DESIGN AND DEVELOPMENT OF AN EFFICIENT MULTIMODAL BIOMETRICS BASED RECOGNITION SYSTEM

A THESIS

SUBMITTED TO THE DELHI TECHNOLOGICAL UNIVERSITY

FOR THE AWARD OF THE DEGREE OF

DOCTOR OF PHILOSOPHY

IN

Computer Science and Engineering

SUBMITTED BY

KESHAV GUPTA

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

DELHI TECHNOLOGICAL UNIVERSITY

DELHI-110042 (INDIA)

October 2020

DELHI TECHNOLOGICAL UNIVERSITY

Certificate

This is to certify that the thesis entitled **"Design and Development of an efficient Multimodal Biometrics based Recognition System"** being submitted by Keshav Gupta (Reg. No.: 2K16/PhD/CO/10) for the award of degree of Doctor of Philosophy to the Delhi Technological University is based on the original research work carried out by him. He has worked under my supervision and has fulfilled the requirements which to my knowledge have reached the requisite standard for the submission of this thesis. It is further certified that the work embodied in this thesis has neither partially nor fully submitted to any other university or institution for the award of any degree or diploma.

Dr. Gurjit Singh Walia
(Supervisor)
Scientist 'E', SAG
DRDO

Prof. Kapil Sharma
(Supervisor)
Professor, Deptt. of IT
Delhi Technological University

Prof. Rajni Jindal
Head of the Department, Deptt. of CSE
Delhi Technological University

Declaration of Authorship

I hereby declare that all information in the thesis entitled “Design and Development of an efficient Multimodal Biometrics based Recognition System” has been obtained and presented in accordance with academic rules and ethical conducts as laid out by Delhi Technological University. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Keshav Gupta

2k16/PHD/CO/10

Department of Computer Science & Engineering

Delhi Technological University (DTU)

New Delhi -110042

Acknowledgements

First and foremost, I would like to thank God for giving me guidance and strength to perform this research work. My heartfelt and sincere thanks to Dr. Kapil Sharma, Head of Department, Department of Information Technology, for his invaluable guidance, constant encouragement and unconditional support in carrying out my research work. He helped in creating an environment so conducive for learning and gave me full academic freedom to pursue my research with ease and confidence. He has been very patient with me and his loving, caring and friendly attitude made me endure all the hardships and shortcomings during continuance of this research work. This period has been an enriching experience of working under his guidance. I am really thankful for his endless support and encouragement throughout this work.

Further, I am very much indebted to Dr. Gurjit Singh Walia, Scientist 'E', DRDO, New Delhi, who has really been instrumental in shaping my research and without whom this work would not have seen the light of the day. His wisdom, intellectual, brilliance, constant guidance and endeavour to seek perfection transformed many aspects of my life, made me a better person and triggered in me the miraculous drive to work hard. His rare academic and professional acumen, admirable dedication and commitment to his subject have always been a source of motivation for me. Due to his incessant support and valuable inputs my research period passed as smooth as a fish swims in the river. Besides being my mentor, he has been a pillar of strength and I am deeply indebted to him for guiding me with his extensive knowledge and insightful discussions. I hope for and look forward to his continued guidance in future.

I am deeply grateful to Prof. Yogesh Singh, Vice Chancellor, Delhi Technological University. He has been a constant source of inspiration for me throughout my research and teaching career. I am thankful to him for constantly encouraging and supporting me in this endeavour of mine. I also thanks Dr. Rajni Jindal, DRC Chairperson and HoD Department of Computer Science for her constant support and motivation.

A special thanks to my family. This work could not have been possible without the unrelenting support of my family. They supported me in every possible way to ease my research journey. I also acknowledge with thanks the contribution of all my other teachers and friends for their direct and indirect help and support in this work.

Keshav Gupta

List of Publications

1. Keshav Gupta, Gurjit Singh Walia, and Kapil Sharma. ”Quality based adaptive score fusion approach for multimodal biometric system.” Applied Intelligence 50, no. 4 (2020): 1086-1099, SCI, (IF: 2.882)

2. Keshav Gupta, Gurjit Singh Walia, Kapil Sharma (2020), “Novel Approach for Multimodal Feature Fusion to Generate Cancelable Biometric”, The Visual Computer, Springer, SCIE, (IF: 1.412)

3. Keshav Gupta (2017), “Advances in multi modal biometric systems: a brief review”. In International Conference on Computing, Communication and Automation (ICCCA). IEEE, 2017.

4. Keshav Gupta, Gurjit Singh Walia, and Kapil Sharma, ”Multimodal Biometric System using Grasshopper Optimization.” In 2019 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS), pp. 387-391. IEEE, 2019.

5. Keshav Gupta, Gurjit Singh Walia, and Kapil Sharma, ”Adaptive multimodal biometric recognition system using optimal combination of modality”, communicated to SCIE journal(under review).

Abstract

Biometric systems provide various benefits over traditional pin-based authentication systems. Also, Multimodal Biometric Systems are extensively employed over unimodal counterparts for user authentication in the digital world. Here, information from multiple sources is combined to reach a final decision. While, Score level fusion combines outcomes of individual classifiers to make a final decision, feature fusion combines individual features from complimentary biometric traits to generate a superior feature. However, the application of multimodal systems to security-critical applications is limited mainly due to non-adaptiveness of these systems to the dynamic environment and inability to distinguish between spoofing attack and the noisy input image. Further, the issue of data privacy and theft is of great concern. Also, most of the biometric systems suffer from the issue of score confliction of individual classifiers.

A multimodal biometric system, which adaptively combines the scores from individual classifiers, is proposed to address these issues. For this, three modalities viz. face, finger, and iris are used to extract individual classifier scores. These classifier scores are adaptively fused considering that concurrent modalities are boosted and discordant modalities are suppressed. The conflicting belief among classifiers is resolved not only to achieve optimum fusion of classifier scores but also to cater dynamic environment. The proposed quality based score fusion also distinguishes between spoofing attacks and noisy inputs as well. The performance of the proposed multimodal biometric system is experimentally validated using three chimeric multimodal databases.

A novel cancelable multimodal biometric system is proposed that combines multiple traits by means of a projection-based approach. The proposed approach generates a cancelable biometric feature that is used to obtain revocable and noninvertible templates. Cancelable features are generated by projecting the feature points onto a random plane obtained using a user-specific key. The point of projection is then transformed into cylindrical coordinates and a combined cancelable feature is obtained. Extensive experiments are performed over 3 chimeric multimodal databases and results reveal high performance. Also, the proposed method is successfully analyzed for privacy concerns, namely revocability, non-invertibility, and unlinkability. Moreover, the proposed system demonstrated tolerance against various security attacks like brute force attacks, attacks via record multiplicity, and substitution attacks. Also, a novel optimized score level fusion using Grasshopper optimization is proposed where the performance optimization of individual classifiers is performed and a concurrent solution is achieved by means of proportional conflict redistribution rules. The system does not require any classifier training and exhibits high performance. The proposed system is robust against the dynamic environment and exhibits high reliability.

Table of Contents

List of Figures

List of Tables

Chapter 1

Introduction

Chapter 1

Introduction

Identity confirmation is very critical in today's digital world. Traditional pin and password methods are becoming obsolete day by day as it is easier to break them with an increase in technology. To address this, biometric systems which use people's physiological traits like face, fingerprints etc. are considered as more appropriate solutions in terms of robustness, reliability, and accuracy. Biometric systems using only a single modality like a fingerprint, face, etc. are known as unimodal systems. Unimodal systems possess different issues such as non-universality, intraclass variations, noise in input data, spoof attacks, and distinctiveness [83]. These issues are mostly handled by multimodal systems which combines information from multiple biometric modalities [83, 34].

The initial biometric systems used only a single modality for authentication. Features from modalities like face, fingerprint, iris, fingervein, palmprint etc. were extracted and used for biometric recognition [83]. Later, multimodal systems came into existence to overcome various challenges imposed by unimodal systems. After extensive investigation, many researchers have concluded that multimodal systems are more efficient in addressing various challenges [34]. Complementary modalities can compensate the shortcomings of one another to provide better performance during challenging conditions. For instances, fingerprint biometric can be easily collected but suffers from problems like

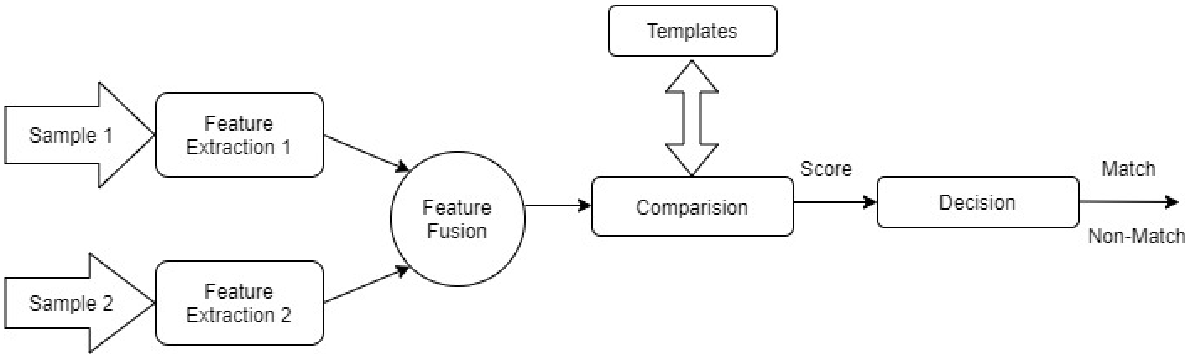


Fig. 1.1 *Multimodal Biometric Recognition System with Feature Level Fusion [1]*

non-universality, noise, skin disease etc. along with moderate performance. On the other hand, iris modality is comparatively difficult to collect but provides accurate results and difficult to forge. Also, Face modality is easily accessible and gives fair results but suffers from challenges like illumination and pose variation, expressions, occlusion, makeup etc. Similarly, identification process is relatively slower for palmprint modality and prolonged exposure to infra-red radiations in case of fingervein may cause medical issues. Thus, it is evident that a single modality is not sufficient enough to create an effective biometric recognition system.

Multimodal Biometric systems fuse together information obtained from multiple biometric traits using various techniques such as feature fusion, score fusion, and decision level fusion. [83, 34]. Fusion can be performed in serial and parallel modes. Researchers have worked on multimodal biometric systems at different fusion levels to show their efficiency over other traditional methods. For instance, Hossain et al [33] proposed a serial fusion approach over face and iris modality. Here, multiple classifiers were arranged in a serial mode using 'best to worst' approach. On the other hand, Yang et al. fused the features of finger vein and fingerprint modalities to generate a more discriminative feature [125]. The working of a feature level fusion based biometric system is shown in Fig. 1.1 [1].

Although the feature set contains the highest amount of information, incompatibility in

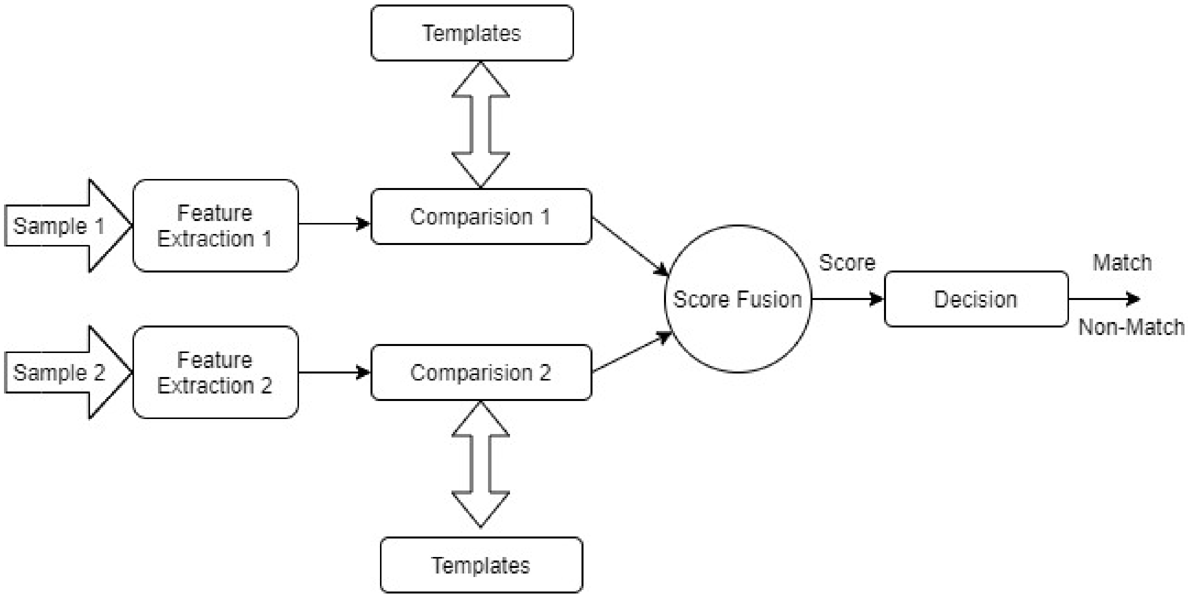


Fig. 1.2 *Multimodal Biometric Recognition System with Score Level Fusion [1]*

type and dimension of features extracted from different modalities limits the application of feature level fusion. Generally, score level fusion is used to overcome the issues of feature level fusion [91]. For example, Peng et al. proposed a t-norm based fusion method which combined multiple classifier scores to generate a final score [71]. The score fusion provided a trade-off between ease of use and efficiency. Fusion can also be performed at the decision level. For instance, Prabhakar and Jain worked in combining the results of four different fingerprint matching algorithms [76]. Fusion at the decision level is quite inflexible because of low information available and choice of the classifier. The most commonly used approach is fusion at score level due to low computation complexity and sufficient information content to discriminate [83, 34]. A sample multimodal biometric system with score level fusion is depicted in Fig. 1.2 [1].

However, these systems mostly considered modalities either from same region or very few modalities for score level fusion. Also, most of the available techniques are not robust or adaptive to location or environment variations. Further, feature acquisition module needs to cater for degradation of acquired samples for better identification of subject.

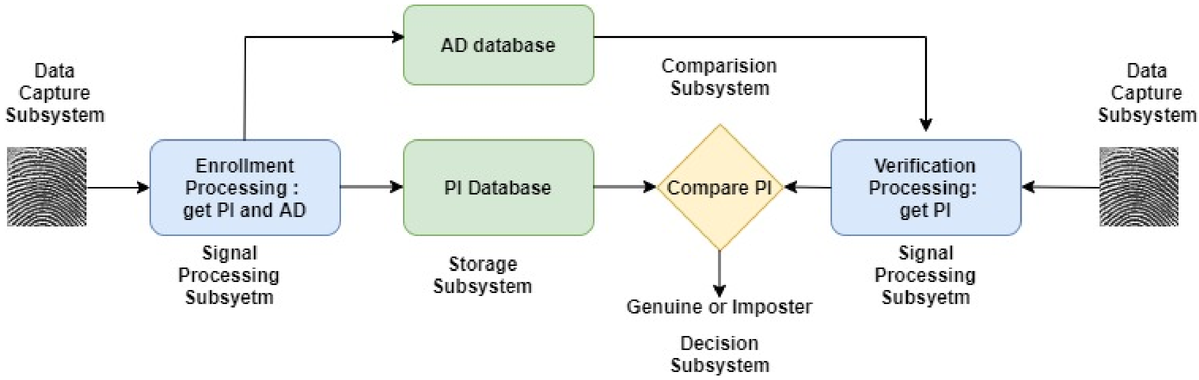


Fig. 1.3 *Template Protection in a Biometric Recognition System [78]*

Generally, multimodal systems are very helpful in dealing with above-stated issues but no protection is available for biometric data itself in case of template hacking or database stealing. Moreover, most of the biometric systems suffer from single point of failure. Thus, if the security measure fails, system will get compromised. Further, security of biometric data should be of top priority as biometric information cannot be replaced easily. If biometric templates are stolen, the user's identity is compromised for multiple applications and subject to cross-application attacks as well. Overall, it not only threatens the security, but it may also incur a significant financial or social loss. To resolve these issues, cancelable biometrics is widely used.

Cancelable biometric systems use a pseudo biometric template instead of the original template for matching and verification purposes. The working of cancelable biometric system is shown in Fig. 1.3 [78].

These pseudo templates are generated from original templates using various transformation mechanisms. For instance, in non-invertible geometric transformations, a feature domain transformation is applied using transformation techniques such as Cartesian, polar and functional transformation [79]. Random projection is also used as a non-invertible transformation [72][73] wherein an extracted feature $x \in F_n$ is projected to a random subspace $Y \in F_n \times N$ with n<N and all element of y are independently realized from a random

variable as z = Yx where z is random projection vector. A random convolution method was proposed in [90] to produce cancelable templates wherein a user-specific kernel is used to encrypt the biometric data. Bio-convolving is also a convolution-based approach for generating cancelable templates [56]. In this, biometric template was segmented into various sequences and a transformed sequence is generated using linear convolution. An extension of random projection is bio hashing [35] wherein a bio-hash template was generated using a user-specific random number. Random permutation of features is also been used by many researchers for generating cancelable templates [129]. There are also various salting methods where a random pattern or noise is mixed with the original template. The techniques used for the cancelable biometric template must exhibit properties viz. revocability, security, diversity, and accuracy. Also, for multimodal biometric recognition systems, optimal combination of classifiers is equally important. Optimization of system parameters can increase the accuracy of entire system. In sum, a lot of solutions have been provided under each category but there is still scope of improvement that can be considered for developing robust and adaptive biometric recognition systems.

1.1 Thesis Overview

The thesis comprises of six chapters and a brief description of these chapters is given below:

Chapter 1:- This chapter will cover the introduction and purpose of the outlined research topic. It will also contain the main idea for the development of the thesis. In addition, the potential application areas and main challenges in multimodal biometric recognition systems are covered.

Chapter 2:- This section will cover the state-of-the-art techniques developed in existing research work on "Multimodal biometric systems under score level fusion and feature level fusion with cancelable templates". Further, details pertaining to the generated database will be discussed. It will also highlight the research gaps in the existing work that has stimulated the development of research objectives. Also, the details related to accomplish the objective 1 and 2 will be discussed.

Chapter 3:- This section will highlight the discussion of the methodology adopted to accomplish the adaptive score fusion for multimodal biometric system. In addition, it will also cover the observations and discussion of results.

Chapter 4:- This section will highlight the discussion of the methodology adopted to accomplish the development of multimodal biometric system with optimization techniques. The feature and score optimization is performed for higher performance. The obtained experimental results will also be elaborated against the other compared state-of-the-art.

Chapter 5:- This section will highlight the discussion of the methodology adopted to accomplish the development of a multilevel security framework for multimodal biometric system. The brief details highlighting the accuracy and the effectiveness of the proposed methodology will also be discussed.

Chapter 6:- This section will contain the brief summary of all the ideas, observations and contributions of the resultants obtained in each objective. Also, the future directions are sketched in this section.

Chapter 2

Literature Review

Chapter 2

Literature Review

Recently, multimodal biometric systems are extensively investigated for achieving robust and reliable solutions. In this section, we explicitly reviewed recent literature which is closely related to our work. The various approaches for biometric recognition are briefly reviewed and are detailed as follows.

2.1 Score Level Fusion

Generally, multimodal biometric systems perform fusion at feature level, score level and at the decision level. Score level fusion is considered as a suitable approach as it not only increases the reliability of the results but also reduces the overall complexity. There are various score fusion techniques proposed by researchers. For example, in [71], T-norms were used to fuse matching scores evaluated from multiple hand modalities like finger knuckle print, palm print, finger vein, and fingerprint. Evaluated scores were also normalized and score fusion was performed using different T-norms. Similarly, Nanni et al [63] used statistical and machine learning approaches for a combination of various fingerprint matchers on 4 FVC2006 databases. Authors investigated various score level fusion algorithms to check the best approach for score fusion and correlation among multiple fingerprint classifiers. Also, Abderrahmane et al [4] proposed weighted quasi-arithmetic mean (WQAM) to perform score fusion estimated via different trigonometric functions. In [18], age classification was performed on the basis of face and ocular fusion. In [101], authors proposed a multiple-instance score fusion using a finger-knuckle print of 4 different fingers. Match scores were first normalized and then combined together to make a decision. In [105], score fusion using likelihood ratio via copula models was performed. Similarly, authors in [108] proposed a score level fusion technique using likelihood ratio under the assumption of Naïve Bayes. The likelihood ratio was estimated via operation points on ROC. Results were evaluated over the Face Recognition Grand Challenge (FRGC) 2D-3D face database. However, the biometric modalities were chosen from a single body part, these methods mostly suffered from universality problem.

To resolve the issue of universality, traits belonging to multiple regions were adopted. For instance, In [97], iris and facial features were fused at score level. In this, each individual classifiers was assigned with a weight and a weighted score level fusion was performed. The fused score is used to take the final decision. Similarly, weighted score level fusion was used for animal classification using facial images [106]. Also, Sim et al [98] presented a score fusion technique to combine similarity scores from the face and iris biometric traits. The experiments were performed on self-made ”Universiti Teknologi Malaysia Iris and Face Multimodal Datasets” (UTMIFM) dataset along with the ORL face database and UBIRIS version 2.0 database. Also, Mukherjee et al [59] presented a score fusion method where different similarity scores were mapped to a single amalgamated match score for decision making. Parameters were tuned using differential evolution (DE) to reduce the overlapping of genuine and imposter score distribution area in a frequency distribution plot. Results were evaluated over two databases each having four different modalities viz. iris, fingerprint, left and right ear. Further, in [52] a probabilistic score fusion algorithm was presented where the fusion was cast into an optimization problem. The effectiveness of the algorithm was demonstrated on two databases viz NIST-BSSR1 and XM2VTS-benchmark respectively. In [38], matcher performance-based (MPb) fusion scheme was proposed to carry out score fusion. Also, score fusion for multiple biometric traits was performed using DSmT Theory [92, 64]. In [15], a hybrid approach using both score and decision level fusion was followed. Scores from individual classifiers were fused using Mean-closure weighting (MCW) and a decision was made based on DS theory over 3 virtual multimodal databases. In [84], a score fusion technique which combined scores from iris and face modalities was proposed. The authors deployed a fuzzy clustering method to effectively localize iris images improving the overall results.

