UNIVERSITY OF CALGARY

Confidence-Based Rank Level Fusion For Multimodal Biometric Systems

by

Hossein Talebi

A THESIS
SUBMITTED TO THE FACULTY OF GRADUATE STUDIES
IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE
DEGREE OF MASTER OF SCIENCE

GRADUATE PROGRAM IN COMPUTER SCIENCE

CALGARY, ALBERTA

November, 2015

Abstract

In recent years, the inevitable need for reliable biometric identity management systems in applications such as border crossing, welfare distribution, and accessing critical facilities has drawn researchers' attention to the area of biometric. The intrinsic limitations of unimodal biometric systems such as non-universality, sensitivity to noisy sensor data, inter and intra class variations and spoof attacks have resulted in significant attention toward multimodal biometric systems. An important aspect of a multimodal biometric system is the fusion of information from multiple biometric sources. This thesis focuses on using the notion of Resemblance Probability Distributions to calculate confidence measures for different biometric matchers and use these confidence measures in the fusion module to improve the identification rate of the system. This thesis approaches the problem of low inter class variation and low quality data by proposing Rank List Reinforcement and Confidence-based Ranked List Selection methods.

Table of Contents

List of Tables

List of Figures and Illustrations

List of Symbols, Abbreviations and Nomenclature

Symbol	Definition
CBRLS	Confidence Based Ranked List Selection
CMC	Cumulative Match Characteristic
FAR	False Accept Rate
FERET	Facial Recognition Technology
FLDA	Fishers Linear Discriminant Analysis
FRR	False Reject Rate
HD	Hamming Distance
LDA	Linear Discriminant Analysis
PCA	Principal Component Analysis
RLR	Ranked List Reinforcement
RPD	Resemblance Probability Distribution
SVM	Support Vector Machine
USTB	University of Science and Technology Beijing

Chapter 1

INTRODUCTION

Nowadays, the emerging need for reliable identity management systems has resulted in a significant attention to this research domain. Identity management systems have been a crucial component of infrastructures that require prevention of impostors from accessing classified resources. These systems have a broad range of applications from government usage, such as border crossing, welfare disbursement, and accessing critical facilities, to more individual oriented usage, such as accessing social networks, accounts and web-based services (e.g. on-line banking). The broad range of the applications and the crucial role of identity management in these practices require identity systems that are able to offer a high level of security.

The task of identity management systems is to give privileges to users based on comparing the information that users provide with the references stored in the database. Over the years, different practices such as knowledge-based (password) and token-based (access cards) are developed to register users to an identity management system. Even though these approaches are easy to implement and have been used in many applications, losing, sharing, and manipulation of these types of identity representations are probable and can endanger the system security [1]. The above issues with conventional methods have shifted researchers' and industry's attention toward biometric-based security approaches, which cannot be stolen, lost, manipulated, and shared [1].

Biometrics are human characteristics that are unique among different individuals. Human's biometrics can be categorized into physiological and behavioral [6]. Figure 1.1 shows some examples of physiological biometrics like face, ear, iris, fingerprint, palmprint, and retina, along with some behavioral biometrics such as voice, signature, and gait. Appli-

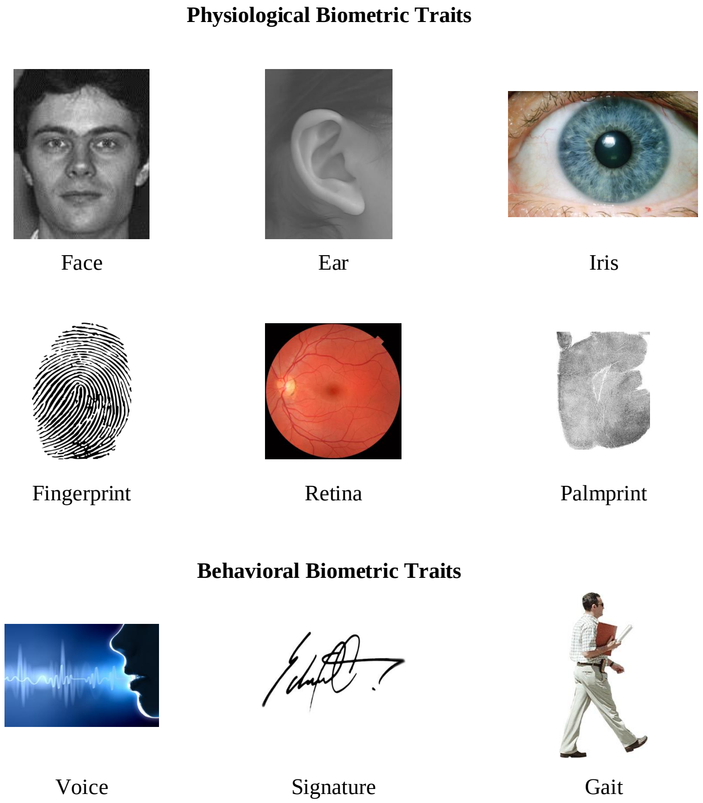


Figure 1.1: Different types of physiological and behavioral biometrics. (Images downloaded from Google image search)

