively. The decimal equivalents of these binary strings provide the x and y attributes of the minutiae and chaff points. Finally, let the obtained set of vault points be represented as $M_v = \{(x_i, y_i)^v\}_{i=1}^{n_t+n_c}$.

- The minimum distance is calculated from each point of the set M_v to all the selected minutiae points of the probe image. If the obtained distance is greater than the threshold t_2, then the points from set M_v are considered as chaff points. This procedure is known as coarse filtering [30] and it filters most of the chaff points and produces a new set $M'_v = \{(x_k, y_k)\}_{k=1}^{N}$. It is observed that some of the chaff points may still remain there in the set M'_v, hence these are further removed by utilizing our proposed filtering technique which is based on the relative distance minutiae matching. The technique is being explained in detail in the next point.

- **Relative distance minutiae matching:** Set M'_v is further filtered to obtain the final set of genuine minutiae points to define the unlocking set. To get the unlocking set, for every minutiae point in the probe image, a point that satisfies the following two conditions is chosen from the set M'_v.

  - Distance between probe minutiae and chosen vault minutiae points is less than the threshold t_2.

  - Distance of the chosen vault point from the singular point is the same as the distance of the probe minutia point from the singular point. This condition is imposed as the relative distance does not vary due to translation or rotation.

- Let the final set of filtered points from vault V_M be L'. It is required that the number of points in the set L' should be greater than or equal to u_{min} which is basically $(p+1)$, as at least these many points are needed to reconstruct the polynomial using Lagrange polynomial interpolation. Now, all possible combinations of $(p+1)$ points from the set L' are obtained and a polynomial is constructed for each combination using the Lagrange interpolation method. The constructed polynomial for any combination can be given as follows.

$$P'(x) = c'_p x^p + c'_{p-1} x^{p-1} + ... + c'_0 \tag{3.9}$$

where, $c'_0, c'_1, ..., c'_p$ are the coefficient of the constructed polynomial $P'(x)$ using Lagrange interpolation method.

- The coefficients of the polynomial P' are then used to generate a $16 \times (p+1)$ long bit-string K'' by following the reverse procedure used during enrollment. Further, the binary string K'' is decoded using a CRC decoder to detect the error. If there is no error in K'', then the CRC code (*i.e.* 16-bit least significant bit) is removed from K'' and the remaining binary string gives the secret key. If the obtained value is the same as K, then the authentication is considered successful otherwise, the same procedure is followed for the remaining combinations of $(p+1)$ points. If there is not a single combination of $(p+1)$ points exist which can release the secret key K, then the authentication with respect to the considered probe fingerprint image is declared failed.

3.2 Experimental Analysis

The proposed technique has been evaluated on three publicly available fingerprint databases, $viz.$, FVC2002 DB1, FVC2002 DB2, and FVC2004 DB1. The description of these databases has been provided in Section 1.4. The experimental analysis has been performed in terms of the recognition performance and security.

3.2.1 Performance analysis

In order to evaluate the performance of the proposed technique, GAR, FAR, and EER are used as evaluation metrics. The details of these metrics are provided in Section 1.2.4. To compute these metrics, the 1-versus-1 (1-vs-1) protocol is being used as discussed in Section 1.4. The summary of different parameters being used in the fuzzy vault implementation is given in Table 3.1. It provides information of the number of genuine minutiae points (n_t) that are selected after performing the processing during the enrollment and the value of maximum genuine probe minutiae points (n'_s) being used. The degree of encoding polynomial decides the length of the secret key K where for degree p, it is 2^p bits. Hence, at least $(p + 1)$ points are needed to unlock the secret key during the authentication, and if the number of selected genuine minutiae points in the fingerprint image (either gallery or probe) is less than the required minimum $(p + 1)$, then the fingerprint impression is not considered in encoding or decoding processes. In order to encode the attributes of minutiae points (that is, x and y coordinates), the length of the bit strings B_x and B_y is kept 8-bit long under the Galois field $Gf(2^{16})$. We have considered the number of chaff points nearly ten times to the number of genuine minutiae points in the image. Other than these parameters, there are three different thresholds that have been used. These are t_1, t_2, and t_3, which are used for the computation of well-separated minutiae points, for removing the chaff points from the vault points, and for relative distance filtering, respectively.

Table 3.1: Parameters used for the implementation of a fuzzy vault

Parameters	**FVC2002 DB1**	**FVC2002 DB2**	**FVC2004 DB1**
Authentic points in a vault (V_M), n_t	22-30	22-30	22-30
Maximum value of n'_s	25	25	25
Encoding polynomial degree, p	8-10	8-10	8-10
Number of chaff points, n_c	200	200	200
Number of points in a vault (V_M), $n_t + n_c$	222-230	222-230	222-230
Threshold for well-separated minutiae, t_1	25	25	25
Threshold for filtering out the chaff points, t_2	12-14	12-14	8-12
Threshold for relative distance filtering, t_3	8, 10	8, 10	8, 10

Table 3.2: Percentage value of GAR and FAR using different threshold values and 1-vs-1 protocol

Databases	p	**GAR / FAR on Threshold, t_2 & t_3**					
		14 & 10	**14 & 8**	**13 & 10**	**13 & 8**	**12 & 10**	**12 & 8**
FVC2002 DB1	8	93 / 3.39	91 / 1.09	92 / 2.50	91 / 0.72	89 / 1.05	87 / 0.32
	9	90 / 1.23	88 / 0.40	88 / 0.78	85 / 0.28	83 / 0.30	81 / 0.10
	10	85 / 0.30	83 / 0.04	83 / 0.24	82 / 0.04	81 / 0.04	80 / 0.04
FVC2002 DB2	8	97 / 3.11	94 / 0.98	95 / 2.32	92 / 0.66	95 / 1.09	92 / 0.26
	9	95 / 1.01	92 / 0.20	92 / 0.70	90 / 0.14	92 / 0.28	90 / 0.06
	10	92 / 0.40	89 / 0.06	90 / 0.24	88 / 0.04	87 / 0.12	85 / 0.04

There are different scenarios that have been used in the literature to evaluate the fuzzy vault based techniques. In a few works, authors have used one sample for gallery and one sample for probe, whereas, in a few others, two samples for gallery and one for the probe have been used. There are a few more combinations, which have been experimented with. In these analyses, it has been observed that though encoding of the vault using one sample is desired, it is challenging, and the performance of the system gets enhanced if more than one sample are used in the encoding process as it makes more information available in the vault. To evaluate the proposed technique, we have used just one sample for the gallery and one for the probe. The evaluation process is similar to the one followed in the 1-vs-1 protocol, as discussed earlier. Results obtained by the proposed technique under the 1-vs-1 protocol for different values of parameters are given in Table 3.2. In the table, the values of GAR and

FAR are given by considering the varying value of p (the degree of the polynomial), and the thresholds t_2 and t_3 for FVC2002 DB1 and FVC2002 DB2 databases. It is clearly observed from Table 3.2 that as the degree of polynomial p increases, the value of FAR decreases. However, increasing the value of p does not always provide good performance as it may reduce the value of GAR to a quite extent. On the other hand, decreasing the value of p may increase the value of FAR to a quite extent. Hence, it is desired to choose the degree of the polynomial in such a way that the overall performance of the biometric system in terms of the EER is optimum. As depicted in Table 3.3, we find that when the value of p is chosen in the range of 8 to 10, optimal performance in terms of the EER as well as GAR / FAR is obtained for $p = 8$. If the value of p is chosen to be less than 8 or greater than 10, the performance deteriorates as evident from the values of the GAR and the FAR. Further, the results of the proposed technique obtained on the three different databases demonstrate the effectiveness of the technique. To show the superiority of the proposed technique over the existing techniques, results are compared and shown in Table 3.3. It is evident from the table that the proposed technique achieves the highest GAR among the competitive techniques. Similarly, the value of FAR is lower than the existing techniques for the high degree of the polynomial and is always less than 1% for all the databases. This makes the proposed technique an effective and robust technique to protect the fingerprint template.

The Receiver Operating Characteristics (ROC) curves, which plot the values of GAR vs. FAR, are also drawn for different databases, considering the degree of polynomial p as 8. To plot the ROC curves, the values of GAR and FAR are computed for different values of thresholds t_2 and t_3. The intersection point of the EER-line and ROC curve gives the value of EER, which is obtained on the three different databases for the proposed technique as depicted in Figure 3.7. The performance of the proposed technique is compared with that of the recent techniques in terms of EER, and it is presented in Table 3.3. The comparison

Table 3.3: Comparison of the performance of the proposed technique with various existing techniques in terms of percentage values of GAR, FAR, and EER

Various techniques	**GAR / FAR (EER)%**		
	FVC2002 DB1	**FVC2002 DB2**	**FVC2004 DB1**
Nandkumar et al. [30]	-	91 / 0.01 (-)	-
Li et al. [117]	85 / 0.00 (-)	93 / 0.00 (-)	-
Yang et al. [118]	81 / 0.38 (8.46)	83 / 0.09 (5.7)	-
Nagar et al. [119]	-	85 / 0.13 (3)	-
Hartloff et al. [120]	63.46 / 0.29 (13.2)	73.52 / 0.23 (9)	-
Yang et al. [81]	- / - (5.93)	- / - (4)	-
Jin et al. [79]	- / - (4.36)	- / - (1.77)	- / - (24.71)
Sandhya and Prasad [80]	- / - (4.71)	- / - (3.44)	-
Proposed technique			
$p = 8$	91 / 0.72 (4.00)	94 / 0.98 (3.10)	77 / 6.7 (11.95)
$p = 9$	85 / 0.28 (4.60)	92 / 0.20 (3.40)	67 / 3.52 (16.46)
$p = 10$	82 / 0.04 (5.51)	89 / 0.06 (4.89)	62 / 1.77 (18.35)

"-" denotes non-availability of data.

shows that the proposed technique achieves a much lower value of EER as compared to the existing techniques on the FVC2002 DB1, FVC2002 DB2, and FVC2004 DB1 databases as shown in Table 3.3 except for [79] on the FVC2002 DB2 database. However, the proposed technique has performed better as compared to this technique [79] on FVC2002 DB1 and FVC2004 DB1 databases where later one is considered as a quite challenging database. Hence, the overall comparison shows the superiority and robustness of the proposed technique over the existing techniques.

3.2.2 Security analysis

The security of fuzzy vault has been discussed extensively in [30, 49] with respect to three attack scenarios. We use the same scenarios to analyze the security of the proposed technique.

- Brute force attack: In this attack scenario, an attacker tries to unlock the vault using

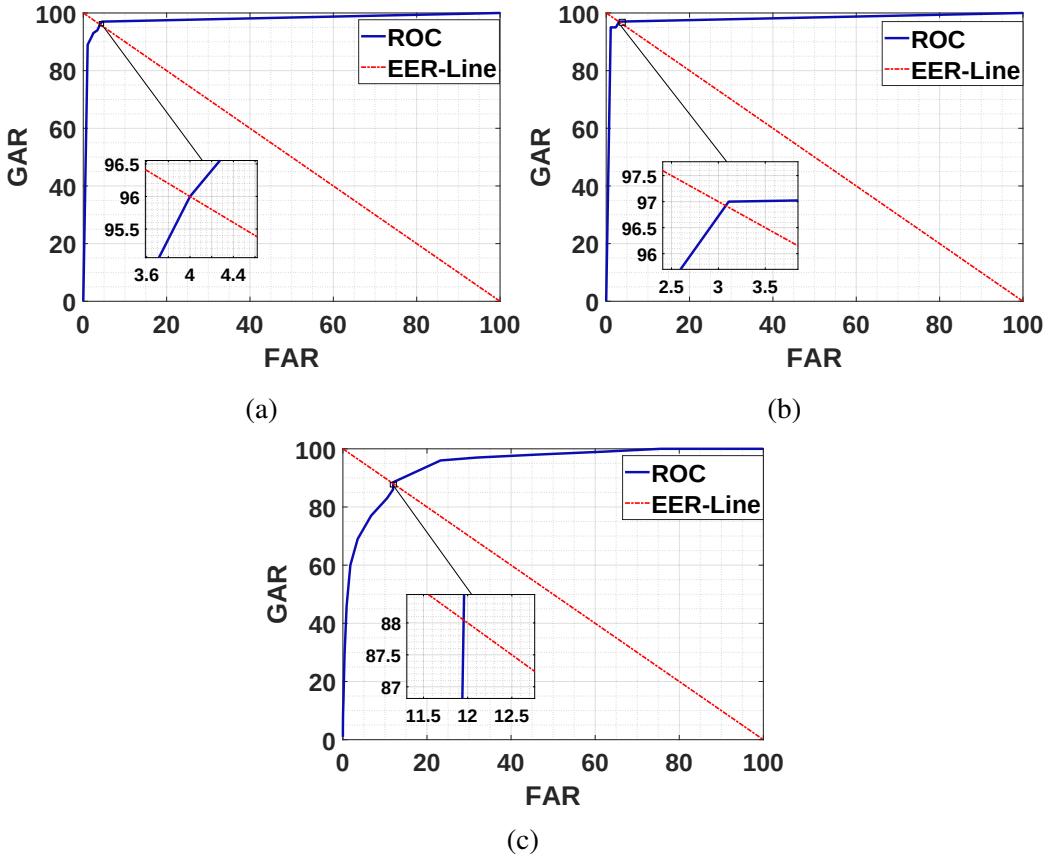


Figure 3.7: Plots of ROC curves using the proposed technique: (a) FVC2002 DB1, (b) FVC2002 DB2, (c) FVC2004 DB1 databases, where the degree of polynomial (p) is considered 8.

all possible combinations of the points (that is, (n_t) genuine and (n_c) chaff points) of vault V_M. Considering the degree of encoding polynomial as p, an attacker has to search all combinations of size $p+1$ from the total $n_t + n_c$ points, which is a huge number and is infeasible to attempt. For example, if $n_t = 20$, $n_c = 200$, and $p = 8$, then the total number of combinations that are possible are ${}^{222}\mathrm{C}_9$ which is approximately 3.06×10^{15}. Out of these combinations, only ${}^{22}\mathrm{C}_9 \approx 4.9 \times 10^5$ combinations are genuine which can unlock the vault, hence the probability of getting the vault unlocked is just $\frac{4.9\times10^5}{3.06\times10^{15}} \approx 1.6 \times 10^{-10}$ which is quite small and negligible. Thus, it is computationally infeasible for an intruder to unlock the vault by using the brute force attack. An instance of representing the secured vault points (abscissa only,

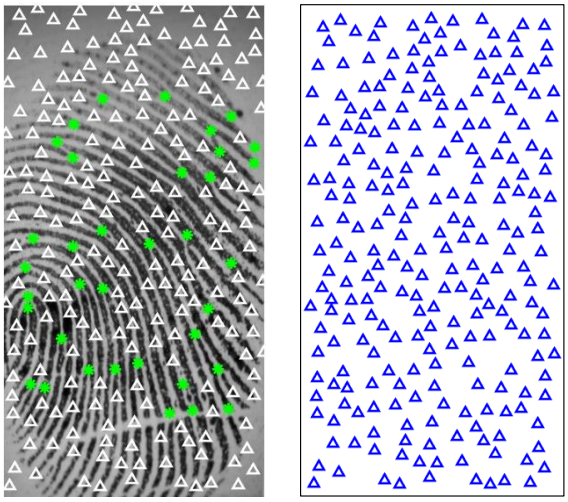


Figure 3.8: Secured vault points (abscissa only, $\{(m_t)_i\}_{i=1}^{n_t} \cup \{(m_c)_i\}_{i=1}^{n_c}$); in the left figure, $triangles$ and $stars$ represent chaff points and minutiae, respectively, whereas in the right figure, $triangles$ show both chaff and minutiae.

$\{(m_t)_i\}_{i=1}^{n_t} \cup \{(m_c)_i\}_{i=1}^{n_c}$) has been given in Figure 3.8. It is clear from Figure 3.8 that an intruder can at the most get access to the points shown on the right side of the figure, where it is infeasible to extract original minutiae locations as it is mixed with a large number of chaff points.

- Key inversion attack: In this attack scenario, an attacker tries to guess or recover the secure key by checking for all possibilities. In our fuzzy vault implementation, the size of CRC encoded key K' is kept as $16 \times (p+1)$. If an attacker has intercepted the vault records, then it is possible that the attacker can guess the key K' to extract the genuine points from the vault records after generating the polynomial using K'. In our implementation, we have used the degree of polynomial p as 8, 9, and 10, which makes the size of K' ($16 \times (p+1)$) as 144, 160, and 176 respectively. Hence, the total number of guesses for these selections would be 2^{144}, 2^{160}, and 2^{176}, respectively. As we see, these are very large numbers and hence, guessing is almost impossible.

- Auxiliary information: We have used PCA based technique for alignment where there

Table 3.4: Security analysis of the proposed technique for different attack scenarios

S.No.	**Brute Force Attack**	**Key Inversion Attack**	**Attack on Stored Auxiliary information**
(1)	Attacker tries all possible combinations of size $p+1$ from the total $n_t + n_c$ vault points.	Attacker tries to guess the secured key K' to unlock the vault if the vault records are compromised.	Attacker can try to access the auxiliary information stored in the database for alignment at the time of verification.
(2)	In the proposed technique, if $n_t = 20$, $n_c = 200$, and $p = 8$, then the probability of getting the vault unlocked is negligible as it is approximately equal to 1.6×10^{-10}.	In the proposed technique, three different sizes of the secure key, *i.e.*, 144, 160, and 176, are considered. Hence the total guesses would be 2^{144}, 2^{160}, and 2^{176}.	In this work, an alignment technique based on PCA has been proposed, which does not store auxiliary information in the database.
(3)	Hence, it is infeasible to access the original minutiae information from the vault in the proposed technique.	Thus, it makes the guessing of secure key infeasible to get access to the vault.	Thus, there is no chance of getting attacked by an attacker using the auxiliary information.

is no requirement of storing any kind of auxiliary information in the database. Hence, auxiliary information based attacks are not possible in our case as possible in techniques proposed in [30].

The security analysis with respect to the three different scenarios discussed above is summarized in Table 3.4. The experimental analysis in terms of the performance and security clearly shows the effectiveness and robustness of the proposed fuzzy vault based fingerprint template protection technique.

Chapter 4

A Non-invertible Transformation Based Technique to Protect a Fingerprint Template

In the previous chapter, an approach to protect the fingerprint template has been discussed by means of the fuzzy vault scheme. Although the original fingerprint information gets secure enough in this approach, it suffers in terms of the recognition performance. In addition, the computed templates are not revocable and diverse. Therefore, in order to rectify these issues, we have utilized one of the cancelable biometrics techniques, $i.e.$, non-invertible transformation based template protection approach. The non-invertible transformation based techniques prevent the reconstruction of original fingerprint data from the compromised template and avoid unauthorized access to the system. Hence, in this chapter, we propose a technique based on the non-invertible transformation to protect a fingerprint template. In the technique, we transform minutiae in a fingerprint by using the original minutiae locations and orientation information, along with a user keyset. We also use a PCA

The work presented in this chapter has been published in the paper: "*A non-invertible transformation based technique to protect a fingerprint template*", IET Image Processing, 1–15 (2021). DOI: 10.1049/ipr2.12130

based approach to align the probe and gallery templates of fingerprint images as discussed in the previous Chapter 3. The evaluation of the proposed technique is carried out on seven different fingerprint databases taken from FVC2000, FVC2002, and FVC2004 considering all four essential requirements, $viz.$, revocability, diversity, security, and performance. Further, the obtained results are compared with other existing state-of-the-art techniques in the literature, and the comparative results show that our proposed technique is highly robust and performs exceptionally well compared to the other existing techniques. The significant contributions of this chapter are mentioned below.

- The proposed technique generates a non-invertible 3D user template which ensures the security of the fingerprint data of a user stored in the database.

- A large number of distinct user templates can be constructed from the same biometric data using different values of keysets. This makes the templates fully unlinkable and renewable (or revocable).

- The transformed user templates are highly secure as it is infeasible to restore the original fingerprint data from the transformed template even if an adversary gets the information of the keyset.

- The proposed technique has shown a good performance even in the case of challenging databases such as FVC2002 DB3, FVC2004 DB1, and FVC2004 DB2.

A detailed discussion of the various steps of the proposed technique and the experimental analysis is provided below.

4.1 Proposed Technique

Minutiae points in a fingerprint image hold rich details of ridge patterns which makes them very useful to compare two fingerprint images. We leverage this property of minutiae points to construct a secure user template. We propose a technique to produce a secure fingerprint-based biometric template with the help of a non-invertible transformation. The technique considers an original biometric template computed from a fingerprint image and transforms it with the help of a keyset $\{d, \alpha\}$ to produce a secured version of the original template. The original fingerprint-based template is defined with the help of locations of the minutiae points along with their orientation information. To enroll a user with the recognition system, the secure template is computed from the original template and is stored in the database. An example of fingerprint image with minutiae points marked on it is shown in Figure 3.2(b). In a fingerprint recognition system, the alignment of fingerprint templates is an important concern while performing the matching. This is true irrespective of whether we are matching the original fingerprint templates or secure templates obtained from the original templates. To handle this in the proposed technique, we make use of a PCA based approach where a secure fingerprint template is aligned by orienting it to a unique direction and the angle of the rotation is calculated by using a fingerprint image. Since in the proposed technique, transformed locations of minutiae points have been used to construct the secure template and the transformation being used is non-invertible, it is infeasible for an attacker to reconstruct the actual fingerprint image (or obtain the original minutiae attributes) by stealing the stored template. The overview of the proposed technique is shown in Figure 4.1. A detailed description of various steps followed to create a secure fingerprint template is provided below.

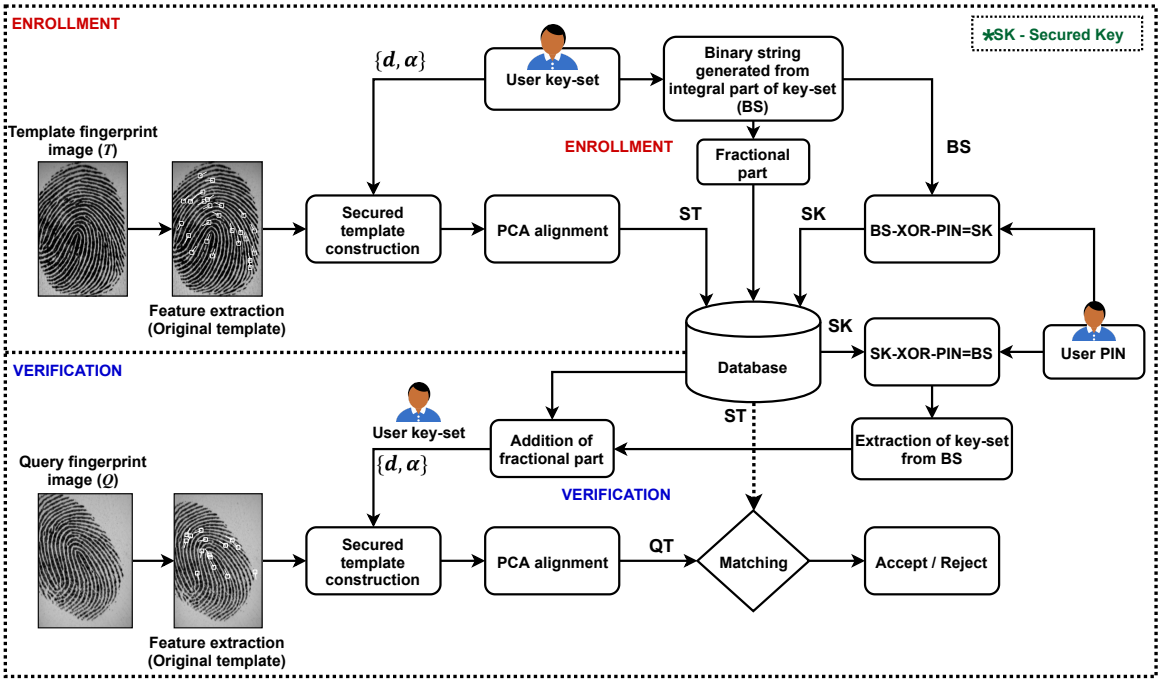


Figure 4.1: Flowchart of the proposed template protection technique where **ST** and **QT** stand for secure fingerprint template and query fingerprint template, respectively.