Poh et al [74] incorporated quality during fusion which determined the reliability of the results given by fusion methods. In this, the quality information was used by Bayesian framework working with discriminative and generative classifiers to improve system's performance. Similarly, in [75], authors proposed a quality-dependent technique for score normalization in order to minimize the performance degradation. Also, Kabir et al [37] proposed a novel normalization and weighting technique for score level fusion. Further, authors in [95] investigated a joint sparse representation including a quality measure for each modality which optimized individual classifier scores. In [104], social behavioural information was fused with physiological biometric traits at score level to improve performance. Also, Kihal et al [42] used iris and 3D cornea features for biometric authentication. Min, Max, sum and weighted-sum was used for score Level fusion. Similarly, these approaches were also used for fusion in [77, 40]. Gao et al [22] proposed a score level adaptive binary fusion to adaptively fuse matching distance before and after reconstruction of Finger-knuckle print. Similarly, Ribaric et al [82] performed matching score level fusion by means of total similarity measure using hand geometry, finger and palm-print as biometric modalities. However, the performance for these methods was compromised under a dynamic environment and vulnerable against spoofing attacks. Also, the conflict in match scores and the optimal combination was limitedly addressed among the techniques.

2.2 Classifier Optimal Fusion

Individual classifier scores are generally optimized to resolve conflicting match scores. Nandakumar et al [61] proposed an optimal match score fusion technique on the basis of a likelihood ratio test. A finite Gaussian mixture model was created using genuine and impostor score distribution. Experiments were conducted on 3 publicly available datasets NIST-BSSR1, XM2VTS-benchmark and WVU database. To resolve the conflict among classifier scores, Walia et al [120] presented a score fusion approach using PCR-6 with Backtracking Search Optimization. Similarly, authors in [57] proposed a score fusion technique incorporating belief functions for iris and face modality. Authors used Denoeux and Appriou models to convert matching scores into belief assignments and PSO was used to compute the confidence factor. DS theory was then used to combine the masses and PCR-5 to predict the user's class. Also, Liau and Isa [53] used support vector machines(SVM) to perform weighted score level fusion of optimized face and iris feature scores. In [30], authors developed a fast optimization technique which required only first order information for optimization process. Similarly, Particle Swarm Optimization was used to optimize various parameters based on varying system requirements. [115, 85]. Similarly, veluchamy and karlmarx [116] used fractional firefly optimization to evaluate optimal weight scores for fusion.

In [118] authors used graph diffusion technique to secure the biometric template and optimally fuse the individual classifier scores. Also, Kumar and Kumar [46] explored multimodal systems to adapt to different security levels. An Ant Colony Optimization (ACO) based parameter manipulates various other parameters like threshold, fusion technique, weights, etc. depending upon the given security level. Grey wolf optimizer was used in [49, 96] to tune the fusion parameters for multimodal biometric system. Similarly, Bianco and Napoletano [7] optimized multiple biometric signals for various hyperparameters using sequential model based optimization. Further, Ajay et al [45] used hybrid PSO to optimize individual classifier scores before fusion process. Also, Eskandari and Sharifi [17], backtracking search algorithm[BSA] is used to perform parameters optimization. However, the performance of these systems degraded in the presence of noisy input data. Also, latest optimization algorithms were not incorporated for parameter optimization.

2.3 Template Protection

Cancelable biometrics are used to protect templates by performing the matching and storage in a different domain [62]. Generally, in the case of template stealing, the stolen template is revoked and an entirely different template is created by altering the key. Thus it fulfils the necessary requirements for template protections namely revocability, non-invertibility, diversity and accuracy [62][68]. Transformation performed on biometric data can be mainly classified as non-invertible transforms and biometric salting. Biometric salting can be additionally classified as projection-based transformations, noise-based transformation, and convolution-based transformation.

Transformations based on random projection projects biometric data to a random subspace using various transformation techniques. The most popular technique in this category is bio-hashing [35, 6] which projects the features into the orthonormal sub-space. It provides good discrimination capability and high performance. However, this method suffers from the problem of irreversibility if both template and transformation matrix are compromised. In [111] authors proposed an extension of the bio hash technique to address the issue of stolen-token scenarios. In this, the authors used a novel multi-state discretization technique instead of a simple threshold scheme. Pillai et al proposed a new variant of random projection namely Sectored random Projection [72] technique where the biometric feature is segmented into various sectors, then on each sector, the random projection is applied and concatenation was performed to generate the cancelable template. This method not only caters to the issue of useful iris area reduction, but it is also robust to common iris outliers. To improve non-invertibility, Teoh et al [110] introduced a novel technique, random multi-space quantization (RMQ), wherein the biometric feature vector was mapped with a sequence of random sub-spaces using a pseudo-random sequence. In the second step, quantization was performed based on a threshold value. Teoh et al also proposed a multi-space random projections technique [112] which is a two-factor cancelable formulation and feature vector obtained from biometric modalities is projected to multiple random subspaces based on a user-specific pseudo-random number. Wang et al proposed a random projection with vector translation method [123] for cancelable biometrics wherein biometric data was projected using a Gaussian random variable. Also, Paul et al [69] proposed a random cross-folding method using random projection and selection to create cancelable templates. In order to make it a user-dependent dynamic process, Yang et al proposed a non-linear projection process in which the projection vector was dynamically decided by feature vector itself [125]. In general, most of the projection techniques discussed are vulnerable to attacks such as inverse operations if both templates and transformation matrix are stolen [50]. Accordingly, researchers have proposed other methods like random convolution transformations for generating cancelable templates.

In random convolution(RC) based transformations, cancelable templates are generated by convolving the biometric feature using a random kernel. Savvides et al. [90] used Minimum Average Correlation Energy (MACE) filters as a convolution method to generate cancelable templates. In [86], authors used the concept of locality sensitive hashing to generate secure, cancelable iris features. Maiorana et al proposed a Bio-convolving technique where a set of non-invertible transformations were performed on sequence-based biometric representation [56]. But if kernel used for transformation is known, it can be vulnerable to inverse attacks. To overcome this issue, an algorithm using curtailed circular convolution was proposed [121]. The algorithm convolved input binary features in a circular manner using random binary strings imparting non-invertibility. In [94], the authors used the quality of fingerprint features to determine the presence of live fingerprint. Similarly, Ali et al. [5] used a user key set to modify minutiae information from fingerprint to produce cancelable templates. Further, Trivedi et al. [114] used a binary user key on fingerprint modality to generate cancelable templates. Lee et al [51] used novel cancelable biometric scheme that did not require alignment for fingerprint biometric. Similarly, Wang and Li [122] generated cancelable palmprint template using Orthogonal Index of Maximum (OIOM) hash and Minimum Signature Hash (MSH). Also, Mai et al [55] used randomized CNN to generate secure face templates using user-specific keys.

In [109], bidirectional associative memory (BAM) was used to bind biometric templates to random bit-strings generating cancelable templates. Also, Canuto et al [14] used ensemble system for cancelable transformation in multimodal systems. Further, Takahashi and Naganuma [107] used correlation invariant random filtering (CIRF) by generalising it on the basis of a quotient polynomial ring for generating secure templates. In [87], transformed features were computed from local and distant structure using fingerprint modality. Similarly, Gao and Zhang [23] mapped real minutiae to a synthetic template to generate cancelable biometric. Further, Sandhya et al [88] used Delunay Triangle to construct cancelable feature set for fingerprint modality. On the other hand, wu et al. [124] presented ECG as a biometric and generated revocable templates using signal subspace collapsing. Similarly, Kim and Chun [43] used ECG as cancelable biometric by using generalized likelihood ratio test in compressive sensing domain. Further, ECG modality was fused with fingerprint using CNN for a cancelable multimodal biometric system [31]. The cancelable biometrics is also widely used with multimodal biometric systems to remove various limitations imposed by unimodal systems.

Rathgeb and Busch used adaptive bloom filters to transform iris feature for both eyes of a single subject and fused them at feature level [81, 80]. This method provided improved performance but vulnerable to template linking. A Random Permutation Principal Component Analysis (RP-PCA) method was introduced by Kumar et al. [48] to generate cancelable biometric using face, iris, and ear modality. The accuracy of the system was unaffected and the robustness of the system was improved. Similarly, Murakami et al [60] used permutation based indexing for securing the biometric templates efficiently. Also, Dwivedi and dey [16] created a hybrid scheme for a cancelable multi-biometric system combining Mean-Closure Weighting (MCW) with Dempster-Shafer (DS) theory.

This scheme showed robustness against score variability and considerable performance improvement over uni-modal counterparts. Similarly, Walia et. al [119] proposed a cancelable biometric system by performing cross-diffusion of graphs. Later, PCR-6 was used to fuse belief masses from individual classifiers. Experimental results demonstrated better performance than many existing techniques. In [128], authors used biometric layering to conceal the user identity over multiple fingerprints. Also, Sui et al [103] created a bio-capsule after fusing multiple modalities and using it for authentication. Chang et al [9] used bit-wise encryption technique to generate cancelable multimodal biometric system. Kaur and Khanna [41] proposed a novel random distance technique for transformation in a multi-biometric scenario using face, palmprint, and finger-vein as input modalities. Similarly, walia et al [117] used key images to generate cancelable features and dimension reduction. A multifold random projection was introduced by Paul and Gavrilova [70] for a multimodal biometric system with improved recognition performance. Chin et al. [11] proposed a template protection scheme wherein original fingerprint and palmprint templates were arranged in random rectangles using user-specific keys. Later, statistical features were extracted and fused at the feature level to generate cancelable templates. Similarly, Gomez-Barrero et al. [25] used bloom filters on face-finger vein and face-iris to generate protected templates and a weighted feature level fusion was performed to generate the multimodal cancelable template. With increasing attacks on biometric systems, detection of fake biometric is equally important as the protection of biometric data.

Based on the above discussion, it is evident that securing biometric systems from various attacks should be of top priority. Also, biometric systems should be adaptive to dynamic environmental conditions. Further, accuracy and performance of the system is very important. Accordingly, multimodal biometric systems are proposed which are not only adaptive in nature but also improves the overall security of the biometric system.

2.4 Performance validation

For performance validation of the proposed biometric systems, robust evaluation metrics are chosen. In addition, different biometric samples from multiple benchmarked datasets are chosen for performance evaluation. The details related to the exploited evaluation metrics and the benchmark datasets is discussed in the following sections.

2.4.1 Evaluation Metrics

The proposed system's performance is quantitatively analyzed by means of Decidability Index (DI), Equal Error Rate (EER), and Recognition Index(RI). Further, the results are compared with other state-of-the-art fusion methods. During this process, feature extraction and score calculation techniques are kept the same for evaluation of all the methods. Decidability Index (DI) is a performance metric used to quantify the distance between genuine and imposter score distributions and is calculated using Eq. 2.1

$$DI = \frac{|\mu_g - \mu_i|}{\sqrt{(\sigma_g^2 - \sigma_i^2)/2}} \tag{2.1}$$

Here, μ_g , μ_i denotes the mean values, and σ_g and σ_i denotes the standard deviation values of genuine and imposter scores distributions, respectively. A high decidability index value suggests a higher ability of the classifier to separate genuine from imposters. Equal Error Rate (EER) is calculated by plotting ROC curves where the false acceptance rate (FAR) is plotted against the genuine acceptance rate (GAR). It provides the measure of the accuracy of the proposed biometric system. Recognition Index (RI) provides the recognition rate at rank-1 and can be used for performance evaluation. Cumulative Matching Characteristics (CMC) curves show the relationship between rank and the recognition rate.

2.4.2 Benchmark Datasets

Various authors have proposed numerous models for biometric systems, most of which was evaluated on publicly available datasets. These datasets provide a common base for evaluation of various biometric systems. The details of the publicly available benchmarked datasets is as follows:

- **CASIA**: It is a Face Image Database (ver 5.0) containing 2500 facial images from 500 users. Images are captured using a Logitech USB camera. All images are in 16 bit color BMP format having resolution of 640×480.(Casia-FaceV5, http://biometrics.idealtest. org/)
- **CASIA Iris Database**: Casia IrisV1 database contains 756 iris images from 108 subjects in two different sessions. All captured images are in BMP format having a resolution of 320*280 [3]
- **CAS-PEAL Database**: CAS-PEAL-R1 face database accommodates a total of 30,863 facial images from 1040 individuals out of which 595 are males and 445 females. The database is captured using 9 cameras to capture facial images with different poses, facial expressions, six accessories, and various lighting and background changes [24].

- **MCYT database**: MCYT fingerprint database is obtained using two different sensors. These sensors namely CMOS-based capacitive capture device, and an optical capture device have a resolution of 500 dpi. Twelve samples with each sensor were captured for each fingerprint from 330 subjects. Image resolution for captured images is 300x300 for sensor 1 and 256x400 for sensor 2 respectively [66].

- **FVC 2006**: FVC2006 DB1-A contains 1680 uncompressed, 256 gray-levels fingerprint images from 140 subjects in BMP format. The images are acquired using an electric Field sensor with image size 96x96 having a resolution of 250 dpi [8].

- **IITD Iris Database**: IITD PolyU iris database images are captured with the help of a digital CMOS camera containing 5 samples from each eye of 224 subjects having a size of 320x 240 pixels [47].

- **MMU Iris Database**: MMU2 Iris database consists of 995 iris images in BMP format having resolution 320x238 pixels from 100 volunteers [2].

2.5 Research Gap

Based on the literature survey potential research gaps were identified. The details of the identified research gaps is as follows:

- Most of the datasets include only a single modality for a particular user.

- Most of the datasets doesn't include the real-time scenarios which may actually happen during biometric recognition. The real-time scenario includes the environmental variations due presence of sunlight, fog, humidity etc.

- There is only limited number of samples available for a particular user in a dataset.
- Most of the techniques, considered modalities either from same region or very few modalities for score level fusion
- Most of the available techniques are not robust or adaptive to location or environment variations.
- Requirement of a technique which can estimate the reliabilities of each modality for effective fusion process.
- Most of the techniques considered limited performance matrices for the evaluation of biometric system performance.
- Output from each individual classifier need to be optimized for better system's performance.
- Most of the biometric systems suffer from single point of failure.
- Compromise of biometric data results in permanent loss of an individuals identity, and hence, is a growing concern.
- To achieve complete non-invertibility is most challenging as it tends to degrade the performance.
- Cancelable templates need to be robust against wide range of adversary attacks.

2.6 Research Motivation

Biometric Recognition is an imperative field of Pattern analysis which aim to recognize/authenticate genuine users. A lot of work under various biometric models has been proposed but it is still open and challenging due to dynamic environmental conditions like illumination variations, full or partial occlusion, humidity etc. To adapt such variations, single modality is not sufficient to provide robust solutions. Most of the available research work is not efficient enough to address various environmental challenges. Hence, development of a robust and adaptive biometric recognition model is paramount that can address these challenges. This work is motivated by the fact that multiple biometric modalities are necessary for developing robust and adaptive solutions. The adaptive score level fusion of multiple modalities is another direction that can be evaluated with the aim to provide adaptive multimodal biometric systems. Using score level fusion, various biometric systems were provided but performance under dynamic environment was limitedly addressed. Moreover, these systems were evaluated over limited datasets only. Optimization of various biometric parameters like matching scores can be explored to provide better recognition performance. Multilevel biometric recognition systems can be explored further with the aim to cater the issue of single point of failure. Moreover, security of biometric data is of utmost importance. This problem can be resolved by using cancelable biometric systems which are non-invertible and robust against various security threats.

2.7 Research Objective

This research was focused to develop an adaptive, robust and highly accurate multimodal biometric recognition system. The objectives which were considered in the current studies are as follows:

- To study various state-of-the-art techniques, datasets and performance metrics for multimodal biometric systems.
- Creation of multimodal dataset for various biometric traits.
- To design and develop an adaptive multimodal biometric system with score level fusion technique and to make a comparative analysis with the existing systems.
- To carry out the optimization of Multimodal biometric system for some of its critical performance metrics using combination of various features and classifiers.
- To design and develop an efficient multi-level security system for the developed multi modal biometric system.

2.8 Significant Findings

The following were the key findings of the present work

- An extensive literature review was performed and biometric modalities were categorized on the basis of region of origin.
- An in-house multimodal biometric dataset is created which can be used for research purposes by other researchers as well.

The significant findings of literature review are published in [26].

Chapter 3

Adaptive Multimodal Biometric System

Chapter 3

Adaptive Multimodal Biometric System

Generally, multimodal biometric systems provide desired accuracy using fixed rules for combination and security level. But under dynamic conditions and ever-changing environment, the same rules may not be applicable or equally efficient. Keeping this issue in mind, an adaptive multimodal biometric system with score level fusion technique is proposed, which maps the matching scores into different domain by boosting or suppressing their values based on the threshold and security requirements to reach a final decision. The proposed method can effectively distinguish between low-quality images and spoofing attacks. The next section presents a detailed overview of the proposed method.

3.1 Proposed Multimodal Biometric System

The architecture of the proposed multimodal biometric system is presented in Fig. 3.1. In this, three biometric features viz. Iris(i), Face(f), and Fingerprint(p) are fused using the proposed adaptive score level fusion.

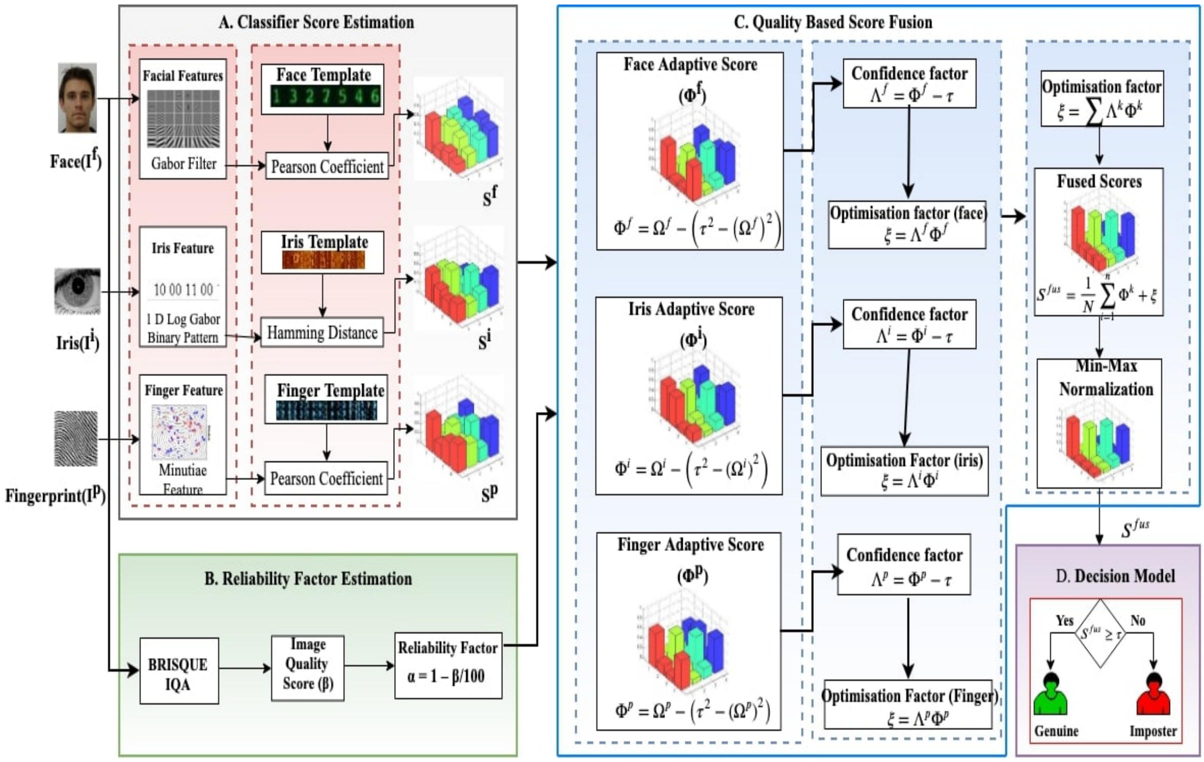


Fig. 3.1 *Overview of the Proposed Multimodal Biometric System. Features from query image are extracted and compared with stored templates to generate individual classifier scores. Combined with reliability factor, scores are fused based on the proposed score fusion method to reach a final decision*

Three biometric features are taken as input and corresponding features are extracted. For iris feature extraction, segmentation is done using an improvised hough transform method followed by normalization into rectangular blocks with fixed dimensions using Daugman's model. Finally, phase data extracted from 1-D log Gabor filter is quantized to encode unique pattern into a bit-wise biometric template. For extracting facial feature, Gabor filters are used which explore various visual properties like orientation selectivity, spatial localization, and spatial frequency characteristics. The feature vector is created by convolving the image with Gabor filters. For fingerprint trait, the input image is first enhanced using binarisation and thinning operations. Further, minutiae-based features are extracted from the corresponding image.

Comparison of the query image is performed with the templates stored in database and similarity match scores are obtained as S^i, S^f and S^p for iris, face and fingerprint respectively. These scores are processed and optimally combined using the proposed fusion model. Fusion model comprises of 3 stages: In the first stage, adaptive scores are calculated from the match scores for each modality. In the next stage, confidence and optimization factors are computed and finally score fusion is performed followed by normalization step. Finally, the fused score is compared with a threshold value to reach a decision. The proposed system is adaptive in nature as an adaptive score is calculated depending upon the distance of match score from a threshold value. Also, each modality is assigned with a reliability factor (α) using input image quality which provides unequal priors depending upon the reliability of input features. The following sub-section presents the details of the proposed Multimodal Biometric System.

3.1.1 Feature Extraction and Classifier Score Estimation

Multimodal modalities viz. iris, face, and fingerprint are processed for generic feature extraction and individual classifier scores are determined. For facial feature extraction, we adopted the Gabor filter approach for edge detection [54] due to low complexity, robustness against noise and other photometric disturbances [113]. This method recognizes a particular region of interest by capturing relevant frequency spectrum at specified orientations to extract features [54]. A Gaussian kernel function $\Upsilon_{\nu,\Theta}(x,y)$ is used to modulate the 2-D Gabor filter in form of a complex sinusoidal wave as in Eq. 3.1

$$\Upsilon_{\nu,\Theta}(x,y) = \exp\left[-\frac{1}{2}\left\{\frac{x^2_{\Theta_n}}{\sigma^2_x} + \frac{y^2_{\Theta_n}}{\sigma^2_y}\right\}\right] \exp(2\pi\nu x_{\mathrm{\Theta_n}}) \tag{3.1}$$

Where,

$$\begin{bmatrix} x_{\Theta n} \\ \\ y_{\Theta n} \end{bmatrix} = \begin{bmatrix} sin\Theta_n & cos\Theta_n \\ \\ -cos\Theta_n & sin\Theta_n \end{bmatrix} \begin{bmatrix} x \\ \\ y \end{bmatrix} \tag{3.2}$$

Here, ν is sinusoidal frequency,σ_x , σ_y are standard deviation along x and y direction of Gaussian envelop and Θ_n is the orientation defined in Eq. 3.3

$$\Theta_n = \frac{\pi}{m}\,(n-1) \tag{3.3}$$

For n=1, 2... m where m represents the orientation count. Here, forty Gabor filters are used to convolve input grey facial image I^f in five scales and eight orientations followed by down-sampling by a factor of four to reduce redundancy before concatenating to form a feature vector, η^f which is stored in the database. Similarly, input facial probe image is convolved with Gabor filter bank to extract feature vector, ψ^f. The similarity match score between store template η^f and input probe image ψ^f is computed using Pearson's correlation coefficient using Eq. 3.4

$$S^f = \frac{cov\left(\eta^f,\ \psi^f\right)}{\sigma_{\eta^f}\sigma_{\psi^f}} \tag{3.4}$$

where *cov* calculates the covariance between two vectors and σ represents their standard deviation.