cation domain and scenario determine the choice of proper biometrics. While biometrics cannot be stolen (like access cards) or forgotten (like passwords), biometric systems exploit the uniqueness of biometrics to identify users [6]. Moreover, biometric offers negative recognition, which is a process that prohibits an impostor to claim multiple benefits using different names (such as welfare disbursement) [6].

This thesis addresses the problem of designing a robust biometric security system in the presence of multiple biometrics and varied quality user data. I develop a multimodal rank level biometric system with a novel concept of resemblance probability distributions. Furthermore, I validate it on databases with different characteristic to evaluate its performance.

A summary of the thesis contributions is identified in Section 1.3 of this chapter.

1.1 Biometric Systems

Biometric systems exploit biometrics for user identification/verification. Practically, every biometric system is comprised of two main modules, namely, enrollment and identification/verification modules [7].

The enrollment module collects biometrics from genuine users and extracts representative features from them. The extracted features accompanied with the identity of the users are stored in a database as references. The identification/verification module collects biometrics from individuals requesting access to the system, extracts the same features as enrollment module and compares them with references in the database to determine their identity or genuineness.

Biometric systems can be divided into unimodal and multimodal systems based on the number of different biometrics or modalities they use [1]. Unimodal biometric systems use one biometric to identify/verify the users of the system. Due to intrinsic limitation of using a single biometric, these systems are not able to maintain a high performance as a result of increasing the number of registered individuals. Multimodal biometric systems consolidate more than one biometric or modality to improve the performance of the system.

Different biometrics or modalities provide the system with more information about the users. A multimodal biometric system benefits from this extra information to increase its precision and is expected to have a higher identification rate than unimodal systems based on each of the modalities [8]. The use of a proper fusion technique is essential in consolidating multimodal information. The improper selection of the fusion technique can negatively impact system performance and would result in a low precision, which can be even lower than each unimodal system. Designing an effective fusion module is one of the challenges in multimodal biometric systems [1].

1.2 Key Challenges of Biometric Systems

The introduction of biometric authentication provided the security systems with compelling advantages over traditional password and token-based systems [6]. Even though biometrics have been deployed in real world security systems, there are some challenges associated with such integration, mostly caused by the increase in the number of users, the quality of data, and the system design. Here, I detail some of the key challenges for these systems:

Noisy data: Noise is unrelated data that is associated with acquired data. It can be as a result of unmaintained acquisition devices (such as dirt of fingerprint sensor) or environmental conditions (such as poor illumination for capturing face images or noisy environment for recording voice biometric). Noise can degrade the quality of acquired biometric and as a result, it can affect the system precision. Noisy data may cause rejection of genuine users [9].

Intra-class variation: The intra-class variation issue is the large variance between the feature points of one class. This can happen in situations where proper features are not extracted from the biometric as well as issues with the sensor, the interaction of the user with the sensor (e.g. tilted head while capturing face biometric), changes in the person's biometric over time and environmental conditions such as different lighting or noise. The intra-class variation can be partially addressed by storing multiple instances of biometrics for each user and updating the instances frequently [10].

Inter-class similarity: The similarity between extracted features of different users causes an overlap between their classes. This overlap increases the false recognition rate of the biometric system. Intra-class similarity can be caused by improper feature selection or inherent similarity of some biometric classes (for example the face biometric of identical twins). The number of users registered in the system also affects the inter-class similarity. Increasing the number of users for the same feature set and system configuration can have a negative impact on the system precision [11].

Non-universality: Universal biometric is a biometric that can be obtained from a large set of users. Some biometrics such as iris or signature suffer from the non-universality. For example a blind person cannot register to a biometric system based on iris and also an illiterate is unable to provide a signature. The non-universality of a biometric increases the failure to enrollment [11].