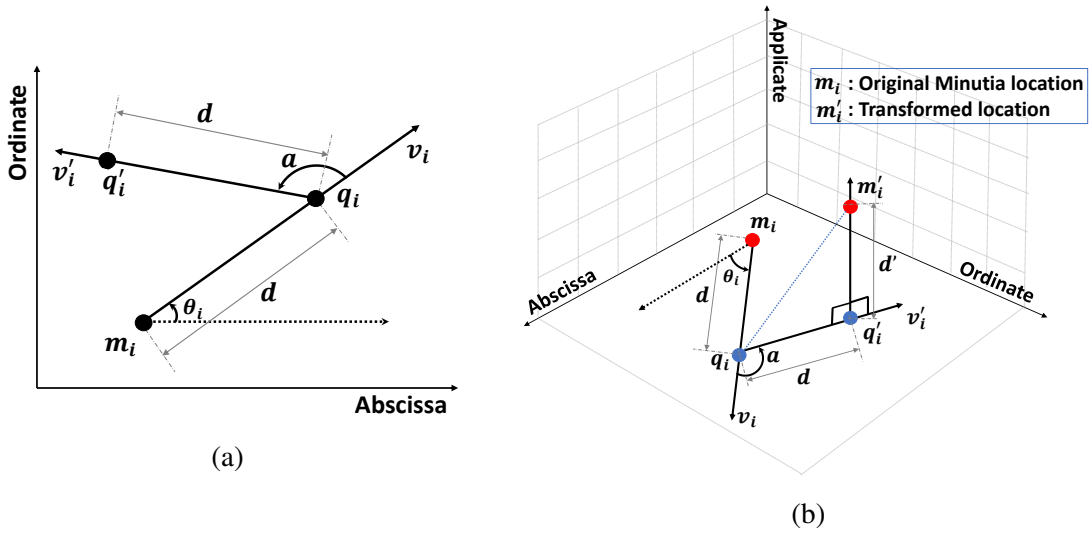
4.1.1 Construction of secure user template

To construct the secure user template, first, features which are basically the location of minutiae points and their orientation information are extracted from the fingerprint image. These features define the original user template for the fingerprint image. A transformation is applied to the features of the original template and a new set of features is obtained in 3D space using the proposed technique. This new set of features defines the secure user template.

Let a set of minutiae points be represented as **M=** $\{(x_i, y_i, \theta_i) : i = 1, 2, ... n\}$, where x_i, y_i, and θ_i represents the x-coordinate, y-coordinate, and orientation value of i^{th} minutia point m_i, respectively, in a fingerprint image T. Further, the orientation value θ_i represents the direction of the ridge with respect to the horizontal axis (abscissa) at minutia point m_i. The vector v_i in Figure 4.2(a) shows the orientation of minutiae-point m_i. To get a secure template by transformation, a point q_i on vector v_i is obtained which is at a distance of d

(first value of user keyset) from the minutia point m_i. The location of q_i is computed as given in Equation 4.1. The obtained point q_i is again moved to a new location q_i' by translating it by a value d along the direction of vector v_i' which is obtained by rotating the vector v_i by an angle α (second value of user key set) with respect to the point q_i as shown in Figure 4.2(a). This gives a new intermediate transformed location for minutiae point m_i. The final transformed location of minutiae point m_i is obtained by translating the point q_i' by a value d' in 3D along a vector that is perpendicular to the plane of vectors v_i and v_i'. This gives a new location m_i' for the original minutiae location m_i where d' is the third key used in the transformation. Formally, the coordinates of point m_i' can be calculated using Equation 4.3. Figure 4.2(b) demonstrates the translation of minutiae point m_i to the final location m_i'. The same procedure is applied to all the minutiae points to get the transformed location for them. It can be noted that the value of the third key d' is dependent on the other two keys, that is d and α. Eventually, d' is the decimal equivalent of a binary number obtained by concatenating the 16-bit binary equivalent of the integral values of the keys d and α as shown in Figure 4.3. The value of d' can be formally calculated using Equation 4.2. The transformed locations of all the minutiae collectively define the secure user template with respect to the original user template obtained from the original minutiae locations.

After computing the secure template, it is centered at the singular point as given in Equation 4.4. Further, the template is rotated by an angle which is computed using PCA as explained in the next section. The centering of the template at a singular point makes the secure template translation invariant whereas rotation helps in aligning the template to a unique direction which in turn makes the matching of the two secure templates rotation invariant. In addition, sometimes a fingerprint may contain more than one singular point. In order to address it, the number of the computed secure templates during enrollment are made equal to the number of singular points present in the fingerprint by computing a tem-



(a) (b)

Figure 4.2: Computation of transformed location of minutiae point m_i (a) Step 1: Translation of point m_i to a new location q'_i on XY-plane using user keyset $\{d,\alpha\}$, (b) Step 2: Translation of minutiae point m_i to a secured location m'_i using user keyset $\{d,\alpha\}$ and d' (which is calculated using $\{d,\alpha\}$).

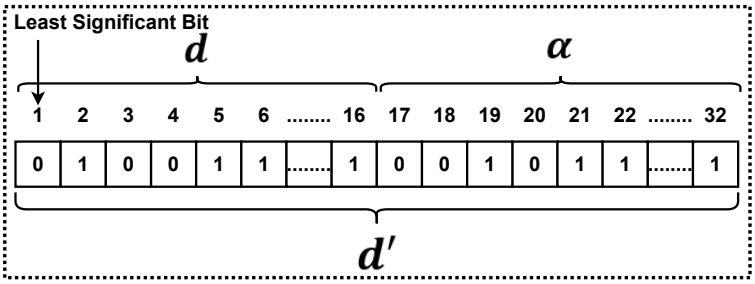


Figure 4.3: Computation of key d' from user keyset $\{d, \alpha\}$.

plate with respect to each singular point. At the time of verification, the secure template is calculated with respect to the singular point which is nearest to the center of the probe fingerprint.

$$q_i^x = x_i + d \times \cos(\theta_i)$$
$$q_i^y = y_i + d \times \sin(\theta_i) \tag{4.1}$$

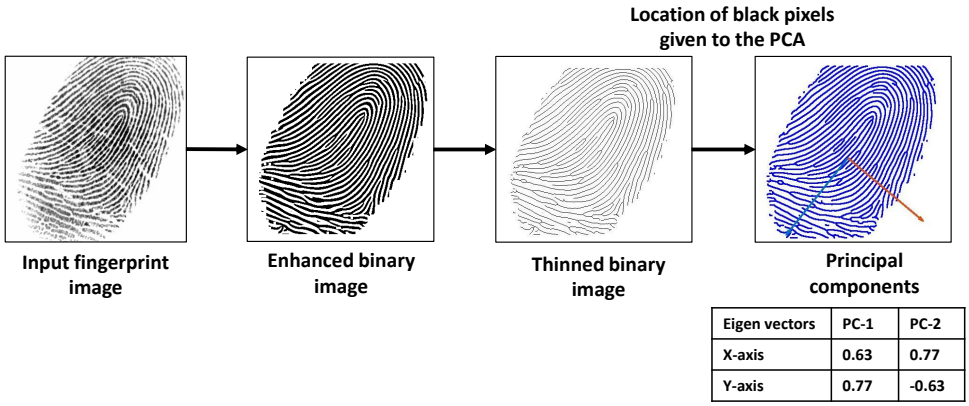
$$d' = \lfloor d \rfloor + \lfloor \alpha \rfloor \times (2^{16}) \tag{4.2}$$

$$\begin{bmatrix} x_i' \\ y_i' \\ z_i' \end{bmatrix} = \begin{bmatrix} q_i^x \\ q_i^y \\ 0 \end{bmatrix} + \begin{bmatrix} d \times \cos(\alpha + \theta_i) \\ d \times \sin(\alpha + \theta_i) \\ d' \end{bmatrix} \tag{4.3}$$

$$\begin{aligned} x_i' &= x_i' - x_{sing} \\ y_i' &= y_i' - y_{sing} \\ z_i' &= z_i' - z_{sing} \end{aligned} \tag{4.4}$$

4.1.2 Alignment using PCA

We make use of PCA to align the secure fingerprint template to a standard axis by utilizing the principal components computed for the input pixel locations of thinned ridges of a fingerprint image as discussed in the last Chapter 3. As we observe, a fingerprint impression captured through a fingerprint sensor is usually of an elliptical (oval) shape. Hence if PCA is applied on the coordinates of the pixels of the fingerprint impression, the two principal components of the PCA would produce the axes of the ellipse circumscribing the fingerprint impression where the first principal component of the PCA represents the direction of the major axis of the ellipse and the second principal component represents the minor axis. To orient the secure fingerprint template to a standard direction, either it can be rotated in such a way that the first and second principal components obtained from the fingerprint image align with the Y- and X- axes, respectively or the transformed minutiae points can be projected along the directions of the principal components. In this work, as the orientation values of the minutiae are utilized to compute the secure template, instead of projecting the minutiae locations along the directions of the principal components, we have rotated the final secure template in such a way that the principal components align with the Y- and X- axes, respectively.



Eigen vectors	PC-1	PC-2
X-axis	0.63	0.77
Y-axis	0.77	-0.63

Figure 4.4: Computing the thinned fingerprint image and its principal components.

In the alignment process, a fingerprint image is first enhanced using [114, 115] to enable accurate computation of ridges in the image. An example of fingerprint enhancement is shown in Figure 4.4. To obtain the thin (one pixel wide) ridges, an enhanced image is first thresholded and later thinned using a morphological operator.

Let $\mathbf{A}$ be a 2D matrix containing coordinates of p points representing the ridge pixels of the thinned fingerprint image. The matrix $\mathbf{A}$ can be formally written as follows where the size of the matrix is $p \times 2$, and each row defines the coordinates of a ridge point of the fingerprint image.

$$\mathbf{A} = \begin{bmatrix} a_1 & b_1 \\ a_2 & b_2 \\ \vdots & \vdots \\ a_p & b_p \end{bmatrix}$$

The matrix $\mathbf{A}$ is analyzed using PCA to get the principal components. As we know that the shape of a fingerprint impression is generally elliptical, the PCA gives the two principal components directed along the major and minor axes of the ellipse bounding the fingerprint image. To compute the principal components in the PCA, first, the covariance matrix is calculated and is followed by the Eigen decomposition of the covariance matrix. Let matrix

U contains the principal components obtained for matrix **A** after Eigen decomposition and is defined as follows.

$$\mathbf{U} = \begin{bmatrix} u_{11} & u_{12} \\ u_{21} & u_{22} \end{bmatrix} \tag{4.5}$$

$$\phi = \tan^{-1}\left(\frac{u_{22}}{u_{12}}\right) \tag{4.6}$$

$$\begin{bmatrix} x_i' & y_i' & z_i' \end{bmatrix} = \begin{bmatrix} x_i' & y_i' & z_i' \end{bmatrix} \times \begin{bmatrix} \cos(\phi) & -\sin(\phi) & 0 \\ \sin(\phi) & \cos(\phi) & 0 \\ 0 & 0 & 1 \end{bmatrix} \tag{4.7}$$

Since the covariance matrix computed for **A** is of size 2×2, the size of the matrix **U** is also obtained as 2×2. This means it contains two Eigenvectors (principal components) as shown in Equation 4.5 where the first column represents the Eigenvector corresponding to the largest Eigenvalue (first principal component) and so on. To align the secure fingerprint template ($i.e.$, transformed minutiae information) to a standard direction, the transformed locations in 3D space are rotated in such a way that the second principal component (*i.e.*, Eigenvector corresponding to the smallest Eigen value) obtained from the fingerprint aligns with X-axis. We calculate the angle made by the second principal component with the X-axis using Equation 4.6.

Before performing the rotation (alignment) of the secure fingerprint template, it is centered to a singular point using Equation 4.4. This helps in making the secure user template computed for the fingerprint, translation-invariant. In Equation 4.4, the coordinates of the singular point are considered as (x_{sing}, y_{sing}, z_{sing}), where the value of z_{sing} is considered as zero. The final transformed location of the original fingerprint template points (minutiae points) after rotating the points of the secure user template by angle ϕ is given by Equation

Algorithm 4.1 Computation of secure fingerprint template

1: **Input:** *Matrix* $\mathbf{M} \in \{(x_i,\ y_i,\ \theta_i) : i = 1, 2, ... n\}$, *singular point* $(x_{sing},\ y_{sing})$, *keyset* $\{d,\ \alpha\}$, *and matrix* $\mathbf{A} \in \{(a_j,\ b_j), : j = 1, 2, ... p\}$ *(for T/Q-fingerprint images)*
2: **Output:** $\mathbf{ST} \in \{(x'_i,\ y'_i,\ z'_i) : i = 1, 2, ... n\}$ *(Secure user template)*
3: /* *Calculation of key* d' *by utilizing the value of keys* d *and* α */
4: $d' = \lfloor d \rfloor + \lfloor \alpha \rfloor \times (2^{16})$
5: /* *Secure fingerprint template computation, from step 6 to step 30* */
6: **for** i = 1 to n **do**
7: $\quad q_i^x = x_i + d \times \cos(\theta_i)$
8: $\quad q_i^y = y_i + d \times \sin(\theta_i)$
9: $$\begin{bmatrix} x'_i \\ y'_i \\ z'_i \end{bmatrix} = \begin{bmatrix} q_i^x \\ q_i^y \\ 0 \end{bmatrix} + \begin{bmatrix} d \times \cos(\alpha + \theta_i) \\ d \times \sin(\alpha + \theta_i) \\ d' \end{bmatrix}$$
10: $\quad$ /* *Reducing translation due to intra-subject variance, from step 11 to 13* */
11: $\quad x'_i = x'_i - x_{sing}$
12: $\quad y'_i = y'_i - y_{sing}$
13: $\quad z'_i = z'_i - z_{sing}$, /* *the value of* $z_{sing} = 0$ */
14: **end for**
15: /* *Aligning the fingerprint to standard direction using PCA* */
16: $m_a = \frac{1}{p} \sum_{j=1}^{p} a_j, m_b = \frac{1}{p} \sum_{j=1}^{p} b_j$
17: $\mathbf{A} = \mathbf{A} - \begin{bmatrix} m_a & m_b \end{bmatrix}$
18: $\mathbf{C} = \frac{1}{(p-1)} \times \mathbf{A^T A}$
19: $\mathbf{C} = \mathbf{USV}^T$, /* Singular value decomposition of matrix **C** */
20: /* *Suppose the values in matrix* $\mathbf{U} = \begin{bmatrix} u_{11} & u_{12} \\ u_{21} & u_{22} \end{bmatrix}$ */
21: $\phi = \tan^{-1}\left(\frac{u_{22}}{u_{12}}\right)$
22: **if** $\phi > 85°$ **then**
23: $\quad \phi = -(90° - \phi)$
24: **end if**
25: **if** $\phi < -85°$ **then**
26: $\quad \phi = (90° + \phi)$
27: **end if**
28: **for** i = 1 to n **do**
29: $$\begin{bmatrix} x'_i & y'_i & z'_i \end{bmatrix} = \begin{bmatrix} x'_i & y'_i & z'_i \end{bmatrix} \times \begin{bmatrix} \cos(\phi) & -\sin(\phi) & 0 \\ \sin(\phi) & \cos(\phi) & 0 \\ 0 & 0 & 1 \end{bmatrix}$$
30: **end for**

4.7. The complete procedure to compute the secure user template (ST) in the algorithmic form is given in Algorithm 4.1. The algorithm summarizes the working of Sections 4.1.1 and 4.1.2, which takes the matrix **M** and **A** as inputs and computes the secure transformed template, which is both translation and rotation-invariant.

In order to achieve translation invariance, first, the algorithm computes the transformed 3D locations of minutiae points, denoted as (x_i', y_i', z_i'), by using the user keys d, α, and d' (combination of d and α as mentioned in Equation 4.2). These transformed locations are completely secure; however, to make them translation-invariant, further, the transformed locations are subtracted by the singular point location, which is basically making the singular point as the origin. After these steps, the translation-invariant secure fingerprint template is being rotated to align by means of the PCA based alignment technique. In the alignment procedure, principal components are computed by considering the pixels of the ridges of the thinned fingerprint image as shown in Figure 4.4, which provides an estimate of rotation angle with respect to the standard axis (X or Y). Further, by utilizing the information computed in the previous step, the final transformed secure fingerprint template, which is both translation and rotation invariant, is obtained as given in Algorithm 4.1. Finally, the aligned secure fingerprint template for a user is stored in the database as a gallery template. The user keyset is also stored in the database so that a similar transformation can be applied to compute the secure template from the probe image during matching. The detailed steps are explained in Sections 4.1.1 and 4.1.2.

In addition to that, we also propose a technique to secure the user keyset by utilizing a user PIN (Personal Identification Number) to prevent the spoofing attack as given in the next section.

4.1.3 Securing the user keyset

While enrolling a subject with the database using a secure user template, the user keyset $\{d, \alpha\}$ used in the computation of a secure user template for a subject is also stored in the database. The storage of user keyset in the database is required to enable us to use the same keyset to convert the query user template to an equivalent secure template. As the

transformation used in obtaining a secure user template is non-invertible, even though both the stored template and the keyset are stolen by an intruder, it is impossible for him/her to reconstruct the original biometric data back from the compromised information. Thus the proposed technique insures the security of the original fingerprint information such as attributes of minutiae points, ridge patterns, etc. in case of an attack on the database. Here we see that though the biometric features are secured, an intruder can get access to the biometric system in the case of a spoofing attack. To prevent it, we propose a protective measure as elaborated below.

4.1.3.1 Protection against Spoof attack

We propose a PIN based technique to protect the template against spoof attack. In case of a spoofing attack, an attacker may get access to the fingerprint authentication system by spoofing biometric data. To handle this situation in the proposed technique, a PIN is assigned to each user. The output of the XOR operation between the binary equivalent of the keyset and the PIN is stored in the database instead of the direct user keyset. Thus, at the time of authentication, without PIN, the keyset will not be unlocked even if the spoofed impression is much similar to the genuine one.

The binary equivalent of integral parts of keys d and α are concatenated and its bitwise XOR operation is computed with the binary equivalent of user PIN at the time of enrollment. The outcome of the bitwise XOR operation is further stored in the database with a secure user template. The reverse of this process is followed during the verification for extraction of keyset to compute a secure probe fingerprint template for matching with the secure gallery fingerprint template stored in the database. The aforementioned process is shown in Figure 4.5. However, when keyset values are fractional then the extracted values of keys can be slightly different from the values used at the time of enrollment, as only integral parts of

keys are converted into a binary string. To handle such cases, fractional parts are separately stored in the database corresponding to each value of keyset $\{d, \alpha\}$ at the time of enrollment, and these fractional parts are added with the extracted integral part of keys d and α during the verification.

The procedure which has been followed to match the secure gallery and probe fingerprint templates is described in the next section.

4.1.4 Matching procedure

Let Q be the probe fingerprint image. To match it with the enrolled secure templates, first, its equivalent secure template is obtained by using the same steps followed during enrollment as mentioned in Sections 4.1.1 and 4.1.2. Let the points in the secure probe template be $q \in \{q_1, q_2, ... q_n\}$ whereas the points in a secure user template stored in the database (secure gallery template) be $t \in \{t_1, t_2, ... t_m\}$. A point q_i in the probe template is matched to a point t_i in the gallery template if point q_i exists within a sphere of radius th centered at point t_i and vice-versa. The value of th works as a threshold used in the proposed technique to find out the matching between any two points belonging to probe and gallery templates respectively. Let m_{qt} be the number of points in the probe template which match to some points of the gallery template and m_{tq} be the number of points of the gallery template which match to some points of the probe image. Then the matching score for a probe and gallery pair is given by Equation 4.8.

$$score = \left[min\left(\frac{m_{qt}}{n}, \frac{m_{tq}}{m}\right) \times 100 \right] \tag{4.8}$$

Sometimes, due to the poor quality of fingerprint images or the availability of only partial fingerprint impressions, PCA does not align the template properly. To overcome this, we match probe and gallery templates multiple times by rotating the probe template

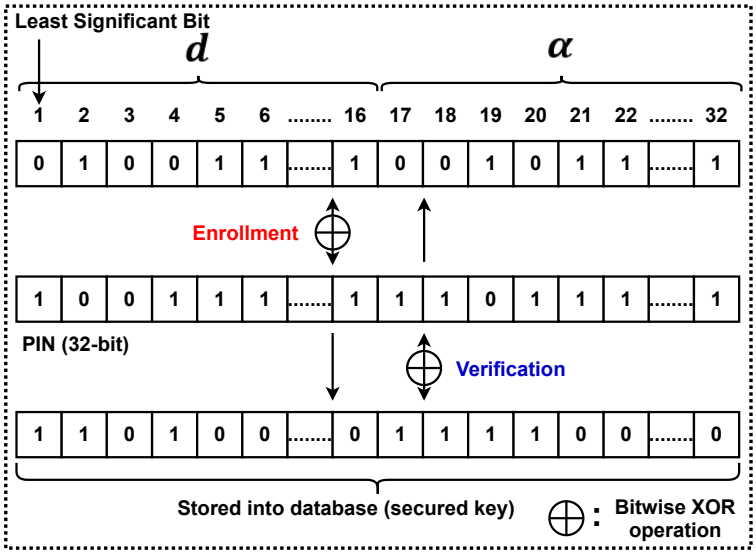
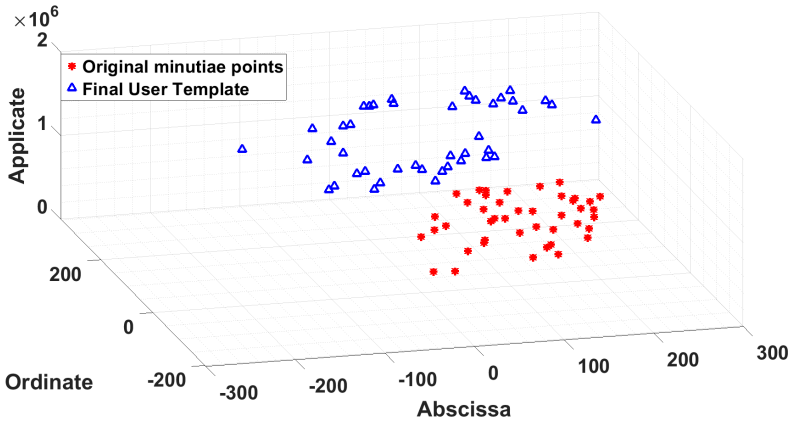


Figure 4.5: Computation of secured key using a PIN to protect the secure template from spoof attack.

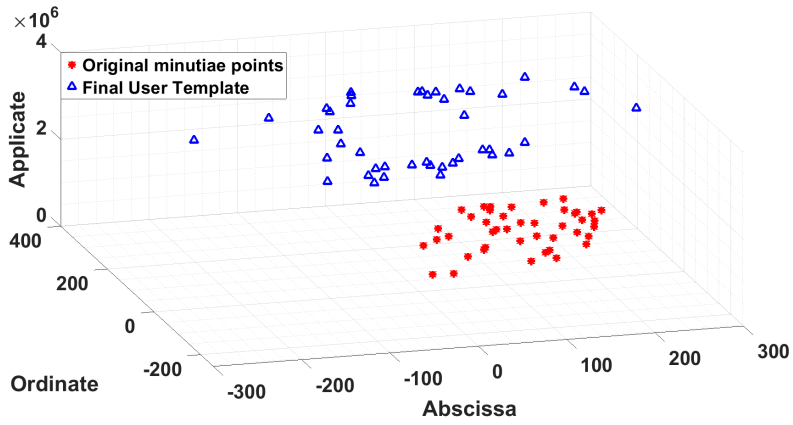
from -5° to $+5^\circ$ with an increment of 1° in each iteration. The best score out of these 11 iterations is considered as the final match score.

4.2 Experimental Analysis

In this section, the proposed technique has been evaluated with respect to four important criteria, *viz.*, revocability, unlinkability, security, and performance, are used in the analysis of a template protection technique. We have used FVC2000 DB2 [25], FVC2002 DB1, FVC2002 DB2, FVC2002 DB3, FVC2002 DB4 [1], FVC2004 DB1, and FVC2004 DB2 [26] fingerprint databases to carry out the experiments. The detailed information of these databases has been provided in Section 1.4. To compute a secure template for the analysis, key values are chosen randomly in a given range. The range of values used for d is (0,1000] whereas the values of α are taken in the range of (0,360]. It can be noted that integer values are considered for d whereas the values of α could be both integers as well as fractional. Further, it is always better to select the keys for different users by maintaining a difference



(a)

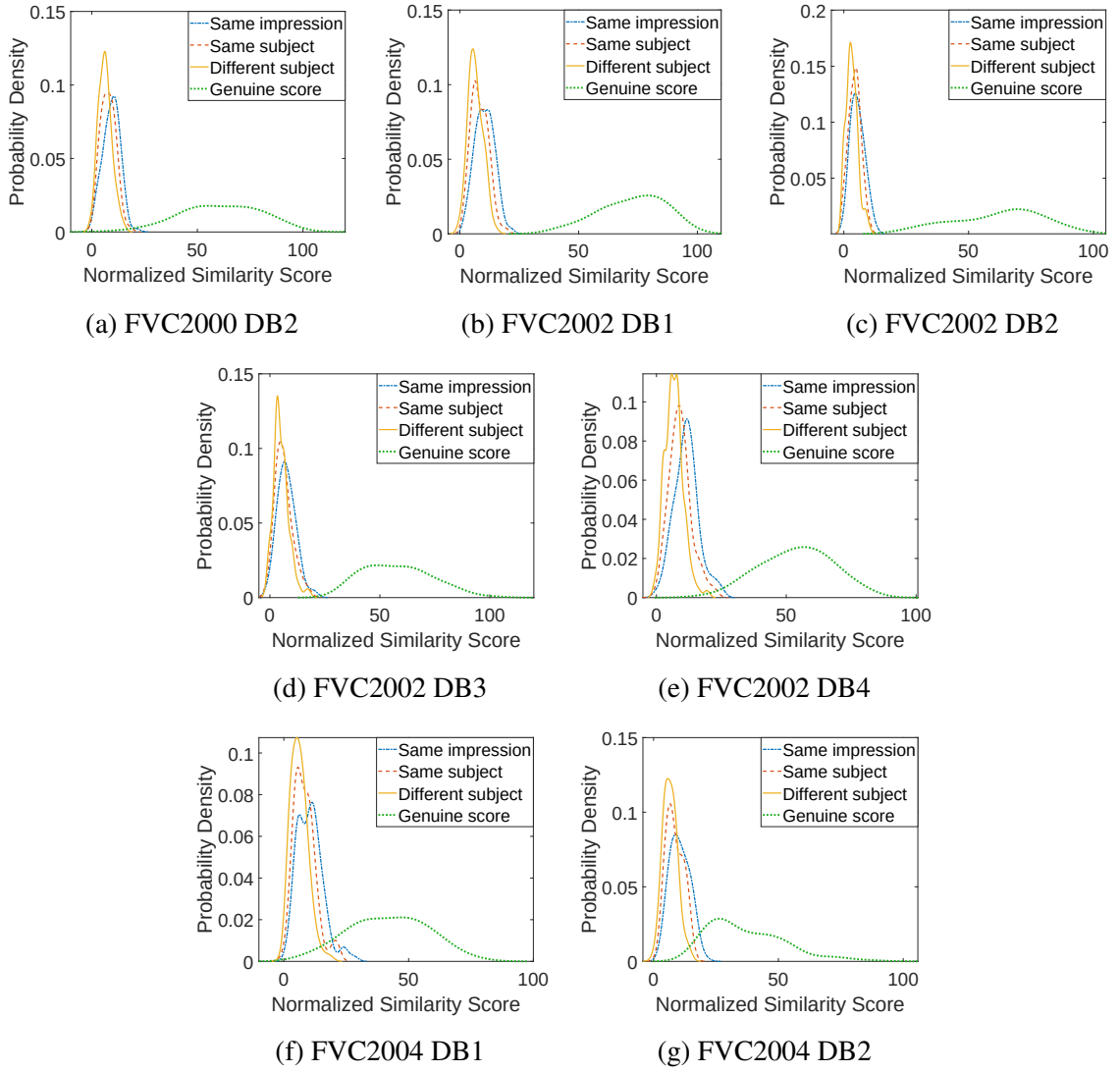


(b)

Figure 4.6: Secure user templates computed for a fingerprint image using two different key sets.

of at least 1 between the two consecutive keys, especially, in the case of fractional values.