For fingerprint feature extraction, a minutiae-based technique is employed. This technique is widely used by researchers [20, 102] for its high performance, low complexity and its analogy with methods used by forensic experts for fingerprint recognition. In this, input finger image I^p is first pre-processed through binarization and thinning. Binarization increases the contrast between ridges and valleys using Eq. 3.5

$$B\left(m,n\right)=\left\{\begin{array}{ll} 1, & if\ I\left(m,n\right)\geq\ t \\ \\ 0, & otherwise \end{array}\right\} \tag{3.5}$$

Where $I\left(m,n\right)$ represents the intensity value at pixel position (m,n) and t is threshold value. Thinning reduces ridges to unit-pixel thickness also known as skeletons and is performed using inbuilt morphological functions on binary images at Matlab platform. Minutiae are located over the thinned image using a 3x3 sliding window in a circular anti-clockwise manner to produce rutovitz crossing number (CN) [102] which defines the type of minutia and can be computed using Eq. 3.6

$$CN=\ \frac{1}{2}\sum_{j=1}^{8}\left|q_j-q_{j-1}\right| \tag{3.6}$$

Where q_j represents pixel values of eight neighbors of any pixel q. Depending upon the value of CN, ridge pixel may be classified as isolated, ending, continuing, bifurcation and crossing point. A ridge pixel with a CN of 0 corresponds to isolated, 1 corresponds to a ridge ending, a CN of 2 corresponds to a continuing ridge point, a CN of three corresponds to a bifurcation and CN of 4 represents crossing point. Each minutia is then represented as a vector M=[m,n,CN,θ] Where, (m,n) represents the coordinates of pixel p and θ is minutia orientation. For input finger image I^p, a feature template, η^p is generated by combining n minutiae using Eq. 3.7

$$\eta^p = [M_1, M_2, \ldots M_n] \tag{3.7}$$

Similarly, a feature template, ψ^p for input probe image is generated. For computing the similarity match scores, minutiae are matched based on spatial distance and directional difference and a total number of matching minutiae are computed. Score S^p is computed between the acquired probe image and stored template using Eq. 3.8 as

$$S^p = \frac{n_{match}^2}{n_\eta n_\psi} \tag{3.8}$$

Here, n_{match} represents the number of matching minutiae between two templates and n_η, n_ψ represents the total number of minutiae extracted.

For extracting the iris features, binary templates are generated using Khalil and Chadi [39] method as it improves the speed and accuracy of the iris segmentation process by accepting high quality images which also reduce the recognition error and produce a discriminating feature vector so as to improve the recognition accuracy and computational efficiency. In this, iris segmentation from input image I^i is performed using circular Hough transform [127] which provides center and radius of the iris. Further, the iris segment is normalized into a rectangular block with fixed dimensions using Daugman's rubber sheet model [12]. Additionally, localized iris texture is transformed from Cartesian to polar coordinates and iris texture is mapped in the radial direction using polar coordinates. The normalized iris is convolved with 1D Log-Gabor filter [21] whose frequency response is defined using Eq.3.9:

$$G\left(\rho\right) = \exp\left\{-0.5 \times \frac{log\left(\frac{\rho}{\rho_0}\right)^2}{log\left(\frac{\sigma}{\rho_0}\right)^2}\right\} \tag{3.9}$$

Where ρ_0 represents central frequency and σ provides filter bandwidth. The extracted phase data from this convolution is quantized to four levels corresponding to four different phases. This results in a unique binary pattern, generating iris feature binary template η^i. Similarly, a feature template, ψ^i for iris probe image is also generated. The similarity between the input query image and the stored template is calculated using hamming distance in Eq. 3.10.

$$HD\left(\eta^i,\ \psi^i\right) = \frac{1}{N}\sum_{j=1}^{n}\eta^i \bigotimes \psi^i \tag{3.10}$$

The hamming distance calculated between two templates is then converted into matching scores using the radial basis function (RBF) kernel in the range of [0, 1]. Using the RBF kernel, the match score between the input query image and the stored templates is computed as per Eq. 3.11

$$S^i = exp\left(-\frac{HD\left(\eta^i, \psi^i\right)}{2\sigma^2}\right) \tag{3.11}$$

The calculated match scores from three modalities S^i, S^f, S^p are passed to the proposed fusion model to generate a fused score. The design of the proposed fusion model is discussed in the next section.

3.1.2 Quality Based Adaptive Score Fusion

The fusion process is very important in a multimodal biometric system for making a decision. Here, we have proposed an adaptive score level fusion method with reliability factor (α) corresponding to each modality giving unequal priors depending upon the quality of input features. The proposed method performs boosting and suppression of individual classifier scores, which makes it adaptive under dynamic environment and robust against spoofing attacks.

Biometric image samples acquired under a dynamic environment may contain extra added noise. A reliability factor (α) based on image quality is calculated which provides a measure of reliability for each modality. Reliability factor (α) is estimated based on the No-reference quality assessment of input images. For this purpose, Blind/Referenceless image Spatial Quality Evaluator (BRISQUE) is adopted [58] which is used as an image quality metric. Here, Mean subtracted Contrast Normalized (MSCN) image is generated from the intensity image (I) using Eq. 3.12.

$$I'_k(x,y) = \frac{I_k(x,y) - \mu_k(x,y)}{\sigma_k(x,y) + 1} \tag{3.12}$$

where $k \in \{f, p, i\}$, (x,y) are spatial indices, μ and σ represents the mean and standard deviation respectively. Further, a Generalized Gaussian Distribution (GDD) is applied to obtain changes in coefficients distribution in the noisy image using Eq. 3.13.

$$f_k(x; p, \sigma^2) = \frac{p}{2q_k\Gamma(1/p)} \exp\left(-\left(\frac{|x|}{q}\right)^p\right) \tag{3.13}$$

where

$$q_k = \sigma\sqrt{\frac{\Gamma(1/p)}{\Gamma(3/p)}} \tag{3.14}$$

for $k \in \{f, p, i\}$, Γ is the gamma function, p is a shape parameter and σ^2 controls variance. Further, a brisque score is calculated using support vector regression (SVR) model trained on image database having similar distortions. The input image is compared to the SVR model with an RBF kernel providing a score value (β) in a range of 1-100. A low score value indicates a high quality of input image. Poor quality of the input query image suggests a high probability of the input image being fake or synthetic/reconstructed. In such cases, input biometric feature cannot be trusted and the reliability of biometric input image is reduced accordingly as per Eq. 3.15.

$$\alpha_k = 1 - \beta_k/100 \tag{3.15}$$

for $k \in \{f, p, i\}$, moreover, high quality input biometric feature results in high reliability. Thus, an overall reliability factor (α) is calculated for each biometric trait which denotes the reliability of each subject. This reliability factor (α) is incorporated with individual classifiers match scores (S^k) to generate optimized match scores with unequal priors using Eq. 3.16.

$$\Omega^k = \alpha_k * S^k \tag{3.16}$$

For $k \in \{f, p, i\}$ representing face, finger and iris modality. Thus, the reliability factor helps to tackle fake biometric features but also various dynamic environmental conditions where one modality is more reliable than any other modality by providing unequal priors. Individual classifier scores are optimized by calculating the adaptive scores (Φ^k) for each modality using Eq. 3.17 as

$$\Phi^k = \Omega^k - \left(\tau^2 - \Omega^{k^2}\right) \tag{3.17}$$

Where, τ is an optimal threshold value and Ω^k denotes the match scores of individual classifiers for $k \in \{f, p, i\}$ representing the face, finger and iris modality. Further, a confidence factor (Λ) for each modality is calculated from the threshold value using Eq. 3.18 which indicates the score difference from the threshold value. Higher the difference, value of confidence factor will be high for both genuine and imposter scores.

$$\Lambda^k = \Phi^k - \tau \tag{3.18}$$

Using adaptive score, Φ_i and Confidence factor Λ_i, an Optimisation factor, ξ is computed for each modality as per Eq. 3.19

$$\xi = \sum_{j=1}^{n} \Lambda^k \Phi^k \tag{3.19}$$

where n denotes the number of modalities. Optimization factor, ξ helps in determining the level of boosting or suppression to be done for individual match scores. The final fused score is estimated using Eq. 3.20 and is passed to a decision model for classification into genuine or imposter class.

$$S^{fus} = \frac{1}{N}\sum_{i=1}^{n}\Phi^{k} + \xi \tag{3.20}$$

The proposed score fusion is adaptive in nature as it performs boosting and suppression of individual classifier scores using Eq. 3.17 which helps in creating distinguished decision boundary for genuine and imposter class and robust against spoofing attacks as it incorporates quality based reliability factor using Eq. 3.16.

3.1.3 Decision Model

The fused score is normalized using min-max approach and a final decision is performed using an optimal threshold value (τ) if the normalized fused score is greater than τ, then it is considered as Genuine else imposter. For validation of the proposed method, experiments are performed on three chimeric multimodal datasets generated using benchmark images. The next section provides the details of datasets used and its overall analysis.

3.2 Experimental Validation

The performance of the proposed multimodal biometric system is evaluated over three multimodal databases in both qualitative and quantitative manner. In qualitative analysis, face, fingerprint and iris modalities are combined to generate a final score and are compared with individual classifier match scores. On the other hand, during quantitative analysis, various performance metrics like Decidability Index (DI), Equal Error Rate

(EER), and Recognition Index (RI) are determined. In addition, the performance of the proposed score level fusion method is compared with other state-of-the-art methods.

3.2.1 Database & Experimental Design

We have obtained our Multimodal datasets from various benchmark datasets to validate our proposed algorithm. These Chimeric datasets are obtained by uniquely combining benchmark datasets namely CAS-PEAL Large-Scale Chinese Face Database [24], Casia-Face version 5.0 (Casia-FaceV5, http://biometrics.idealtest. org/), MCYT Bimodal Database [66], FVC2006 DB1-A fingerprint database [8], Casia iris database (Casia-IrisV1, http://biometrics.idealtest. org/), IITD PolyU iris database [47] and MMU2 iris database [2]. Few Sample images of the mentioned datasets are available in Fig. 3.2.

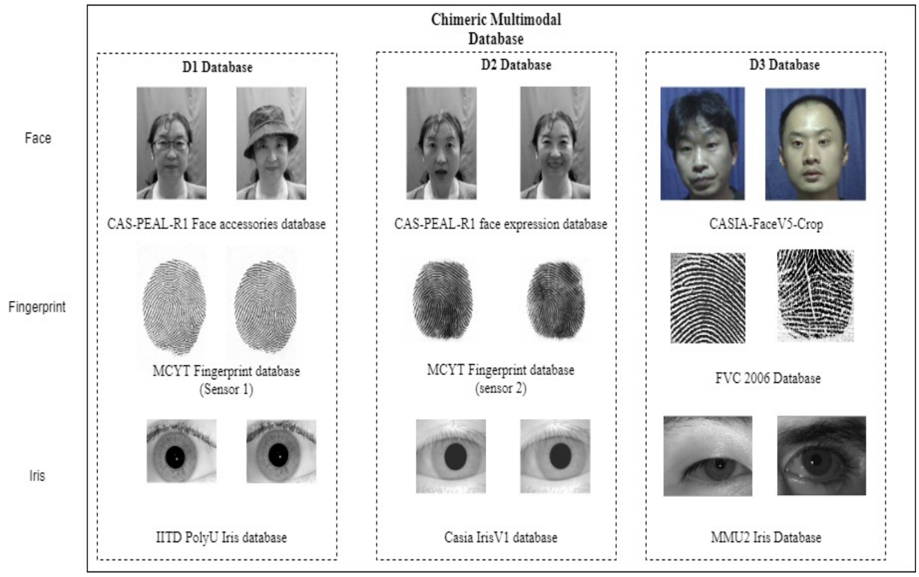

Chimeric Multimodal Database
D1 Database
D2 Database
D3 Database
Face
CAS-PEAL-R1 Face accessories database
CAS-PEAL-R1 face expression database
CASIA-FaceV5-Crop
Fingerprint
MCYT Fingerprint database (Sensor 1)
MCYT Fingerprint database (sensor 2)
FVC 2006 Database
Iris
IITD PolyU Iris database
Casia IrisV1 database
MMU2 Iris Database

Fig. 3.2 *Sample multimodal database images from the benchmark datasets*

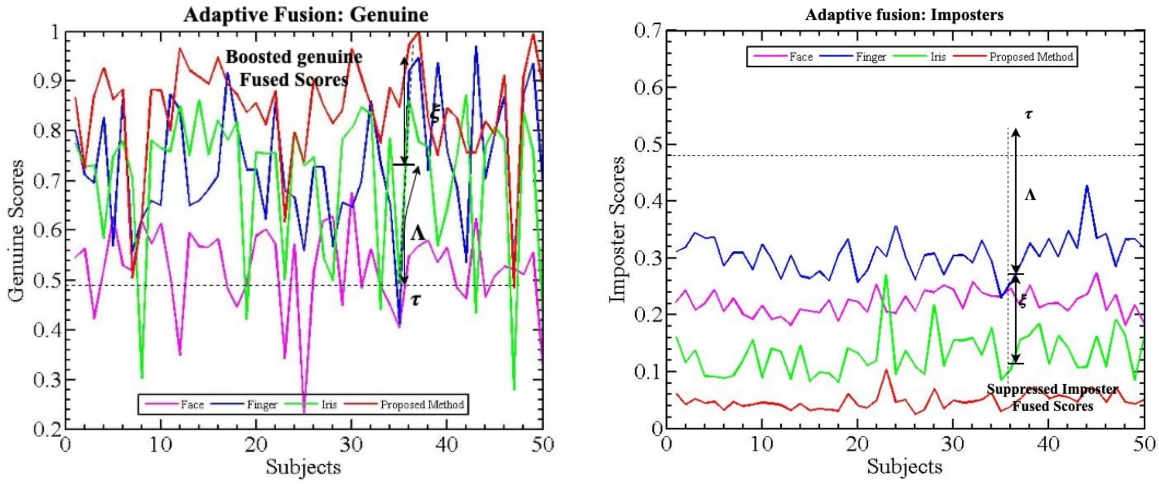
Three chimeric datasets are created namely D1, D2 and D3 to validate the proposed multimodal biometric system. D1 contains samples from N distinct subjects from CAS-PEAL-R1 accessories face database, MCYT fingerprint database from sensor 1 and IITD iris PolyU database. A virtual multimodal dataset containing N subjects is created by combining distinct subjects from each of the above-mentioned datasets. Similarly, D2 dataset is created from distinct subjects each from CAS-PEAL-R1 expression face database, MCYT fingerprint database from sensor 2 and Casia IrisV1 iris database and D3 dataset is created from distinct subjects each from Casia V5 face database, FVC2006 DB1-A fingerprint database, and MMU2 iris database. Also, all the subjects are different in D1, D2 and D3 database. In addition, a consolidated multimodal dataset, D4 of 3N subjects is also created by merging all subjects from D1, D2, and D3 databases. Five-fold cross-validation is performed with five different samples considering each sample as input subject once. We have implemented the proposed system on MATLAB 2018a platform with the hardware configuration of 4GB RAM and Intel i3 processor. The next section presents a qualitative analysis of the proposed system.

3.2.2 Performance Validation

The proposed adaptive multimodal biometric system is validated in a qualitative and quantitative manner. A qualitative analysis of the proposed system is presented in the next section.

3.2.2.1 Qualitative Validation

The performance of the proposed adaptive multimodal biometric system is validated over three multimodal databases and scores from individual classifiers are combined together using the proposed fusion method by boosting and suppression of the individual classifier match scores based on optimal threshold τ. For this, an adaptive score is calculated where scores above the optimal threshold are boosted to high values while scores below the threshold are suppressed to lower values. In the next step, a confidence factor (Λ^k) is calculated corresponding to adaptive match scores using Eq. 3.18 such that higher the value of score from the threshold, higher will be the corresponding confidence factor. Similarly, lower score values yield a low confidence factor corresponding to adaptive match scores. Further, an optimization factor is calculated using the confidence factor from individual classifiers. Boosting or suppression is carried out based on the value of the optimization factor which is decided on the basis of combined consensus from individual classifiers. The value of the optimization factor will be high if all three individual classifiers consider the subject to be genuine resulting in a boosted fused score. Similarly, if all individual classifiers consider a subject to be an imposter, a more suppressed fused score is generated as shown in Fig. 3.3.



(a) *Genuine Score values*

(b) *Imposter Score values*

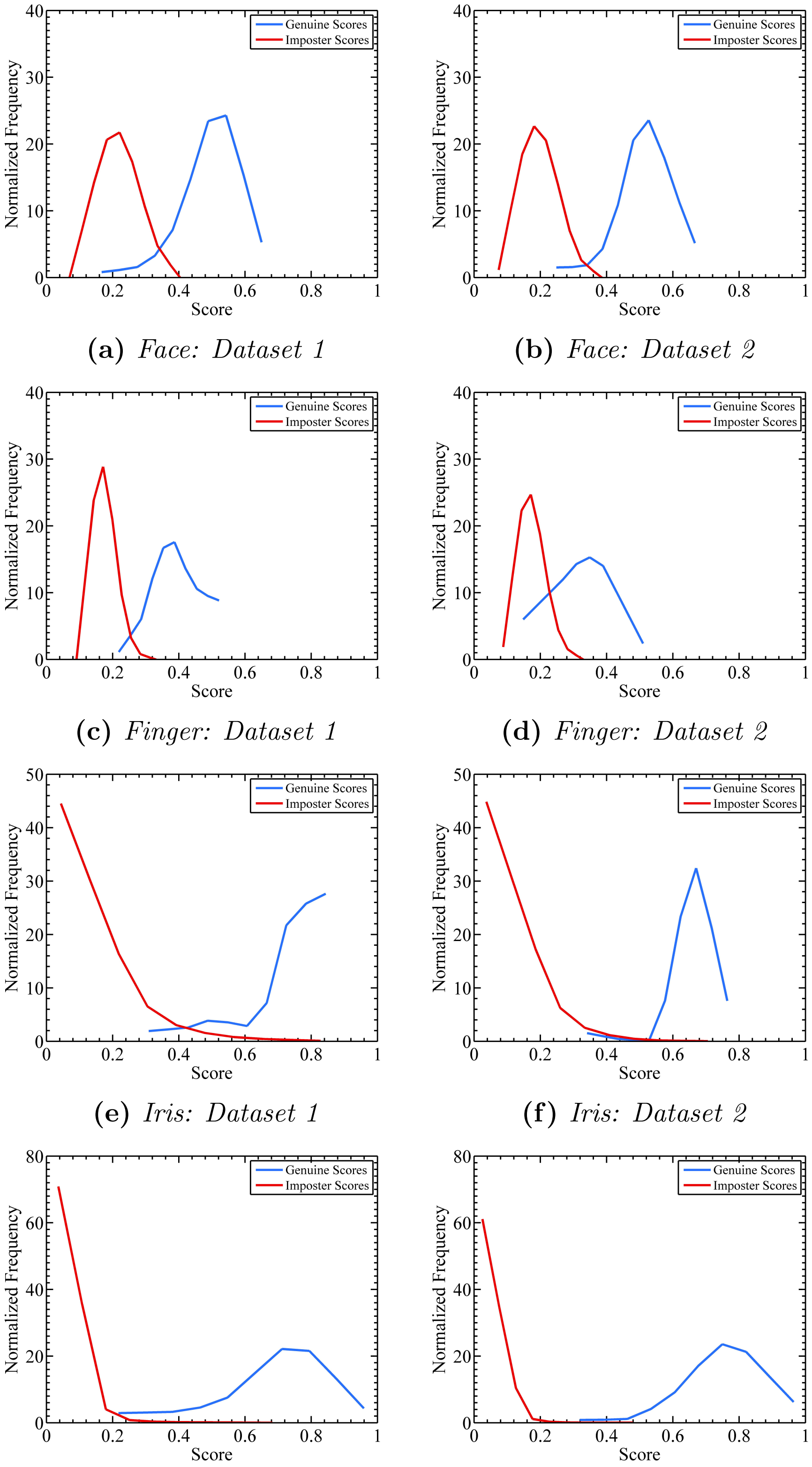
Fig. 3.3 *Comparision of Individual Classifier Scores with fused scores after boosting and suppression of (a) Genuine Scores and (b) Imposter scores*

Hence, score values change adaptively depending upon their distance from the threshold value. These two steps largely contribute to the boosting and suppression of individual classifier match scores and add to the adaptive nature of the proposed biometric system. Boosting factor calculated from these two steps determines the amount of boosting and suppression to be performed and is used during the final score fusion process. This also leads to a higher separation between the peaks of genuine and imposter score distribution. The score distributions for individual classifiers as well as fusion model are presented in Fig. 3.4. The figure shows frequency of scores for genuine and imposter users denoted by red and blue plots. The plots clearly show that the average imposter score value is very low as compared to average genuine values. Reliability factor (α) is also introduced corresponding to every individual input probe image depicting its reliability depending upon the environmental conditions, equipment used, etc. This reliability factor is computed using no-reference image quality scores provided by BRISQUE. If the input probe image possesses high noise, its quality will be low and vice-versa which helps in addressing various environmental challenges.

The frequency distribution of genuine and imposter scores of all 3 individual classifiers shows the smaller distance between peak values. This is generally due to irregularities in captured images, noise, and other environmental conditions. It basically represents a high rate of false acceptance and false rejection with smaller distance resulting in the decreased overall efficiency of the individual classifiers. On the other hand frequency distribution of scores for the proposed biometric system clearly shows the larger distance between Genuine and imposter classes and is also depicted in the quantitative analysis of results obtained.

3.2.2.2 Quantitative Validation

Quantitative analysis of the proposed system is performed on the basis of accuracy analysis, adaptivity analysis, and time-complexity analysis.