Spoof attacks: Spoof attack is the altering of biometrics in order to cause failure in recognition or creating artificial biometrics of someone's biometric to maliciously access the system. Examples of spoof attack are changing someones fingerprint by scratching the finger to avoid recognition as well as artificially creating a fingerprint sample of a person. Spoof attack is more probable in behavioral biometrics such as voice or signature, since someone can imitate the same biometric as somebody else. The spoof attack can be addressed by checking the aliveness of the subject in case of physical biometric and requiring challenging-responses for behavioral biometric [7].

Security: Since biometrics are intrinsic characteristics of individuals, the leaking of biometrics from the system's database is the violation of users' privacy. Violation of this privacy not only endangers the current system, but also endangers all the other accounts of users that work with the same biometrics and can result in spoof attacks [12].

The aforementioned challenges in biometric systems can be addressed by using multiple biometrics [1]. The extra information provided by using more than one biometric can compensate for noisy data coming from one of the biometric sources. This extra information can also improve the intra-class variation and inter-class similarity. Multimodal biometric systems can also be configured in order to compensate for lack of one biometric to address the non-universality issue. Using multiple biometrics makes the spoof attack harder since the impostor needs to provide more than one biometric of a user.

1.3 Contributions of the Thesis

This thesis focus is on increasing the identification rate in the multimodal biometric system. The main contributions lie in proposing novel approaches for rank level fusion in biometric system based on the idea of resemblance probability distributions. A summary of research contributions in this thesis is as follows:

- Introducing the notion of Resemblance Probability Distribution (RPD) that can be used as a supplementary information along with the ranked list of each biometric matcher to improve the recognition rate and accuracy of the system.
- Proposing the concept of ranked list reinforcement in order to utilize the RPDs in rank level fusion multimodal biometric system (Outcomes appeared in [13]).
- Proposing a novel confidence-based ranked list selection procedure based on RPDs to address the problem of noisy data and inter-class similarity (Outcomes appeared in [14]).
- Augmenting the system with the ranked list reinforcement and confidence-based ranked list selection, which increases the confidence of the lists and results in a higher accuracy in the final decision.
- Generalizing the notion of RPDs to clusters of users and adapting the ranked list reinforcement and confidence-based ranked list selection approaches to operate on clusters.

In addition to the major research contributions, there are the following experimental and development contributions:

- Investigating the effect of reduction of the number of clusters on the multimodal system performance.

- Studying the effect of correlated biometrics e.g. frontal face, profile face, and ear and uncorrelated biometrics e.g. frontal face, ear, and iris to evaluate the performance of the proposed RPD based fusion techniques.

- Implementing and testing unimodal biometrics systems for frontal face, profile face, ear, and iris.

- Developing and testing an architecture for multimodal rank level fusion system with three biometric modalities.

A detailed description of methodology to achieve those contributions is presented below:

- Contribution 1. In this thesis, I introduce the notion of Resemblance Probability Distribution (RPD). RPDs capture the resemblance of different users based on the distance of their data points in the feature space. RPDs of all the registered users are a representation of feature points distribution. The information provided by RPDs can be used as supplementary information along with ranked list of each matcher to improve the recognition rate and accuracy of the system. RPDs can be utilized in various ways to provide extra information about the underlying data that matchers use to make their decisions. Here, I use RPDs along with the rank level fusion for multimodal biometric systems. Rank level fusion is a relatively new trend and has not been studied as other levels of fusion such as score level and decision level. Unlike score level, there is no need for normalization in rank level and this can prohibit the large computational complexity and inaccuracy of final decision due to improper normalization technique. The rank level is not as abstract as decision level, which only provides the final decision of matchers. Furthermore, some off-the-shelf biometric matchers only provide the ranked lists and rank level fusion is the only feasible consolidation technique for them. Here, I propose two approaches, namely ranked list reinforcement and confidence-based ranked list selection, to use this valuable information in rank level fusion to improve the final decisions' accuracy.

- Contribution 2. In order to utilize the RPDs in rank level fusion, I propose the concept of ranked list reinforcement. In multimodal systems, the improvement of recognition rate using different modalities is because of using information about different aspects of the subjects. In the ranked list reinforcement, I took one step further and re-ordered each ranked list based on information provided by RPDs and other ranked lists. The correlation analysis between the RPDs of each user and ranked lists can reveal information about the confidence of ordering in ranked lists. Utilization of RPDs in this manner can alleviate the misclassification due to low quality data and inter-class similarity of modalities. In essence, the reinforcement offers a new rank for each identity in each ranked list by considering its current rank and the confidence of all the other lists about this identity being the actual user's identity. The ranked list reinforcement increases the confidence of the lists and results in a higher accuracy in the final decision.