The standard performance metrics that are used to evaluate the proposed technique are FRR, FAR, GAR, and EER. These have been discussed in Section 1.2.4. In addition, the 1-versus-1 (1-vs-1) matching protocol has been used to evaluate the proposed technique as mentioned in Section 1.4. Statistical techniques have also been used to analyze the experimental results for different databases. The Kolmogorov-Smirnov test (KS-test) and the t-test have been used to carry out the statistical analysis. A detailed discussion on the analysis of the results based on the aforementioned four criteria is presented below.



(a) FVC2000 DB2 (b) FVC2002 DB1 (c) FVC2002 DB2

(d) FVC2002 DB3 (e) FVC2002 DB4

(f) FVC2004 DB1 (g) FVC2004 DB2

Figure 4.7: Distribution of scores using kernel smoothing function in four different cases to show the unlinkability (diversity) of secure fingerprint template on different databases.

4.2.1 Revocability analysis

A template protection technique is said to possess the property of revocability, if it is possible to replace the stored user template in the biometric database with a completely new template in the situation when the stored template gets compromised. In the proposed technique, it is possible to generate a completely new secure template for a user from his/her fingerprint data by changing the keyset. Since a stored template can be replaced by a new

template, which is completely different from the stored one, an adversary cannot get access to the biometric system by using the compromised template. An example of secure templates constructed by the proposed technique using different keys and the same fingerprint image is shown in Figure 4.6. From the figure, we can see that the two templates are very different from each other though they have been obtained from the same fingerprint data. Further, to analyze the revocability of the proposed technique, a framework that is used in [121], has also been utilized. According to this framework, the pseudo-genuine score is calculated for each subject which is a matching score between the stored template and a template computed using different keysets and the same fingerprint data. The mean and variance of these scores along with the imposter and genuine scores are calculated for all the databases as given in Table 4.1. It is clearly observed from the table that the mean and variance values of pseudo-genuine and imposter scores are nearly similar and are very far from the mean and variance of the genuine scores. This clearly depicts that the renewed template is completely different from the stored one and the overall technique can be considered as highly renewable.

Table 4.1: Mean and variance values of genuine (μ_g and σ_g^2), pseudo-genuine (μ_{pg} and σ_{pg}^2), and imposter scores (μ_i and σ_i^2) for revocability analysis

Database	μ_g	σ_g^2	μ_{pg}	σ_{pg}^2	μ_i	σ_i^2
FVC2000 DB2	0.61	3.31	0.09	0.15	0.08	0.12
FVC2002 DB1	0.73	1.84	0.10	0.16	0.08	0.13
FVC2002 DB2	0.62	3.11	0.05	0.08	0.04	0.06
FVC2002 DB3	0.58	2.25	0.07	0.16	0.06	0.14
FVC2002 DB4	0.54	1.85	0.11	0.22	0.09	0.18
FVC2004 DB1	0.41	0.15	0.10	0.03	0.13	0.05
FVC2004 DB2	0.36	0.14	0.12	0.05	0.14	0.06

4.2.2 Unlinkability analysis

It is observed that in the proposed technique, there is no link found between the user templates which are constructed using the same fingerprint data and different keysets. This makes the templates generated by the proposed technique diverse in nature. Further, the existence of diversity in the templates can also prevent the cross-matching attack as the templates that are stored in different biometric systems for the same biometric data of a subject would be unlinkable from each other. To further analyze and show the unlinkability of user templates computed by the proposed technique, we have utilized the process mentioned in [21]. Accordingly, we have calculated the matching score of two templates which have been selected based on the following four cases.

- **Same impression:** In this case, templates are constructed using the same fingerprint impression of a subject by utilizing different keysets. After computing the templates, the matching score between them is computed. The same procedure is repeated for all the subjects present in the database to compute the matching scores.

- **Same subject:** In this case, templates are constructed using different fingerprint impressions of the same subject by utilizing different keysets and the matching scores are calculated for all the subjects of the database.

- **Different subjects:** In this case, templates are constructed using fingerprint impressions of two different subjects by utilizing different keysets and the matching scores are calculated for all the subjects of the database.

- **Genuine score:** In this case, templates are constructed using two different samples of the same subject by utilizing the same keys for both templates.

In each case, two templates are constructed for each subject present in the database.

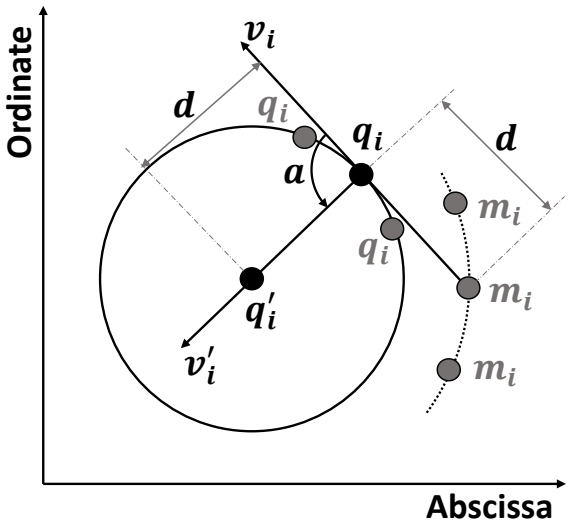


Figure 4.8: Representing the security (non-invertible nature of secure fingerprint template) provided by the proposed technique.

Thus, the total number of matching scores for each database used in the experimentation would be 100 as each of them contains 100 subjects. The scores of the first three cases are compared with the genuine score obtained in the fourth case. Figure 4.7 shows these comparisons for all the databases. It can be clearly seen from the figure that the distribution of pseudo-genuine scores calculated based on the first three cases is completely different from the distribution of the genuine matching scores computed in the fourth case for all the databases. This shows that the templates constructed in the proposed technique using different keysets are unlinkable to each other. Moreover, according to a generalized framework mentioned in [6], if the distribution of the same impression (mated samples) and different subjects (non-mated samples) overlap with each other as shown in Figure 4.7, it shows that the templates are fully unlinkable. So in the event of an attack on a database, if compromised templates are replaced by completely new templates, it will make it impossible for an intruder to get access to the system by using the compromised user template due to the unlinkability of the old and new user templates.

4.2.3 Security analysis

A template protection technique is called secured if it is computationally infeasible to reconstruct the original fingerprint data from the stored user template. Since a non-invertible transformation has been used in the proposed technique to compute the secure user template from an original minutiae points based user template, it is difficult to invert the secure template and get the original fingerprint data from it, even when the keyset is available. Moreover, since there is no information stored in the database regarding the orientation of the minutiae points, it makes it even more difficult to construct the ridge patterns of the original fingerprint image. The security of templates in the proposed technique has been analyzed by considering the following event of an attack.

4.2.3.1 Non-invertibility analysis

To analyze the non-invertibility of the template in the proposed technique, let us assume that an adversary has stolen the secure template and keyset values from the database. As demonstrated in Figure 4.8, in that case, by utilizing the values of d and α, the location q_i' in XY-plane can be computed. However, for finding the original location of a minutia point m_i corresponding to the transformed location m_i', the location of point q_i is needed. We see that there are infinite possibilities for the location q_i around the point q_i' on the circumference of the circle with radius d. For instance, if we just assume that there are 360 possibilities on the circle, the total number of possibilities to find out all the original locations of minutiae points would be 360^n, where n represents the total number of minutiae points present in a fingerprint image. Thus, it is clearly infeasible for an adversary to compute the original location of minutiae points from the compromised template even when the user keyset is available.

4.2.3.2 Attack via Record Multiplicity (ARM)

In the event of ARM attack, an adversary uses multiple templates that have been computed using the same fingerprint image and different keysets to get the original template and fingerprint image information by attempting to relate them. However, it is infeasible to reconstruct the original template and further the fingerprint image in the proposed approach. In order to show this, let us assume that an adversary has gotten three transformed templates ST_1, ST_2, and ST_3 which are obtained using the same fingerprint image and three different keysets $\{d_1, \alpha_1\}$, $\{d_2, \alpha_2\}$, and $\{d_3, \alpha_3\}$, respectively. The k^{th} transformed location of minutiae in ST_1 cannot be linked with the K^{th} transformed location in both ST_2 and ST_3 templates as three of them are computed using different keysets. Also, the values of d'_k as shown in Figure 4.3 are very different among all these three transformed templates. Moreover, by utilizing the framework presented in [6, 21], it has been shown earlier that the templates are highly unlinkable as well as non-invertible. Hence, it is clear that the proposed technique provides security against the ARM attack.

4.2.3.3 Brute force attack

In the brute force attack scenario, an adversary tries all possibilities to get back the original template from the transformed template stored in the database. In the proposed technique, keysets are stored in the database after performing the bitwise XOR operation between the keyset and user-defined PIN (32-bit) as shown in Figure 4.5. Let us consider the assigned PIN comes under the range of a minimum decimal number of 4-digits to a maximum decimal number of 9-digits. Hence, first, to unlock the keyset, there are $9 \times 10^3(10^0 + 10^1 + ... + 10^5) \approx 9.9 \times 10^8$ possibilities for the PIN (32-bit) out of that only a combination can unlock the keyset, thus the probability to guess the value of PIN correctly is $\frac{1}{9.9 \times 10^8} \approx 1.01 \times 10^{-9}$. In addition to that, there are approximately 360^n (n number of

Table 4.2: Percentage EER of the proposed technique compared with existing techniques under the same-key scenario

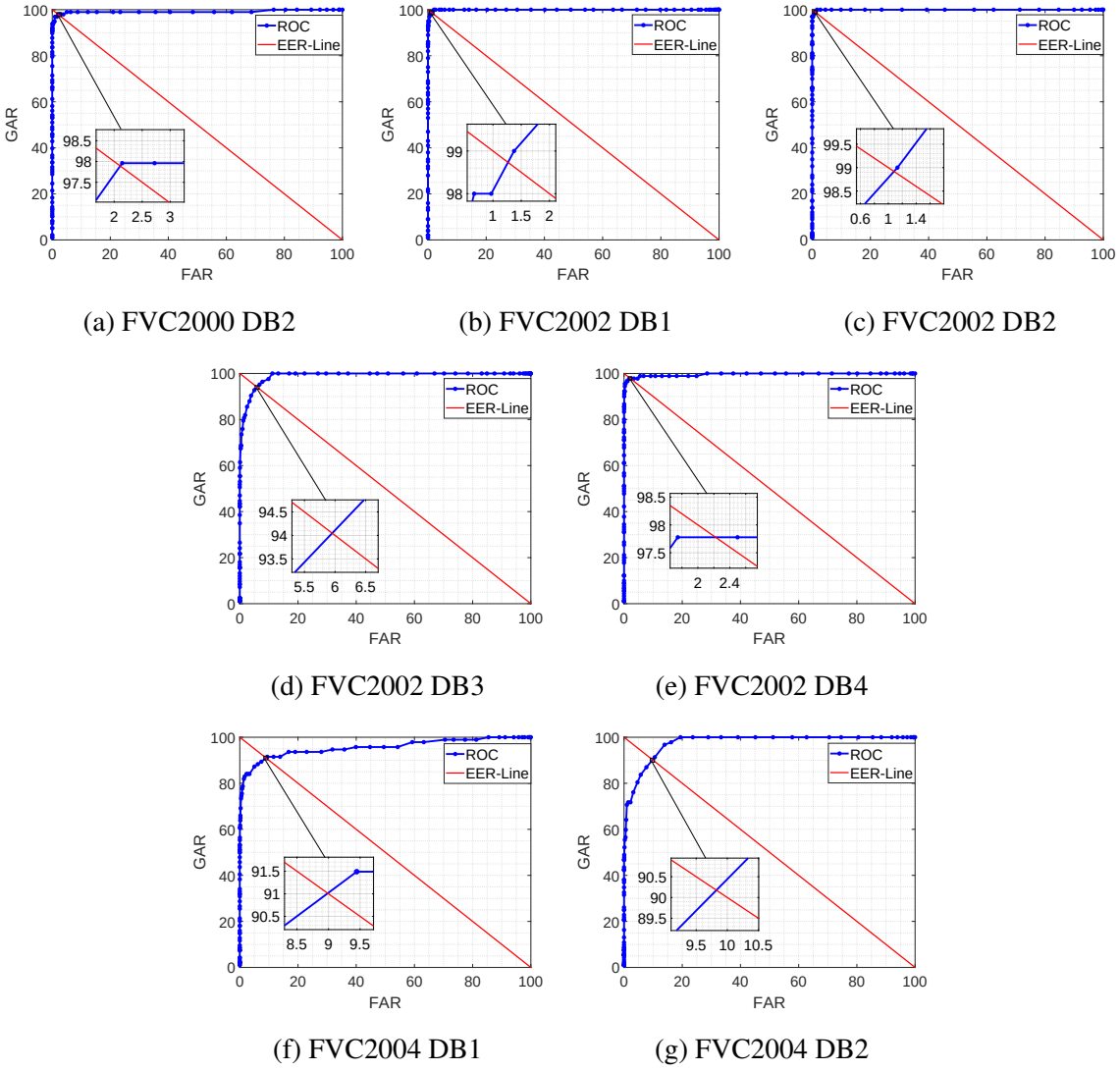
Various techniques	**FVC2000**	**FVC2002**				**FVC2004**	
	DB2	**DB1**	**DB2**	**DB3**	**DB4**	**DB1**	**DB2**
Ahmad et al. [69]	-	9	6	27	-	-	-
Wang and Hu [70]	-	3.5	4	7.5	-	-	-
Jin et al. [77]	-	5.19	5.65	-	-	16.35	8.66
Ferrara et al. [76]	-	0	0.37	4.94	3.37	-	-
Yang et al. [81]	-	5.93	4	-	-	-	-
Yang et al. [47]	-	3.38	0.59	9.80	16.52	-	14.88
Jin et al. [79]	-	4.36	1.77	-	-	24.71	21.82
Sandhya and Prasad [80]	-	4.71	3.44	8.79	-	-	-
Wang and Hu [83]	-	3	2	7	-	-	-
Sandhya et al. [84]	-	3.96	2.98	6.89	-	12.17	13.29
Sandhya and Prasad [86]	-	2.19	1.6	6.14	-	11.89	12.71
Ali et al. [97]	-	2	1	3.1	-	-	-
Trivedi et al. [99]	6.81	-	-	-	-	-	-
Yang et al. [100]	-	-	1	-	-	-	10
Trivedi et al. [102]	-	1.2	2.1	-	-	-	-
Proposed Technique	**2.09**	**1.25**	**1.08**	**5.95**	**2.22**	**8.95**	**9.82**

Note: "-" denotes non-availability of data.

original minutiae) possibilities for trying to guess the original minutiae locations from a transformed template out of which n are the correct guesses thus the probability to guess the minutiae points is given as $\frac{24}{9.9\times10^8\times360^{24}} \approx 1.08 \times 10^{-69}$, if $n = 24$. It clearly shows that the probability to guess the original minutiae locations is negligible and hence the proposed technique is highly robust against the brute force attack.

4.2.4 Analysis of recognition performance

In this section, the recognition performance of the proposed technique is being analyzed on seven different databases, *viz.*, FVC2000 DB2, FVC2002 DB1, FVC2002 DB2, FVC2002 DB3, FVC2002 DB4, FVC2004 DB1, and FVC2004 DB2. As aforementioned, the evaluation has been carried out using different metrics such as FAR, FRR, GAR, and EER in the same-key attack scenario, where the same user keyset is used by all the subjects



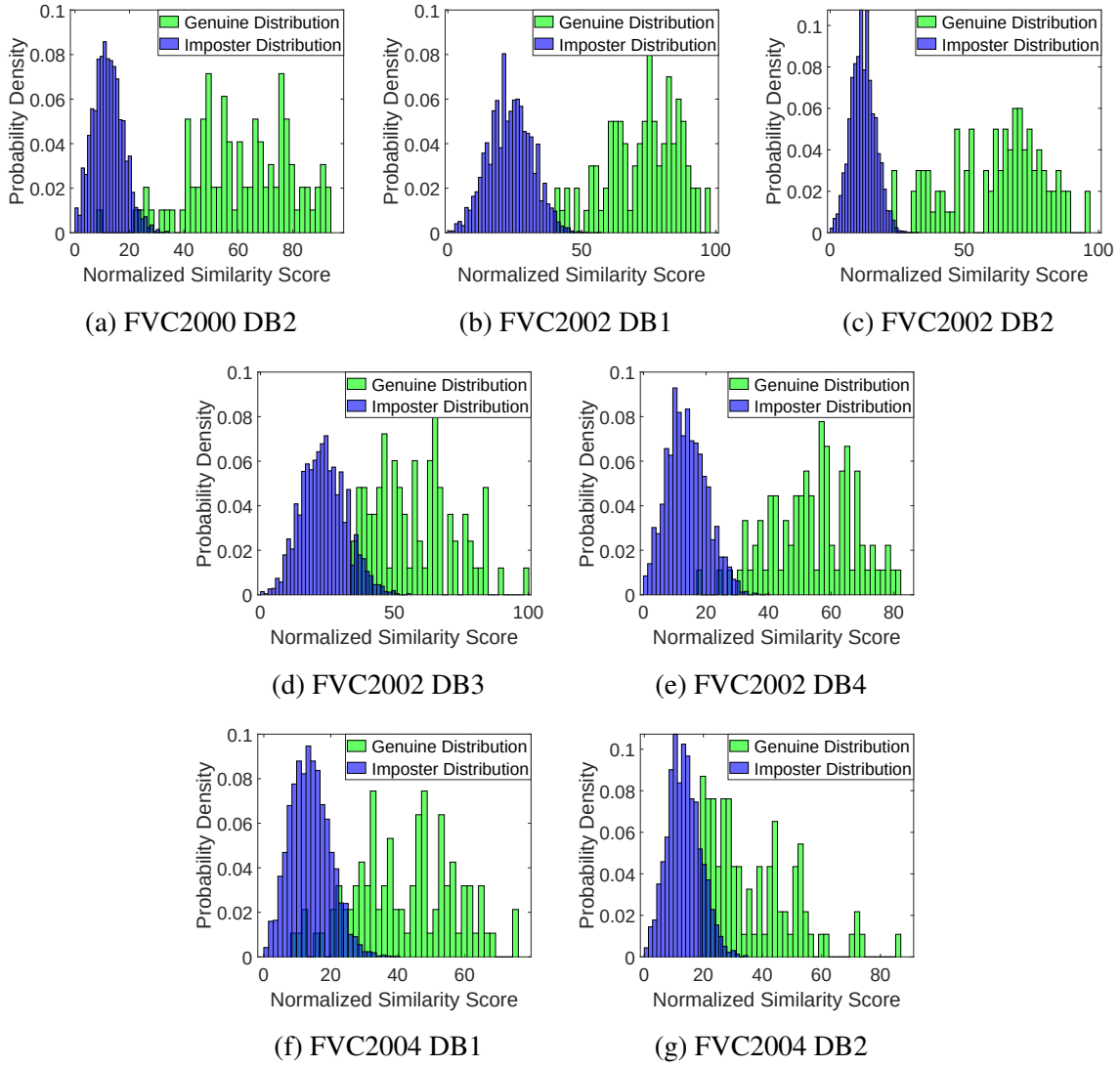
(a) FVC2000 DB2 (b) FVC2002 DB1 (c) FVC2002 DB2

(d) FVC2002 DB3 (e) FVC2002 DB4

(f) FVC2004 DB1 (g) FVC2004 DB2

Figure 4.9: ROC plots for the proposed technique on different databases in the same-key scenario.

of a database. The comparison of results with the existing techniques has been performed based on the EER values. The values of EER obtained on different databases for the proposed technique and their comparison with that of the existing techniques are given in Table 4.2. It can be observed from the table that the performance of the proposed technique is superior to that of the existing techniques except for the technique proposed by Ferrara et al. in [76]. However, the technique in [76] does not possess the revocability property whereas the template produced in the proposed technique is completely revocable. Also, the se-



(a) FVC2000 DB2 (b) FVC2002 DB1 (c) FVC2002 DB2

(d) FVC2002 DB3 (e) FVC2002 DB4

(f) FVC2004 DB1 (g) FVC2004 DB2

Figure 4.10: Distribution of Genuine/Imposter scores for the proposed technique on different databases in same-key scenario.

cure templates produced by the proposed technique using different keysets are found to be unlinkable with each other which makes them diverse as well. Although the quality of fingerprint images is not good in FVC2002 DB3 and FVC2002 DB4 databases, the proposed technique has outperformed most of the techniques in the case of FVC2002 DB3 whereas has produced comparable performance in the case of FVC2002 DB4 database, as seen from Table 4.2. In addition, the proposed technique has performed quite well as compared to the existing techniques in the case of more challenging databases, $i.e.$ FVC2004 DB1 and

Table 4.3: Comparison of Kolmogorov-Smirnov test values of the proposed technique with existing techniques for the same-key scenario

Various techniques	**FVC2000**	**FVC2002**				**FVC2004**	
	DB2	**DB1**	**DB2**	**DB3**	**DB4**	**DB1**	**DB2**
Moujahdi et al. [91]	-	0.78	-	-	-	-	-
Sandhya et al. [80]	-	0.91	0.93	0.75	-	-	-
Sandhya et al. [84]	-	0.92	0.94	0.86	-	-	-
Sandhya et al. [86]	-	0.96	0.97	0.89	-	0.82	0.73
Proposed Technique	**0.97**	**0.99**	**0.98**	**0.99**	**0.98**	**0.83**	**0.85**

Note: "-" denotes non-availability of data.

FVC2004 DB2, as given in Table 4.2. Further, receiver operating characteristics (ROC) curves are also plotted to show the performance of the proposed technique. The ROC curve depicts the rate of change in GAR with respect to FAR calculated at different threshold values (varying from 0% to 100% with step size of 0.1) and it also depicts the robustness of an authentication system. The point where the EER-line and the ROC curve intersect each other gives the value of EER. So the EER value can be calculated by taking the FAR or 1-GAR value at the intersecting point of the ROC curve and EER-line as shown in Figure 4.9. ROC curves for all the databases are shown in Figure 4.9 for the same key scenario. All these curves are obtained as desired showing the robustness of the proposed technique. The distribution of genuine and imposter scores is given in Figure 4.10 for all the databases under the same key scenario. It is clearly visible from the figure that the distribution of genuine and imposter scores are significantly different from each other. In addition, a statistical analysis is performed as described in the following section to show the significant difference between genuine and imposter scores.

4.2.5 Statistical analysis

We have performed statistical analysis to show the separation of genuine and imposter scores in the proposed technique. We have used the Kolmogorov-Smirnov test [23] and

Table 4.4: Results of t-test for different databases performed using genuine and imposter scores at 5% significance level, where "t_s" and "t_c" denote $|t-stat|$ and $t-critical$ values, respectively

Various databases	$\|t_s\|$	t_c	$\|t_s\| > t_c$
FVC2000 DB2	26.44	1.9847	True
FVC2002 DB1	31.62	1.9839	True
FVC2002 DB2	28.01	1.9842	True
FVC2002 DB3	20.70	1.9889	True
FVC2002 DB4	21.01	1.9866	True
FVC2004 DB1	16.14	1.9804	True
FVC2004 DB2	13.15	1.9817	True

student's t-test [24] for this purpose.