(a) *Face: Dataset 1* **(b)** *Face: Dataset 2*

(c) *Finger: Dataset 1* **(d)** *Finger: Dataset 2*

(e) *Iris: Dataset 1* **(f)** *Iris: Dataset 2*

(g) *Proposed Method: Dataset 1* **(h)** *Proposed Method: Dataset 2*

Fig. 3.4 *Frequency Distribution Curves for D1 and D2 databases for (a) Face images over D1 (b) face images over D2(c) Fingerprint images over D1(d) Fingerprint images over D2 (e) Iris images over D1 (f) Iris images over D2(g) Proposed Method over D2 database (h) Proposed Method over D2 database*

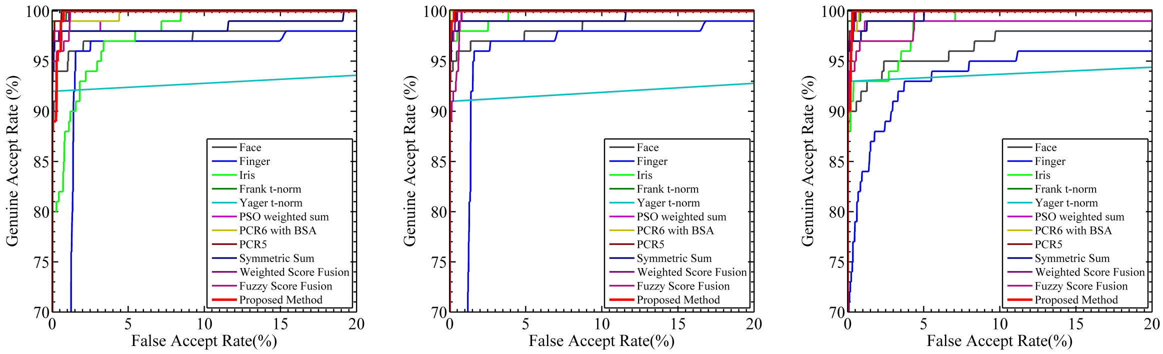
3.2.2.2.1 Accuracy Analysis .

The accuracy of the proposed system is analyzed using performance metrics namely EER, DI, and RI. The performance of the proposed method is compared with state-of-the-art techniques using these metrics as well. EER, DI, and RI values for various methods viz. T-norms (2011)[32], score fusion using PCR5 (2018) [93], score fusion using PCR6 with BSA (2019) [120], PSO weighted sum (2009) [100], Symmetric Sum (2018) [10], weighted score fusion (2014) [99] and fuzzy approach based score fusion (2016) [19] are compared with the proposed fusion method in Table. 3.1

TABLE 3.1: Comparison of EER, DI, and RI values for D1, D2 and D3 databases

DB / Method	**D1 Database**			**D2 Database**			**D3 Database**			**D4 Database**		
	EER	**DI**	**RI**	**EER**	**DI**	**RI**	**EER**	**DI**	**RI**	**EER**	**DI**	**RI**
Face	3.98±0.23	3.88±0.35	95±0.75	2.99±0.19	4.58±0.37	95±0.75	5.01±0.21	4.11 ±0.19	93±0.50	3.33±0.28	4.50 ±0.26	95±0.50
Finger	2.97±0.20	2.77±0.42	89±0.50	3.04±0.24	2.78±0.28	90±0.45	6.02±0.17	2.33±0.31	88±1.00	3.60±0.12	2.19±0.42	90±0.75
Iris	3.47±0.32	4.96±0.42	88±1.11	2.88±0.24	7.51±0.46	88±1.11	4.01±0.25	5.79±0.18	92 ±0.80	3.34 ±0.13	5.61±0.27	91±1.00
Frank t-norm [32]	0.95±0.12	5.46±0.11	98±0.11	0.11±0.08	4.52±0.18	98±0.11	0.92±0.29	4.59±0.22	99±0.20	1.02±0.21	4.18±0.29	98±0.10
PCR5 [93]	0.79 ±0.26	5.13±0.16	98±0.31	0.20±0.15	7.98±0.21	99±0.15	0.22±0.17	7.67±0.14	98±0.40	0.69±0.16	6.83±0.15	98±0.20
PCR6 with BSA [120]	0.99±0.22	5.78±0.28	98±0.51	0.78±0.22	7.82±0.18	98±0.35	0.87±0.16	7.56±0.17	99±0.10	0.91±0.23	5.80±0.25	98±0.25
PSO wtd. sum [100]	1.99±0.27	5.17±0.29	97±0.51	0.89±0.27	6.88±0.19	98±0.55	1.06±0.19	6.23±0.12	98±0.45	1.47±0.29	5.61±0.29	98±0.50
Symmetric sum [10]	2.00±0.31	4.93±0.35	95±0.47	1.00±0.23	7.20±0.18	98±0.55	1.14±0.19	4.17±0.13	96±0.75	1.64±0.17	5.12±0.25	96±0.60
Yager t-norm [32]	4.0±0.36	2.62±0.21	90±0.41	4.50±0.31	2.23±0.33	90±0.50	3.50±0.38	2.64±0.25	91±0.60	4.21±0.27	2.57±0.43	90±1.00
Weighted Score Fusion [99]	1.01±0.26	5.11±0.11	97 ±0.45	0.74±0.21	6.36±0.23	97 ±0.50	0.76±0.28	6.16±0.26	97 ±0.50	0.87±0.25	5.39±0.29	97±0.50
Fuzzy Score Fusion [19]	1.08±0.21	4.92±0.24	99±0.50	0.88±0.31	4.18±0.23	95±0.40	2.99±0.27	3.52±0.14	96±0.50	1.65±0.18	2.95±0.34	97±0.45
Proposed Method	0.87±0.14	5.14±0.34	98±0.64	0.11±0.05	7.95±0.43	98±0.64	0.16±0.10	6.71±0.22	99±0.50	0.61±0.16	5.96±0.39	99±0.45

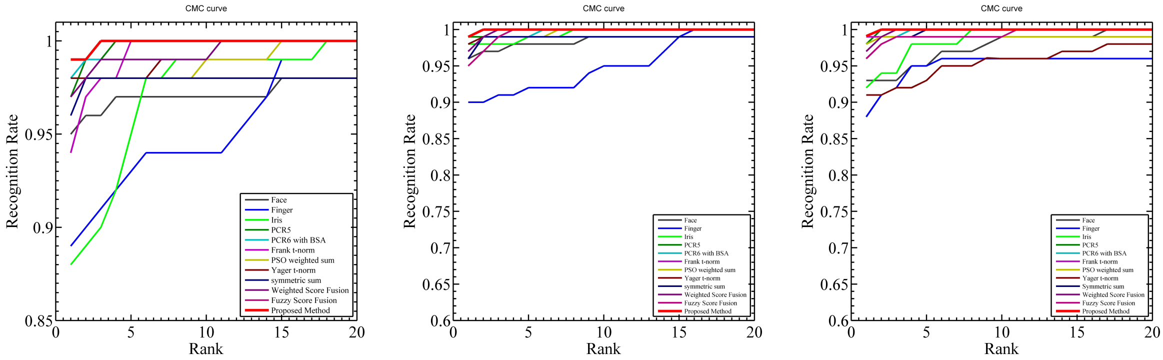
The EER value for proposed score level fusion method is 0.87 for D1 database, 0.11 for D2 database, 0.16 for D3 database and 0.61 for consolidated D4 database which is lowest in comparison with other state-of-the-art methods. The efficiency of the proposed system is also depicted by high decidability value of 5.14 for D1 database, 7.95 for D2 database, 6.71 for D3 database and 5.96 for D4 database and supported by ROC and CMC curves in Fig. 3.5 and 3.6 respectively. It is due to boosting and suppression of match scores which effectively distinguishes between Genuine and Imposter classes by creating a clear decision boundary. The variation among EER values is due to the use of different datasets and five-fold cross validation.



(a) *D1 Database* **(b)** *D2 Database* **(c)** *D3 Database*

Fig. 3.5 *Performance comparision of evaluated methods: ROC curves for D1, D2 and D3 database (a) ROC curves for various fusion techniques over Database D1 (b) ROC curves for various fusion techniques over Database D2 (c) ROC curves for various fusion techniques over Database D3*

Quantitative analysis reveals that limitations of individual classifiers were effectively addressed by the proposed fusion method providing higher accuracy and more reliable results. The complimentary traits are fused together making system adaptive to dynamic environmental conditions and robust against spoofing attacks. The Roc curves in Fig. 3.5 and CMC curves in Fig. 3.6 shows the proposed fusion method performs better in comparison to single modality as well as other fusion methods.

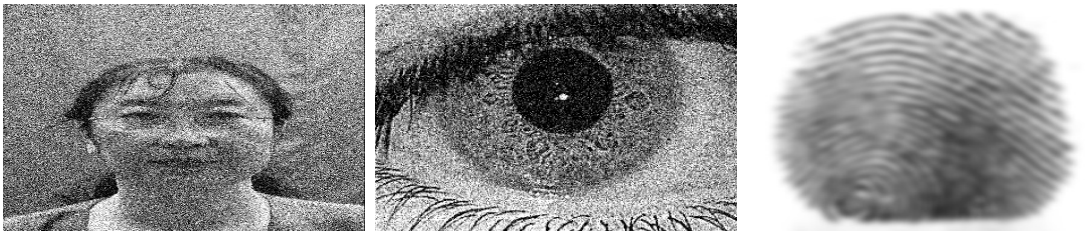


(a) *D1 Database* **(b)** *D2 Database* **(c)** *D3 Database*

Fig. 3.6 *CMC curves for D1, D2 and D3 databases (a) comparison of CMC curves of various fusion techniques over Database D1 (b) comparison of CMC curves of various fusion techniques over Database D2 (c) comparison of CMC curves of various fusion techniques over Database D3*

3.2.2.2.2 Adaptivity Analysis .

To prove the adaptive nature of the proposed system, a new database was created by introducing extra noise to the original database which imitates acquired samples in a dynamic environment and spoofing attacks. For this purpose, Gaussian noise with $\sigma = 0.05$ and offset $\delta = 0.01$ was introduced in iris and face images while for fingerprint images a Gaussian filter with a standard deviation of 0.4 is used. Sample images from the noise-induced database are shown in Fig. 3.7



(a) *Gaussian Noise* **(b)** *Gaussian Noise* **(c)** *Blurred*

Fig. 3.7 *Sample images from Noisy database*

Matching scores were calculated using noisy images as input probe images and the performance of the proposed biometric system was evaluated. During the fusion process, firstly, the noise was introduced in a single modality followed by noise introduction in two modalities and in the end noise was introduced in all three modalities and system's performance was measured in form of EER as tabulated in Table 3.2.

TABLE 3.2: Comparision of EER values for D1, D2 and D3 databases after adding Noise

Noise in modality	**D1 Database**	**D2 Database**	**D3 Database**
$\bar{f}pi$	2.01±0.23	1.00±0.32	2.43±0.28
$f\bar{p}i$	1.80±0.17	0.15±0.21	0.91±0.15
$fp\bar{i}$	2.08±0.32	2.86±0.36	2.01±0.41
$\bar{f}\bar{p}i$	2.95±0.22	1.99±0.38	3.49±0.57
$\bar{f}p\bar{i}$	4.98±0.65	24.27±2.61	16.42±1.95
$f\bar{p}\bar{i}$	4.99±1.23	4.01±1.66	3.45±1.35
$\bar{f}\bar{p}\bar{i}$	39.85±4.72	58.07±5.81	60.78±5.08

where $\bar{f}$, $\bar{p}$, $\bar{i}$ represents noisy modality for face, finger, and iris respectively. Low EER values indicate that the proposed system is able to give optimal performance when noise is introduced in one or two modalities. This represents dynamic environmental conditions where the acquired input probe image contains noise. The performance of system exponentially decreases when the input probe images from all three modalities were noisy. This represents a spoofing attack situation where synthetic/reconstructed samples with poor image quality are used. Thus the proposed multimodal biometric system is adaptive in nature withstanding dynamic environmental conditions and robust against spoofing attacks.

3.2.2.2.3 Time Complexity Analysis .

The computational efficiency of the proposed system is analyzed though time-complexity analysis of score fusion process of various methods. The time taken per subject by the proposed system is compared with other state-of-the-art methods in Table 3.3. It is evident from the results that the performance of the proposed method is comparable to other methods and better than its unimodal counterparts. The proposed method not only shows high performance but also provided added advantages after incorporating reliability factor.

Table 3.3: Comparision of time complexity for various Biometric recognition methods

Method	**Time(ms)**
Face	29.08
Finger	17.37
Iris	20.81
PCR5 [93]	17.43
PCR6 with BSA [120]	20.44
PSO wtd. Sum [100]	29.16
Symmetric Sum [10]	23.56
Frank t-norm [32]	20.26
Yager t-norm [32]	21.85
Weighted Score Fusion [99]	22.15
Fuzzy Score Fusion [19]	51.85
Proposed Method	20.56

In sum, the proposed fusion model optimally fuses complementary features making it adaptive to the dynamic environment and robust against spoofing attacks. Various facial distortion, iris off-angle blur, and insufficient boundary information in fingerprints limits the performance of individual classifiers and is also revealed in quantitative analysis. On the other hand, the proposed fusion method not only overcome these limitations by adaptively combining individual classifiers but also makes the system robust against spoofing attacks. An adaptive fusion is performed by boosting and suppression of match scores.

Image quality is incorporated which boosts the adaptive nature of the proposed system under dynamic environment and robustness against spoofing attacks as compared with other state-of-the-art methods. The performance of the proposed method is validated with high decidability index, recognition index and low EER value are compared with other state-of-the-art methods. Moreover, lower time complexity makes the proposed system suitable for various real-time industry and security application. Hence, the proposed system shows improved performance along with adaptivity under dynamic environment and robust against spoofing attacks.

3.3 Significant Findings

The following were significant findings of the proposed adaptive multimodal biometric system with score level fusion.

- An adaptive multimodal biometric system using score fusion technique is proposed having three complimentary modalities namely fingerprint, iris and face.
- Boosting of concurrent classifier scores and suppression of discordant classifier scores is performed simultaneously. This approach creates a clear and distinguished decision-boundary between an imposter and a genuine class.
- The reliability factor is calculated using no-reference quality measurement techniques for each modality. This not only adds to its adaptive nature but also makes it more robust under a dynamic environment and against spoof attacks.
- The proposed method is experimentally validated over three multimodal chimeric datasets generated using benchmarked images. The results depict high performance,

low error rate and better detection of fake biometrics as compared to state of the art techniques.

The experimental results along with other findings were published in [28].

Chapter 4

Multimodal Biometric System with Optimal Fusion

Chapter 4

Multimodal Biometric System with Optimal Fusion

Multimodal Biometric systems combine information from multiple sources to reach a final decision. Score level fusion combines outcomes of individual classifiers to make a final decision. However, most of the biometric systems suffer from the issue of score confliction of individual classifiers. Similarly, during feature level fusion, individual feature vectors also need to be optimized so that they can be compatible for fusion. Further, the length of feature vectors also needs to be optimized so as to reduce the overall space complexity. To resolve these issues, we have proposed a novel optimized score level fusion using Grasshopper optimization where the performance optimization of individual classifiers is performed and a concurrent solution is achieved by means of proportional conflict redistribution rules. Here, two complementary biometric features viz. fingerprint and iris are used. These biometric traits offer convenience along with the availability of economical devices. While fingerprint is very easy to use, iris pattern is invariant over long term and hard to spoof. Thus, proposed system provides high security and robustness while being economical. Also, same biometric are used for optimal feature level fusion to generate cancelable templates. The proposed system not only provides high performance but also reduce overall space requirement by 75%. Further, the proposed system is adaptive to dynamic environmental changes and robust against various security threats.

4.1 Proposed methodology for Optimal Fusion

The process of fusion is paramount in any multimodal biometric system. However, conflict among individual classifier scores need to beresolved. Also, biometric features can be of varying length and occupy more space leading to scalability issues. Thus, there is a need to optimize these features and scores so as to improve the overall performance of the system and also reduce its space complexity. Next sub-section describes the architecture and performance analysis of the optimized Feature level fusion technique.

4.1.1 Optimized Feature Level Fusion

We have proposed a feature level fusion method with template protection. The proposed method is not only adaptive but also robust against various attacks. Fig. 4.1 represents the architecture of the proposed system. Here, a cancelable template is generated by optimal fusion of Iris(i) and Fingerprint(f) modalities with user-specific keys.

Features from iris modality are extracted by image pre-processing combined with Local Binary Pattern(LBP) [65]. Also, features from fingerprint modality are extracted by first performing binarization and thinning operations. Next, minutiae-based features are generated from the input image.

Feature points at i^{th} position of the iris feature vector is considered as abscissa and fingerprint feature as ordinate. Combining them together, a point (χ_i, ψ_i) is defined in a

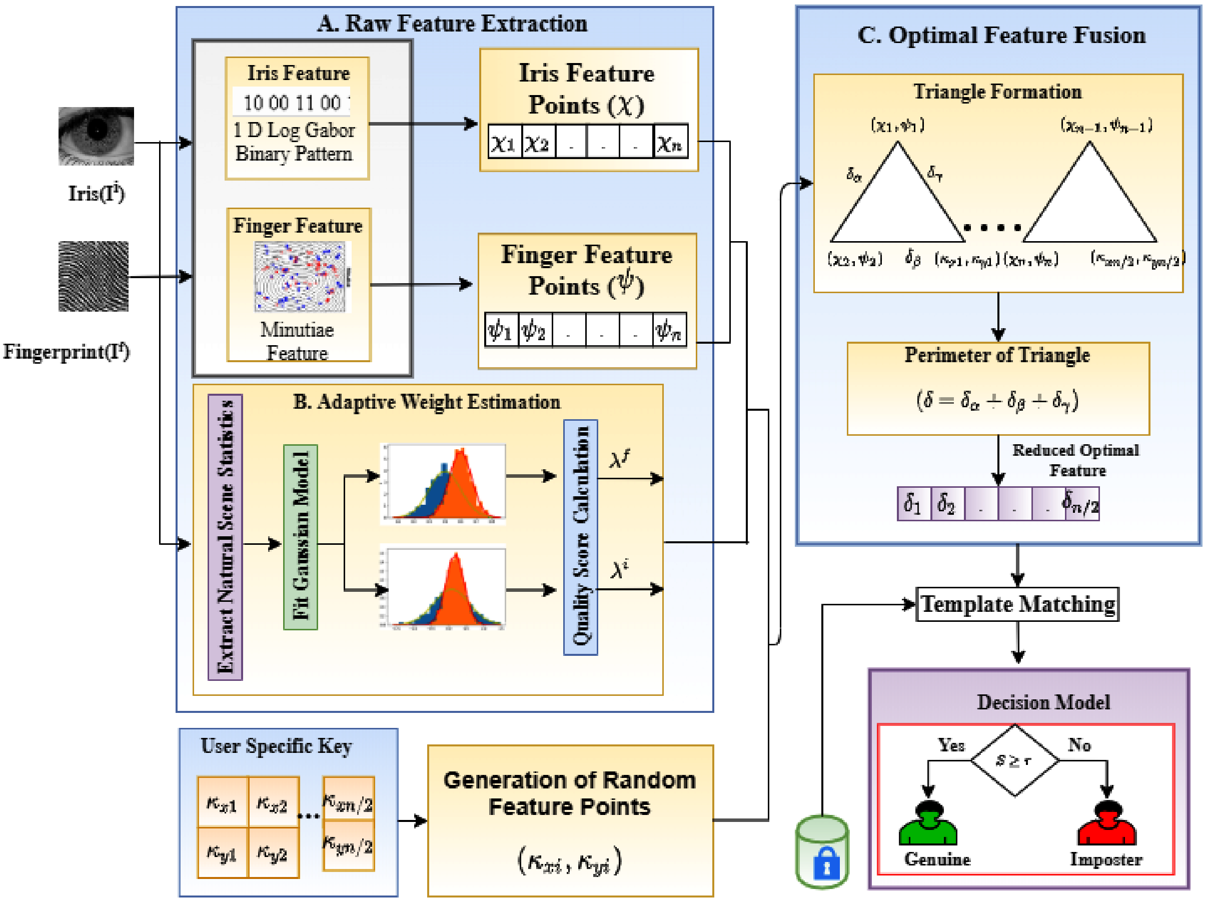

A. Raw Feature Extraction
Iris Feature
10 00 11 00
1 D Log Gabor Binary Pattern
Finger Feature
Minutiae Feature
Iris(I^i)
Fingerprint(I^f)
Iris Feature Points (χ)
χ_1 χ_2 . . . χ_n
Finger Feature Points (ψ)
ψ_1 ψ_2 . . . ψ_n
B. Adaptive Weight Estimation
Extract Natural Scene Statistics
Fit Gaussian Model
Quality Score Calculation
λ^f
λ^i
C. Optimal Feature Fusion
Triangle Formation
(χ_1, ψ_1)
(χ_{n-1}, ψ_{n-1})
δ_α
δ_γ
(χ_2, ψ_2)
δ_β
$(\kappa_{x1}, \kappa_{y1})$
(χ_n, ψ_n)
$(\kappa_{xn/2}, \kappa_{yn/2})$
Perimeter of Triangle
$(\delta = \delta_\alpha + \delta_\beta + \delta_\gamma)$
Reduced Optimal Feature
δ_1 δ_2 . . . $\delta_{n/2}$
Template Matching
Decision Model
Yes
$s \geq \tau$
No
Genuine
Imposter
User Specific Key
κ_{x1} κ_{x2} ... $\kappa_{xn/2}$
κ_{y1} κ_{y2} $\kappa_{yn/2}$
Generation of Random Feature Points
$(\kappa_{xi}, \kappa_{yi})$

Fig. 4.1 *Overview of the proposed optimal fusion scheme scheme. Input sample quality is evaluated and combined with extracted features from the input query images. Feature Vectors and user key is used to generate triangle. The perimeter of each triangle is computed and combined together to generate a cancelable template. This is compared with stored templates to evaluate similarity score to reach a final decision.*

cartesian coordinate system. Similarly, $(i+1)^{th}$ feature points are used to create a second point. Further, one more point $(\kappa_{xi}, \kappa_{yi})$ is extracted from a user-specific key. These three points are used to plot a triangle whose perimeter δ_i is computed. The perimeter values for all subsequent triangles are concatanated together to generate a fused cancelable template. A similarity score is calculated by matching the generated template with the stored templates in the database. Finally, the match score is compared with an optimal threshold value to reach a final decision. The proposed system is adaptive in nature as image quality is used. The in-depth details of the proposed system are presented in the next subsection.