- Contribution 3. This thesis also proposes a novel confidence-based ranked list selection procedure based on RPDs. Different biometrics have different discrimination ability for recognizing users. This discrimination ability can be considered as a global factor that describes how each matcher works in total. Apart from this fact, the discrimination ability of each biometric matcher can be different for different users. Users with unique biometrics can be recognized with a higher confidence while users with less unique biometrics might be misclassified as other users. The novel confidence-based ranked list selection procedure considers the confidence of each matcher for each test query and finds the best set of ranked lists to provide the highest confidence for any specific test query. This approach selects ranked lists adaptively based on their performance for each test query so that it utilizes the ranked lists that possess the maximum discrimination for that specific test query. Confidence-based ranked list selection procedure is also able to address the problem of noisy data and inter-class similarity by adaptively ignoring the results from matchers that produce ranked lists with low confidence values.

- Contribution 4. This thesis also generalizes the idea of resemblance probability distributions to clusters of users. Users can be clustered based on the extracted features from their biometrics. Clustering of users provides the system with faster response time and lower time complexity. The clusters' resemblance probabilities can be utilized with both ranked list reinforcement and confidence-based ranked list selection approaches with some minor modifications.

- Contribution 5. The number of clusters is an effective factor for a reasonable recognition rate. Decreasing the number of clusters results in considering less information from the distribution of data, while it improves the response time of the system. This thesis also analyses the trade-off between the response time and the accuracy of the system. The analysis of this trade-off can provide insights on the optimum number of clusters depending on the application.

- Contribution 6. Multimodal biometric systems have the highest performance when there are low correlations between the inputs of the fusion module. Highly correlated inputs will not provide new insight about the user and it would work the same as a unimodal system. Here, I studied the effect of correlated biometrics e.g. frontal face, profile face, and ear and uncorrelated biometrics e.g. frontal face, ear, and iris to evaluate the performance of RPD-based fusion techniques. This analysis provides insights on how to select a proper set of biometrics as the input of a multimodal system and it also sheds light on the effectiveness of RPDs in fusion.

- In addition to above, I have implemented and tested unimodal biometrics systems for frontal face, profile face, ear, and iris. The soundness of this individual systems is a key to a successful multimodal system. These unimodal systems are also important to compare the effectiveness of multimodal systems.

- I have developed and tested an architecture for multimodal rank level fusion system with three biometric modalities. Testing the system using various rank level fusion techniques and the approaches based on RPDs shows the effectiveness of RPDs in rank level fusion.

1.4 Proposed Methodology

The main focus of this thesis is to improve the accuracy of multimodal biometric rank level fusion system. The system works with three biometrics, namely face, ear, and iris, which are all captured from the facial area. Face is a common and accepted biometric for identification. Face is an available and universal biometric that is unique and difficult to circumvent. The performance of face biometric is another factor that makes it common in biometric systems. Although acquiring iris images are costly, they provide unique patterns that make them discriminative to use as a biometric for person recognition. Since ear is also extracted from the facial region, it makes the system more focused on a same region of the human body and easier to implement for real world applications. Different matchers are used to classify these individual biometrics. The result of the biometric matchers are used as inputs to the RPD-based rank level fusion module. The ranked list reinforcement and confidence-based ranked list selection approaches and their extension using clustering are the proposed RPD-based fusions that help the system to make the final decision with a higher accuracy. These methods will be extensively tested and proven to be efficient in chapter 5.

1.5 Organization of the Thesis

The thesis has been organized as follows: Chapter 1 provided an introduction on biometric system design and the challenges in this area. It also mentioned the summary of contributions and a big idea on the design of the proposed multimodal system.

Chapter 2 covers the background on multimodal biometric systems by comparing two different objectives of these systems. It explains the advantages of using different modalities/biometrics for a biometric system and then provides information on different levels of fusion for these modalities. At the end, it looks deeper at the rank level fusion methods, which are the focus of this thesis.

The architecture of the multimodal biometric system is described in chapter 3. It starts by explaining the overview of the system and then illustrates the biometric matchers for frontal face, profile face, ear, and iris. The hierarchical clustering is also described for the clustering-based RPDs approaches.

The novel notion of resemblance probability distributions is introduced in chapter 4. Ranked list reinforcement and confidence-based ranked list selection are proposed as two approaches using RPDs to improve the recognition rate of the system. The notion of RPDs is also extended to clusters of users in order to provide the system with a lower response time.