- **Kolmogorov-Smirnov (KS) test:** It is a non-parametric and distribution-free statistical test to find out the difference between two sets of samples. The value of KS-test varies in the range [0, 1], where a lower value shows that the two sets are completely similar to each other whereas a higher value shows that the two sets are significantly different to each other. The results of KS-test performed on the genuine and imposter scores computed using the proposed technique for different databases are given in Table 4.3. It can be clearly seen from the table that the values of the KS-test obtained for the proposed technique are close to 1 and are much higher as compared to the same obtained for other existing techniques. This shows that the genuine and imposter scores computed in the proposed technique are well-separated and are significantly different from each other.

- **Student's t-test:** It is a statistical hypothesis test used to show the significant difference between two sets of observations. We have performed a two-sample unpaired t-test at the significance level of 5%. The results of the t-test obtained for all the databases for genuine and imposter scores obtained using the proposed technique are shown in Table 4.4. In the t-test, if the value of $|t-stat|$ is greater than the value of

$t-critical$, then the null hypothesis is rejected and it represents that the input samples are significantly different from each other. It is clearly seen from Table 4.4 that for all databases, obtained values of $|t-stat|$ are greater than the value of $t-critical$. This substantiates that the genuine and imposter distributions are well-separated.

In summary, this chapter has proposed a fingerprint template generation using the non-invertible transformation, where the original minutiae locations are non-invertibly transformed by means of a user keyset. In order to align the secure fingerprint templates, a fingerprint alignment approach based on PCA has been utilized. The proposed technique has been evaluated on seven publicly available fingerprint databases by considering all four essential requirements. From the experimental analysis, it is evident that the generated secure templates are revocable, unlinkable, and robust against various attack scenarios. Further, the obtained results are compared with the existing techniques in terms of the EER value and the comparison clearly shows the effectiveness of the proposed technique.

Chapter 5

Adaptation of Pair-Polar Structure to Generate a Secure Fingerprint Template

In the previous chapter, a non-invertible transformation based technique has been proposed to generate the secure fingerprint template. Although the templates are secure and the proposed technique has performed quite well, an extra step of fingerprint alignment and singular point dependency still exist. Therefore, in order to eliminate these limitations, we propose a secure and alignment-free fingerprint template protection technique in this chapter by exploiting the pair-polar minutiae structures. In the proposed technique, a fingerprint based secure user template is represented in the form of a set of binary vectors. These vectors are computed from the many-to-one mapping of the transformed pair-polar coordinates (which are obtained using a non-invertible transformation) into a 3D grid. Results of the proposed technique are analyzed in terms of revocability, unlinkability, security, and performance on six publicly available databases of the Fingerprint Verification Competition (FVC) 2002 and 2004. The overall analysis of the results clearly shows the effectiveness of the proposed technique as compared to the existing state-of-the-art techniques. Further, the

The work presented in this chapter has been published in the paper: "*Adaptation of pair-polar structure to protect the fingerprint template*", IEEE Transactions on Industrial Informatics, 19(2), 1947-1956 (2022). DOI: 10.1109/TII.2022.3195938

summary of the significant contributions of this chapter is given below.

- The proposed technique computes a secure and alignment-free user template, which utilizes the pair-polar structure of minutiae and is independent from the use of a singular point.

- The non-invertible transformation and many-to-one mapping of pair-polar coordinates assure the infeasibility of reconstruction of the fingerprint image along with maintaining the discriminative property of the biometric data even after performing the transformation.

- The generated binary template is highly revocable and unlinkable. Further, the performance of the proposed technique is found to be superior compared to the existing state-of-the-art techniques, even on challenging databases such as FVC2002 DB3 and FVC2004 (DB1 & DB2).

- The computed templates are highly secure against various attack scenarios and prevent a fingerprint-based biometric system from illegitimate access and the loss of the user's original fingerprint data.

- Due to all these advantages, the proposed technique not only provides secure access to resources and sensitive data but also provides security against the permanent identity loss of a user.

A detailed description of the various steps involved in the proposed technique is discussed as follows.

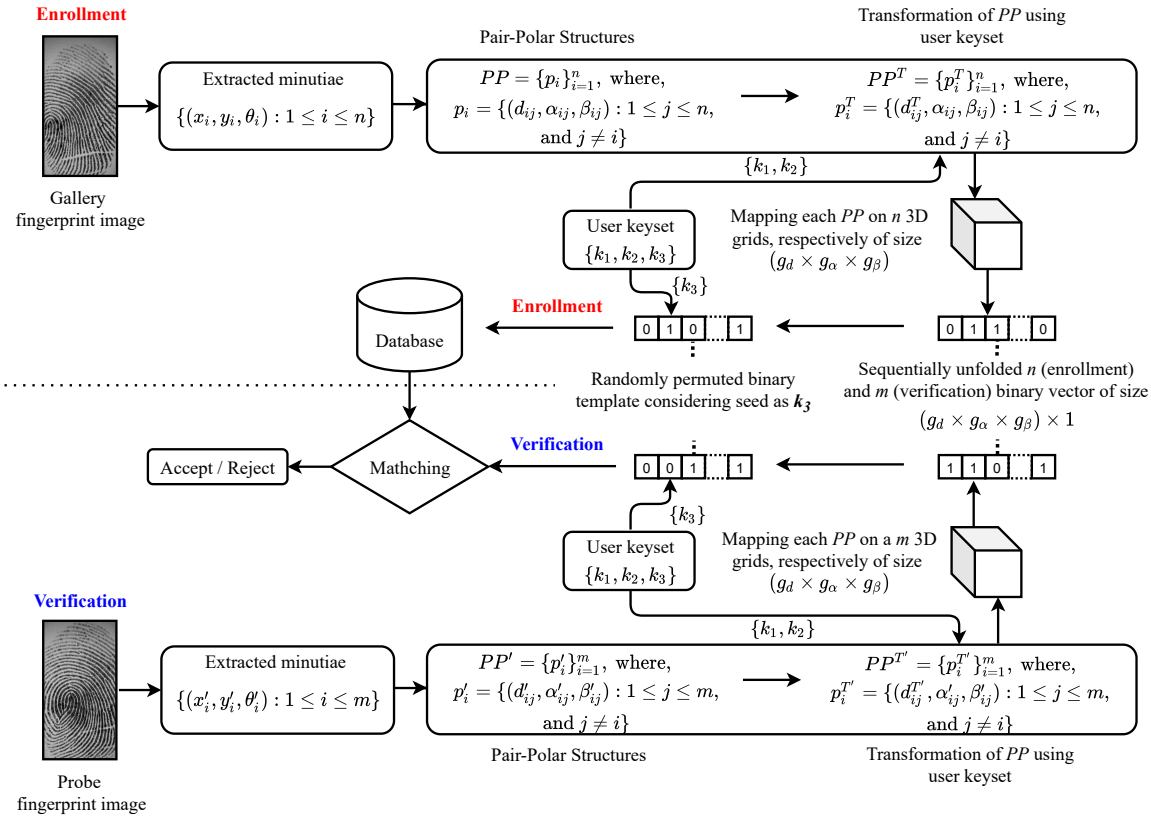


Figure 5.1: A schematic diagram depicting the working of the proposed technique.

5.1 Proposed Technique

This chapter proposes a secure fingerprint template protection technique using the pair-polar minutiae structure. The technique is alignment-free and does not rely on the use of singular point locations, which are prone to change due to the quality difference between two different fingerprint images of a subject. Also, the extraction of a singular point from an arch-type fingerprint impression does not produce consistent detection. A schematic diagram depicting the overall working of the proposed technique is shown in Figure 5.1. Further, the detailed working of different steps, starting from the minutiae extraction to the final matching procedure in the transformed domain, is given below.

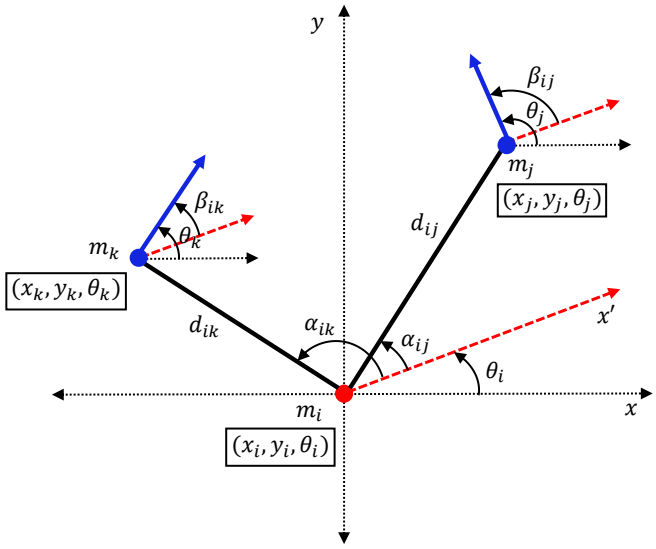


Figure 5.2: Representation of pair-polar minutiae structure.

5.1.1 Minutiae extraction and computation of pair-polar structure

The location and orientation values of minutiae are used to compute the secure fingerprint user template in the proposed technique. In order to extract the minutiae, we have utilized Verifinger-SDK (Demo version) [27], which returns the location and orientation values of the minutiae. Let the extracted minutiae set from a fingerprint be represented as $\mathrm{M} = \{(x_i, y_i, \theta_i) : 1 \leq i \leq n\}$, where (x_i, y_i) denotes the location of i^{th} minutia point, θ_i denotes its orientation, and n denotes the total number of minutiae present in the fingerprint image.

Furthermore, to compute the pair-polar structures [50, 69] of the minutiae for a fingerprint image, a minutia point m_i is considered as the reference point. The reference minutia point m_i is serving as the center point of the polar representation whereas its orientation θ_i is serving as the X-axis or 0° axis. Now, pair-polar coordinates of all the remaining minutiae are computed in the form of $p_i = \{(d_{ij}, \alpha_{ij}, \beta_{ij}) : 1 \leq j \leq n \text{ and } j \neq i\}$ with respect to the reference minutia m_i. Here, d_{ij} is the Euclidean distance between the minutiae m_i and m_j, α_{ij} is the orientation of the line connecting m_i to m_j with respect to θ_i in the anti-clockwise

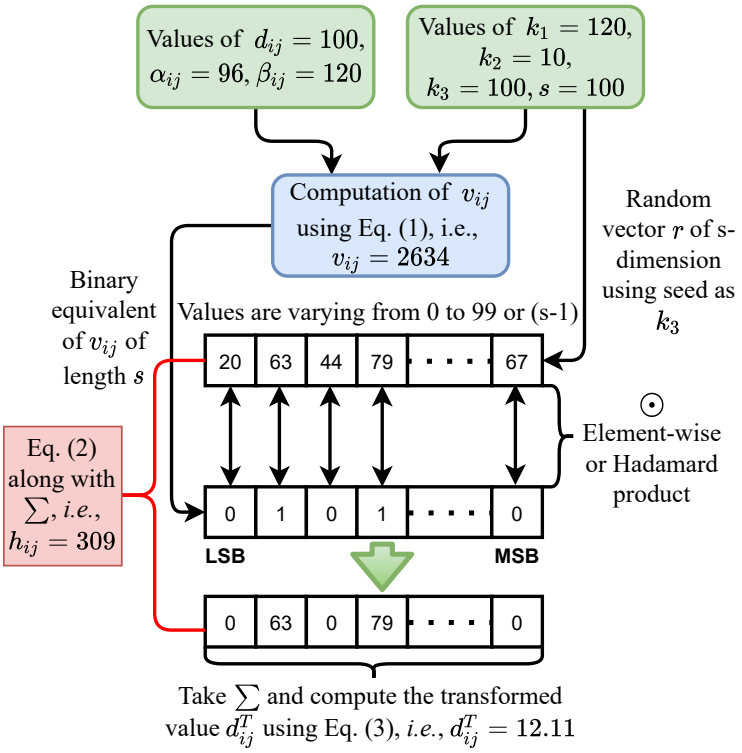


Figure 5.3: An example of representing the transformation of pair-polar coordinates considering $\max(dim) = 388$.

direction, and β_{ij} is the difference in orientation of minutiae m_i and m_j. The pair-polar minutiae structure is depicted in Figure 5.2, where pair-polar coordinates are computed by considering m_i as the reference minutia point. To compute the rotation and translation invariant fingerprint template, pair-polar coordinates of minutiae points, denoted as $PP = \{p_i\}_{i=1}^{n}$, are computed with respect to each minutia. These coordinates are further used to construct the secure template utilizing the steps discussed in the forthcoming subsections.

5.1.2 Transformation of pair-polar coordinates

Due to many-to-one mapping, the features extracted in the previous subsection are quite strong to generate a secure user template. However, since this will reveal the quantized values of pair-polar coordinates to an intruder, the transformed pair-polar coordinates are being calculated using a user keyset $\{k_1, k_2, k_3\}$ to enhance the security of the template. The trans-

formed pair-polar coordinates are denoted as $PP^T = \{p_i^T\}_{i=1}^n$, where $p_i^T = \{(d_{ij}^T, \alpha_{ij}, \beta_{ij}) : 1 \leq j \leq n \text{ and } j \neq i\}$. The transformed value d_{ij}^T for distance d_{ij} is computed as given below.

$$v_{ij} = \left\lceil \frac{k_1(d_{ij}(d_{ij} + \alpha_{ij} + \beta_{ij}))}{k_2} \right\rceil \tag{5.1}$$

$$h_{ij} = \sum_{l=1}^{s} r_l \text{Bin}_l(v_{ij}) \tag{5.2}$$

$$d_{ij}^T = \max(dim) \left(\frac{h_{ij}}{s(s-1)} \right) \tag{5.3}$$

where, r is an s-dimensional integer vector and is generated by randomly choosing integer values between a specific range of numbers (considered as 0 to $s-1$) while considering the seed as a user key, k_3. Further, Bin(v_{ij}) represents a $s-$bits long binary string equivalent to v_{ij}, and dim is the dimensions of a fingerprint image where max(dim) represents the size of the maximum dimension of the corresponding fingerprint image. Here, an intermediate representation v_{ij} of d_{ij} is computed using user-specific keys k_1 and k_2 in Equation 5.1, whereas Equation 5.2 computes the sum of element-wise or Hadamard product between the Bin(v_{ij}) and r. At last, the value of h_{ij} is re-scaled between 0 to $max(dim)$ to compute the value, d_{ij}^T. An example to show the computation of transformed value, d_{ij}^T, is presented in Figure 5.3. Since the transformation is non-invertible, the transformed value (*i.e.,* d_{ij}^T) protects the original information of pair-polar coordinates and makes it infeasible for an intruder to get the original minutiae locations from the transformed values. The obtained transformed values of pair-polar coordinates are further used to generate the secure user template that is represented in binary form.

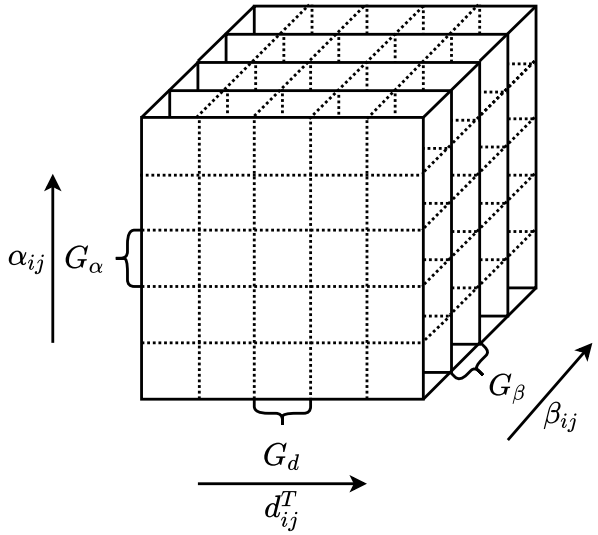


Figure 5.4: Representation of 3D grid used in the mapping of transformed pair-polar features.

5.1.3 Mapping and generation of secure user template

In order to generate the secure fingerprint template, first, the transformed values of pair-polar coordinates of minutiae with respect to each minutia point are mapped in a 3D grid of size $g_d \times g_\alpha \times g_\beta$, where the size of each cell is calculated as follows.

$$G_d = \left\lceil \frac{\max(dim)}{g_d} \right\rceil; G_\alpha = \left\lceil \frac{2\pi}{g_\alpha} \right\rceil; G_\beta = \left\lceil \frac{2\pi}{g_\beta} \right\rceil \tag{5.4}$$

Here, G_d, G_α, and G_β represent the size of each cell in a grid corresponding to the three dimensions, $i.e.$, for d_{ij}^T, α_{ij}, and β_{ij}, respectively. The maximum possible values for these dimensions are considered as $\max(dim)$, 2π, and 2π, respectively. The transformed pair-polar coordinates obtained with respect to each minutia point are mapped into the 3D grid one by one separately. This makes the total number of grids equal to the total number of minutiae ($i.e.$, n) present in the fingerprint image. The mapping of the transformed pair-polar coordinates that are calculated with respect to a minutia point m_i, is carried out as follows.

$$\begin{bmatrix} x_d^j \\ y_\alpha^j \\ z_\beta^j \end{bmatrix} = \begin{bmatrix} \lceil d_{ij}^T / G_d \rceil \\ \lceil \alpha_{ij} / G_\alpha \rceil \\ \lceil \beta_{ij} / G_\beta \rceil \end{bmatrix} \tag{5.5}$$

where, the value of $j = 1, 2, ..., n$ and $j \neq i$. Further, the value of a grid cell where $(d_{ij}^T, \alpha_{ij}, \beta_{ij})$ is mapped is set to 1. It can be noted that there are chances of getting the same grid cell being mapped to multiple coordinates; however, in such cases as well, the value is set to 1 only. Further, the value of the remaining cells is set to 0. The graphical representation of a 3D grid with respect to a minutia point is shown in Figure 5.4. Now, the 3D grids corresponding to each reference minutia point are sequentially unfolded to generate a set of binary vectors $b_{g\times 1}^i$, where the value of $i = 1, 2, ..., n$ and $g = g_d g_\alpha g_\beta$. Based on this, an intermediate user template is generated as a binary matrix, $\mathrm{B}_{g\times n} = [b^1, b^2, ..., b^n]$, where b^i is a column vector, and $i = 1, 2, ..., n$.

Eventually, to compute the final secure user template, each column vector of B is permuted by utilizing a random permutation matrix $\mathrm{P}_{g\times g}$, which is generated by considering the user key k_3 as the seed. Thus, the final secure user template T_f, which is essentially a binary matrix, is obtained as follows.

$$\mathrm{T}_f = \mathrm{P}_{g\times g}\mathrm{B}_{g\times n} \tag{5.6}$$

In the matrix T_f, the i^{th} column is a permuted version of the corresponding binary string b^i. The procedures of computing the pair-polar coordinates and the secure user template are shown in Algorithms 5.1 and 5.2, respectively. Further, the template T_f is stored in the database as a secure gallery fingerprint template at the time of enrollment. Similarly, at the time of authentication, the secure probe template is computed using the aforementioned

Algorithm 5.1 Computation of pair-polar structures

Input: A set of minutia points, M $= \{(x_i, y_i, \theta_i) : 1 \leq i \leq n\}$
Output: pair-polar coordinates of the minutia points, $PP = \{p_i\}_{i=1}^{n}$ where $p_i = \{(d_{ij}, \alpha_{ij}, \beta_{ij}) : 1 \leq j \leq n \text{ and } j \neq i\}$
Initialize: $PP = \text{zeros}(n, n-1, 3)$ /* Matrix of size $n \times (n-1) \times 3$ containing zeros */
for $i \leftarrow \{1, n\}$ **do**
    $j \leftarrow 1$
    $m_i = (x_i, y_i)$ /*Selecting i^{th} reference minutia */
    while $j \leq n$ **do**
        if $j \neq i$ **then**
            $m_j = (x_j, y_j)$ /*Selecting j^{th} minutia */
            /*Distance b/w i^{th} and j^{th} minutia points */
            $PP(i, j, 1) = ||m_i - m_j||_2$ /* value of d_{ij} */
            /*Angle b/w line segment m_i, m_j and x$-$axis */
            $PP(i, j, 2) = \tan^{-1}\left(\frac{y_j - y_i}{x_j - x_i}\right)$ /* computation of α_{ij} */
            /*Difference b/w the orientation of m_i and m_j minutia points*/
            $PP(i, j, 3) = |\theta_j - \theta_i|$ /* value of β_{ij} */
            /*Updating the value of $PP(i, j, 2)$ between 0 to 2π*/
            if $(y_j - y_i) < 0$ and $(x_j - x_i) > 0$ **then**
                $PP(i, j, 2) = 2\pi - |PP(i, j, 2)|$
            end if
            if $(x_j - x_i) < 0$ and $(y_j - y_i) > 0$ **then**
                $PP(i, j, 2) = \pi - |PP(i, j, 2)|$
            end if
            if $(x_j - x_i) < 0$ and $(y_j - y_i) < 0$ **then**
                $PP(i, j, 2) = \pi + |PP(i, j, 2)|$
            end if
            /*Difference b/w $PP(i, j, 2)$ and orientation of m_i to compute final α_{ij}*/
            $PP(i, j, 2) = |PP(i, j, 2) - \theta_i|$ /* value of α_{ij} */
        end if
        $j \leftarrow j + 1$
    end while
end for

steps, and matching is performed with the stored gallery template in the transformed domain. It is apparent from the above discussion that the mapping of transformed pair-polar coordinates to the 3D grid is many-to-one and also, it is evident that only the quantized values are revealed from the binary string generated from the mapped grid if the user template is compromised. This is an important characteristic of the proposed technique and helps

Algorithm 5.2 Computation of secure binary user template

Input: A set of transformed pair-polar structures, $PP^T = \{p_i^T\}_{i=1}^n$ and grid size as $g_d \times g_\alpha \times g_\beta$
Output: secure binary user template, T_f
Initialize: $G_d = \left\lceil \frac{\max(dim)}{g_d} \right\rceil$; $G_\alpha = \left\lceil \frac{2\pi}{g_\alpha} \right\rceil$; $G_\beta = \left\lceil \frac{2\pi}{g_\beta} \right\rceil$; $Grid = \text{zeros}(g_d, g_\alpha, g_\beta, n)$; $g = g_d g_\alpha g_\beta$
for $i \leftarrow \{1, n\}$ **do**
    $j \leftarrow 1$
    while $j \leq n$ **do**
        if $j \neq i$ **then**
            /*Computation of cell position in i^{th} 3D grid for transformed value of j^{th} pair-polar coordinate $(d_{ij}^T, \alpha_{ij}, \beta_{ij})$ */
            $x_d^j = \lceil \frac{d_{ij}^T}{G_d} \rceil$
            $y_\alpha^j = \lceil \frac{\alpha_{ij}}{G_\alpha} \rceil$
            $z_\beta^j = \lceil \frac{\beta_{ij}}{G_\beta} \rceil$
            /*Assigning selected cell value as 1 */
            $Grid(x_d^j, y_\alpha^j, z_\beta^j, i) = 1$
        end if
        $j \leftarrow j + 1$
    end while
end for
$\mathrm{P} = \text{randp}(g \times g)$ /*Random permutation matrix */
$\mathrm{B}_{g \times n} \leftarrow Grid_{g_d \times g_\alpha \times g_\beta \times n}$ /* Sequentially unfolding */
$\mathrm{T}_f \leftarrow \mathrm{P}_{g \times g} \mathrm{B}_{g \times n}$ /*Final secure template */

in maintaining the security of the user template. More analysis on this is provided in the experimental analysis section. In the next section, the matching procedure adopted in the proposed technique to match the two user templates is elaborated.

5.1.4 Matching procedure

During authentication, matching between the secure gallery and probe user templates is performed in the transformed domain to make the process completely secure. Let the number of minutiae in the probe and gallery templates be m and n, respectively. Further, let T_f^{Pro} and T_f^{Ga} be the probe and gallery templates, respectively. To perform matching, the binary string b_i^{Pro} (which is the i^{th} column in the user template matrix) of T_f^{Pro} with respect

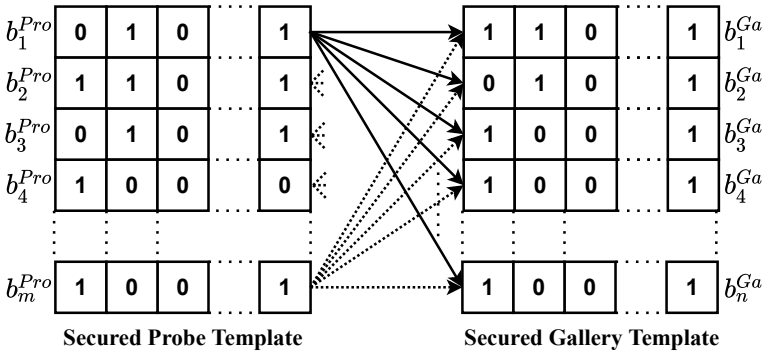


Figure 5.5: Matching of the transformed probe and gallery user templates.

to i^{th} reference minutia point is matched with all the binary strings of T_f^{Ga} with respect to the gallery minutia points. The matching score for each binary string of T_f^{Pro} is calculated as described below.

$$\mathrm{S}_{ij} = \frac{(m+n-2)\sum_{l=1}^{g} b_{il}^{Pro} * b_{jl}^{Ga}}{(m-1)^2+(n-1)^2} \tag{5.7}$$

where, "$*$" represents the bit-wise and operator and the size of matrix S is $m \times n$. To compute the final score (S_f), an average value of maximum scores corresponding to each binary vector of probe template, obtained after matching it with gallery templates, is considered and used in the computation as follows.

$$\mathrm{S}_{max}^{i} = \max(\mathrm{S}_{ij}), \text{ where } j = 1, 2, ..., n \tag{5.8}$$

$$\mathrm{S}_f = \frac{\sum_{i=1}^{m} \mathrm{S}_{max}^{i}}{m} \tag{5.9}$$

where S_{max}^{i} represents the maximum matching score when i^{th} binary string is being matched with all the binary strings of the gallery template. The complete matching procedure is described in Figure 5.5.