4.1.1.1 Multimodal Feature Extraction

Biometric modalities viz. iris and fingerprint are processed using feature extraction techniques to determine individual feature vectors. For fingerprint features are extracted using a minutiae-based technique which is widely used by researchers [20, 102] as it provides low complexity with high performance. For this, first of all, binarization and thinning operations are performed as a pre-processing step on input query fingerprint image I^f. Binarization operation helps in increasing the contrast between ridges and valleys as shown in Eq. 4.1

$$B\left(x,y\right) = \begin{Bmatrix} 1, & if\ I\left(x,y\right) \geq \ h \\ \\ 0, & otherwise \end{Bmatrix} \tag{4.1}$$

Where $I\left(x,y\right)$ shows intensity value at pixel position (m,n) and h represents the value of threshold. Also, a thinning operation is used to reduce ridges to the unit-pixel thickness and is carried out using in-built morphological functions in the Matlab platform on binary images. Rutovitz crossing number (CN) is computed by locating the minutiae over the thinned image using a sliding window of size 3x3 in an anti-clockwise manner [102]. The CN defines the minutia type and is calculated using Eq. 4.2

$$CN = \frac{1}{2}\sum_{k=1}^{8}|p_k - p_{k-1}| \tag{4.2}$$

Where p_k is the pixel values of immediate neighbors for pixel k. The value of CN is used to classify ridge pixel as isolated, continuing, ending, crossing point and bifurcation.

Further, minutia is represented as a vector $m = [x, y, CN, \theta]$ having (x, y) as the pixel coordinates and θ as angle of orientation. For input fingerprint query image I^f, an extracted feature vector, η^f is created by combining n minutiae using Eq. 4.3

$$\eta^f = [m_1, m_2, \dots m_n] \tag{4.3}$$

For iris feature extraction, input iris image I_i is pre-processed involving localization and normalization processes. In the first step, an integro-differential operator is used for localizing iris and pupillary boundaries. In the second step, Daugman's rubber sheet model [12] is used to normalize the localized iris into a fixed-sized rectangular block. Further, the processed image is quantified using the histogram of LBP. From LBP histogram values $l_1, l_2 \dots l_n$, feature vector for iris η^i is generated using Eq. 4.4

$$\eta^i = (l_1, l_2 \dots \dots l_n) \tag{4.4}$$

This creates a unique pattern, generating iris feature η^i. The extracted feature vectors η^i and η^f are fused together using the proposed method to generate a cancelable feature which is discussed in the next subsection.

4.1.1.2 Optimal Feature Fusion Approach

In the proposed fusion scheme, every user is provided with a unique key (κ^k), where $k \in [1, N]$ to generate a random feature point in cartesian coordinate system as shown in Eq. 4.5.

$$\kappa^k = \begin{bmatrix} \kappa^k_{x1} & \kappa^k_{x2} & . & . & \kappa^k_{xn/2} \\ \\ \kappa^k_{y1} & \kappa^k_{y2} & . & . & \kappa^k_{yn/2} \end{bmatrix} \tag{4.5}$$

Here k represents the k^{th} user. The length of the key is half to the length of feature vectors and consists of two rows containing abscissa and ordinate values for each point randomly distributed in the range [-1000, 1000]. The random points generated using user-specific key are used in plotting a triangle. In this, feature vectors obtained during the feature extraction process are optimaly fused together using proposed technique. Each feature point of the iris feature vector is considered as abscissa and each feature point of the fingerprint feature vector is considered as ordinate in a cartesian coordinate system. In case of different feature size, padding can be used so that every feature vector contain an equal number of feature points. Moreover, the abscissa and ordinates at the corresponding positions are combined to describe a point(Q) (χ, ψ) such that any user can be defined as in Eq. 4.6.

$$\upsilon = \begin{bmatrix} (\chi_1, \psi_1) & (\chi_2, \psi_2) & (\chi_3, \psi_3) & . & . & (\chi_n, \psi_n) \end{bmatrix} \tag{4.6}$$

For simplicity, the above equation can also be represented as shown in Eq. 4.7

$$\upsilon = \begin{bmatrix} Q_1 & Q_2 & Q_3 & . & . & Q_n \end{bmatrix} \tag{4.7}$$

Also, as discussed above, each user is provided with a unique user-specific key (κ^k) of dimension $2 \times n/2$. The key is used to create different random points R_i in cartesian system. Further, a triangle is plotted with Q_i, Q_{i+1} and R_i as its vertices as shown in Figure 4.2

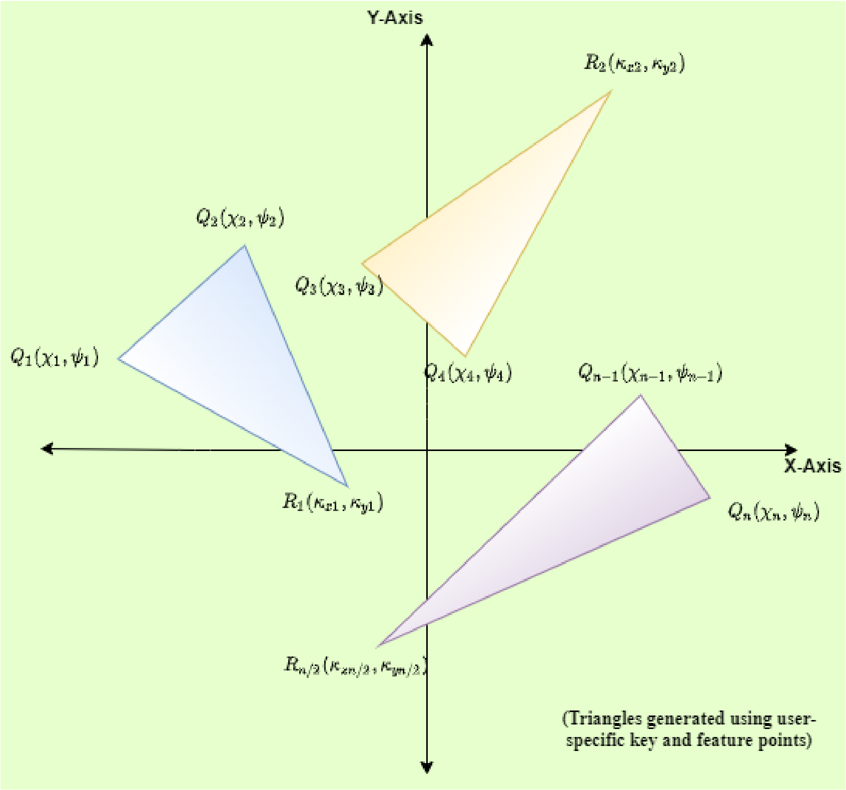

Y-Axis
$R_2(\kappa_{x2},\kappa_{y2})$
$Q_2(\chi_2,\psi_2)$
$Q_3(\chi_3,\psi_3)$
$Q_1(\chi_1,\psi_1)$
$Q_4(\chi_4,\psi_4)$
$Q_{n-1}(\chi_{n-1},\psi_{n-1})$
X-Axis
$R_1(\kappa_{x1},\kappa_{y1})$
$Q_n(\chi_n,\psi_n)$
$R_{n/2}(\kappa_{xn/2},\kappa_{yn/2})$
(Triangles generated using user-specific key and feature points)

Fig. 4.2 *Triangle generation from feature points using user-specific key*

For each triangle, its perimeterδ_i is calculated as Eq. 4.8.

$$\delta = \delta_\alpha + \delta_\beta + \delta_\gamma \tag{4.8}$$

where $\delta_\alpha, \delta_\beta, \delta_\gamma$ represents the length of three sides of the triangle. In the last step, the perimeter(δ) values corresponding to each triangle for k^{th} user, are concatenated together to generate a fused vector ζ^k that is cancelable, non-invertible in nature and reduced size as shown in Eq. 4.9.

$$\zeta^k = (\delta_1, \delta_2, \delta_3, ...\delta_{n/2}) \tag{4.9}$$

The size of generated template is half of the length of original feature vector and occupies only 25% of the actual space. Further, in case of template theft, if perimeter (δ) values are compromised, it will lead to ambiguous values of the vertices of triangle and original feature points will not be exposed. Thus, the generated template is highly non-invertible and robust against theft. The cancelable feature obtained is compared with the stored templates to generate a final match score(S). The final decision is performed based on an optimal threshold value (τ), if the match score(S) is greater than τ, then it is considered as Genuine else imposter. The next section provides details of the architecture of the optimal score fusion method.

4.1.2 Optimized Score Level Fusion

In this section, a novel authentication system combining two different features viz. fingerprint and iris is proposed. Its architecture is shown in Fig. 4.3.

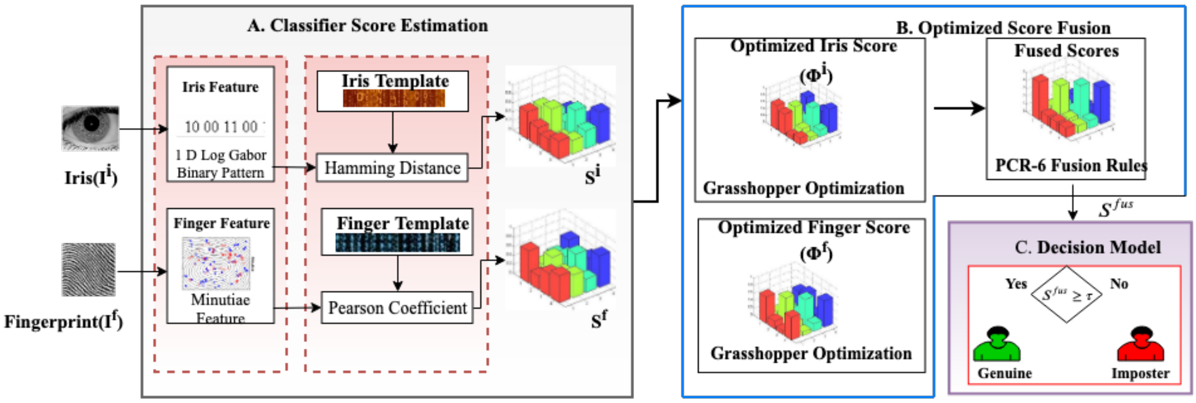


Fig. 4.3 *Overview of the Proposed Multimodal Biometric System*

As shown above, input biometric images are subjected to feature extraction process and corresponding feature vectors are obtained. During, iris feature extraction, rectangular iris sheets are obtained using daugman method on which 1-D log Gabor filter is applied. The output is converted into bits for various phases. Here, multiple bits are calculated corresponding to every pixel value which is used as a feature vector for captured iris modality. Also. for fingerprint modality, input image is processed to extract minutiae from which false minutiae are removed to increase accuracy. Further, feature vectors thus obtained are matched with templates stored in database to generate individual match scores S^i and S^f. In the next stage, optimized score fusion takes place, which consists of two stages. Firstly, individual classifier scores are optimized using Grasshopper Optimization Algorithm (GOA) [89] followed by fusion of optimized scores using PCR-6 fusion rules. The Grasshopper Optimization Algorithm (GOA) to determine an optimized weight is discussed in next section.

4.1.2.1 Grasshopper Optimization Algorithm

This is a nature-inspired algorithm which follows the swarming behavior of grasshoppers. Saremi et al. proposed this algorithm to calculate the shape of architectural structures [89]. The movement of the grasshoppers is mainly influenced by three factors: gravity force, wind advection and social interaction. The swarm behavior can be mathematically represented as:

$$Z_i = F_i + W_i + S_i \tag{4.10}$$

where Z_i represents position of the i^{th} grasshopper. F_i, W_i and S_i indicate the gravity force, wind advection and social interaction on the i^{th} grasshopper, respectively. However, instead of using Eq. 4.10, an improved version is generally used to solve problems which is defined as

$$Z_i^d = \alpha \left(\sum_{n=1, n \neq m}^{N} \alpha \frac{ub_d - lb_d)}{2} \beta \left(\left| x_n^d - x_m^d \right| \right) \frac{x_n - x_m}{d_{mn}} \right) + \widehat{T}_d \tag{4.11}$$

where ub_d and lb_d is the upper and lower bound in the d^{th} dimension, respectively. $\widehat{T}_d$ shows value corresponding to best solution obtained of the d^{th} dimension. $d_{mn} = \left| x_n - x_m \right|$ shows the distance between the m^{th} grasshopper and n^{th} grasshopper. β is a designed function that can be calculated by $\beta(r) = fe^{-r/l} - e^{-r}$. f and l are two constants. α helps in decreasing the number of iterations and also balances the optimization process. It is computed by

$$\alpha = \alpha_{max} - t \frac{\alpha_{max} - \alpha_{min}}{t_{max}} \tag{4.12}$$

where α_{max} and α_{min} are the maximum and minimum values, respectively. t represents current iteration and t_{max} represents the highest number of iterations.

4.1.2.2 Optimal fusion using PCR-6 rules

The proposed system combines two complementary biometric features viz. fingerprint and iris. Information from both the modalities is fused together using Shafer's model. During the authentication process, a person can be classified as either genuine or imposter. Both modalities provide different belief factor for a person. Final belief for the person is estimated by resolving conflicts among given biometric features. $m_f\,(gen)$ and $m_i(gen)$

represent belief masses for fingerprint and iris respectively. Moreover, the possibility of a person being imposter can be calculated for each trait by

$$m_j\,(imp) = \ 1 - m_j(gen) \tag{4.13}$$

Where $j \in \{f, i\}$ correspond to fingerprint and iris respectively.

Also, Conjunctive consensus can be calculated as

$$m_{fi}\,(gen) = \prod_{j=1}^{n} m_j\,(gen) \tag{4.14}$$

$$m_{fi}\,(imp) = \prod_{j=1}^{n} m_j\,(imp) \tag{4.15}$$

where $j \in \{f, i\}$. Moreover, overall conflict between the two modalities is estimated by adding partial conflicting masses of genuine and imposter scores of individual classifiers given by

$$\begin{aligned} m_{fi}\,(gen \cap imp) = m_f\,(gen) \times m_i\,(imp) + m_f\,(imp) \\ \times m_i\,(gen) + m_f\,(gen) \times m_i\,(gen) \end{aligned} \tag{4.16}$$

In the next step, 'gen' and 'imp' mass contribution is computed in redistribution using PCR – 6 rules.

$$\frac{x_1}{m_i(gen)} = \frac{y_1}{m_f(imp)} = \frac{m_i(gen) \times m_f(imp)}{m_i\,(gen) + m_f\,(imp)} \tag{4.17}$$

$$\frac{x_2}{m_i(imp)} = \frac{y_2}{m_f(gen)} = \frac{m_i(imp) \times m_f(gen)}{m_i\,(imp) + m_f\,(gen)} \tag{4.18}$$

overall weight is estimated as sum of x_j and y_j and their respective consensus

$$m_{pcr6}\,(gen) = m_{fi}\,(gen) + x_1 + x_2 \tag{4.19}$$

$$m_{pcr6}(imp) = m_{fi}\,(imp) + y_1 + y_2 \tag{4.20}$$

$m_{pcr6}(gen)$ and $m_{pcr6}(imp)$ shows the fused score for a person, whether to classify as genuine or an imposter. Next, the decision is made using an optimal threshold value to classify the person as either genuine or imposter.

4.2 Experimental Validation

The proposed systems are experimentally validated over multimodal chimeric databases. For this, various performance metrics like Equal Error Rate (EER), Decidability Index (DI), and Recognition Index (RI) are determined to estimate the system's performance. Also, their performance is compared with other state-of-the-art methods. The next subsection provides the detailed analysis of optimal feature fusion technique.

4.2.1 Optimal Feature Level Fusion

The performance analysis of the proposed system is performed over three different chimeric databases generated using benchmark images. The database and experimental details are discussed in the next section.

4.2.1.1 Database & Experimental Design

The multimodal datasets are obtained using images from various benchmark datasets for experimental validation. Here, the Chimeric datasets are created by uniquely combining benchmark datasets namely MCYT Bimodal Database [66], IITD PolyU iris database [47], Casia iris database (Casia-IrisV1, http://biometrics.idealtest. org/), FVC2006 DB1-A fingerprint database [8], and MMU2 iris database [2]. The experimental validation is performed on three chimeric datasets namely D1, D2, and D3. D1 contains fingerprint samples of N different subjects from the MCYT database (sensor 1) and IITD iris PolyU database. Thus a virtual multimodal dataset is created for N subjects by combining the above-mentioned datasets. Similarly, D2 is created by combining N distinct subjects from the MCYT database (sensor 2) and the Casia Iris-V1 database. Also, the D3 dataset is obtained by combining N distinct subjects from the MMU2 iris database and the FVC2006 DB1-A database. Further, all the subjects in D1, D2, and D3 databases are completely different. In addition, five-fold cross-validation is carried out to obtain balanced results. The proposed system is implemented over a hardware configuration of the Intel i3 processor and 4GB RAM using the MATLAB 2018a platform. The performance analysis of the proposed system is discussed in the next section.

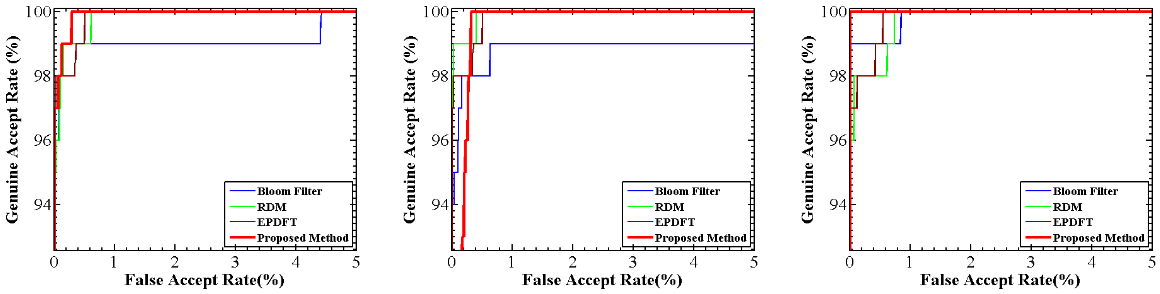
4.2.1.2 Performance Analysis

The proposed system's performance is quantitatively analyzed by means of various performance metrics namely Decidability Index (DI), Equal Error Rate (EER), and Recognition Index(RI). Also, the results thus obtained are compared with other state-of-the-art techniques. During this process, the same techniques for generic feature extraction and score calculation are used for evaluating other methods. The performance metric values for various methods viz. Random Distance Method (RDM) [41], Bloom Filters [25] and Enhanced Partial Discrete Fourier Transform (EP-DFT) [126] are compared with the proposed method in Table. 4.1

Table 4.1: Comparison of EER, DI, and RI values for D1, D2 and D3 databases

DB Method	D1 Database			D2 Database			D3 Database		
	EER	**DI**	**RI**	**EER**	**DI**	**RI**	**EER**	**DI**	**RI**
RDM[41]	0.60±0.23	7.28±0.35	97±0.25	0.40±0.19	7.68±0.37	98±0.75	0.71±0.21	7.11±0.19	99±0.50
Bloom Filter[25]	0.97±0.20	5.77±0.42	96±0.50	1.14±0.24	4.98±0.28	97±0.45	0.92±0.17	5.33±0.31	98±0.58
EPDFT[126]	0.49±0.32	7.96±0.42	98±1.11	0.78±0.24	6.21±0.46	97±0.90	0.61±0.25	5.79±0.18	97 ±0.80
Proposed Method	0.14±0.12	7.58±0.29	99±0.84	0.16±0.15	6.71±0.24	99±0.75	0.09±0.10	9.31±0.22	99±0.80

The EER value for the proposed optimal feature level fusion method is 0.14 for the D1 database, 0.16 for the D2 database and 0.09 for the D3 database which is lowest in comparison with other state-of-the-art methods is also supported by ROC curves in Fig. 4.4. ROC curves of various state-of-the-art techniques are plotted and compared for three different databases. The proposed method with red plot shows higher performance as compared to other techniques.



(a) *D1 Database* (b) *D2 Database* (c) *D3 Database*

Fig. 4.4 *Performance comparision of evaluated methods: ROC curves for D1, D2 and D3 database (a) ROC curves for various techniques over Database D1 (b) ROC curves for various techniques over Database D2 (c) ROC curves for various techniques over Database D3*

The efficiency of the proposed system is also depicted by a high decidability value of 7.58 for the D1 database, 6.71 for the D2 database and 9.31 for the D3 database and the variation among EER values is due to the use of different datasets and five-fold cross-validation. Further, Performance analysis reveals that the limitations of individual classifiers were effectively addressed by the proposed fusion method providing higher accuracy and more reliable results. The proposed system also optimize the features to reduce the overall space requirements. Next section describes the performance analysis of the optimized Score level fusion technique.

4.2.2 Optimal Score Level Fusion

The experimental validation is performed over a self-generated chimeric multimodal database. Further, the performance is measured by means of Equal Error Rate (EER) and Decidability Index (DI). Moreover, the proposed system is also compared with other state-of-the-art methods using these metrics.

4.2.2.1 Database Design

The self-generated multimodal chimeric dataset is generated using images from benchmark datasets to validate our proposed algorithm. Here, the images samples from MCYT Bimodal Database [66] and IITD PolyU iris database [47] are combined uniquely. Also, Sample images of chimeric multimodal dataset are shown in Fig. 4.5.

The self-generated chimeric dataset contains image samples from 100 distinct subjects from both benchmarked datasets.Thus, the virtual multimodal dataset created for 100 subjects having image samples for both fingerprint and iris modality. Also, three-fold cross-validation is performed using three different samples considering each sample as input once. For implementation purposes, the MATLAB 2016b platform is used along with a system configuration of 4GB RAM having Intel i5 processor.

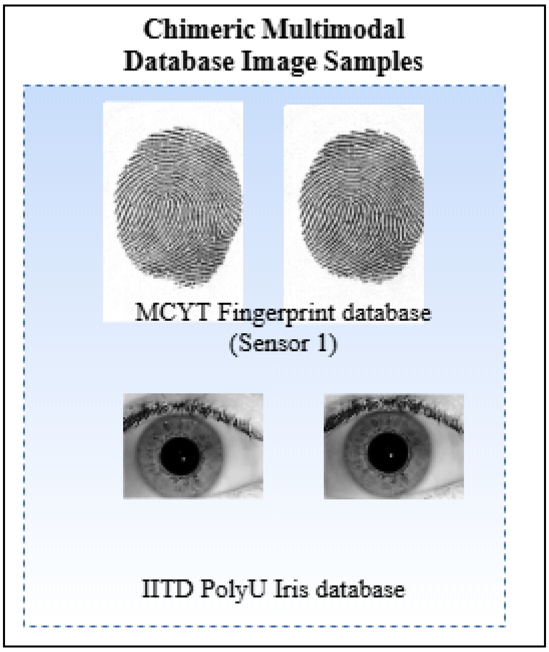


Fig. 4.5 *Multimodal database sample images*

4.2.2.2 Performance Validation

The performance validation of the proposed system is performed on the basis of EER and DI. Also, EER and DI values are compared with various state-of-the-art techniques as well. EER and DI values for various methods viz. PSO weighted sum [100], sum rule [44], min rule [44] and max rule [44] are compared with the proposed method in Table. 4.2

Table 4.2: DI and EER value Comparison for various methods

Method	**EER**	**DI**
Finger	2.97±0.10	2.77±0.31
Iris	3.47±0.22	4.96±0.46
Sum rule	1.15 ±0.25	4.83±0.26
Min rule	1.55±0.62	4.48±0.18
PSO wtd. sum	1.99±0.46	4.30±0.39
Max rule	1.50±0.72	4.55±0.25
Proposed Method	0.79±0.13	5.24±0.24

The proposed method shows an EER value of 0.79 and DI value of 5.24 for the self-generated chimeric multimodal database. Also, these values are best in comparison to other state-of-the-art and unimodal methods which proves the superiority of the proposed system. The variation in performance metric values is because of using three-fold cross validation. Performance validation shows that the proposed system effectively resolves the issues of individual classifiers by giving more accurate and reliable results. The complementary information from fingerprint and iris is fused which makes the system highly robust and economical to use as well.

4.3 Significant Findings

The significant findings for the proposed work are as follows:

- Multimodal biometric systems having iris and fingerprint modality have been proposed which overcomes the shortcomings of unimodal systems like universality, spoofing attacks, etc.
- Biometric features are optimized such that the final template occupies only 25% of the initial space requirement, thus reducing the overall space complexity.
- Individual classifier scores are optimized using Grasshopper Optimization Algorithm(GOA) which improves the overall system's performance and accuracy.
- The performance evaluation of the proposed methods evaluated over chimeric dataset shows high decidability index and low EER value as compared with other state-of-the-art methods.

- Also, the proposed systems exhibits very low response time making it suitable real world scenarios.

  In addition, the experimental results along with significant findings of the proposed work are published in [27]. Also, one more research article for optimal feature fusion is under review in an SCIE Journal.

Chapter 5

Multimodal Template Protection Framework

Chapter 5

Multimodal Template Protection Framework

Most of the biometric systems suffer from single point of failure. Thus, security at multiple levels are required to address single point of failure. Also, the security of biometric data should be of top priority as biometric information cannot be replaced easily. If biometric templates are stolen, the user's identity is compromised for multiple applications and subject to cross-application attacks as well. Overall, it not only threatens the security, but it may also incur a significant financial or social loss. To resolve these issues, cancelable biometrics is widely used. On the basis of above discussion, a cancelable biometric system with multiple points of security is developed which is discussed in next section.

5.1 Proposed Cancelable Biometric System

Fig. 5.1 represents the architecture of the proposed system. In this, a cancelable template is generated for Iris(i) and Fingerprint(p) features using the proposed technique with user-specific keys.

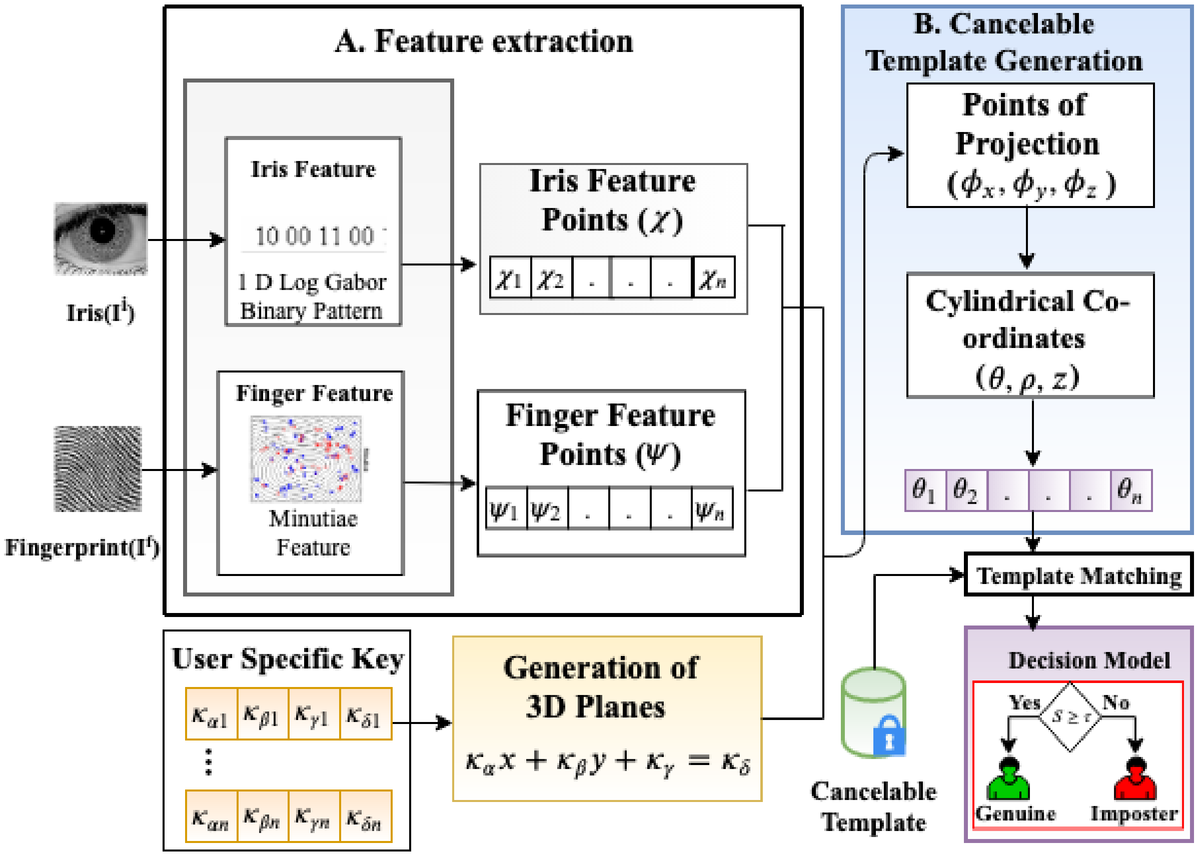

A. Feature extraction
Iris Feature
10 00 11 00
1 D Log Gabor Binary Pattern
Finger Feature
Minutiae Feature
Iris Feature Points (χ)
χ_1 χ_2 . . . χ_n
Finger Feature Points (Ψ)
ψ_1 ψ_2 . . . ψ_n
Iris(I^i)
Fingerprint(I^f)
B. Cancelable Template Generation
Points of Projection (ϕ_x, ϕ_y, ϕ_z)
Cylindrical Co-ordinates (θ, ρ, z)
θ_1 θ_2 . . . θ_n
Template Matching
Decision Model
Yes
$S \geq \tau$
No
Genuine
Imposter
User Specific Key
$\kappa_{\alpha 1}$ $\kappa_{\beta 1}$ $\kappa_{\gamma 1}$ $\kappa_{\delta 1}$
$\kappa_{\alpha n}$ $\kappa_{\beta n}$ $\kappa_{\gamma n}$ $\kappa_{\delta n}$
Generation of 3D Planes
$\kappa_\alpha x + \kappa_\beta y + \kappa_\gamma = \kappa_\delta$
Cancelable Template

Fig. 5.1 *Overview of the proposed cancelable template generation scheme. Extracted features from the input query image are projected onto a plane obtained using a user-specific key. The points of projection are transformed into cylindrical coordinates to generate cancelable templates. These are compared with stored templates to evaluate similarity score to reach a final decision.*

The proposed cancelable biometric system takes two biometric modalities viz. iris and fingerprint and feature vectors are extracted. For extracting features from iris modality, image pre-processing combined with Local Binary Pattern(LBP) [65] is performed[13]. LBP not only provides low computation but also immune to changes in image grey levels. For fingerprint modality, the input query image is preprocessed by performing binarization and thinning operations. Next, feature extraction is performed to generate minutiae-based features from the input image.

Feature points at i^{th} position of the iris feature vector is considered as abscissa and fingerprint feature as ordinate. Combining them together, a point (χ_i, ψ_i) is defined in a cartesian coordinate system. Each point thus obtained is projected onto a plane corresponding to each feature point obtained using a user-specific key. The points of projection thus obtained are transformed into a cylindrical space to obtain corresponding feature points. The azimuth values are considered for generating cancelable templates so as to achieve non-invertibility. A similarity score is calculated by matching the generated feature with the stored templates in the database. Finally, the match score is compared with an optimal threshold value to reach a final decision. The proposed system is non-invertible in nature as only the azimuth values are considered for generating the cancelable templates. The in-depth details of the proposed system are presented in the next subsection.

5.1.1 Multimodal Feature Extraction

Biometric modalities viz. iris and fingerprint are processed using feature extraction techniques to determine individual feature vectors. For fingerprint features are extracted using a minutiae-based technique which is widely used by researchers [20, 102] as it provides low complexity with high performance. For this, first of all, binarization and thinning operations are performed as a pre-processing step on input query fingerprint image I^f. Binarization operation helps in increasing the contrast between ridges and valleys as shown in Eq. 5.1

$$B\left(x,y\right)=\left\{\begin{array}{cc} 1, & if\ I\left(x,y\right)\geq\ h \\ \\ 0, & otherwise \end{array}\right\} \tag{5.1}$$

Where $I\left(x,y\right)$ shows intensity value at pixel position (m,n) and h represents the value of threshold. The threshold value is calculated using Otsu's method to evaluate global threshold for an image [67]. Also, a thinning operation is used to reduce ridges to the unit-pixel thickness and is carried out using in-built morphological functions in the Matlab platform on binary images. Rutovitz crossing number (CN) is computed by locating the minutiae over the thinned image using a sliding window of size 3x3 in an anti-clockwise manner [102]. The CN defines the minutia type and is calculated using Eq. 5.2

$$CN = \frac{1}{2}\sum_{k=1}^{8} |p_k - p_{k-1}| \tag{5.2}$$

Where p_k is the pixel values of immediate neighbors for pixel k. The value of CN is used to classify ridge pixel as isolated, continuing, ending, crossing point and bifurcation. Further, minutia is represented as a vector $m = [x, y, CN, \theta]$ having (x, y) as the pixel coordinates and θ as angle of orientation. For input fingerprint query image I^f, an extracted feature vector, η^f is created by combining n minutiae using Eq. 5.3

$$\eta^f = [m_1, m_2, \ldots m_n] \tag{5.3}$$

For iris feature extraction, input iris image I_i is pre-processed involving localization and normalization processes. In the first step, an integro-differential operator is used for localizing iris and pupillary boundaries. In the second step, Daugman's rubber sheet model [12] is used to normalize the localized iris into a fixed-sized rectangular block. Further, the processed image is quantified using the histogram of LBP. From LBP histogram values $l_1, l_2 \ldots l_n$, feature vector for iris η^i is generated using Eq. 5.4

$$\eta^i = (l_1, l_2 \ldots\ldots l_n) \tag{5.4}$$

This creates a unique pattern, generating iris feature η^i. The extracted feature vectors η^i and η^f are fused together using the proposed method to generate a cancelable feature which is discussed in the next subsection.

5.1.2 Multimodal Feature Fusion

The fusion process is very important in a multimodal biometric system for making a decision. Here, we have proposed a feature level fusion method with template protection. The proposed method generates a cancelable template which is revocable, non-invertible and robust to various types of attacks such that true biometric feature will not be revealed to the attacker. Every user is provided with a complex unique key (κ^k), where $k \in [1, N]$ used to create random 3-D planes as shown in Eq. 5.5.

$$\kappa^k = \begin{bmatrix} \kappa^k_{\alpha 1} & \kappa^k_{\beta 1} & \kappa^k_{\gamma 1} & \kappa^k_{\delta 1} \\ \kappa^k_{\alpha 2} & \kappa^k_{\beta 2} & \kappa^k_{\gamma 2} & \kappa^k_{\delta 2} \\ . & . & . & . \\ \kappa^k_{\alpha n} & \kappa^k_{\beta n} & \kappa^k_{\gamma n} & \kappa^k_{\delta n} \end{bmatrix} \tag{5.5}$$

Here k represents the k^{th} user. The length of the key is equivalent to the length of feature vectors and consists of n rows containing 4 co-efficient values namely $\kappa^k_{\alpha i}$, $\kappa^k_{\beta i}$, $\kappa^k_{\gamma i}$, and $\kappa^k_{\delta i}$ where $i \in [1, n]$ and having values randomly distributed in the range [-1000, 1000]. The user key is used to generate a random plane defined using Eq. 5.6 for each feature point as shown above in Fig. 5.1

$$\kappa_{\alpha i}x + \kappa_{\beta i}y + \kappa_{\gamma i}z = \kappa_{\delta i} \tag{5.6}$$

where $i \in [1, n]$. The random planes generated using user-specific keys are used in combining multiple features using the proposed approach. In this, feature vectors obtained during the feature extraction process are fused together by means of the proposed projection-based approach. Each feature point of the iris feature vector is considered as abscissa and each feature point of the fingerprint feature vector is considered as ordinate in a cartesian coordinate system. In case of different feature size, padding can be used so that every feature vector contain an equal number of feature points. Moreover, the abscissa and ordinates at the corresponding positions are combined to describe a point(Q) (χ, ψ) such that any user can be defined as in Eq. 5.7.

$$\upsilon = \begin{bmatrix} (\chi_1, \psi_1) & (\chi_2, \psi_2) & (\chi_3, \psi_3) & . & . & (\chi_n, \psi_n) \end{bmatrix} \tag{5.7}$$

For simplicity, the above equation can also be represented as shown in Eq. 5.8

$$\upsilon = \begin{bmatrix} Q_1 & Q_2 & Q_3 & . & . & Q_n \end{bmatrix} \tag{5.8}$$

Also, as discussed above, each user is provided with a unique user-specific key (κ^k) of dimension $n \times 4$. The key is used to create a different random plane corresponding to each point Q. Further, an orthogonal projection is performed from each of these points(Q) on the corresponding plane and point of projection(P) is obtained as shown in Figure 5.2

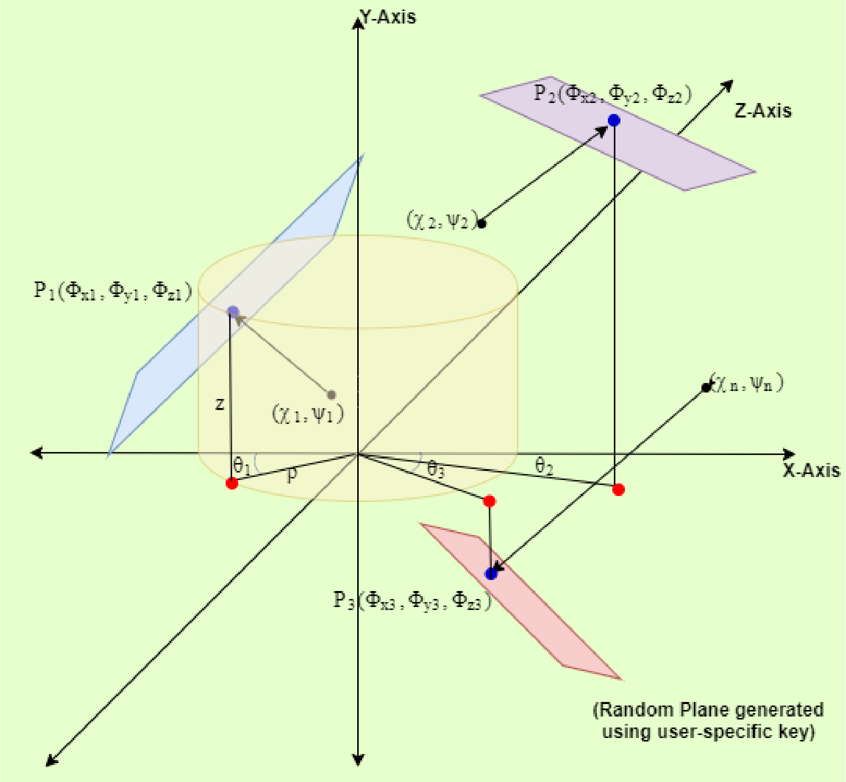


Fig. 5.2 *Projection of feature points on random planes*

For k^Pth user, each orthogonal projection from point $Q_i^k(\chi, \psi)$ on the random planes obtained using key κ^k generates a point $P_i^k(\phi_x, \phi_y, \phi_z)$ as in Eq. 5.9.

$$\begin{bmatrix} P_1^k & P_2^k & . & . & P_n^k \end{bmatrix} = \begin{bmatrix} (Q_1^k & Q_2^k & . & . & Q_n^k \end{bmatrix} \begin{bmatrix} \kappa_{\alpha 1}^k & \kappa_{\beta 1}^k & \kappa_{\gamma 1}^k & \kappa_{\delta 1}^k \\ \kappa_{\alpha 2}^k & \kappa_{\beta 2}^k & \kappa_{\gamma 2}^k & \kappa_{\delta 2}^k \\ . & . & . & . \\ \kappa_{\alpha n}^k & \kappa_{\beta n}^k & \kappa_{\gamma n}^k & \kappa_{\delta n}^k \end{bmatrix} \tag{5.9}$$

In the next step, each point of projection (P_i^k) is transformed into cylindrical co-ordinates using a function f defined as in Eq. 5.10

$$P_i^k(\theta, \rho, z) = f(P_i^k(\phi_x, \phi_y, \phi_z)) \tag{5.10}$$

where,ρ and θ are determined using Eq. 5.11 and Eq. 5.12 respectively.

$$\rho = \sqrt{{\phi_x}^2 + {\phi_y}^2} \tag{5.11}$$

$$\theta = \tan^{-1} \frac{\phi_y}{\phi_x} \tag{5.12}$$

In the cylindrical coordinate system, point P is represented as θ, ρ, z. In the last step, the azimuth(θ) values corresponding to each point of projection(P_i^k) for k^{th} user, are concatenated together to generate a fused vector ζ^k that is cancelable and non-invertible in nature as shown in Eq. 5.13.

$$\zeta^k = (\theta_1, \theta_2, \theta_3, ...\theta_n) \tag{5.13}$$

The purpose of conversion to a 3D cylindrical coordinate system is to provide a higher dropout ratio as compared to the 2D coordinate system. Since only azimuth values are used to generate the cancelable template, a dropout ratio of 66.6% is achieved. On the other hand, a 2D point of projection would have led to a dropout ratio of 50% only. Further, in case of template theft, if azimuth (θ) values are compromised, it will lead to ambiguous values of ϕ_x and ϕ_y as evident from the equation 5.12 and original feature points will not be exposed. Thus, the generated template is highly non-invertible and robust against theft. Also, the feature vectors from both Iris and Fingerprint modality of dimension $1 \times n$ are combined and converted into a single vector of dimension $1 \times n$. The cancelable feature obtained is compared with the stored templates to generate a final match score(S). The final decision is performed based on an optimal threshold value (τ), if the match score(S) is greater than τ, then it is considered as Genuine else imposter. The next section provides details of the experimental validation of the proposed method.

5.2 Experimental Validation

The experimental validation of the proposed multimodal biometric system is performed over three multimodal chimeric databases. During privacy analysis, the proposed system is analyzed for unlinkability, non-invertibility, and revocability. Also, the system is analyzed for various attacks like record multiplicity, substitution, and brute force attacks to establish the robustness of the system. On the other hand, various performance metrics like Equal Error Rate (EER), Decidability Index (DI), and Recognition Index (RI) are determined to estimate the system's performance. Also, the proposed system's performance is compared with other state-of-the-art methods.

5.2.1 Database & Experimental Design

The multimodal datasets are obtained using images from various benchmark datasets for experimental validation. Here, the Chimeric datasets are created by uniquely combining benchmark datasets namely MCYT Bimodal Database [66], IITD PolyU iris database [47], Casia iris database (Casia-IrisV1, http://biometrics.idealtest. org/), FVC2006 DB1-A fingerprint database [8], and MMU2 iris database [2]. Sample images from the mentioned benchmarked datasets are shown in Fig. 5.3.

The experimental validation is performed on three chimeric datasets namely D1, D2, and D3. D1 contains fingerprint samples of N different subjects from the MCYT database

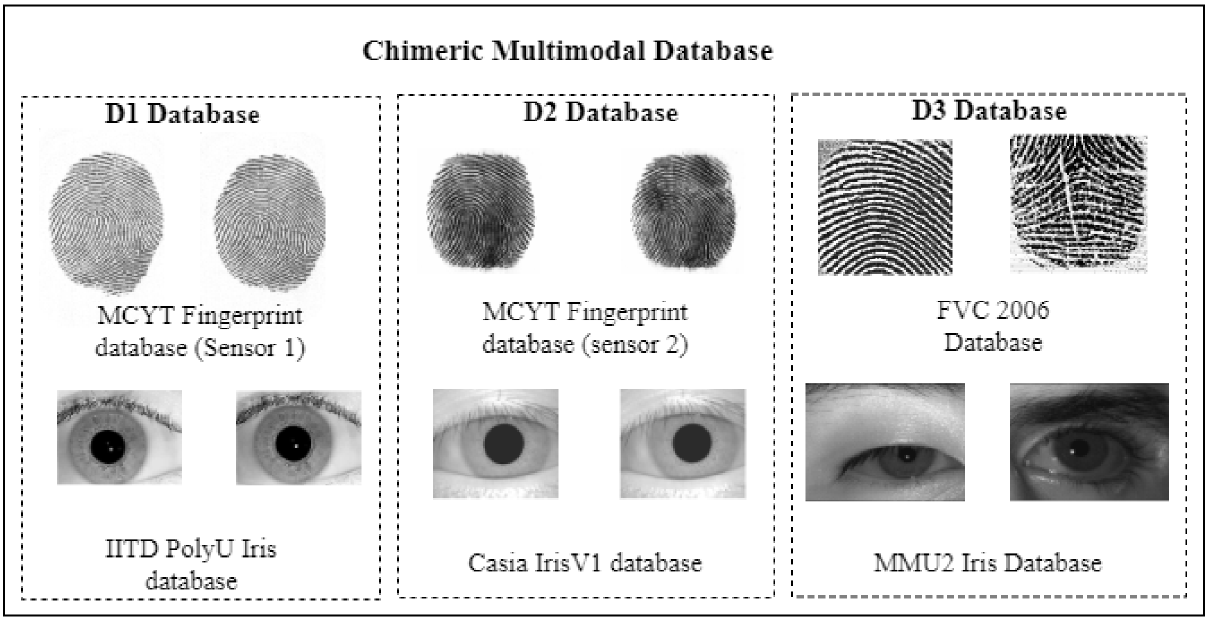


Fig. 5.3 *Sample multimodal database images from the benchmark datasets*

(sensor 1) and IITD iris PolyU database. Thus a virtual multimodal dataset is created for N subjects by combining the above-mentioned datasets. Similarly, D2 is created by combining N distinct subjects from the MCYT database (sensor 2) and the Casia Iris-V1 database. Also, the D3 dataset is obtained by combining N distinct subjects from the MMU2 iris database and the FVC2006 DB1-A database. Further, all the subjects in D1, D2, and D3 databases are completely different. In addition, five-fold cross-validation is carried out to obtain balanced results. The proposed system is implemented over a hardware configuration of the Intel i3 processor and 4GB RAM using the MATLAB 2018a platform. The performance analysis of the proposed system is discussed in the next section.