5.2 Experimental Analysis

In this section, the proposed technique has been analyzed by considering the recognition performance along with revocability, diversity/unlinkability, and security aspects of the generated user template. In the evaluation process, we have utilized six publicly available fingerprint databases, $viz.$, FVC2002 (DB1, DB2, DB3, and DB4) [1] and FVC2004 (DB1 and DB2) [26]. A brief description of these databases is provided in Section 1.4. Further, the detailed experimental analysis of the proposed technique on these databases is provided below.

5.2.1 Recognition performance analysis

There are four different metrics that have been used to assess the recognition performance of the proposed template protection technique, and these are FAR, FRR, GAR, and EER. In addition, 1-vs-1 and FVC protocols are being used to calculate the inter-class and intra-class matching scores to get the values of FAR and FRR, respectively. A brief description of these performance metrics and protocols has been provided in Sections 1.2.4 and 1.4, respectively.

The experiments have been performed by considering the two attack scenarios, *viz.* stolen-key (same-key) attack scenario and plain-key (different-key) attack scenario. In the first attack scenario, the same keyset has been used to construct the secure template throughout a database. In contrast, in the latter one, a different keyset for each subject is used to construct the secure template in the database. Further, the EER values have been calculated employing these attack scenarios as well as the protocols for each database. To generate the secure user template, the size of the grid, that is the values of g_α, g_β, and g_d have an important role to play. Hence, in order to get an optimal grid size, the experimentation is being performed where the EER value is computed by varying the parameters g_α, g_β, and

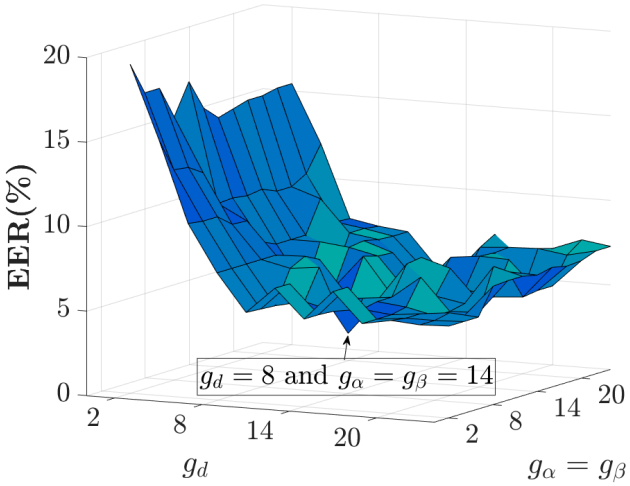


Figure 5.6: Finding the optimum value of parameters for grid size with the help of EER. The lowest EER value for which the optimum parameters (g_d, g_α, g_β) are obtained is pointed by an arrow on the EER surface plot.

g_d. In the process, since the parameters g_α and g_β represent angles, their values are kept equal. The set of parameter values for which the best EER is achieved is considered optimal. The process of parameters tuning is performed on combined FVC2002 DB1_b, DB2_b, DB3_b, and DB4_b databases which are provided in FVC2002 database[1] for the purpose of parameters tuning. The database contains 40 subjects where 8 fingerprint samples are present per subject. In the experimentation, the value of g_d is fixed starting from 2 to 24 and the value of EER is computed by varying the value of $g_\alpha = g_\beta = 2$ to 24. Among these computations, the best EER is achieved for $g_d = 8$ and $g_\alpha = g_\beta = 14$ as depicted in Figure 5.6. Hence, these values are used for parameters g_d, g_α, and g_β in further experimentation.

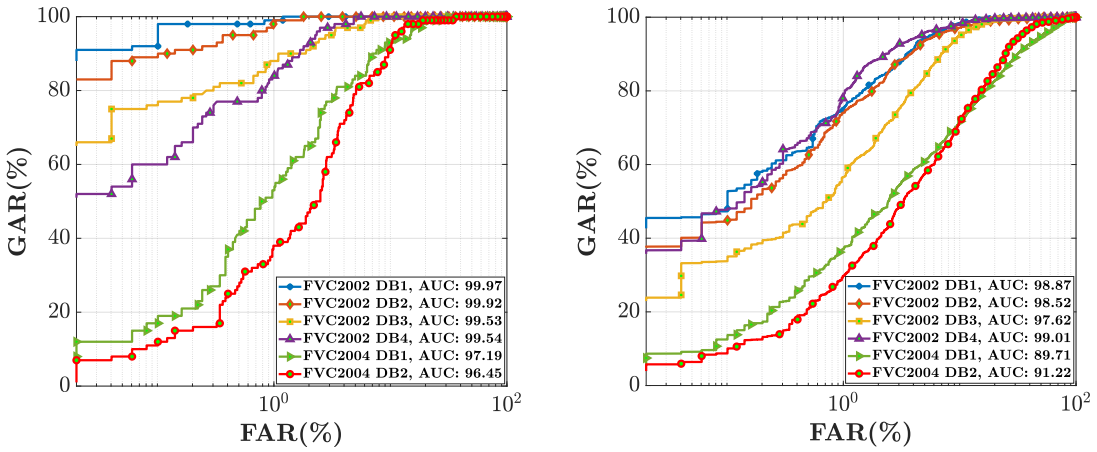
In the plain-key attack scenario, the proposed technique attains an EER of 0% in all the databases for both protocols ($i.e.$, 1-vs-1 and FVC). This attack scenario shows the best case of the performance as the keysets are different for each subject in the database. When we analyze the worst-case scenario, which happens in the stolen-key attack scenario, the proposed technique performs quite well here too as compared to the existing state-of-the-

Table 5.1: EER (%) values of the proposed technique compared with the existing techniques for 1-vs-1 and FVC protocols under the stolen-key attack scenario

Various techniques	**FVC2002 (EER%)**								**FVC2004 (EER%)**			
	DB1		**DB2**		**DB3**		**DB4**		**DB1**		**DB2**	
	1v1	**FVC**	**1v1**	**FVC**	**1v1**	**FVC**	**1v1**	**FVC**	**1v1**	**FVC**	**1v1**	**FVC**
Ahmad et al. [69]	9	-	6	-	27	-	-	-	-	-	-	-
Wang and Hu [70]	3.5	-	4	-	7.5	-	-	-	-	-	-	-
Kumar et al. [74]	-	-	-	4.98	-	-	-	-	-	-	-	-
Jin et al. [77]	5.19	-	5.65	-	-	-	-	-	16.35	-	8.66	-
Ferrara et al. [76]	0	3.33	0.37	1.76	4.94	7.78	3.37	-	-	-	-	-
Yang et al. [81]	5.93	-	4	-	-	-	-	-	-	-	-	-
Yang et al. [47]	3.38	11.84	0.59	10.38	9.80	16.52	16.52	15.63	-	-	14.88	20.61
Ahn et al. [73]	-	7.18	-	3.61	-	11.80	-	11.46	-	-	-	-
Jin et al. [79]	4.36	-	1.77	-	-	-	-	-	24.71	-	21.82	-
Sandhya and Prasad [80]	4.71	-	3.44	-	8.79	-	-	-	-	-	-	-
Wang and Hu [83]	3	4	2	3	7	8.5	-	-	-	-	-	-
Sandhya et al. [84]	3.96	-	2.98	-	6.89	-	-	-	12.17	-	13.29	-
Sandhya and Prasad [86]	2.19	-	1.6	-	6.14	-	-	-	11.89	-	12.71	-
Ali et al. [97]	2	-	1	-	3.1	-	-	-	-	-	-	-
Yang et al. [100]	-	-	1	-	-	-	-	-	-	-	10	-
Trivedi et al. [102]	1.2	-	2.1	-	-	-	-	-	-	-	-	-
Yang et al. [105]	1.0	-	2.0	-	4.0	-	-	-	-	-	11.0	-
Lahmidi et al. [104]	3.09	-	1.83	-	-	-	-	-	-	-	-	-
Proposed Technique	**1.0**	**5.3**	**1.0**	**5.7**	**3.3**	**7.7**	**3.0**	**4.7**	**8.9**	**18.3**	**9.6**	**17.3**

Note: "-" denotes non-availability of data and "**1v1**" *represents* 1-vs-1 *protocol.*

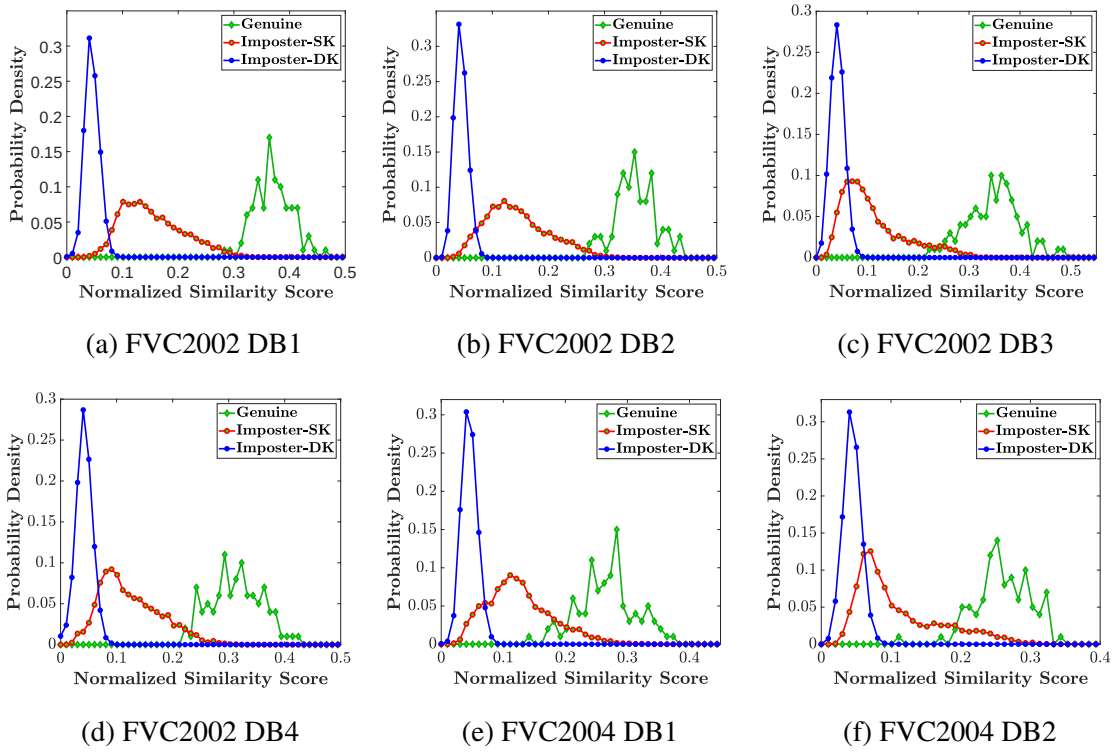
art techniques. The EER(%) values that are obtained in the stolen-key attack scenario with respect to 1-vs-1 and FVC protocols are given in Table 5.1. It can be clearly seen in the table that the proposed technique has performed exceptionally well as compared to the existing techniques for both 1-vs-1 and FVC protocols, except for [76] and [83]. However, the technique [76] generates fingerprint templates that are not revocable, whereas the proposed technique possesses the revocability property. Further, the values of EER for the proposed technique are slightly low as compared to [83] in the case of FVC protocol for FVC2002 DB1 and FVC2002 DB2 databases. Nevertheless, the EER values of the proposed technique are superior for the FVC2002 DB3 database in the case of FVC protocol whereas superior for all the databases in the case of 1-vs-1 protocol when compared to the results of [83]. The proposed technique has slightly under-performed for the FVC2002 DB2 database in the case of FVC protocol as compared to [74] and [73]; however, the approaches which are discussed in these works do not utilize the user keyset whereas our proposed technique utilizes the user keyset, which increases the privacy of the fingerprint template and enables the capabilities



(a) (b)

Figure 5.7: ROC plots of the proposed technique along with AUC (represented in percentage) for different databases in the stolen-key scenario considering (a) 1-vs-1 protocol and (b) FVC protocol.

of the essential properties. Further, Receiver Operating Characteristics (ROC) curves are plotted for all the databases considering the stolen-key attack scenario and both protocols. The ROC curve represents the change in GAR with respect to the change in FAR. In the ROC curve, if the value of Area Under the Curve (AUC) is equal or close to 100%, it represents the high effectiveness of the technique. The ROC plots of the proposed technique for different databases are shown in Figure 5.7(a) and Figure 5.7(b). As desired, it is clearly seen from the plots that the values of AUC are very close to 100% for all the databases for both protocols. Further, the distribution of matching scores for different databases considering both stolen-key and plain-key scenarios are plotted in Figure 5.8. As desired, it can be seen from the figure that the genuine score distributions of all the databases are significantly different from their corresponding imposter score distributions for the plain-key as well as for the stolen-key attack scenarios.



(a) FVC2002 DB1 (b) FVC2002 DB2 (c) FVC2002 DB3

(d) FVC2002 DB4 (e) FVC2004 DB1 (f) FVC2004 DB2

Figure 5.8: Distribution of genuine and imposters scores for the proposed technique on different databases considering stolen-key and plain-key attack scenarios, where SK represents same-key/stolen-key scenario and DK represents different-key/plain-key scenario.

5.2.2 Revocability analysis

Revocability is an ability of a template protection technique, which allows replacing a stored template with a completely different new template for a user when the stored template has been compromised. As the correlation between the stored template and the new template is desired to be negligible, an adversary cannot access the biometric system by means of the compromised template. In this section, two different analyses based on existing frameworks [21, 121] have been provided to establish the fact that the proposed technique computes a completely revocable template. To do that, we have calculated the mean and the variance of pseudo-genuine scores and have compared them with the mean and the variance of genuine and imposter scores in the first analysis. Pseudo-genuine scores are the scores calculated by matching the user templates generated using different keysets and the same fingerprint im-

age. Here, for each database, a total of 1000 pseudo-genuine scores are calculated in which a keyset is used to compute the gallery template using a fingerprint image for each subject. Further, by using the same fingerprint image, 10 more pseudo-genuine probe templates are generated by using 10 different keysets to compute the matching scores. The mean and the variance of these scores are compared with that of the genuine and the imposter scores calculated for the stolen-key scenario for all the databases. This comparison is given in Table 5.2, where it can be clearly observed that the values of the mean of the imposter and pseudo-genuine scores are nearly equal to each other, whereas they both are very different from the mean values of the genuine scores of all the databases. Moreover, the variance of pseudo-genuine scores is very far from the variance of the genuine and imposter scores while considering the stolen-key attack scenario. This clearly shows that if the compromised template is matched with the replaced new template, the compromised template will behave like an imposter template.

In addition to this analysis, we have also evaluated the proposed technique for the revoked template attack as discussed in [21]. This attack has two variants as discussed below.

- Type-I attack: Biometric system is attacked using the compromised (revoked) template, where the database contains a new different template computed using the same fingerprint impression as used in the revoked one and a different keyset.

- Type-II attack: Biometric system is attacked using the compromised (revoked) template, where the database contains a new different template computed using a different fingerprint impression of the same subject and a different keyset.

These attacks have been performed considering the 0% FAR case, and it is found that not even a single revoked template is falsely accepted in the proposed technique as depicted in Table 5.3. Hence, both of these analyses show that the secure templates obtained in the

Table 5.2: Comparison of mean (μ) and variance (σ) of genuine, imposter, and pseudo-genuine score distributions for all the databases

Databases		Genuine	Imposter	Pseudo-genuine
FVC2002 DB1	μ	0.37	0.15	0.04
	σ^2	0.0021	0.0029	0.0002
FVC2002 DB2	μ	0.35	0.14	0.04
	σ^2	0.0022	0.0029	0.0001
FVC2002 DB3	μ	0.34	0.11	0.04
	σ^2	0.0030	0.0035	0.0002
FVC2002 DB4	μ	0.31	0.12	0.04
	σ^2	0.0022	0.0026	0.0002
FVC2004 DB1	μ	0.27	0.12	0.04
	σ^2	0.0045	0.0025	0.0002
FVC2004 DB2	μ	0.26	0.11	0.04
	σ^2	0.0039	0.0036	0.0001

Table 5.3: The number of matched templates (%) in the event of revoked template attack for all the databases at 0% FAR

Databases	Type-I Attack	Type-II Attack
FVC2002 DB1	0	0
FVC2002 DB2	0	0
FVC2002 DB3	0	0
FVC2002 DB4	0	0
FVC2004 DB1	0	0
FVC2004 DB2	0	0

proposed technique are highly revocable.

5.2.3 Unlinkability analysis

This section presents the analysis of the unlinkability/diversity of the secure templates computed using the proposed technique. The property of unlinkability requires that the secure templates generated by a template protection technique should be very distinct from each other in terms of similarity so that the different attacks (such as correlation and ARM attacks) can be prevented in a biometric system. We have utilized two different scenarios to show the unlinkability of templates generated by the proposed technique. First, the unlink-

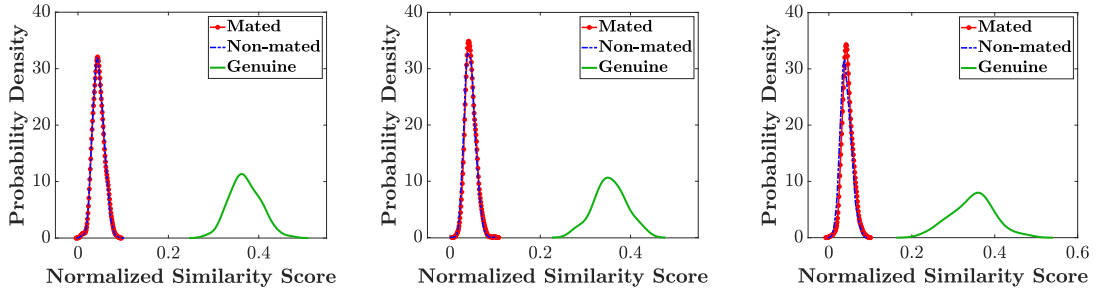
Table 5.4: Global unlinkability measure $\mathrm{D}_{\leftrightarrow}^{sys}$ [6] of the proposed technique for all the databases

Databases	$\mathrm{D}_{\leftrightarrow}^{sys}$
FVC2002 DB1	0.0019
FVC2002 DB2	0.0009
FVC2002 DB3	0.0013
FVC2002 DB4	0.0017
FVC2004 DB1	0.0020
FVC2004 DB2	0.0018

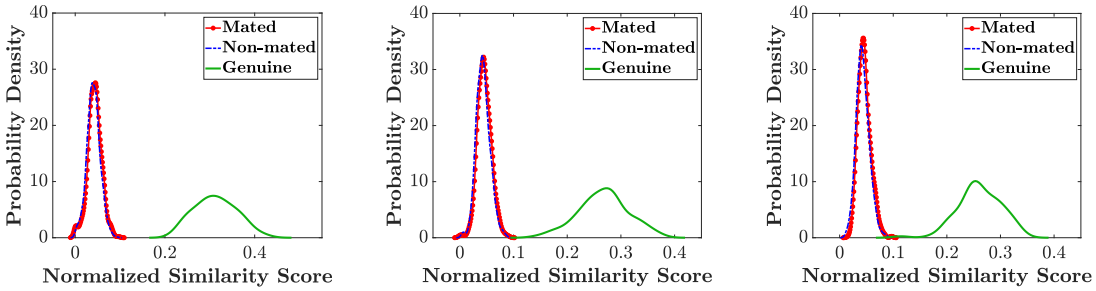
ability analysis is being carried out based on a recent general framework proposed in [6], and second, it has been performed based on the approach discussed in [7].

According to the framework given in [6], if the mated and non-mated distributions overlap, it shows the highly unlinkable nature of the computed templates. In addition, the value of a global measure $\mathrm{D}_{\leftrightarrow}^{sys}$ [6], which is computed using the mated and non-mated distributions, varies between 0 to 1 and defines the high unlinkability of a system if the value is near to zero. In order to perform this analysis, mated score and non-mated score distributions have been estimated for the proposed technique along with the value of $\mathrm{D}_{\leftrightarrow}^{sys}$. Mated scores are computed by matching the templates that are generated from the same fingerprint impression and different keysets; whereas, non-mated scores are computed by matching the templates that are generated from the fingerprint impressions of different subjects and by using different keysets. For the proposed technique, the resultant mated and non-mated scores distributions along with the genuine scores have been plotted in Figure 5.9, and the obtained values of $\mathrm{D}_{\leftrightarrow}^{sys}$ are shown in Table 5.4 for all the databases. As desired, we can observe from the figure that the distributions of mated and non-mated scores overlap with each other, whereas they are very far from the genuine score distributions for all the databases. Also, it is seen that the values of $\mathrm{D}_{\leftrightarrow}^{sys}$ are near to zero. Hence, this analysis strongly supports the unlinkability of the secure templates computed using the proposed technique.

In the second analysis which is based on the framework discussed in [7], False Cross

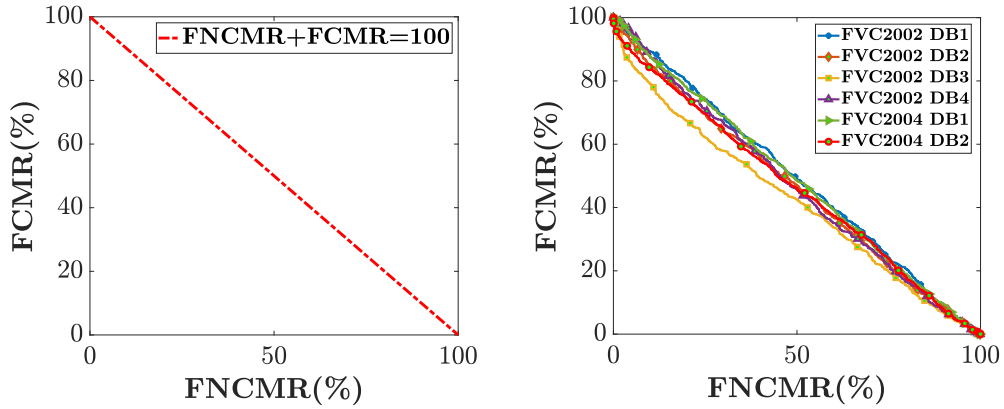


(a) FVC2002 DB1 (b) FVC2002 DB2 (c) FVC2002 DB3



(d) FVC2002 DB4 (e) FVC2004 DB1 (f) FVC2004 DB2

Figure 5.9: Distribution of mated, non-mated, and genuine (stolen-key attack scenario) scores plotted to show the unlinkability of the secure fingerprint template generated in the proposed technique on different databases.



(a) (b)

Figure 5.10: FNCMR *vs.* FCMR plots: (a) for an ideal case of unlinkability, (b) for the proposed technique on different databases.

Match Rate (FCMR) and False Non-Cross Match Rate (FNCMR) are computed for all the databases utilizing the secure templates generated by the proposed technique. Here, FCMR defines the rate of successful matches between the non-mated samples, whereas the FNCMR

denotes the rate of unsuccessful matches between the mated samples. We have computed these rates at different thresholds and have plotted them for all the databases in Figure 5.10. As mentioned in [7], for a technique that generates completely unlinkable templates, the sum of FNCMR (%) and FCMR (%) should always be equal to 100. Such an ideal case is being depicted in Figure 5.10(a). For the proposed technique, the FNCMR *vs.* FCMR plots fall nearly on FNCMR + FCMR $= 100$ line for all the databases as shown in Figure 5.10(b). Hence, it is clearly evident from this analysis that the secure templates generated in the proposed technique are highly unlinkable in nature.

5.2.4 Security analysis

Security is one of the important properties which ensures the privacy of a user's biometric data and prevents unauthorized access to a biometric system. This section analyzes the security aspect of the user template generated by the proposed technique considering the non-invertibility, brute-force attack, attack via record multiplicity (ARM attack), and false accept attack scenarios.