5.2.2 Performance Analysis

The proposed system's performance is quantitatively analyzed by means of various performance metrics namely Decidability Index (DI), Equal Error Rate (EER), and Recognition

Index(RI). Also, the results thus obtained are compared with other state-of-the-art techniques. During this process, the same techniques for generic feature extraction and score calculation are used for evaluating other methods.

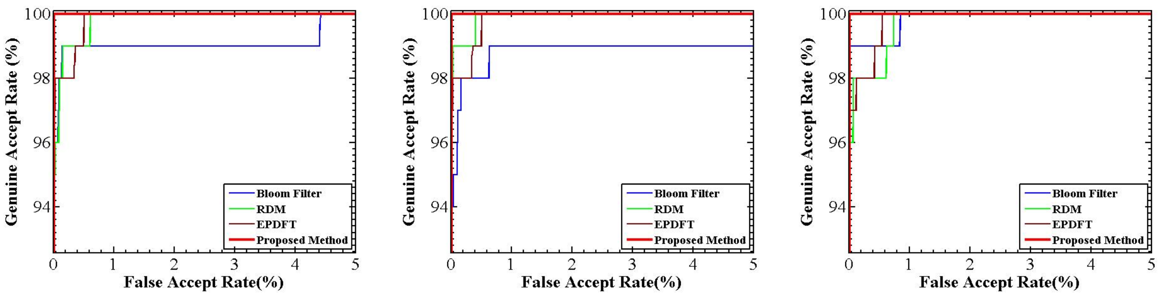
5.2.2.1 Accuracy Analysis

The accuracy of the proposed system is analyzed and compared with state-of-the-art techniques using performance metrics namely EER, DI, and RI. The performance metric values for various methods viz. Random Distance Method (RDM) [41], Bloom Filters [25] and Enhanced Partial Discrete Fourier Transform (EP-DFT) [126] are compared with the proposed method in Table. 5.1

Table 5.1: Comparison of EER, DI, and RI values for D1, D2 and D3 databases

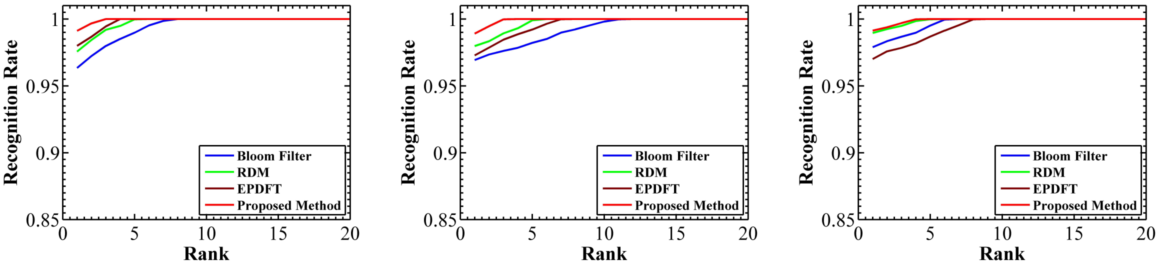
DB / Method	**D1 Database**			**D2 Database**			**D3 Database**		
	EER	**DI**	**RI**	**EER**	**DI**	**RI**	**EER**	**DI**	**RI**
RDM[41]	0.60±0.23	7.28±0.35	97±0.25	0.40±0.19	7.68±0.37	98±0.75	0.71±0.21	7.11±0.19	99±0.50
Bloom Filter[25]	0.97±0.20	5.77±0.42	96±0.50	1.14±0.24	4.98±0.28	97±0.45	0.92±0.17	5.33±0.31	98±0.58
EPDFT[126]	0.49±0.32	7.96±0.42	98±1.11	0.78±0.24	6.21±0.46	97±0.90	0.61±0.25	5.79±0.18	97 ±0.80
Proposed Method	0.005±0.004	22.14±0.34	99±0.94	0.003±0.005	18.45±0.43	99±0.95	0.004±0.10	9.71±0.22	99±0.90

The EER value for the proposed score level fusion method is 0.005 for the D1 database, 0.003 for the D2 database and 0.004 for the D3 database which is lowest in comparison with other state-of-the-art methods. The efficiency of the proposed system is also depicted by a high decidability value of 22.14 for the D1 database, 18.45 for the D2 database and 9.71 for the D3 database and supported by ROC and CMC curves in Fig. 5.4 and 5.5 respectively. The ROC and CMC curves of various state-of-the-art techniques are compared with the proposed system for three different databases. The proposed method shows higher performance as compared to other techniques. The variation among EER values is due to the use of different datasets and five-fold cross-validation.



(a) *D1 Database* (b) *D2 Database* (c) *D3 Database*

Fig. 5.4 *Performance comparision of evaluated methods: ROC curves for D1, D2 and D3 database (a) ROC curves for various cancelable biometric techniques over Database D1 (b) ROC curves for various cancelable biometric techniques over Database D2 (c) ROC curves for various cancelable biometric techniques over Database D3*



(a) *D1 Database* (b) *D2 Database* (c) *D3 Database*

Fig. 5.5 *CMC curves for D1, D2 and D3 databases (a) comparison of CMC curves of various cancelable biometric techniques over Database D1 (b) comparison of CMC curves of various cancelable biometric techniques over Database D2 (c) comparison of CMC curves of various cancelable biometric techniques over Database D3*

Accuracy analysis reveals that the limitations of individual classifiers were effectively addressed by the proposed fusion method providing higher accuracy and more reliable results. The proposed system also improves the privacy of every user making it robust against various issues like template thefts and safeguarding the identity of every user which is also discussed in the next subsection.

5.2.3 Privacy Analysis

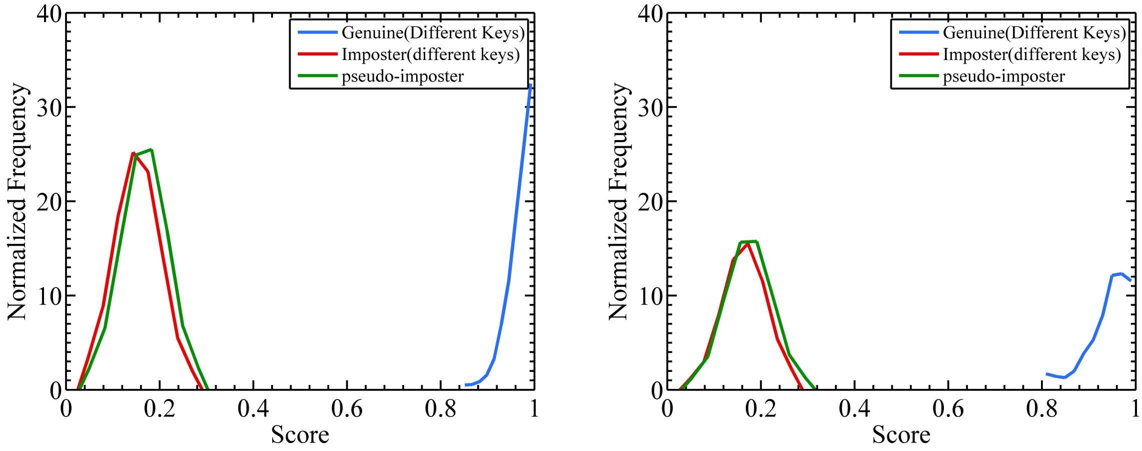
The performance analysis confirms the high accuracy of the proposed system by means of various performance metrics. The proposed biometric system also ensures user privacy by exhibiting the properties like non-invertibility, revocability, and unlinkability.

5.2.3.1 Non-Invertibility

In order to fulfill the criteria of non-invertibility, it must be infeasible to create the original biometric traits even if the key and the transformed template both are compromised. In a situation when both user-specific key and transformed templates are stolen, non-invertibility in the proposed method is achieved by choosing only the azimuth(θ) values during the generation of cancelable templates. Since 67% of the information is discarded, it is not possible to trace back to the original points of projection. Even if points of projection are estimated, it is impossible to find the actual source of projection as there can be infinite points over that line connecting the feature point, Q and projected point on the plane, P. Thus the proposed method exhibits non-invertibility of biometric templates.

5.2.3.2 Revocability

For a cancelable biometric system, if the stored templates are stolen, then they are discarded and new templates are generated using a new set of keys. Revocability states that templates generated from the same features should not be correlated. The revocability test is performed to measure the difference between the newly generated template and the old template. In order to check the revocability of the proposed system, 100 different keys were used to obtain 100 transformed templates. Every new user-specific key generates a different random plane and hence different templates. The distribution of imposter vs pseudo-imposter is shown in Fig.5.6 which shows that the pseudo-imposter distribution is very similar to imposter distribution. It shows that there is no correlation between the old and new transformed templates. This suggests that transformed templates are treated as different individuals but they were created from the biometric features of the same subject. Thus, the revocability analysis shows that the stolen template can be easily replaced by a new template by using a different set of keys in the proposed system.

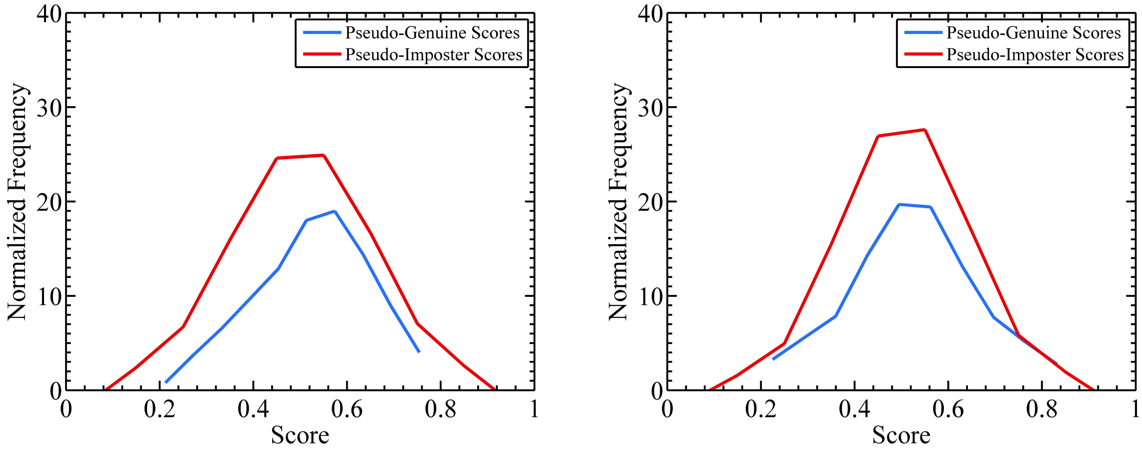


(a) *Database D1* **(b)** *Database D2*

Fig. 5.6 *Comparision of Genuine, Imposter and Pseudo-Imposter Distribution for a) D1 Database and b) D2 Database*

5.2.3.3 Unlinkability

Unlinkability states that multiple biometric templates of a single subject must be unlinkable provided different keys are used. This secures the identity of the subject when it is enrolled in multiple applications. In order to analyze unlinkability, the procedure described in [36] is adopted. For this, pseudo-genuine scores are introduced which refers to the match scores between the different templates of the same user by using different user-specific keys. Also, the pseudo-imposter scores are also calculated between different templates generated using a different user-specific key. In this scenario, if we plot the pseudo-imposter and pseudo-genuine distribution, the overlapping nature of both the distribution suggests that the templates generated from the same or different users are indistinct in nature which is also evident from Fig. 5.7. On the other hand, if pseudo-genuine and pseudo-imposter distributions are separated, it will be easier to identify the templates from the same user. The struggle in differentiating the templates leads to the unlinkability of the system.



(a) *Database D1* **(b)** *Database D2*

Fig. 5.7 *Comparision of Pseudo-Genuine and Pseudo-Imposter Distribution for a) D1 Database and b) D2 Database*

Privacy analysis clearly indicates that the proposed system preserves the privacy of each user by means of revocability, unlinkability, and non-invertibility. The complementary traits are fused together generating a cancelable template making system highly secure and robust against various attacks which are discussed in the next subsection.

5.2.4 Security Analysis

The security of the biometric system is of utmost priority. No adversary, in any case, may be able to break through the system as it will arise many security problems. The proposed biometric system is also analyzed against many such attacks.

5.2.4.1 Brute Force Attack

Brute Force attack assumes that the adversary possesses no previous knowledge about the transformed or the original biometric feature. Each possible combination is used to generate and match the cancelable template. Even if the intruder knows the length of the template, there will be a total of 2^{29*n} possibilities for each element in the template of the proposed technique. Thus,an exceptionally high brute force effort will be required to generate a template,which makes it computationally infeasible.

5.2.4.2 Attacks via record multiplicity

During attacks via record multiplicity (ARM), the adversary possesses multiple transformed templates of the same user and tries to establish a connection so as to develop an image of the original biometric trait. For example, let's take two transformed templates T1 and T2 created using a different key for the same user. Also, during privacy analysis, unlinkability between these templates was proven experimentally. Further, the i^{th} value of T1 depends upon the point of projection P_1 and it cannot be connected to i^{th} value of T2 as it depends upon its points of projection P_2.P_1 and P_2 will always be different as different keys are chosen. Therefore, the attacker cannot mount ARM attack even after having different copies of transformed templates from the same user.

5.2.4.3 Blended Substitution attacks

In the blended substitution, the attacker combines its data with user data in a single template. The blended template allows both users and attackers to authenticate against the same ID simultaneously. In the proposed approach, blended substitution is not feasible since, with only half of the user or attacker's attribute, the matching score would be rejected as an imposter for both user and attacker.

5.3 Significant Findings

- First level security is deployed by using a user-specific key without which biometric recognition cannot be performed. Thus the user in possession of the key will be able to access the system.
- Second security level is deployed by converting original biometric feature into a Cancelable biometric templates using a novel transformation approach. Thus protecting the biometric data of all usersin case of a system breach.
- A clear decision boundary is revealed between genuine and imposter distribution.
- The cancelable templates generated are non-invertible, revocable and unlinkable. Also, the cancelable templates are also robust against various security attacks like brute force, attacks via record multiplicity and blended substitution attacks.
- Qualitative and quantitative analysis on 3 different multimodal datasets reveals that the proposed method performs favorably against the state-of-the-art methods.

In addition, the experimental results along with significant findings of the proposed work were published in [29].

Chapter 6

Conclusion & Future Directions

Chapter 6

Conclusion and Future Directions

This chapter will summarize the major contributions and achievements that come out of the present work. Despite the significant contributions, no research is said to be complete unless it directs to a few topics for future research. Hence, the potential work that can be explored further under present studies is briefly discussed as directions to future work in the Section. 6.2

6.1 Summary of Major Contributions

The main motive behind this thesis work is to design and develop an adaptive, robust and accurate multimodal biometric system. To address the research gaps identified during literature review, several novel contributions proposed under present work are summarized as follows.

- Latest trends in biometric recognition system exploiting information from complementary modalities are analyzed. Also, multimodal biometric systems for various fusion schemes are investigated and briefly reviewed. Further, image samples from multiple modalities are captured and analyzed in a self generated dataset. Captured biometric samples incorporate various environmental challenges to determine the real-time performance of various biometric systems.

- A novel adaptive score fusion technique for a multimodal biometric system using three biometric traits viz. fingerprint, face, and iris is proposed. The proposed technique performed boosting and suppression of individual scores from each modality. Reliability factor based on image quality is evaluated for each individual modality to resolve the problem of dynamic environment. It provides unequal prior to each classifier based on the quality of input images. The high value of the reliability factor improves the overall impact of the corresponding modality during score fusion. This not only helps in dealing with various problems of the dynamic environment but also very effective against spoofing attacks as well. Moreover, a multimodal biometric system with iris and fingerprint modality is proposed. Here, individual classifier scores are optimized using GOA. Later, the optimized scores are fused together using PCR-6 fusion rules. The Proposed method exhibits high performance and reliability. Also, a multilevel multimodal biometric system ensuring not only high performance but also robustness to security and privacy concerns is proposed. The proposed system is robust against single point of security failure. The feature size is reduced to half thereby requiring low computational and space complexity. The security analysis of the proposed fusion mechanism shows that the approach is able to defend various attacks, thereby, assuring user-privacy and data-security. Moreover, the generated templates are highly revocable, thus can be regenerated in case the data gets compromised. Hence, the proposed approach can be deployed for biometric authentication in security-critical applications.

- Exhaustive qualitative and quantitative analysis of the proposed biometric systems on benchmark datasets proved their robustness and efficiency against other state-of-the-art systems during biometric recognition challenges. For Adaptive score level fusion model, the proposed system is evaluated on three chimeric multimodal databases generated from benchmark images of fingerprint, face and iris modality. On average of the outcome, the proposed system achieved EER of 0.5, DI of 6.45 and RI of 98.5 against various state of the art methods. Further, the proposed biometric system with grasshopper optimization achieved EER of 0.79 and DI of 5.24. Moreover, the biometric system proposed under multi-level multimodal system exhibit very high performance with EER of 0.004, DI of 16.63 and RI of 99 on image samples multiple benchmarked datasets

6.2 Directions of Future Works

In the present work, various multimodal biometric systems were investigated and explored at length to provide novel contributions to the domain. Despite that, there are certain research areas that emerge out of the present work which demand future investigation. These areas are summarized as directions to future work and are detailed as follows.

- Adaptive score level fusion model can be extended to incorporate user specific traits for estimating Reliability factor. This will result in an increase in the adaptive nature of the system and a more wide variety of challenges may be addressed. The proposed biometric system can also be customized to work at multiple security levels as per requirements.

- Multilevel multimodal biometric system may be investigated to incorporate image quality as a reliability factor into the proposed system. It will help in enhancing the adaptivity of the system so that it may address various other challenges like poor quality input images, improper sensor interaction, etc.

REFERENCES

References

[1] Derawi biometrics. http://biometrics.derawi.com/?page_id=101. Accessed: 2020-07-03.

[2] MMU2 Iris Database[Online]. Available:http://pesona.mmu.edu.my/~ccteo/. Accessed: June, 2019.

[3] *Institute of Automation, Chinese Academy of Science: CASIA v1.0 Iris Image Database, 2008.*, (accessed February 3, 2020). http://www.nlpr.ia.ac.cn/english/irds/irisdatabase.htm.

[4] H. Abderrahmane, G. Noubeil, Z. Lahcene, Z. Akhtar, and D. Dasgupta. Weighted quasi-arithmetic mean based score level fusion for multi-biometric systems. *IET Biometrics*, 9(3):91–99, 2020.

[5] S. S. Ali, I. I. Ganapathi, S. Prakash, P. Consul, and S. Mahyo. Securing biometric user template using modified minutiae attributes. *Pattern Recognition Letters*, 129:263–270, 2020.

[6] R. Belguechi, E. Cherrier, C. Rosenberger, and S. Ait-Aoudia. Operational bio-hash to preserve privacy of fingerprint minutiae templates. *IET Biometrics*, 2(2):76–84, 2013.

[7] S. Bianco and P. Napoletano. Biometric recognition using multimodal physiological signals. *IEEE Access*, 7:83581–83588, 2019.

[8] R. Cappelli, M. Ferrara, A. Franco, and D. Maltoni. Fingerprint verification competition 2006. *Biometric Technology Today*, 15:7–9, 2007.

[9] D. Chang, S. Garg, M. Hasan, and S. Mishra. Cancelable multi-biometric approach using fuzzy extractor and novel bit-wise encryption. *IEEE Transactions on Information Forensics and Security*, 15:3152–3167, 2020.

[10] M. Cheniti, N.-E. Boukezzoula, and Z. Akhtar. Symmetric sum-based biometric score fusion. *IET Biometrics*, 7(5):391–395, 2018.

[11] Y. J. Chin, T. S. Ong, A. B. J. Teoh, and K. Goh. Integrated biometrics template protection technique based on fingerprint and palmprint feature-level fusion. *Information Fusion*, 18:161–174, 2014.

[12] J. Daugman. How iris recognition works. *IEEE Trans. on Circuits & Systems for Video Technology*, 14(1):21–30, 2004.

[13] J. G. Daugman. High confidence visual recognition of persons by a test of statistical independence. *IEEE transactions on pattern analysis and machine intelligence*, 15(11):1148–1161, 1993.

[14] A. M. de Paula Canuto, M. C. Fairhurst, and F. Pintro. Ensemble systems and cancellable transformations for multibiometric-based identification. *IET Biometrics*, 3(1):29–40, 2014.

[15] R. Dwivedi and S. Dey. A novel hybrid score level and decision level fusion scheme for cancelable multi-biometric verification. *Applied Intelligence*, 49(3):1016–1035, 2019.

[16] R. Dwivedi and S. Dey. A novel hybrid score level and decision level fusion scheme for cancelable multi-biometric verification. *APPL INTELL*, 49(3):1016–1035, 2019.

[17] M. Eskandari and O. Sharifi. Optimum scheme selection for face–iris biometric. *IET Biometrics*, 6(5):334–341, 2017.

[18] M. Eskandari and O. Sharifi. Effect of face and ocular multimodal biometric systems on gender classification. *IET Biometrics*, 8(4):243–248, 2019.

[19] K. Fakhar, M. E. Aroussi, M. N. Saidi, and D. Aboutajdine. Fuzzy pattern recognition-based approach to biometric score fusion problem. *Fuzzy Sets and Systems*, 305:149–159, 2016.