5.2.4.1 Non-invertibility

This property provides an assurance that the reconstruction of the original fingerprint image is infeasible from the secure user template. It is an important property and needs to be followed by any template protection technique in order to provide the privacy to the user's biometric data. In the proposed technique, transformed pair-polar coordinates of minutiae points are mapped into a 3D grid to compute a secure binary template using many-to-one mapping, which makes it infeasible for an intruder to get back to the original pair-polar coordinates from the secure user template. Further, it may be possible to get the quantized values of the transformed pair-polar coordinates $(d_{ij}^T, \alpha_{ij}, \beta_{ij})$ from the binary string by an

intruder. Here, the quantized value would be the location of a cell of size ($G_d \times G_\alpha \times G_\beta$) in the 3D grid. Hence, the total number of possibilities to select a single value of coordinate would be given by ($G_d \times G_\alpha \times G_\beta$) with respect to a minutia (considering each integer as a single value). Now, if n is the total number of minutiae present in a fingerprint image, the total number of combinations possible to select transformed pair-polar coordinates will be given as $(G_d \times G_\alpha \times G_\beta)^{n-1}$ which gives the huge number of possibilities. Moreover, in the technique, the value of distance d_{ij} from a reference minutia m_i to minutia m_j is transformed by using a non-invertible transformation function and a user keyset. Hence, there will be 2^s different combinations of binary equivalent of v_{ij}, which are needed to get back the original value of d_{ij} from d_{ij}^T with respect to a minutia as discussed in Section 5.1.2. Now, let us assume that we have n number of minutiae points, then the total number of different combinations would be $2^{s(n-1)}$. Therefore, computing the transformed pair-polar coordinates from the quantized values and original value of d_{ij} from d_{ij}^T collectively exhibits a huge number of possibilities that are infeasible to compute and hence, it strongly supports the non-invertible nature of the secure user template.

5.2.4.2 Brute-force attack

In this attack scenario, an attacker tries all the possibilities either to get back the original minutiae information and reconstruct the original fingerprint from the secure template or to get illegitimate access to the biometric system. The secure user template generated in the proposed technique is robust against this attack scenario. To establish this fact, let us assume that the intruder has got access to the secure user template which in turn provides the quantized values of the transformed pair-polar coordinates, $i.e.$, $p_i^T = \{(d_{ij}^T, \alpha_{ij}, \beta_{ij}) : 1 \leq j \leq n-1 \text{ and } j \neq i\}$. The size of a small unit in a grid (used for quantization) is considered as $g_d = 8$ for d_{ij}^T, $g_\alpha = 14$ for α_{ij}, and $g_\beta = 14$ for β_{ij}. So while considering

a minutia m_i as a reference point and to get the original transformed values of pair-polar coordinates from the quantized value, the total possibilities that are encountered will be equal to $(\frac{\max(dim)}{8} \times \frac{\pi}{7} \times \frac{\pi}{7})^{n-1}$ where n is the total number of minutiae points present in the fingerprint. Let us consider that $n = 30$ (typically a fingerprint image contains 30 or more minutiae points) then the total number of possibilities will be $comb = (\frac{\max(dim)}{8} \times \frac{\pi}{7} \times \frac{\pi}{7})^{29}$, which gives a huge number of possibilities to try out. In addition, the value of distance d_{ij}^T is a transformed value and to get the original distance d_{ij} from it, the total number of possibilities to check will be equal to 2^s for a single minutia, which is equivalent to 2^{100} if $s = 100$ (as discussed in Section 5.1.2). So for all the minutiae points, the total number of possibilities to check will be equal to $2^{100(n-1)}$, which is basically 2^{2900} as typically the value of n would be equal to 30. Thus, the probability of getting back the original pair-polar coordinates of $n = 30$ minutiae points will be equal to $\frac{29}{2^{2900}+comb}$, which is negligible (≈ 0). This depicts the highly robust nature of the proposed technique against the brute-force attack for the reconstruction of the fingerprint image. Further, if an attacker only knows about the final structure of the secure template, then the total number of combinations to get the illegitimate access will be equal to 2^{1568} as the size of the secure template with respect to a reference minutiae is 1568-bits (computed by unfolding the $8 \times 14 \times 14$ grid). Again, these many combinations are infeasible to compute which further confirms the robustness of the proposed technique against the brute force attack.

5.2.4.3 False accept attack

In this attack scenario, the attempts are fewer as compared to the brute-force attack to get illegitimate access, when an intruder somehow has the knowledge of the matching score or the number of 1s in the binary template. In the proposed technique, the number of 1s in a binary string (b_i^{Ga}) of a secure gallery template is nearly equal to the number of minutiae

points (that is, n) present in the fingerprint image. Now, let us consider that the average number of minutiae points present in a fingerprint image of a user is equal to 30. Then the total number of possible binary templates with respect to a reference minutia point to get the illegitimate access would be approximately $\binom{1568}{30}$, which is a very huge number and infeasible to compute and try out to get the access. In addition, suppose an attacker somehow gets the information about the average matching score (that is, the number of matched bits) that is approximately 30% at 0% FAR case in the proposed technique. Then, to guess the original binary string with respect to a reference minutia point, $\binom{1568}{0.3\times30}$ possible combinations (assuming $n = 30$) of binary strings are approximately needed to try out to get the access, which is again infeasible to compute. Thus, this analysis clearly shows the robustness of the proposed technique against the false accept attack.

5.2.4.4 Attack via Record Multiplicity (ARM)

In the ARM attack, by inspecting and comparing the multiple transformed templates compromised from the different or same biometric system, an attacker tries to find out some information regarding the original features of the fingerprint image. This can be feasible when the transformed template is obtained by performing a slight change in the original features of the fingerprint. In the proposed technique, first, pair-polar coordinates are computed from the minutiae points $(d_{ij}, \alpha_{ij}, \beta_{ij})$, and then the values of d_{ij} are transformed using a user keyset $\{k_1, k_2, k_3\}$. Further, the pair-polar coordinates with transformed d_{ij} are mapped into a 3D grid by means of many-to-one mapping. Hence, just comparing the two user templates which are in the form of binary strings or, in the worst-case quantized values, will not provide any fruitful information about the original features of the fingerprint image. Hence it is infeasible to perform the ARM attack on a secure user template generated by the proposed technique.

In summary, an alignment-free and non-invertible fingerprint template generation technique has been proposed in this chapter. In order to generate the final secure template, pair-polar structures of the minutiae are transformed by means of non-invertible transformation and user keys. Further, the transformed pair-polar structures are mapped in a 3D grid to generate the binary strings followed by the random permutation of the binary strings. The proposed technique has been evaluated in terms of various standard performance metrics by considering the all four essential criteria. Finally, the overall analyses with respect to all four essential criteria depict the effectiveness and robustness of the proposed technique as compared to the existing approaches.

Chapter 6

Generation of Secure Fingerprint Template using Pair-Polar Structure of Minutiae and DFT

In the previous chapter, the secure user template has been defined in the form of binary vectors, and it has been generated by mapping the transformed pair-polar coordinates in a 3D grid. However, if we map the original pair-polar coordinates in a 3D grid at the first place and non-invertible transformation is performed on the computed binary vectors, in that case, the overall performance is increased. This performance improvement is happening because the positions of pair-polar coordinates in a 3D grid are correctly recorded when we use them directly without any transformation. Therefore, by keeping this in mind, we propose a novel fingerprint template protection technique in this chapter, which computes a binary fingerprint template based on the mapping of pair-polar structures of minutiae in a 3D grid, and then secures the template by utilizing Discrete Fourier Transform (DFT) followed by a random permutation of the resultant binary vectors. The proposed technique

The work presented in this chapter has been published in the paper: "*Generation of secure fingerprint template using DFT for consumer electronics devices*", IEEE Transactions on Consumer Electronics, 1-10 (2022). (Early Access) DOI: 10.1109/TCE.2022.3217234

is an alignment-free, non-invertible, singular point independent technique, and conforms to all the essential requirements of a fingerprint template protection technique. The technique has been analyzed in terms of revocability, diversity, security, and performance by using four publicly available fingerprint databases of the Fingerprint Verification Competition (FVC) 2002 and 2004. The EER values of the technique for all the four databases are compared with that of the state-of-the-art techniques, and the superiority of the results clearly depicts the robustness and effectiveness of the proposed technique. The key contributions of this research work are as follows.

- The proposed technique computes an alignment-free and singular point independent cancelable template, which can be easily revoked in the event of an attack.
- The secure templates generated by the proposed technique are non-invertible, which prevents the reconstruction of fingerprint image using the compromised template.
- The secure templates generated by the proposed technique are unlinkable to each other, which ensures the prevention of cross-match attack using multiple templates.
- The recognition performance of the proposed technique is highly encouraging even in the case of challenging databases such as FVC2004 DB1 and FVC2004 DB2.

A detailed discussion of the proposed technique is provided in the following sections.

6.1 Proposed Technique

In the proposed technique, the original fingerprint template, which is the collection of minutiae points, is secured by using a non-invertible transformation based on the DFT. We have utilized the pair-polar structures [50, 69] of minutiae points, which represent the local association of minutiae points in terms of angles and distances. The use of this information

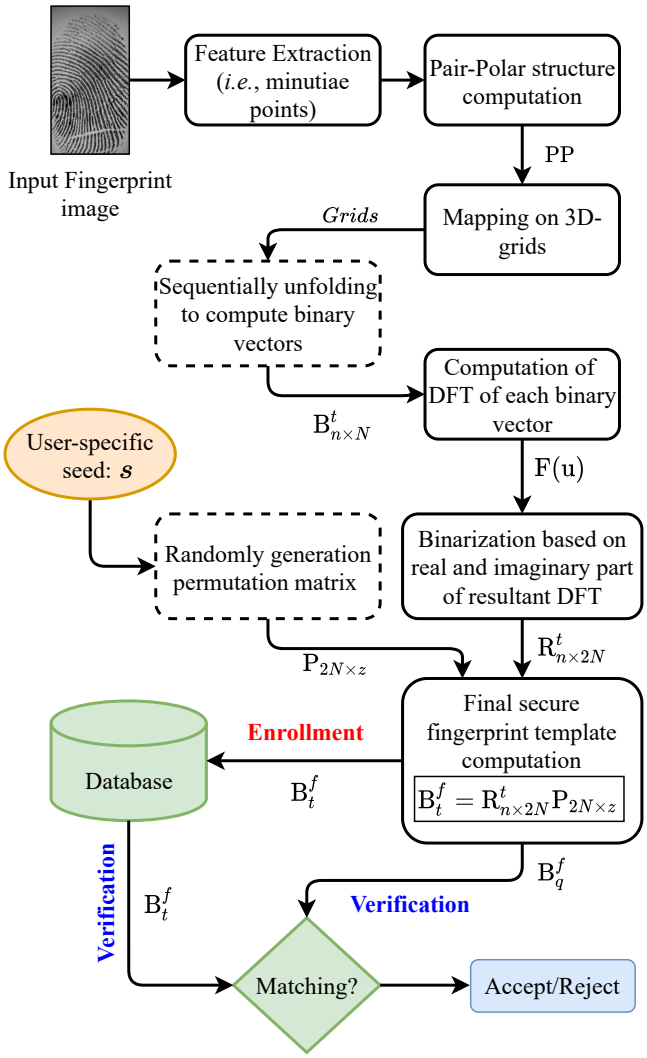


Figure 6.1: Block diagram depicting the overview of the proposed technique.

makes the constructed secure template alignment-free in the proposed technique. Various steps involved in the proposed technique are depicted in Figure 6.1. Firstly, the fingerprint impression is captured through a sensor, then the extraction of minutiae points is performed. Further, the secure fingerprint template is computed by a sequence of steps, as shown in Figure 6.1. A user-specific key ($i.e.$, seed s) is utilized to enable the revocability of the template, which can be separately given by the users, or the system can randomly generate it for different users. A detailed description of the various steps of the proposed technique is further discussed in the following subsections.

6.1.1 Construction of pair-polar structure

Let there be a minutiae set $\mathrm{M} = \{m_i : 1 \leq i \leq n\}$, where m_i and n represent the i^{th} minutia point and the total number of minutiae present in a fingerprint image, respectively. Further, let $m_i = (x_i, y_i, \theta_i)$, where (x_i, y_i) and θ_i represent the location and the orientation values of a minutiae point, respectively. While considering each m_i as a reference minutia, the pair-polar structure can be represented as $\mathrm{PP} = \{p_i : 1 \leq i \leq n\}$, where p_i is given as $p_i = \{(d_{ij}, \alpha_{ij}, \beta_{ij}) : 1 \leq j \leq n \text{ and } j \neq i\}$. Here, the values of d_{ij}, α_{ij}, and β_{ij} are computed as given in Equation 6.1 with respect to i^{th} reference minutia (x_i, y_i, θ_i) and the j^{th} minutia (x_j, y_j, θ_j).

$$\begin{aligned} d_{ij} &= ||m_i - m_j||_2, \\ \alpha_{ij} &= \left| \arctan \frac{y_j - y_i}{x_j - x_i} - \theta_i \right|, \\ \beta_{ij} &= |\theta_i - \theta_j| \end{aligned} \tag{6.1}$$

An example of a pair polar structure is depicted in Figure 6.2. Further, in the technique, pair-polar structures obtained by considering each minutia as a reference point are used to construct the binary fingerprint template.

6.1.2 Computation of binary fingerprint template

Once the pair-polar structures (PP) of all minutiae points are computed, each structure is further mapped into a 3D grid defined by dimensions d, α, and β, separately for each reference minutiae point. Hence, the total number of 3D grids after performing the mapping is equivalent to the total number of minutiae points (n) in a fingerprint image. The size of each grid is given as $g_d \times g_\alpha \times g_\beta$ whereas the values being represented by each cell of the grid along the three dimensions ($i.e.$, d, α, and β) are given as G_d, G_α, and G_β, respectively.

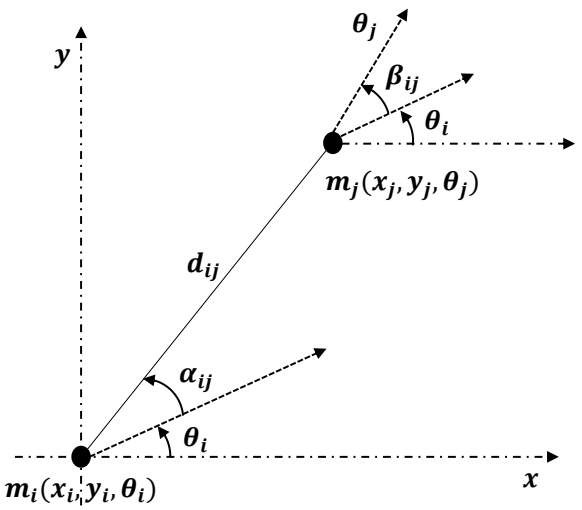


Figure 6.2: An example of pair-polar structure of minutia point m_j with respect to a reference minutia m_i.

The values of G_d, G_α, and G_β are computed as $\lceil d_{max}/g_d \rceil$, $\lceil \alpha_{max}/g_\alpha \rceil$, and $\lceil \beta_{max}/g_\beta \rceil$, respectively. Here, d_{max}, α_{max}, and β_{max} represent the maximum possible value of the corresponding dimension. Further, to compute the mapped location of each entry of set p_i in a 3D grid, the values of d_{ij}, α_{ij}, and β_{ij} are divided by G_d, G_α, and G_β, respectively, as given below.

$$x_d^j = \left\lceil \frac{d_{ij}}{G_d} \right\rceil; y_\alpha^j = \left\lceil \frac{\alpha_{ij}}{G_\alpha} \right\rceil; z_\beta^j = \left\lceil \frac{\beta_{ij}}{G_\beta} \right\rceil \tag{6.2}$$

where, $j = 1, 2, ..., n$ and $j \neq i$. Now, all the grid cells are initialized to zero. Further, the grid-cells corresponding to locations $(x_d^j, y_\alpha^j, z_\beta^j)$, where $j = 1, 2, ..., n$ and $j \neq i$, are set to one and this value remains one for a grid cell even if there are more than one values mapped to the same location. Subsequently, binary vectors of size $1 \times N$ (where $N = g_d g_\alpha g_\beta$) are generated by sequentially unfolding the computed 3D grid corresponding to each reference minutia point. These binary vectors (b^i, where $i = 1, 2, ..., n$) are further combined to form the binary fingerprint template, which is given as $\mathrm{B}_{n\times N}^t = [b^1\ b^2 ... b^n]^T$.

6.1.3 Computation of secure fingerprint template

After obtaining the binary fingerprint template B^t, it is secured by utilizing the N-point DFT and then further binarizing the values of the real and imaginary parts of DFT. The DFT of each binary vector present in the template B^t is computed using the following equation.

$$\begin{aligned} f^i(u) = \sum_{k=0}^{N-1} b_k^i e^{-j2\pi uk/N}, \text{ where } u = 0, 1, ..., N-1 \\ \mathrm{F}(u) = \left[f^1(u)\ f^2(u)...f^n(u)\right]^T \end{aligned} \tag{6.3}$$

where, $f^i(u)$ is a complex vector consisting the N-point DFT of i^{th} binary vector b^i of template B^t and $\mathrm{F}(u)$ is a matrix of size $n \times N$, containing N-point DFT of all binary vectors present in the template B^t. Let $f^i(u)$ be given as $f_k^i(u) = \{real(f_k^i(u)) + j\ imag(f_k^i(u)) :$ where $k = 1, 2, ..., N\}$. Now, the real and imaginary parts of k^{th} value of complex vector $f^i(u)$ are binarized separately to compute the secure intermediate binary template in such a way that if the value of $real(f_k^i(u)) > 0$ and $imag(f_k^i(u)) > 0$, then the value is set to 1 in the resultant binary vector otherwise it would be set to 0. This binarization makes it infeasible for an intruder to perform the inverse DFT in case the template is compromised.

Thus, the size of the resultant binary vector denoted as r^i would be of size $1 \times 2N$ as two bits are computed for each complex value $f_k^i(u)$ of $f^i(u)$, that is with respect to real and imaginary parts. The binarization process is performed for all the complex vectors present in the matrix $\mathrm{F}(u)$. The resultant binary matrix is represented as $\mathrm{R}^t = [r^1\ r^2...r^n]^T$, where the size of matrix would be $n \times 2N$. Finally, in order to compute the secure fingerprint template, the resultant binary vectors are permuted using a random permutation matrix $\mathrm{P}_{2N \times z}$ as given in Equation 6.4. Here, the value of $z < 2N$, which makes the infinite possibilities to get back the R^t from the final secure fingerprint template.

$$\mathrm{B}_t^f = \mathrm{R}_{n\times 2N}^t \mathrm{P}_{2N\times z}, \text{ where } z < 2N \tag{6.4}$$

In Equation 6.4, B_t^f is the final secure fingerprint template, which is a non-invertible template and it is infeasible to get back the original information of minutiae points from this secure fingerprint template. All these steps are concisely incorporated in Algorithm 6.1. The obtained secure fingerprint template is finally stored in the database for authentication purposes.

6.1.4 Computation of similarity between secure templates

We make use of bit-error computed between binary vectors to measure the similarity between the two secure fingerprint templates. Since the bit-error computation happens in the transformed domain, it makes the proposed technique completely secure. Let a query template for a fingerprint having m minutiae points and corresponding to them m binary vectors, be represented as B_q^f. Further, let a template stored in the database for a fingerprint having n minutia points and corresponding to them n binary vectors be represented as B_t^f. Then, the similarity between a query and a stored template (from the database) is given by computing the bit-error between each binary vector b_q^i of the query template and all the binary vectors $(b_t^1, b_t^2, ..., b_t^n)$ of the stored template. The final similarity score, $score$, is computed as follows.

$$score = z - \min_{b_q^k \in \mathrm{B}_q^f} \left\{ \min_{b_t^i \in \mathrm{B}_t^f} \{BitErr(b_q^k, b_t^i)\} \right\} \tag{6.5}$$

where, the values of i and k are given as $1 \leq i \leq n$ and $1 \leq k \leq m$, respectively. Here, the $BitErr(b_q^k, b_t^i)$ represents the bit-error between the k^{th} binary vector of query template and i^{th} binary vector of the stored template. Therefore, if the value of $score$ is high for

Algorithm 6.1 Computation of secure fingerprint template

Input: minutiae, $\mathrm{M} = \{(x_i, y_i, \theta_i) : 1 \leq i \leq n\}$ pair-polar structure, PP $= \{p_i : 1 \leq i \leq n\}$ and seed key s
Output: secure fingerprint template, B_t^f
Initialize: $G_d = \left\lceil \frac{d_{max}}{g_d} \right\rceil$; $G_\alpha = \left\lceil \frac{\alpha_{max}}{g_\alpha} \right\rceil$; $G_\beta = \left\lceil \frac{\beta_{max}}{g_\beta} \right\rceil$; $Grid =$ zeros$(g_d, g_\alpha, g_\beta, n)$; $N = (g_d g_\alpha g_\beta)$
/*zeros(r, c, h, n) gives the matrix of size $r \times c \times h \times n$ */
for $i \leftarrow \{1, n\}$ **do**
    $j \leftarrow 1$
    while $j \leq n$ **do**
        if $j \neq i$ **then**
            $x_d^j = \lceil \frac{d_{ij}}{G_d} \rceil$, $y_\alpha^j = \lceil \frac{\alpha_{ij}}{G_\alpha} \rceil$, $z_\beta^j = \lceil \frac{\beta_{ij}}{G_\beta} \rceil$
            $Grid(x_d^j, y_\alpha^j, z_\beta^j, i) = 1$
        end if
        $j \leftarrow j + 1$
    end while
end for
/* Sequential unfolding */
$\mathrm{B}_{n \times N}^t = [b^1\ b^2 ... b^n]^T \leftarrow Grid_{g_d \times g_\alpha \times g_\beta \times n}$
$\mathrm{R}^t = Null$
for $i \leftarrow \{1, n\}$ **do**
    $f^i(u) = \sum_{k=0}^{N-1} b_k^i e^{-j2\pi uk/N}$, $u = 0, 1, .., N-1$
    /* $\{f_k^i(u) = real(f_k^i(u)) + j\ imag(f_k^i(u))\}$ */
    $r^i = Null$
    for $k \leftarrow \{1, N\}$ **do**
        if $real(f_k^i(u)) > 0$ **then** $r_{k_1}^i = 1$
        else $r_{k_1}^i = 0$
        end if
        if $imag(f_k^i(u)) > 0$ **then** $r_{k_2}^i = 1$
        else $r_{k_2}^i = 0$
        end if
        $r^i = \left[r^i\ r_{k_1}^i\ r_{k_2}^i\right]$
    end for
    $\mathrm{R}^t = [\mathrm{R}^t\ r^i]^T$
end for
$\mathrm{B}_t^f \leftarrow \mathrm{R}_{n \times 2N}^t \mathrm{P}_{2N \times z}$ /*$z < 2N$ and P, random permutation matrix computed by using seed as s */

the two secure templates being compared, it represents a high similarity between them else represents a low similarity.

6.2 Experimental Analysis

The proposed technique has been validated on four publicly available FVC databases, $viz.$, FVC2002 DB1, FVC2002 DB2, FVC2004 DB1, and FVC2004 DB2. A brief description of these databases has been provided in Section 1.4. The proposed technique has been analyzed in terms of recognition performance, revocability, diversity, and security. A detailed description of the analysis is given below.

6.2.1 Recognition Performance

In order to evaluate the recognition performance of the proposed technique, FAR, FRR, GAR, and EER have been used as the performance measures. Further, standard 1-vs-1 and FVC verification protocols have been used to compute the different performance measures. The details of the performance metrics and evaluation protocols are provided in Sections 1.2.4 and 1.4, respectively. Further, the verification is performed under two different attack scenarios, which are plain-key attack scenario (or different key scenario where different seed s is assigned to each subject) and stolen-key attack scenario (or same key scenario where same seed s is assigned to all the subjects).

The obtained EER value for the proposed technique is found to be 0% for all the databases in the case of a plain-key attack scenario (it is the best-case scenario) as depicted in Tables 6.1 and 6.2. Further, the proposed technique has performed much superior than the existing techniques in the case of stolen-key attack scenario (which is the worst-case scenario) as well. The percentage EER values obtained in the case of stolen-key attack scenario have been incorporated in Tables 6.1 and 6.2 for the proposed technique for all the databases. As depicted in Tables 6.1 and 6.2, the performance of the proposed technique is superior compared to the existing techniques under the 1-vs-1, and FVC protocol except for [76]. However, the technique in [76] does not satisfy the revocability property, whereas

Table 6.1: Percentage EER values under the 1-vs-1 protocol

Various techniques	**FVC2002**		**FVC2004**	
	DB1	**DB2**	**DB1**	**DB2**
Jin et al. [77]	5.19	5.65	16.35	8.66
Ferrara et al. [76]	0	0.37	-	-
Yang et al. [81]	5.93	4	-	-
Yang et al. [47]	3.38	0.59	-	14.88
Jin et al. [79]	4.36	1.77	24.71	21.82
Li et al. [50]	0.83	0	-	14.10
Sandhya et al. [84]	3.96	2.98	12.17	13.29
Wang and Hu [83]	3	2	-	-
Sandhya and Prasad [86]	2.19	1.6	11.89	12.71
Ali et al. [97]	2	1	-	-
Yang et al. [100]	-	1	-	10
Trivedi et al. [102]	1.2	2.1	-	-
Ali et al. [98]	1.63	1	-	-
Yang et al. [105]	1	2	-	11
Lahmidi et al. [104]	3.09	1.83	-	-
Proposed technique (stolen-key)	**0.71**	**0.97**	**4.28**	**6.25**
Proposed technique (plain-key)	**0**	**0**	**0**	**0**

Note: "-" denotes non-availability of data

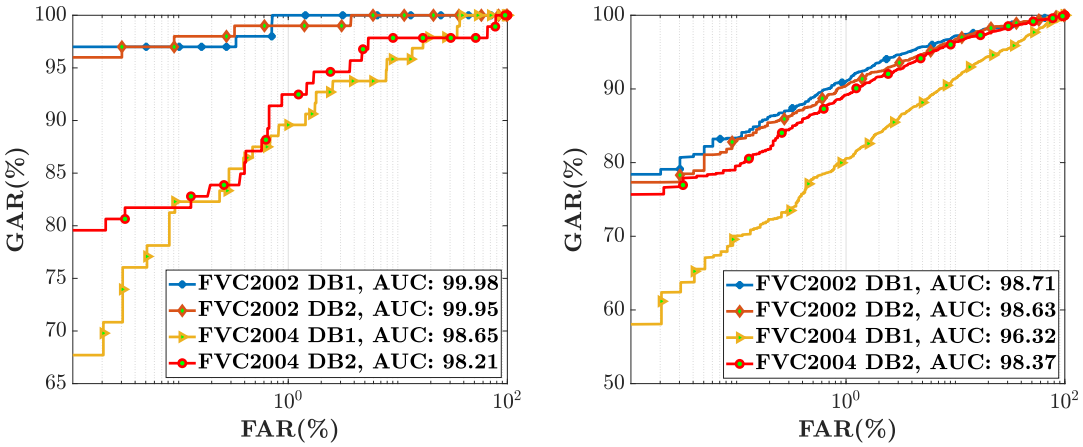
the proposed technique presents the generation of entirely revocable user templates. Moreover, in the FVC protocol, the performance of the proposed technique is inferior compared to existing techniques such as [50, 73] for a single database FVC2002 DB2 as depicted in Table 6.2. Nonetheless, the average EER(%) values of the proposed technique, $i.e.$, 5.0 and 4.8, are superior to the average EER(%) values of the existing approaches [50, 73], $i.e.$, 6.5 and 5.4, respectively. Also, the existing technique [83] has performed slightly better than the proposed technique under the FVC protocol. However, the template computed in the proposed technique is in the binary format and lighter in size. In addition, the approach in [83] has not been tested on challenging fingerprint databases, namely FVC2004 DB1 and FVC2004 DB2, whereas we have evaluated the proposed technique for these challenging databases and obtained results are superior as compared to the existing techniques as shown in Table 6.2.

Table 6.2: Percentage EER values under the FVC protocol

Various techniques	**FVC2002**		**FVC2004**	
	DB1	**DB2**	**DB1**	**DB2**
Ahn et al. [73]	7.18	3.61	-	-
Ferrara et al. [76]	3.33	1.76	-	-
Wang and Hu [83]	4	3	-	-
Li and Hu [50]	5	3.37	-	11.13
Yang et al. [47]	11.84	10.38	-	20.61
Proposed technique (stolen-key)	**4.48**	**5.17**	**9.12**	**5.37**
Proposed technique (plain-key)	**0**	**0**	**0**	**0**

Note: "-" denotes non-availability of data

The receiver operating characteristics (ROC) plots have been analyzed to further check the effectiveness of the proposed technique in terms of the area under the curve (AUC). Ideally, the percentage value of AUC ranges between 0 and 100, where the value near to 100 represents the high efficacy of the designed system. As desired, the values of AUC(%) are near to 100 for the proposed technique under the 1-vs-1 and FVC protocols, as shown in Figure 6.3(a) and Figure 6.3(b), respectively, for all the databases. In addition to this, histograms of genuine and imposter score distributions are drawn in order to depict the significant difference between them. It is clearly evident from Figure 6.4 that the genuine score distribution is very distant from the imposter distribution in both the cases of plain-key attack (PK) and stolen-key attack (SK) scenarios. We have also incorporated the statistical analysis to depict the segregation of genuine and imposter score distributions by means of the Kolmogorov-Smirnov test (KS-test) [23] and student's t-test [24]. In general, the resultant value of the KS-test comes between 0 and 1, where a higher value depicts better segregation of the two input distributions ($i.e.$, genuine and imposter score distributions in our case). The computed values of the KS-test for the proposed technique are found to be close to 1 for all the databases, as shown in Table 6.3. Further, the two-sample unpaired t-test is being performed under the 5% significance level. In the t-test, if the value of $|t - stat|$ is greater than the value of $t - critical$, then the given input distributions are considered well-



(a) 1-vs-1 protocol (b) FVC protocol

Figure 6.3: ROC plots of the proposed technique for different fingerprint databases with AUC (% value) under the stolen-key attack scenario and both the verification protocols.

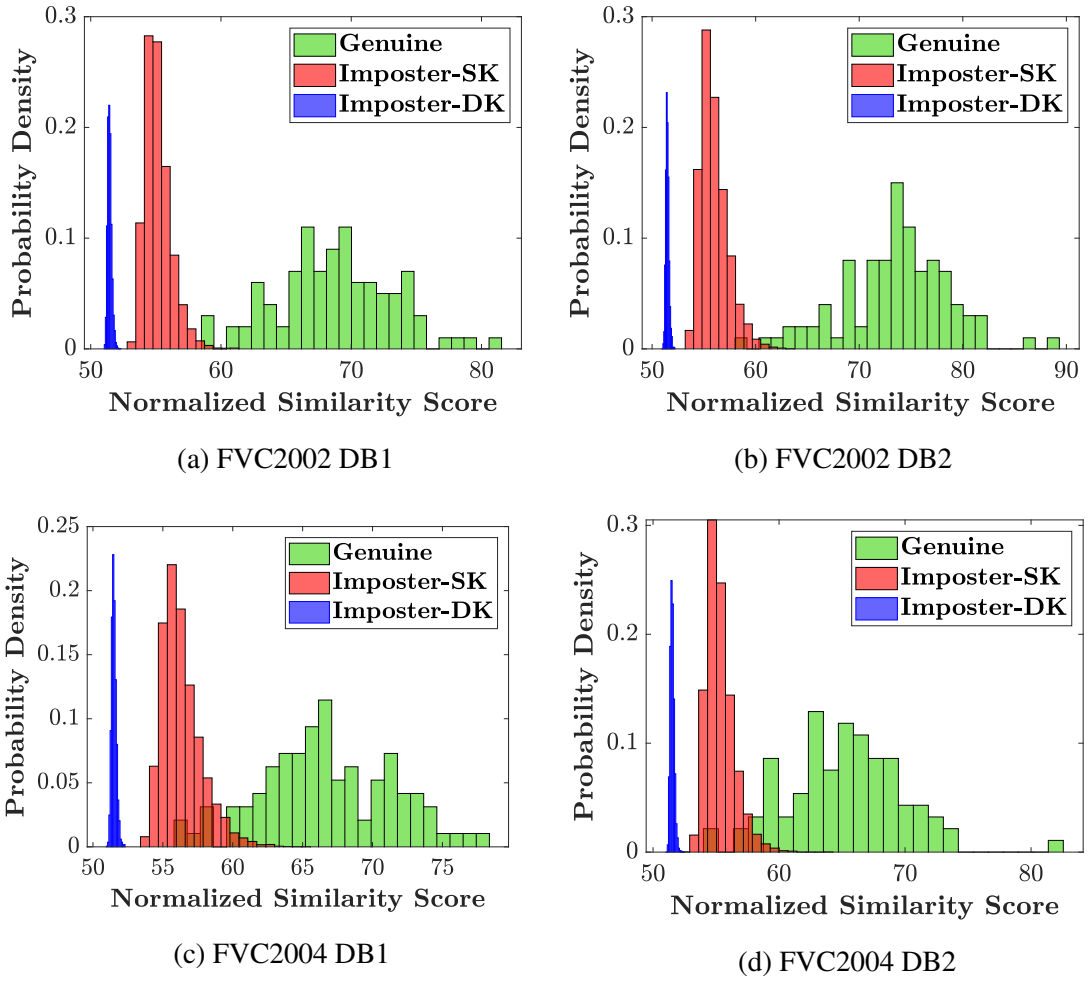
Table 6.3: Comparison of the values generated in KS-test

Various techniques	**FVC2002**		**FVC2004**	
	DB1	**DB2**	**DB1**	**DB2**
Moujahdi et al. [91]	0.78	-	-	-
Ali et al. [97]	0.97	0.98	-	-
Sandhya et al. [84]	0.92	0.94	-	-
Ali et al. [98]	0.98	0.98	-	-
Sandhya and Prasad [86]	0.96	0.97	0.82	0.73
Proposed Technique (stolen-key)	**0.99**	**0.99**	**0.91**	**0.92**

Table 6.4: Results of t-test for all the databases, where "t_s" and "t_c" represent $|t - stat|$ and $t - critical$ values, respectively

Databases	$\|t_s\|$	t_c	$\|t_s\| > t_c$
FVC2002 DB1	30.48	1.9842	True
FVC2002 DB2	33.49	1.9842	True
FVC2004 DB1	21.68	1.9852	True
FVC2004 DB2	20.44	1.9860	True

separated from each other. The t-test results of all the databases for the proposed technique are shown in Table 6.4, where the aforementioned criterion of well-separation is clearly followed. In summary, all the above analyses strongly demonstrate the effectiveness of the proposed technique in terms of the recognition performance.



(a) FVC2002 DB1

(b) FVC2002 DB2

(c) FVC2004 DB1

(d) FVC2004 DB2

Figure 6.4: Distribution of genuine, imposter-SK (stolen-key), and imposter-DK (different-key or plain-key) scores for different databases in the proposed technique.

6.2.2 Revocability

Any template protection technique is called revocable if it allows replacing the compromised template in the database with an entirely new secure template. The new secure template is generated by means of the same biometric data which is used to compute the compromised template with a different transformation key. To show the revocability of the proposed technique, revoked template attacks (Type-I and Type-II attacks) [21], have been employed. In the case of Type-I attack, an attempt to access a biometric system is carried out using a compromised template where at the same time, an entirely new template is ob-

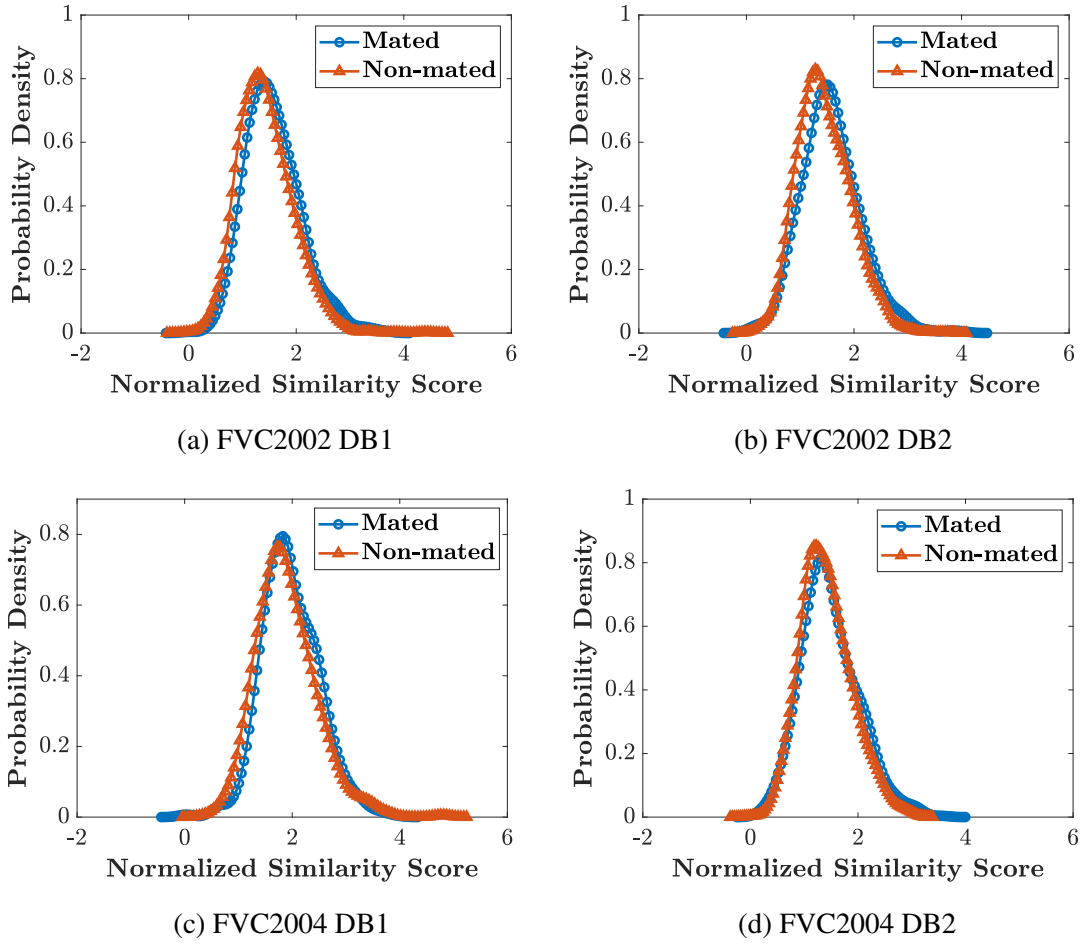
Table 6.5: Percentage values of successful revoked template attacks on different databases for the proposed technique

Revoked template attacks	**FVC2002**		**FVC2004**	
	DB1	**DB2**	**DB1**	**DB2**
Type-I attack	0.0	0.0	0.0	0.0
Type-II attack	0.0	0.0	0.0	0.0

tained using the same fingerprint image, and a different key is replaced in the database after the attack. In contrast, the replaced new template is constructed using a different fingerprint sample of the same subject and a new key in the case of Type-II attack. Ideally, a biometric system should not be accessible by any intruder using the compromised template if the new template has been stored in the database after the attack. This is indeed true for the proposed technique and can be seen from the values of Table 6.5. It is evident from the results that not even a single compromised template has been accepted by the system as a genuine template while performing the Type-I and Type-II attacks. This shows the highly revocable nature of the secure fingerprint template generated by the proposed technique.

6.2.3 Diversity

It is one of the crucial properties for any fingerprint template protection technique in which the secure templates generated from the same fingerprint should be unlinkable from each other. The diversity in secure templates prevents the correlation attack scenario considering that if an attacker gets the multiple secure templates of a user from different fingerprint systems (where a user is enrolled), it should not be possible to gather any information about the original biometric data by correlating the various templates of the user. Further, to show the diversity of the secure fingerprint templates, a general framework discussed in [6] has been utilized. According to this framework, the score distributions of mated and non-mated pairs of templates should overlap to have the diversity among the secure templates gener-



(a) FVC2002 DB1

(b) FVC2002 DB2

(c) FVC2004 DB1

(d) FVC2004 DB2

Figure 6.5: Representation of unlinkability of the proposed technique using the mated and non-mated score distributions drawn for different databases.

ated by a template protection technique. Mated scores are computed between the secure templates that are generated using the same fingerprint sample of a subject and different keys, whereas non-mated scores are computed between the secure templates that are generated for samples of different subjects and different keys. The mated and non-mated score distributions for the proposed technique for all the databases are shown in Figure 6.5. It is evidently shown in the figure that the mated and non-mated score distributions are significantly overlapping for all the databases. In addition, a global measure called $\mathrm{D}_{\leftrightarrow}^{sys}$ has been discussed in the framework proposed in [6]. The value of this measure ranges between 0 and 1, where a value close to 0 represents high unlinkability in the templates. The values of $\mathrm{D}_{\leftrightarrow}^{sys}$

obtained for different databases for the proposed technique are found to be approximately equal to 0.001, which is very close to 0. Thus, both analyses confirm the diverse nature of the secure templates produced by the proposed technique.

6.2.4 Security

This property guarantees that a secure template produced by a technique is safe in terms of non-invertibility and it has resilience against various attack scenarios. The secure template generated using the proposed technique is entirely non-invertible, and it is impossible for an adversary to conduct brute force and cross-match attacks. The analysis in terms of the non-invertibility and mentioned attack scenarios is as follows.

6.2.4.1 Non-invertibility

The secure template obtained in the proposed technique is in binary format, and if it is compromised, it is impossible to reconstruct the original fingerprint image even though the value of the parameter s is accessible. In order to verify it, let us assume that an adversary knows the compromised template B_t^f and the seed s. In that case, the adversary would further require $\mathrm{B}_{n\times N}^t$ to reconstruct the template. We know that the final secure template B_t^f is generated by following the binarization of $\mathrm{F}(u)$ ($N-$point DFT of $\mathrm{B}_{n\times N}^t$ with respect to each row), as mentioned in Section 6.1.3, considering the real and imaginary parts of each complex vector $f^i(u)$. Due to such a binarization scheme, attempting to recover the DFT would result in an endless number of options. As a result, even if an attacker has the compromised template and the seed s, it is infeasible to recover the DFT matrix $\mathrm{F}(u)$ and therefore, $\mathrm{B}_{n\times N}^t$. This clearly shows that the secure template obtained by the proposed technique is robust against the reconstruction of original fingerprint data from it and thus exhibits the non-invertible characteristic.

6.2.4.2 Brute force attack

In this attack scenario, an attacker explores all possibilities for recovering the original minutiae information and reconstructing the fingerprint image from the secure template or gaining unauthorized access to the biometric system by guessing the final template. It is clear from the discussion of non-invertibility that recovering original minutiae information is infeasible because of the endless possibilities to get back the DFT from the secure template. Moreover, trying to get unauthorized access is also infeasible in the proposed technique. The quantitative analysis to support this statement is as follows. Suppose the size of a 3D grid is given as $8 \times 16 \times 16$ where $g_d = 8$, $g_\alpha = 16$, and $g_\beta = 16$, then the length of the binary string after sequentially unfolding the 3D grid would be $N = 2048$. Now, as discussed in Section 6.1.3, each binary string of the final secure template would be of size z, where $z < 2N$. Thus, if the value of $z = 2N - 4$, then the total number of possibilities to guess a binary string would be 2^{2N-4}, $i.e.$, 2^{4092}. Therefore, the probability of correctly predicting a binary string or n binary strings would be highly negligible (≈ 0). Therefore, it clearly shows the robustness of the proposed technique against the brute force attack.

6.2.4.3 Cross-match attack

In the case of a cross-match attack, the attacker may attempt to correlate numerous protected templates obtained from various fingerprint systems (where a user is enrolled) in order to find a pattern associated with the original fingerprint data. However, as discussed in Section 6.2.3, the secure fingerprint templates generated by the proposed technique are unlinkable from one another and do not expose any information about the original fingerprint data. Furthermore, a secure template is a collection of binary vectors produced by the two phases of binarization and hence does not contain any direct information about the orig-

Table 6.6: Comparison between proposed techniques in terms of EER(%) for different fingerprint databases considering 1-vs-1 protocol

Proposed Technique (PT)	**FVC2002**		**FVC2004**
	DB1	**DB2**	**DB1**
PT-1 [Chapter 3]	4.00	3.10	11.95
PT-2 [Chapter 4]	1.25	1.08	8.95
PT-3 [Chapter 5]	1.0	1.0	8.90
PT-4 [Chapter 6]	0.71	0.97	4.28

inal minutiae of the fingerprint image. This clearly shows that acquiring any fruitful details of the original fingerprint template by correlating multiple secure templates is infeasible; hence, the proposed technique possesses resilience against the cross-match attack.

In summary, a non-invertible and alignment-free fingerprint template protection technique based on the pair-polar structures of minutiae points and DFT has been proposed in this chapter. In the technique, an intermediate binary fingerprint template is constructed by mapping the pair-polar coordinates into a 3D grid. The computed binary template is then secured by performing the DFT followed by a second-level binarization process. The obtained output is subsequently used to compute the final secure user template by permuting it using a user-specific seed s. Further, the proposed technique has been evaluated on four different publicly available fingerprint databases by considering the four essential properties. Finally, the results are compared with the existing techniques, and the analyses have depicted the robustness and effectiveness of the proposed technique.

6.3 Comparison of the Proposed Techniques

In this section, we have included a comparison of all four proposed techniques, which are discussed in this thesis. The comparison has been made considering two factors, first is the performance in terms of the EER(%) for the common fingerprint databases used for the experimentation in all four techniques. The comparison of the proposed technique with re-

Table 6.7: Comparison between proposed techniques in terms of multiple properties

Proposed Technique (PT)	**Revocability**	**Diversity**	**Security**	**Requirement of fingerprint alignment**
PT-1 [Chapter 3]	Moderate	Moderate	High	Required
PT-2 [Chapter 4]	High	High	High	Required
PT-3 [Chapter 5]	High	High	High	Alignment-free
PT-4 [Chapter 6]	High	High	High	Alignment-free

spect to performance is shown in Table 6.6. In the second comparison, other properties, such as revocability, diversity, security, the requirement of fingerprint alignment for fingerprint matching, and implementation details are considered. All four proposed techniques have been implemented using Matlab(R) R2019a, and the experimentation has been performed on a machine having Intel(R) Core(TM) i5-7500 processor with 8GB RAM. Further, Table 6.7 depicts the comparison of the proposed techniques with respect to other remaining properties.

Chapter 7

Conclusion and Future Scope of the Work

Fingerprint-based authentication systems are extensively used in numerous applications to secure various resources and sensitive data. In these systems, minutiae are the mainly used features to generate the user template that would be stored in the database for authentication purposes. These systems have shown tremendous benefits over the traditional password and token-based authentication systems. However, the security of the stored user template is essential in fingerprint-based authentication systems due to the immutable nature of the fingerprint information of a user. In a password or token-based system, if an attack happens and the data is compromised, then the password or the token can be changed to prevent unauthorized access. In contrast, in a fingerprint-based authentication system, the immutable nature of the fingerprint data leads to the permanent identity loss of the user if an attack happens on the database. Moreover, it has been discussed in the literature that the reconstruction of the fingerprint image is possible from the compromised fingerprint template that contains the original minutiae information. Therefore, in order to secure the fingerprint template, fingerprint template protection techniques have been discussed in the literature. The key principle of these techniques is that instead of storing the original fin-

gerprint template, a secure transformed/encrypted fingerprint template should be stored in the database. This ensures that even if an adversary attains the stored template, it is infeasible to reconstruct fingerprint images or get original minutiae information from the secure template. By considering template protection as one of the major security and privacy concerns of a fingerprint-based authentication system, various fingerprint template protection techniques have been proposed in this thesis. A brief summary of the contributions of the thesis is provided below.

In Chapter 3, a technique which is based on fuzzy vault has been proposed to protect the fingerprint template of a user. To enhance the performance, a mechanism for selecting strong minutiae points based on relative distance minutiae matching has also been proposed in this work. Further, in a minutiae-based fingerprint authentication system, the alignment of fingerprint templates is one of the crucial tasks for the matching of fingerprints. In this work, a new technique has been proposed to align the minutiae points of a gallery and probe fingerprints by exploiting PCA and thinned version of the fingerprint image. In order to evaluate the proposed technique, three publicly available databases, $viz.$, FVC2002 DB1, FVC2002 DB2, and FVC2004 DB1 have been utilized. Obtained results have been analyzed in terms of performance and security. The performance of the proposed technique has also been compared with that of the existing techniques using metrics such as GAR, FAR, and EER. The comparison shows the superiority of the proposed technique over existing techniques. The security analysis has been performed considering three different possible attack scenarios, and it shows that the proposed technique is secure to protect the fingerprint template from these attacks. Overall, the analysis of the technique based on its performance and resilience towards various attacks have shown the robustness and effectiveness of the proposed technique.

Although the technique proposed in Chapter 3 using a fuzzy vault scheme is secure, the

recognition performance suffers. Moreover, the templates are not diverse in this presented technique. Therefore, in order to deal with these limitations, Chapter 4 has proposed a technique based on a non-invertible transformation to protect fingerprint templates. The transformation has been performed on the locations of the minutiae points in a fingerprint image by utilizing the values of a user keyset. The obtained transformed locations are stored in the database after performing a PCA-based alignment. The transformed locations of minutiae points are computed in such a way that it is computationally infeasible to compute the original location of minutiae points from the stored template even though an intruder may have the user keyset values. The information of orientation at each minutia point is also not stored in the database in this technique, which further makes the reconstruction of fingerprint images an infeasible task. At the time of verification, the probe template has been computed using the same procedure followed during the enrollment. Thus, in the proposed technique, matching is performed between the transformed template of minutiae points instead of the original minutiae locations. We have used FVC2000 DB2, FVC2002 DB1, FVC2002 DB2, FVC2002 DB3, FVC2002 DB4, FVC2004 DB1, and FVC2004 DB2 fingerprint databases to evaluate the performance of the proposed technique. Further, we have used EER as a metric for the evaluation where the Low EER values obtained for the proposed technique as compared to other existing techniques show the superiority of the technique. The results have been analyzed considering four main aspects *viz.* revocability, diversity, security, and performance. Statistical analysis of genuine and imposter score distributions has also been performed to show the well-separation of genuine and imposter scores. The overall analysis of the results in terms of the four essential properties shows the robustness and effectiveness of the proposed technique.

In Chapter 5, an alignment-free cancelable user template protection technique for fingerprint biometrics has been proposed. This eliminates the requirement of explicit alignment

of fingerprint images and dependency on singular point present in the approach discussed in Chapter 4. The technique relies on the pair-polar representation of minutiae points and many-to-one mapping to construct a secure binary user template. In addition to many-to-one mapping, the pair-polar coordinates are transformed by using a non-invertible transformation and a user-defined keyset to make the user template more secure. This enables the revocability and the unlinkability in the computed user templates and enhances the security of the user templates against different attacks without compromising their performances in differentiating the two individuals. The proposed technique has been evaluated on six publicly available fingerprint databases of FVC2002 and FVC2004. The obtained results on these databases have been analyzed with respect to recognition performance, revocability, diversity, and security. The results have also been compared with that of the existing techniques and have been found to be superior in terms of the EER. The overall comparison concerning the performance and the ability to combat different security and privacy issues of users' fingerprint data clearly shows the superiority of the proposed technique.