[20] A. Farina, Z. M.Kovács-Vajna, and A. Leone. Fingerprint minutiae extraction from skeletonized binary images. *Pattern Recognition*, 32(5):877–889, 1999.

[21] D. Field. Relations between the statistics of natural images and the response properties of cortical cells. *Journal of optical society of America*, 4(12):2379–2394, 1987.

[22] G. Gao, L. Zhang, J. Yang, L. Zhang, and D. Zhang. Reconstruction based finger-knuckle-print verification with score level adaptive binary fusion. *IEEE Transactions on Image Processing*, 22(12):5050–5062, 2013.

[23] Q. Gao and C. Zhang. Constructing cancellable template with synthetic minutiae. *IET Biometrics*, 6(6):448–456, 2017.

[24] W. Gao, B. Cao, S. Shan, X. Chen, D. Zhou, X. Zhang, and D. Zhao. The cas-peal large-scale chinese face database and baseline evaluations. *IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans*, 38(1):149–161, 2008.

[25] M. Gomez-Barrero, C. Rathgeb, G. Li, R. Ramachandra, J. Galbally, and C. Busch. Multi-biometric template protection based on bloom filters. *Information Fusion*, 42:37–50, 2018.

[26] K. Gupta. Advances in multi modal biometric systems: a brief review. In *2017 International Conference on Computing, Communication and Automation (ICCCA)*, pages 262–267. IEEE, 2017.

[27] K. Gupta, G. S. Walia, and K. Sharma. Multimodal biometric system using grasshopper optimization. In *2019 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS)*, pages 387–391. IEEE, 2019.

[28] K. Gupta, G. S. Walia, and K. Sharma. Quality based adaptive score fusion approach for multimodal biometric system. *Applied Intelligence*, pages 2824–2836, 2019.

[29] K. Gupta, G. S. Walia, and K. Sharma. Novel approach for multimodal feature fusion to generate cancelable biometric. *The Visual Computer*, pages 1–13, 2020.

[30] S. Gutta and Q. Cheng. Joint feature extraction and classifier design for ecg-based biometric recognition. *IEEE Journal of Biomedical and Health Informatics*, 20(2):460–468, 2016.

[31] M. Hammad, Y. Liu, and K. Wang. Multimodal biometric authentication systems using convolution neural network based on different level fusion of ecg and fingerprint. *IEEE Access*, 7:26527–26542, 2019.

[32] M. Hanmandlu, J. Grover, A. Gureja, and H.M.Gupta. Score level fusion of multimodal biometrics using triangular norms. *Pattern Recognition Letters*, 32(14):1843–1850, 2011.

[33] M. Hossain, J. Chen, and K. Rahman. On enhancing serial fusion based multi-biometric verification system. *Applied Intelligence*, 48(12):4824–4833, 2018.

[34] J.A.Unar, W. C. Seng, and A. Abbasi. A review of biometric technology along with trends and prospects. *Pattern Recognition*, 47(8):2673–2688, 2014.

[35] A. T. B. Jin, D. N. C. Ling, and A. Goh. Biohashing: two factor authentication featuring fingerprint data and tokenised random number. *Pattern Recognition*, 37(11):2245–2255, 2004.

[36] Z. Jin, J. Y. Hwang, Y.-L. Lai, S. Kim, and A. B. J. Teoh. Ranking-based locality sensitive hashing-enabled cancelable biometrics: Index-of-max hashing. *IEEE Transactions on Information Forensics and Security*, 13(2):393–407, 2017.

[37] W. Kabir, M. O. Ahmad, and M. N. S. Swamy. Normalization and weighting techniques based on genuine-impostor score fusion in multi-biometric systems. *IEEE Transactions on Information Forensics and Security*, 13(8):1989–2000, 2018.

[38] W. Kabir, M. O. Ahmad, and M. N. S. Swamy. A multi-biometric system based on feature and score level fusions. *IEEE Access*, 7:59437–59450, 2019.

[39] A. T. Kahlil and F. E. M. A. Chadi. Generation of iris codes using 1d log-gabor filter. *IEEE International Conference on Computer Engineering & Systems*, pages 329–336, 2010.

[40] B. J. Kang and K. R. Park. Multimodal biometric method based on vein and geometry of a single finger. *IET Computer Vision*, 4(3):209–217, 2010.

[41] H. Kaur and P. Khanna. Random distance method for generating unimodal and multimodal cancelable biometric features. *IEEE Transactions on Information Forensics and Security*, 14(3):709–719, 2018.

[42] N. Kihal, S. Chitroub, A. Polette, I. Brunette, and J. Meunier. Efficient multimodal ocular biometric system for person authentication based on iris texture and corneal shape. *IET Biometrics*, 6(6):379–386, 2017.

[43] H. Kim and S. Y. Chun. Cancelable ecg biometrics using compressive sensing-generalized likelihood ratio test. *IEEE Access*, 7:9232–9242, 2019.

[44] J. Kittler, M. Hatef, R. Duin, and J. Matas. On combining classifiers. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 20(3):226–239, 1998.

[45] A. Kumar, V. Kanhangad, and D. Zhang. A new framework for adaptive multimodal biometrics management. *IEEE Transactions on Information Forensics and Security*, 5(1):92–102, 2010.

[46] A. Kumar and A. Kumar. Adaptive management of multimodal biometrics fusion using ant colony optimization. *Information Fusion*, 32(Part B):49–63, 2016.

[47] A. Kumar and A. Passi. Comparison and combination of iris matchers for reliable personal authentication. *Pattern Recognition*, 43(3):1016–1026, 2010.

[48] N. Kumar, S. Singh, and A. Kumar. Random permutation principal component analysis for cancelable biometric recognition. *APPL INTELL*, 48(9):2824–2836, 2018.

[49] P. Kumar, S. Mukherjee, R. Saini, P. Kaushik, P. P. Roy, and D. P. Dogra. Multimodal gait recognition with inertial sensor data and video using evolutionary algorithm. *IEEE Transactions on Fuzzy Systems*, 27(5):956–965, 2019.

[50] P. Lacharme, E. Cherrier, and C. Rosenberger. Preimage attack on biohashing. In *2013 International Conference on Security and Cryptography (SECRYPT)*, pages 1–8. IEEE, 2013.

[51] C. Lee, J. Choi, K. Toh, S. Lee, and J. Kim. Alignment-free cancelable fingerprint templates based on local minutiae information. *IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics)*, 37(4):980–992, 2007.

[52] Y. Liang, X. Ding, C. Liu, and J.-H. Xue. Combining multiple biometric traits with an order-preserving score fusion algorithm. *Neurocomputing*, 171:252–261, 2016.

[53] H. F. Liau and D. Isa. Feature selection for support vector machine-based face-iris multimodal biometric system. *Expert Systems with Applications*, 38(9):11105–11111, 2011.

[54] C. Liu and H. Wechsler. Gabor feature based classification using the enhanced fisher linear discriminant model for face recognition. *IEEE Transactions on Image Processing*, 11(4):467–476, 2002.

[55] G. Mai, K. Cao, X. Lan, and P. C. Yuen. Secureface: Face template protection. *IEEE Transactions on Information Forensics and Security*, 16:262–277, 2021.

[56] E. Maiorana, P. Campisi, J. Fierrez, J. Ortega-Garcia, and A. Neri. Cancelable templates for sequence-based biometrics with application to on-line signature recognition. *IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans*, 40(3):525–538, 2010.

[57] L. Mezai and F. Hachouf. Score-level fusion of face and voice using particle swarm optimization and belief functions. *IEEE Transactions on Human-Machine Systems*, 45(6):761–772, 2015.

[58] A. Mittal, A. K. Moorthy, and A. C. Bovik. No-reference image quality assessment in the spatial domain. *IEEE Transactions on Image Processing*, 21(12):4695–4708, 2012.

[59] S. Mukherjee, K. Pal, B. P. Majumder, C. Saha, B. K. Panigrahi, and S. Das. Differential evolution based score level fusion for multi-modal biometric systems. *IEEE Symposium on Computational Intelligence in Biometrics and Identity Management (CIBIM)*, pages 1–7, 2014.

[60] T. Murakami, R. Fujita, T. Ohki, Y. Kaga, M. Fujio, and K. Takahashi. Cancelable permutation-based indexing for secure and efficient biometric identification. *IEEE Access*, 7:45563–45582, 2019.

[61] K. Nandakumar, Y. Chen, S. C. Dass, and A. Jain. Likelihood ratio-based biometric score fusion. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 30(2):342–347, 2008.

[62] K. Nandakumar and A. K. Jain. Biometric template protection: Bridging the performance gap between theory and practice. *IEEE Signal Processing Magazine*, 32(5):88–100, 2015.

[63] L. Nanni, A. Lumini, M. Ferrara, and R. Cappelli. Combining biometric matchers by means of machine learning and statistical approaches. *Neurocomputing*, 149:526–535, 2015.

[64] K. Nguyen, S. Denman, S. Sridharan, and C. Fookes. Score-level multibiometric fusion based on dempster–shafer theory incorporating uncertainty factors. *IEEE Transactions on Human-Machine Systems*, 45(1):132–140, 2015.

[65] T. Ojala, M. Pietikäinen, and D. Harwood. A comparative study of texture measures with classification based on featured distributions. *Pattern recognition*, 29(1):51–59, 1996.

[66] J. Ortega-Garcia, J. Fierrez-Aguilar, D. Simon, J. Gonzalez, M. Faundez-Zanuy, V. Espinosa, A. Satue, I. Hernaez, J.-J. Igarza, C. Vivaracho, D. Escudero, and Q.-I. Moro. Mcyt baseline corpus: a bimodal biometric database. *IEE Proceedings - Vision, Image and Signal Processing*, 150(6):395–401, 2003.

[67] N. Otsu. A threshold selection method from gray-level histograms. *IEEE Transactions on Systems, Man, and Cybernetics*, 9(1):62–66, 1979.

[68] V. M. Patel, N. K. Ratha, and R. Chellappa. Cancelable biometrics: A review. *IEEE Signal Processing Magazine*, 32(5):54–65, 2015.

[69] P. P. Paul, M. Gavrilova, and S. Klimenko. Situation awareness of cancelable biometric system. *The Visual Computer*, 30(9):1059–1067, 2014.

[70] P. P. Paul and M. L. Gavrilova. A novel cross folding algorithm for multimodal cancelable biometrics. *International Journal of Software Science and Computational Intelligence (IJSSCI)*, 4(3):20–37, 2012.

[71] J. Peng, A. A. A. El-Latif, Q. Li, and X. Niu. Multimodal biometric authentication based on score level fusion of finger biometrics. *Optik*, 125(23):6891–6897, 2014.

[72] J. K. Pillai, V. M. Patel, R. Chellappa, and N. K. Ratha. Sectored random projections for cancelable iris biometrics. *IEEE International Conference on Acoustics, Speech and Signal Processing*, pages 1838–1841, 2010.

[73] J. K. Pillai, V. M. Patel, R. Chellappa, and N. K. Ratha. Secure and robust iris recognition using random projections and sparse representations. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 33(9):1877–1893, 2011.

[74] N. Poh and J. Kittler. A unified framework for biometric expert fusion incorporating quality measures. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 34(1):3–18, 2012.

[75] N. Poh, J. Kittler, and T. Bourlai. Quality-based score normalization with device qualitative information for multimodal biometric fusion. *IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans*, 40(3):539–554, 2010.

[76] S. Prabhakar and A. K.Jain. Decision-level fusion in fingerprint verification. *Pattern Recognition*, 35(4):861–874, 2002.

[77] H. Proença. Ocular biometrics by score-level fusion of disparate experts. *IEEE Transactions on Image Processing*, 23(12):5082–5093, 2014.

[78] S. Rane. Standardization of biometric template protection. *IEEE MultiMedia*, 21(4):94–99, 2014.

[79] N. K. Ratha, S. Chikkerur, J. H. Connell, and R. M. Bolle. Generating cancelable fingerprint templates. *IEEE Trans. Pattern Anal. Mach. Intell.*, 29(4):561–572, 2007.

[80] C. Rathgeb, F. Breitinger, C. Busch, and H. Baier. On application of bloom filters to iris biometrics. *IET Biometrics*, 3(4):207–218, 2014.

[81] C. Rathgeb and C. Busch. Cancelable multi-biometrics: Mixing iris-codes based on adaptive bloom filters. *Computers & Security*, 42:1–12, 2014.

[82] S. Ribaric, D. Ribaric, and N. Pavesic. Multimodal biometric user-identification system for network-based applications. *IEE Proceedings - Vision, Image and Signal Processing*, 150(6):409–416, 2003.

[83] A. Ross and A. Jain. Information fusion in biometrics. *Pattern Recognition Letters*, 24(13):2115–2125, 2003.

[84] K. Roy, J. Shelton, B. O'Connor, and M. S. Kamel. Multibiometric system using fuzzy level set, and genetic and evolutionary feature extraction. *IET Biometrics*, 4(3):151–161, 2015.

[85] K. Roy, J. Shelton, B. O'Connor, and M. S. Kamel. Multibiometric system using fuzzy level set, and genetic and evolutionary feature extraction. *IET Biometrics*, 4(3):151–161, 2015.

[86] D. Sadhya and B. Raman. Generation of cancelable iris templates via randomized bit sampling. *IEEE Transactions on Information Forensics and Security*, 14(11):2972–2986, 2019.

[87] M. Sandhya and M. V. N. K. Prasad. Securing fingerprint templates using fused structures. *IET Biometrics*, 6(3):173–182, 2017.

[88] M. Sandhya, M. V. N. K. Prasad, and R. R. Chillarige. Generating cancellable fingerprint templates based on delaunay triangle feature set construction. *IET Biometrics*, 5(2):131–139, 2016.

[89] S. Saremi, S. Mirjalili, and A. Lewis. Grasshopper optimisation algorithm: theory and application. *Advances in Engineering Software*, 105:30–47, 2017.

[90] M. Savvides, B. V. Kumar, and P. K. Khosla. Cancelable biometric filters for face recognition. In *Proceedings of the 17th International Conference on Pattern Recognition, 2004. ICPR 2004.*, volume 3, pages 922–925. IEEE, 2004.

[91] H. Sellahewa and S. A. Jassim. Image-quality-based adaptive face recognition. *IEEE Transactions on Instrumentation and Measurement*, 59(4):805–813, 2010.

[92] R. Sharma, S. Das, and P. Joshi. Score-level fusion using generalized extreme value distribution and dsmt, for multi-biometric systems. *IET Biometrics*, 7(5):474–481, 2018.

[93] R. Sharma, S. Das, and P. Joshi. Score-level fusion using generalized extreme value distribution and dsmt for multibiometric systems. *IET Biometrics*, 7(5):474–481, 2018.

[94] R. P. Sharma and S. Dey. Fingerprint liveness detection using local quality features. *The Visual Computer*, 35(10):1393–1410, 2019.

[95] S. Shekhar, V. M. Patel, N. M. Nasrabadi, and R. Chellappa. Joint sparse representation for robust multimodal biometrics recognition. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 36(1):113–126, 2014.

[96] H. Sikkandar and R. Thiyagarajan. Soft biometrics-based face image retrieval using improved grey wolf optimisation. *IET Image Processing*, 14(3):451–461, 2020.

[97] H. M. Sim, H. Asmuni, R. Hassan, and R. M.Othman. Multimodal biometrics: Weighted score level fusion based on non-ideal iris and face images. *Expert Systems with Applications*, 41(11):5390–5404, 2014.

[98] H. M. Sim, H. Asmuni, R. Hassan, and R. M.Othman. Multimodal biometrics: Weighted score level fusion based on non-ideal iris and face images. *Expert Systems with Applications*, 41(11):5390–5404, 2014.

[99] H. M. Sim, H. Asmuni, R. Hassan, and R. M.Othman. Multimodal biometrics: Weighted score level fusion based on non-ideal iris and face images. *Expert Systems with Applications*, 41(11):5390–5404, 2014.

[100] N. Srinivas, K. Veeramachaneni, and L. A. Osadciw. Fusing correlated data from multiple classifiers for improved biometric verification. *12th International Conference on Information Fusion, 2009, Seattle, USA*, pages 1504–1511, 2009.

[101] Z. S.Shariatmadar and K. Faez. Finger-knuckle-print recognition performance improvement via multi-instance fusion at the score level. *Optik - International Journal for Light and Electron Optics*, 125(3):908–910, 2014.

[102] S. A. Sudiro, M. Paindavoine, and T. M. Kusuma. Simple fingerprint minutiae extraction algorithm using crossing number on valley structure. *IEEE Workshop on Automatic Identification Advanced Technologies*, pages 41–44, 2007.

[103] Y. Sui, X. Zou, E. Y. Du, and F. Li. Design and analysis of a highly user-friendly, secure, privacy-preserving, and revocable authentication method. *IEEE Transactions on Computers*, 63(4):902–916, 2014.

[104] M. Sultana, P. P. Paul, and M. L. Gavrilova. Social behavioral information fusion in multimodal biometrics. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 48(12):2176–2187, 2018.

[105] N. Susyanto, R. Veldhuis, L. Spreeuwers, and C. Klaassen. Semiparametric likelihood-ratio-based biometric score-level fusion via parametric copula. *IET Biometrics*, 8(4):277–283, 2019.

[106] S. Taheri and . Toygar. Animal classification using facial images with score-level fusion. *IET Computer Vision*, 12(5):679–685, 2018.

[107] K. Takahashi and K. Naganuma. Unconditionally provably secure cancellable biometrics based on a quotient polynomial ring. *IET Biometrics*, 1(1):63–71, 2012.

[108] Q. Tao and R. Veldhuisl. Robust biometric score fusion by naive likelihood ratio via receiver operating characteristics. *IEEE Transactions on Information Forensics and Security*, 8(2):305–313, 2013.

[109] M. Tarek, O. Ouda, and T. Hamza. Robust cancellable biometrics scheme based on neural networks. *IET Biometrics*, 5(3):220–228, 2016.

[110] A. B. Teoh, A. Goh, and D. C. Ngo. Random multispace quantization as an analytic mechanism for biohashing of biometric and random identity inputs. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 28(12):1892–1901, 2006.

[111] A. B. J. Teoh, W. K. Yip, and K.-A. Toh. Cancellable biometrics and user-dependent multi-state discretization in biohash. *Pattern Analysis and Applications*, 13(3):301–307, 2010.

[112] A. B. J. Teoh and C. T. Yuang. Cancelable biometrics realization with multispace random projections. *IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics)*, 37(5):1096–1106, 2007.

[113] T.M.Abhishree, J.Latha, K.Manikantan, and S.Ramachandran. Face recognition using gabor filter based feature extraction with anisotropic diffusion as a pre-processing technique. *Procedia Computer Science*, 45:312–321, 2015.

[114] A. K. Trivedi, D. M. Thounaojam, and S. Pal. Non-invertible cancellable fingerprint template for fingerprint biometric. *Computers & Security*, 90:., 2020.

[115] K. Veeramachaneni, L. A. Osadciw, and P. K. Varshney. An adaptive multimodal biometric management algorithm. *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*, 35(3):344–356, 2005.

[116] S. Veluchamy and L. R. Karlmarx. System for multimodal biometric recognition based on finger knuckle and finger vein using feature-level fusion and k-support vector machine classifier. *IET Biometrics*, 6(3):232–242, 2017.

[117] G. S. Walia, G. Jain, N. Bansal, and K. Singh. Adaptive weighted graph approach to generate multimodal cancelable biometric templates. *IEEE Transactions on Information Forensics and Security*, pages 1–1, 2019.

[118] G. S. Walia, S. Rishi, R. Asthana, A. Kumar, and A. Gupta. Secure multimodal biometric system based on diffused graphs and optimal score fusion. *IET Biometrics*, 8(4):231–242, 2019.

[119] G. S. Walia, S. Rishi, R. Asthana, A. Kumar, and A. Gupta. Secure multimodal biometric system based on diffused graphs and optimal score fusion. *IET Biometrics*, 8(4):231–242, 2019.

[120] G. S. Walia, T. Singh, K. Singh, and N. Verma. Robust multimodal biometric system based on optimal score level fusion model. *Expert Systems with Applications*, 116:364–376, 2019.

[121] S. Wang and J. Hu. Design of alignment-free cancelable fingerprint templates via curtailed circular convolution. *Pattern Recognition*, 47(3):1321–1329, 2014.

[122] X. Wang and H. Li. One-factor cancellable palmprint recognition scheme based on oiom and minimum signature hash. *IEEE Access*, 7:131338–131354, 2019.

[123] Y. Wang and K. N. Plataniotis. An analysis of random projection for changeable and privacy-preserving biometric verification. *IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics)*, 40(5):1280–1293, 2010.

[124] S.-C. Wu, P.-T. Chen, A. L. Swindlehurst, and P.-L. Hung. Cancelable biometric recognition with ecgs: subspace-based approaches. *IEEE Transactions on Information Forensics and Security*, 14(5):1323–1336, 2019.

[125] J. Yang and X. Zhang. Feature-level fusion of fingerprint and finger-vein for personal identification. *Pattern Recognition Letters*, 33(5):623–628, 2012.

[126] W. Yang, S. Wang, J. Hu, G. Zheng, and C. Valli. A fingerprint and finger-vein based cancelable multi-biometric system. *Pattern Recognition*, 78:242–251, 2018.

[127] H. Ye, G. Shang, L. Wang, and M. Zheng. A new method based on hough transform for quick line and circle detection. *IEEE International Conference on Biomedical Engineering and Informatics (BMEI)*, pages 52–56, 2015.

[128] M. Yildiz, B. Yanikoğlu, A. Kholmatov, A. Kanak, U. Uludağ, and H. Erdoğan. Biometric layering with fingerprints: Template security and privacy through multibiometric template fusion. *The Computer Journal*, 60(4):573–587, 2017.

[129] J. Zuo, N. K. Ratha, and J. H. Connell. Cancelable iris biometric. In *2008 19th International Conference on Pattern Recognition*, pages 1–4. IEEE, 2008.

Appendix

Biodata

Keshav Gupta was born on 14th March 1989 in Delhi, India. He received his B.Tech. degree in Computer science and Engineering from University Institute of Engineering and Technology, Kurukshetra University, Kurukshetra (Haryana) in 2011. He received his M.Tech degree in Software Engineering from Delhi Technological University, New Delhi in 2013. He joined Delhi Technological University, New Delhi as part time Ph.D Scholar in Computer Science and Engineering Department under the supervision of Prof. Kapil Sharma and Dr. Gurjit Singh Walia in 2016. His current research focuses on Biometric Systems, Pattern Recognition and machine learning. He works on multimodal biometric recognition systems and has proposed various robust and adaptive biometric systems.