In Chapter 6, instead of transforming the pair-polar structures of the minutiae, they are directly used to compute the binary strings with respect to each reference minutia. Consequently, the overall performance is significantly increased in both 1-vs-1 and FVC protocol as compared to the proposed approaches discussed in the previous chapters. Further, these binary strings are secured by using the DFT followed by a second-level binarization process. The obtained output is subsequently used to compute the final secure user template by permuting it using a user-specific seed s. Finally, the obtained secure template is stored in the database for authentication purposes. The proposed technique has been evaluated on four different publicly available fingerprint databases, $viz.$, FVC2002 DB1, FVC2002 DB2, FVC2004 DB1, and FVC2004 DB2, by considering the four essential properties, such as revocability, diversity, security, and performance. The results are compared with the existing

techniques, and the analyses have depicted the robustness and effectiveness of the proposed technique.

7.1 Future Scope of the Work

This thesis has presented various approaches to protect the fingerprint user template. These approaches deal with various security and privacy issue of the fingerprint authentication system and provide a robust and effective solution. Further, in the future, there are various possibilities to work on as presented below.

- **Hybrid fingerprint template protection:** In the hybrid template protection technique, the functionalities of different fingerprint template protection techniques are combined to form a system such as combining biometric cryptosystems and cancelable biometrics. This designed system provides the advantages of both types of template protection techniques. Hence, the techniques proposed in this thesis can be further extended to develop a hybrid fingerprint template protection technique, especially the technique where the final template is defined in the form of a binary string.

- **Multi-modal biometric system:** In the multi-modal biometric system, the secure template is generated by fusing the features of different biometric modalities or traits. The work presented in this thesis can be extended to develop a multi-modal biometric system, where fingerprint biometric trait is combined with other traits, $e.g.$, finger vein, face, iris, and ear. Here, the fusion of fingerprint with the finger vein is most appropriate as the acquisition of both of these modalities can be performed using a single device at a time.

- **3D fingerprint:** In the thesis, the proposed techniques work on the fingerprint images that are captured using 2D optical and capacitive sensors. However, the presented

techniques can be further explored for a contact-less 3D fingerprint-based authentication system.

- **Sensor interoperability:** Currently, the proposed techniques, especially techniques presented in Chapters 3 and 4, may suffer in the cases where acquisition sensors for enrollment and verification are different. Therefore, the development of the fingerprint template protection technique can be explored in the case where different acquisition sensors are used.

Bibliography

[1] Fingerprint Verification Competition 2002 Database, last accessed: July 2020. [Online]. Available: http://bias.csr.unibo.it/fvc2002/default.asp

[2] CASIA Iris Image Database Version 1.0, last accessed: July 2021. [Online]. Available: http://english.ia.cas.cn/db/201610/t20161026_169399.html

[3] FEI Face Database, last accessed: July 2021. [Online]. Available: https://fei.edu.br/~cet/facedatabase.html

[4] A. Kumar and C. Wu, "Automated human identification using ear imaging," *Pattern Recognition*, vol. 45, no. 3, pp. 956–968, 2012.

[5] 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.

[6] M. Gomez-Barrero, J. Galbally, C. Rathgeb, and C. Busch, "General framework to evaluate unlinkability in biometric template protection systems," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 6, pp. 1406–1420, 2018.

[7] K. Simoens, B. Yang, X. Zhou, F. Beato, C. Busch, E. M. Newton, and B. Preneel, "Criteria towards metrics for benchmarking template protection algorithms," in *2012 5th IAPR Int'l Conference on Biometrics (ICB)*, 2012, pp. 498–505.

[8] A. Juels and M. Wattenberg, "A fuzzy commitment scheme," in *Proc. of Computer and Communications Security, Singapore*, 1999, pp. 28–36.

[9] A. Juels and M. Sudan, "A fuzzy vault scheme," in *Proc. of IEEE Int'l Symposium on Information Theory*, 2002, p. 408.

[10] H. Z. Ur Rehman and S. Lee, "Automatic image alignment using principal component analysis," *IEEE Access*, vol. 6, pp. 72 063–72 072, 2018.

[11] 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, Jan 2004.

[12] A. K. Jain, A. A. Ross, and K. Nandakumar, *Introduction to Biometrics*. Springer Publishing Company, Incorporated, 2011.

[13] A. A. Ross, J. Shah, and A. K. Jain, "Toward reconstructing fingerprints from minutiae points," in *Proc. of SPIE Conf. on Biometric Technology for Human Identification*, 2005, pp. 68–80.

[14] R. Cappelli, D. Maio, A. Lumini, and D. Maltoni, "Fingerprint image reconstruction from standard templates," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 29, no. 9, pp. 1489–1503, Sep. 2007.

[15] F. Chen, J. Zhou, and C. Yang, "Reconstructing Orientation Field From Fingerprint Minutiae to Improve Minutiae-Matching Accuracy," *IEEE Transactions on Image Processing*, vol. 18, no. 7, pp. 1665–1670, 2009.

[16] J. Feng and A. K. Jain, "Fingerprint Reconstruction: From Minutiae to Phase," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 33, no. 2, pp. 209–223, 2011.

[17] A. Ross, J. Shah, and A. K.Jain, "From template to image: Reconstructing fingerprints from minutiae points," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 29, no. 4, pp. 544–560, 2007.

[18] A. Teoh and K. Jaihie, "Secure biometric template protection in fuzzy commitment scheme," *IEICE Electronics Express*, vol. 4, no. 23, pp. 724–730, 2007.

[19] 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, April 2007.

[20] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, *Handbook of Fingerprint Recognition*, 2nd ed. Springer Publishing Company, Incorporated, 2009.

[21] M. Ferrara, D. Maltoni, and R. Cappelli, "A two-factor protection scheme for MCC fingerprint templates," in *Proc. of Int'l Conference of the Biometrics Special Interest Group (BIOSIG)*, 2014, pp. 1–8.

[22] R. Dwivedi and S. Dey, "Score-level fusion for cancelable multi-biometric verification," *Patt. Recogn. Letters*, vol. 126, pp. 58–67, 2018.

[23] R. Wilcox, "Kolmogoro-Smirnov Test," in *Encyclopedia of Biostatistics*. John Wiley & Sons, Ltd, 2005.

[24] D. W. Zimmerman, "A Note on Interpretation of the Paired-Samples t Test," *Journal of Educational and Behavioral Statistics*, vol. 22, no. 3, pp. 349–360, 1997.

[25] D. Maio, D. Maltoni, R. Cappelli, J. L. Wayman, and A. K. Jain, "FVC2000: fingerprint verification competition," *IEEE Trans. on Pattern Analysis and Machine Intelligence*, vol. 24, no. 3, pp. 402–412, 2002.

[26] Fingerprint Verification Competition 2004 Database, last accessed: September 2020. [Online]. Available: http://bias.csr.unibo.it/fvc2004/databases.asp

[27] Neurotechnology, Verifinger SDK (Demo), last accessed: September 2020. [Online]. Available: http://www.neurotechnology.com

[28] E. Zhu, X. Guo, and J. Yin, "Walking to singular points of fingerprints," *Patt. Recogn.*, vol. 56, pp. 116 – 128, 2016.

[29] H. K. Lam, Z. Hou, W. Y. Yau, T. P. Chen, and J. Li, "A systematic topological method for fingerprint singular point detection," in *Proc. of Int'l Conference on Control, Automation, Robotics and Vision*, 2008, pp. 967–972.

[30] 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, Dec 2007.

[31] L. Qiming, G. Muchuan, and C. Ee-Chien, "Fuzzy extractors for asymmetric biometric representations," in *Proc. of IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops*, 2008, pp. 1–6.

[32] A. K. Jain, K. Nandakumar, and A. Nagar, "Biometric template security," *EURASIP J. Adv. Signal Process*, vol. 2008, Jan. 2008.

[33] A. K. Jain, S. Prabhakar, L. Hong, and S. Pankanti, "Filterbank-based fingerprint matching," *IEEE Transactions on Image Processing*, vol. 9, no. 5, pp. 846–859, 2000.

[34] 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.

[35] K. Nandakumar, "A fingerprint cryptosystem based on minutiae phase spectrum," in *Proc. of IEEE Int'l Workshop on Information Forensics and Security*, 2010, pp. 1–6.

[36] P. Li, X. Yang, H. Qiao, K. Cao, E. Liu, and J. Tian, "An effective biometric cryptosystem combining fingerprints with error correction codes," *Expert Systems with Applications*, vol. 39, no. 7, pp. 6562 – 6574, 2012.

[37] Y. Sutcu, S. Rane, J. S. Yedidia, S. C. Draper, and A. Vetro, "Feature transformation of biometric templates for secure biometric systems based on error correcting codes," in *Proc. of IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops*, 2008, pp. 1–6.

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

[39] T. Ahonen, A. Hadid, and M. Pietikainen, "Face description with local binary patterns: Application to face recognition," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 28, no. 12, pp. 2037–2041, 2006.

[40] T. Jabid, M. H. Kabir, and O. Chae, "Local directional pattern (LDP) – A robust image descriptor for object recognition," in *Proc. of IEEE Int'l Conference on Advanced Video and Signal Based Surveillance*, 2010, pp. 482–487.

[41] A. Bentahar, A. Meraoumia, H. Bendjenna, S. Chitroub, and A. Zeroual, "Biometric cryptosystem scheme for internet of things using fuzzy commitment principle," in *Proc. of Int'l Conference on Signal, Image, Vision and their Applications (SIVA)*, 2018, pp. 1–6.

[42] S. Barman, H. P. H. Shum, S. Chattopadhyay, and D. Samanta, "A secure authentication protocol for multi-server-based e-healthcare using a fuzzy commitment scheme," *IEEE Access*, vol. 7, pp. 12 557–12 574, 2019.

[43] S. Shi, J. Cui, X.-L. Zhang, Y. Liu, J.-L. Gao, and Y.-J. Wang, "Fingerprint recognition strategies based on a fuzzy commitment for cloud-assisted iot: A minutiae-based sector coding approach," *IEEE Access*, vol. 7, pp. 44 803–44 812, 2019.

[44] U. Uludag and Anil Jain, "Securing fingerprint template: Fuzzy vault with helper data," in *Proc. of Int'l Conference on Computer Vision and Pattern Recognition Workshop (CVPRW'06)*, 2006, pp. 163–163.

[45] K. Nandakumar, A. Nagar, and A. K. Jain, "Hardening fingerprint fuzzy vault using password," in *Proc. of Advances in Biometrics–ICB 2007*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2007, pp. 927–937.

[46] X. Zhou, A. Opel, J. Merkle, U. Korte, and C. Busch, "Enhanced template protection with passwords for fingerprint recognition," *Proc. of Int'l Workshop on Security and Communication Networks (IWSCN)*, pp. 67–74, 2011.

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

[48] F. Benhammadi and K. Beghdad Bey, "Password hardened fuzzy vault for fingerprint authentication system," *Image and Vision Computing*, vol. 32, no. 8, pp. 487–496, 2014.

[49] B. Tams, P. Mihăilescu, and A. Munk, "Security considerations in minutiae-based fuzzy vaults," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 5, pp. 985–998, 2015.

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

[51] M. Neu, U. Korte, and M. Ullmann, "Improvement of fuzzy vault for multiple fingerprints with angles," in *Proc. of Int'l Conference of the Biometrics Special Interest Group (BIOSIG)*, 2016, pp. 1–8.

[52] 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.

[53] K. Bobkowska, K. Nagaty, and M. Przyborski, "Incorporating iris, fingerprint and face biometric for fraud prevention in e-passports using fuzzy vault," *IET Image Processing*, vol. 13, no. 13, pp. 2516–2528, 2019.

[54] C. Vielhauer, R. Steinmetz, and A. Mayerhofer, "Biometric hash based on statistical features of online signatures," in *Proc. of Int'l Conference on Pattern Recognition*, vol. 1, 2002, pp. 123–126.

[55] Y. Dodis, L. Reyzin, and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," in *Proc. of Advances in Cryptology - EUROCRYPT 2004*, C. Cachin and J. L. Camenisch, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2004, pp. 523–540.

[56] X. Boyen, Y. Dodis, J. Katz, R. Ostrovsky, and A. Smith, "Secure remote authentication using biometric data," in *Proc. of Advances in Cryptology – EUROCRYPT 2005*, R. Cramer, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 2005, pp. 147–163.

[57] 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.

[58] A. Arakala, J. Jeffers, and K. J. Horadam, "Fuzzy extractors for minutiae-based fingerprint authentication," in *Proc. of Advances in Biometrics – ICB 2007*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2007, pp. 760–769.

[59] E.-C. Chang and S. Roy, "Robust extraction of secret bits from minutiae," in *Proc. of Advances in Biometrics–ICB 2007*, S.-W. Lee and S. Z. Li, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2007, pp. 750–759.

[60] Y. Sutcu, Q. Li, and N. Memon, "Secure biometric templates from fingerprint-face features," in *Proc. of IEEE Conference on Computer Vision and Pattern Recognition*, 2007, pp. 1–6.

[61] E. A. Verbitskiy, P. Tuyls, C. Obi, B. Schoenmakers, and B. Skoric, "Key extraction from general nondiscrete signals," *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 2, pp. 269–279, 2010.

[62] Y. Tian, Y. Li, B. Sengupta, N. Li, and C. Su, "Leakage-resilient biometric-based remote user authentication with fuzzy extractors," *Theoretical Computer Science*, vol. 814, pp. 223–233, 2020.

[63] T. Connie, A. Teoh, M. Goh, and D. Ngo, "Palmhashing: a novel approach for cancelable biometrics," *Information Processing Letters*, vol. 93, no. 1, pp. 1 – 5, 2005.

[64] A. B. Teoh and D. C. Ngo, "Biophasor: Token supplemented cancellable biometrics," in *Proc. of Int'l Conference on Control, Automation, Robotics and Vision*, Dec 2006, pp. 1–5.

[65] Jin Zhe and A. T. B. Jin, "Fingerprint template protection with minutia vicinity decomposition," in *Proc. of Int'l Joint Conference on Biometrics (IJCB)*, Oct 2011, pp. 1–7.

[66] S. Chikkerur, N. K. Ratha, J. H. Connell, and R. M. Bolle, "Generating registration-free cancelable fingerprint templates," in *Proc. of IEEE Second Int'l Conference on Biometrics: Theory, Applications and Systems*, Sep. 2008, pp. 1–6.

[67] H. Yang, X. Jiang, and A. C. Kot, "Generating secure cancelable fingerprint templates using local and global features," in *Proc. of IEEE Int'l Conference on Computer Science and Information Technology*, Aug 2009, pp. 645–649.

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

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

[70] S. Wang and J. Hu, "Alignment-free cancelable fingerprint template design: A densely infinite-to-one mapping (DITOM) approach," *Patt. Recogn.*, vol. 45, no. 12, pp. 4129 – 4137, 2012.

[71] T. E. Boult, W. J. Scheirer, and R. Woodworth, "Revocable fingerprint biotokens: Accuracy and security analysis," in *Proc. of IEEE Computer Vision and Pattern Recognition*, 2007, pp. 1–8.

[72] S. Tulyakov, F. Farooq, P. Mansukhani, and V. Govindaraju, "Symmetric hash functions for secure fingerprint biometric systems," *Patt. Recogn. Letters*, vol. 28, no. 16, pp. 2427–2436, 2007.

[73] D. Ahn, S. G. Kong, Y. S. Chung, and K. Y. Moon, "Matching with secure fingerprint templates using non-invertible transform," in *Proc. of Congress on Image and Signal Processing*, vol. 2, 2008, pp. 29–33.

[74] G. Kumar, S. Tulyakov, and V. Govindaraju, "Combination of symmetric hash functions for secure fingerprint matching," in *Proc. of Int'l Conference on Pattern Recognition*, 2010, pp. 890–893.

[75] R. Cappelli, M. Ferrara, and D. Maltoni, "Minutia Cylinder-Code: A New Representation and Matching Technique for Fingerprint Recognition," *IEEE Trans. on Pattern Analysis and Machine Intelligence*, vol. 32, no. 12, pp. 2128–2141, 2010.

[76] M. Ferrara, D. Maltoni, and R. Cappelli, "Noninvertible Minutia Cylinder-Code Representation," *IEEE Trans. on Information Forensics and Security*, vol. 7, no. 6, pp. 1727–1737, 2012.

[77] Z. Jin, A. B. J. Teoh, T. S. Ong, and C. Tee, "Fingerprint template protection with minutiae-based bit-string for security and privacy preserving," *Expert Systems with Applications*, vol. 39, no. 6, pp. 6157 – 6167, 2012.

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

[79] Z. Jin, M. H. Lim, A. B. Jin Teoh, and B. M. Goi, "A non-invertible Randomized Graph-based Hamming Embedding for generating cancelable fingerprint template," *Patt. Recogn. Letters*, vol. 42, pp. 137 – 147, 2014.

[80] M. Sandhya and M. V. N. K. Prasad, "k-Nearest Neighborhood Structure (k-NNS) based alignment-free method for fingerprint template protection," in *Proc. of Int'l Conference on Biometrics*, 2015, pp. 386–393.

[81] W. Yang, J. Hu, S. Wang, and J. Yang, "Cancelable Fingerprint Templates with Delaunay Triangle-Based Local Structures," in *Proc. of Cyberspace Safety and Security*. Springer International Publishing, 2013, pp. 81–91.

[82] Z. Jin, M. H. Lim, A. B. J. Teoh, B. M. Goi, and Y. H. Tay, "Generating Fixed-Length Representation From Minutiae Using Kernel Methods for Fingerprint Authentication," *IEEE Trans. on Systems, Man, and Cybernetics: Systems*, vol. 46, no. 10, pp. 1415–1428, 2016.

[83] S. Wang and J. Hu, "A blind system identification approach to cancelable fingerprint templates," *Patt. Recogn.*, vol. 54, pp. 14 – 22, 2016.

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

[85] J. Khodadoust and A. M. Khodadoust, "Fingerprint indexing based on expanded delaunay triangulation," *Expert Systems with Applications*, vol. 81, pp. 251 – 267, 2017.

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

[87] S. Wang, G. Deng, and J. Hu, "A partial Hadamard transform approach to the design of cancelable fingerprint templates containing binary biometric representations," *Patt. Recogn.*, vol. 61, pp. 447 – 458, 2017.

[88] X. Si, J. Feng, B. Yuan, and J. Zhou, "Dense registration of fingerprints," *Patt. Recogn.*, vol. 63, pp. 87 – 101, 2017.

[89] W. Lee, S. Cho, H. Choi, and J. Kim, "Partial fingerprint matching using minutiae and ridge shape features for small fingerprint scanners," *Expert Systems with Applications*, vol. 87, pp. 183 – 198, 2017.

[90] S. Wang, W. Yang, and J. Hu, "Design of Alignment-Free Cancelable Fingerprint Templates with Zoned Minutia Pairs," *Patt. Recogn.*, vol. 66, pp. 295 – 301, 2017.

[91] C. Moujahdi, G. Bebis, S. Ghouzali, and M. Rziza, "Fingerprint shell: Secure representation of fingerprint template," *Patt. Recogn. Letters*, vol. 45, pp. 189–196, 2014.

[92] A. Jain and M. V. N. K. Prasad, "A novel fingerprint indexing scheme using dynamic clustering," *Journal of Reliable Intelligent Environments*, vol. 2, pp. 159–171.

[93] S. S. Ali and S. Prakash, "Enhanced Fingerprint Shell," in *Proc. of Int'l Conference on Signal Processing and Integrated Networks*, 2015, pp. 801–805.

[94] S. S. Ali and S. Prakash, "Fingerprint Shell Construction with Prominent Minutiae Points," in *Proc. of Annual ACM India Compute Conference*, 2017, pp. 91–98.

[95] S. S. Ali and S. Prakash, "3-Dimensional Secured Fingerprint Shell," *Patt. Recogn. Letters*, vol. 126, pp. 68–77, 2019.

[96] S. S. Ali, G. I. Iyappan, and S. Prakash, "Fingerprint Shell construction with impregnable features," *Journal of Intelligent & Fuzzy Systems*, vol. 36, no. 5, pp. 4091–4104, 2019.

[97] S. S. Ali, G. I. Iyappan, and S. Prakash, "Robust technique for fingerprint template protection," *IET Biometrics*, vol. 7, no. 6, pp. 536–549, 2018.

[98] S. S. Ali, G. I. Iyappan, S. Prakash, P. Consul, and S. Mahyo, "Securing biometric user template using modified minutiae attributes," *Patt. Recogn. Letters*, vol. 129, pp. 263 – 270, 2020.

[99] A. K. Trivedi, D. M. Thounaojam, and S. Pal, "A robust and non-invertible fingerprint template for fingerprint matching system," *Forensic Science International*, vol. 288, pp. 256 – 265, 2018.

[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. S. Ali, G. I. Iyappan, S. Mahyo, and S. Prakash, "Polynomial vault: A secure and robust fingerprint based authentication," *IEEE Trans. on Emerging Topics in Computing*, vol. 9, no. 2, pp. 612–625, 2021.

[102] A. K. Trivedi, D. M. Thounaojam, and S. Pal, "Non-invertible cancellable fingerprint template for fingerprint biometric," *Computers & Security*, vol. 90, p. 101690, 2020.

[103] A. Lahmidi, K. Minaoui, C. Moujahdi, and M. Rziza, "Fingerprint Template Protection Using Irreversible Minutiae Tetrahedrons," *The Computer Journal*, 08 2021.

[104] A. Lahmidi, C. Moujahdi, K. Minaoui, and M. Rziza, "On the methodology of fingerprint template protection schemes conception : meditations on the reliability," *EURASIP Journal on Information Security*, vol. 2022, pp. 1–13, 2022.

[105] W. Yang, S. Wang, M. Shahzad, and W. Zhou, "A cancelable biometric authentication system based on feature-adaptive random projection," *Journal of Information Security and Applications*, vol. 58, p. 102704, 2021.

[106] A. Bedari, S. Wang, and J. Yang, "A two-stage feature transformation-based fingerprint authentication system for privacy protection in IoT," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 4, pp. 2745–2752, 2022.

[107] A. Nagar, K. Nandakumar, and A. K. Jain, "Securing fingerprint template: Fuzzy vault with minutiae descriptors," in *Proc. of Int'l Conference on Pattern Recognition*, 2008, pp. 1–4.

[108] 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.

[109] O. Ouda, K. Nandakumar, and A. Ross, "Cancelable biometrics vault: A secure key-binding biometric cryptosystem based on chaffing and winnowing," in *Proc. of Int'l Conference on Pattern Recognition*, 2021, pp. 8735–8742.

[110] M. Upmanyu, A. M. Namboodiri, K. Srinathan, and C. V. Jawahar, "Efficient biometric verification in encrypted domain," in *Proc. of Advances in Biometrics–ICB 2009*, M. Tistarelli and M. S. Nixon, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009, pp. 899–908.

[111] 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.

[112] M. K. Morampudi, M. V. N. K. Prasad, and U. S. N. Raju, "Privacy-preserving iris authentication using fully homomorphic encryption," *Multimedia Tools and Applications*, vol. 79, no. 27, pp. 19 215–19 237, 2020.

[113] G. Cohen, S. Afshar, J. Tapson, and A. Van Schaik, "Emnist: Extending mnist to handwritten letters," in *Proc. of Int'l Joint Conference on Neural Networks*, 2017, pp. 2921–2926.

[114] S. Chikkerur, C. Wu, and V. Govindaraju, "A systematic approach for feature extraction in fingerprint images," in *Proc. of Int'l Conference on Biometric Authentication*, D. Zhang and A. K. Jain, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2004, pp. 344–350.

[115] H. Lin, W. Yifei, and A. Jain, "Fingerprint image enhancement: algorithm and performance evaluation," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 20, no. 8, pp. 777–789, Aug 1998.

[116] X. Chen, J. Tian, X. Yang, and Y. Zhang, "An algorithm for distorted fingerprint matching based on local triangle feature set," *IEEE Transactions on Information Forensics and Security*, vol. 1, no. 2, pp. 169–177, 2006.

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

[118] W. Yang, J. Hu, and S. Wang, "A delaunay triangle group based fuzzy vault with cancellability," in *Proc. of Int'l Congress on Image and Signal Processing*, vol. 03, 2013, pp. 1676–1681.

[119] A. Nagar, S. Rane, and A. Vetro, "Privacy and security of features extracted from minutiae aggregates," in *Proc. of IEEE Int'l Conference on Acoustics, Speech and Signal Processing*, 2010, pp. 1826–1829.

[120] J. Ratliff, J. Dobler, S. Tulyakov, A. Rudra, and V. Govindaraju, "Towards fingerprints as strings: Secure indexing for fingerprint matching," in *Proc. of Int'l Conference on Biometrics*, 2013, pp. 1–6.

[121] R. Dwivedi, S. Dey, R. Singh, and A. Prasad, "A privacy-preserving cancelable iris template generation scheme using decimal encoding, and look-up table mapping," *Computers & Security*, vol. 65, pp. 373 – 386, 2017.