Experimentation has been conducted on proposed methods to show their effectiveness and their ability to improve the recognition rate of the rank level fusion. The results of this experimentation and the effect correlation between modalities are illustrated in chapter 5.

Chapter 6 concludes the thesis by providing a summary of the work and the contributions. It also provides possible future directions for this research.

Chapter 2

MULTIMODAL BIOMETRIC SYSTEMS

There are several factors needed for a biometric to be considered as optimal. A perfect biometric is one which is unique among different individuals, universal, so that any individual can be registered, permanent, collectible and secure [1]. There is no single biometric that can satisfy all these properties. Multimodal biometric systems are used to alleviate this issue. In such systems, more than one biometric is used to authenticate the users. Using multiple biometrics creates a more unique pattern for each user and makes the system more secure. Due to the advantages provided by multimodal biometric systems, they have been considered as a replacement for unimodal ones.

This chapter explains the basics of biometric systems and the advantages of multimodal biometric systems. It will explain also different scenarios in a multimodal biometric system from the information source point of view. Then, different levels of fusion are discussed and post-mapping fusions are explained in more details. At the end of the chapter, well-known rank level fusion approaches that are going to be used for the experimentation are covered.

2.1 Biometric Systems

Biometrics is the science of recognizing humans based on their measurable unique characteristics [15]. Computer systems have been adapted to measure and analyze biometric characteristics to address the problem of identity establishment. These biometric systems comprise four building blocks, which are sensor, feature extraction, matching, and decision modules [6], as depicted in Figure 2.1.

The sensor module is responsible for acquiring biometric information. It can be a camera capturing face pictures, or a microphone that records voice samples of human. The input to the feature extraction module is the acquired biometric from the sensor module. This module is responsible to extract representative and discriminative features from the input data. A good feature extraction module is the one that does not differentiate between different samples of the same user (high intra-class similarity) and perfectly separates different users (high inter-class variance). The extracted features are stored in a database as templates. The sensor module and feature extraction together form the enrollment section of a biometric system. The matching module is responsible for comparing extracted features from new test queries with the templates in the database to determine the degree of their similarity. Based on the similarity metrics from the matching module, the decision module takes the final authentication decision. Some biometric systems also utilize a quality assessment module after the sensor module in order to ensure that the acquired biometric sample is following the required standards. [6].

Biometric systems can be used for the purpose of verification and identification. In verification, the system is required to answer "Am I the person I am claiming?". In this case, the test template of the person is compared with the stored template of the identity that is claimed [1]. Based on the similarity between these two, the system decides to accept or deny the test template. In the verification process, the test query is compared with only one template in the database [6]. The action of verification is done in daily life for the purpose of accessing back account, accessing email, etc.

In identification, the system answers to "Who is the person that provided this biometric?" question. In this process, the test query of a person is compared to all the registered users in the database. The identification can be a closed-set or open-set. In closed-set identification, the system considers that the person providing the biometric is indeed in the database and then tries to identify [16]. In open-set identification, the task is twofold. The system requires to figure out whether the person is registered to the system and then identifies him/her. Open-set identification is also known as "watch-list" [16]. Figure 2.1 demonstrates the enrollment, verification and identification process in a biometric system.

In this thesis, the designed system is a closed-set identification system that works with face, ear and iris biometrics.

2.2 Advantages of Multimodal Biometric Systems

Usage of multiple modalities to recognize the identity of users provides the system with several advantages. Improving the recognition rate, decreasing the number of errors in enrollment of users, and enhancing the system security can be considered as the most important benefits of using multimodal biometric systems [17].

Utilizing multiple biometrics provides more information about the identity of users and this information can be used in order to make a more reliable decision on the identity of the user. For example, it is quite possible to have two individuals in the system with similar faces, which makes the identity recognition hard for a unimodal system. It is quite unlikely that people with similar faces also have similar fingerprints. This extra information helps the system to enhance the recognition rate. On the other hand, the effect of noise and low quality biometrics on the final recognition result can be decreased by using more than one biometric.

By using multimodal biometrics, it is possible to address the problem of biometric non-universality. The non-universality is the fact that some individuals in the population cannot provide certain biometrics or their biometrics are not suitable for recognition [18]. For example, some blind individuals cannot provide iris biometric. Many multimodal biometric systems are able to work in case one of the biometrics is missing and use the other biometrics to recognize the identity of the user.

In order to pass the identification layer, an impostor should provide the multimodal biometric system with more than one biometric simultaneously. Using multiple biometrics makes the penetration of the system harder and yields to a higher security level. Some

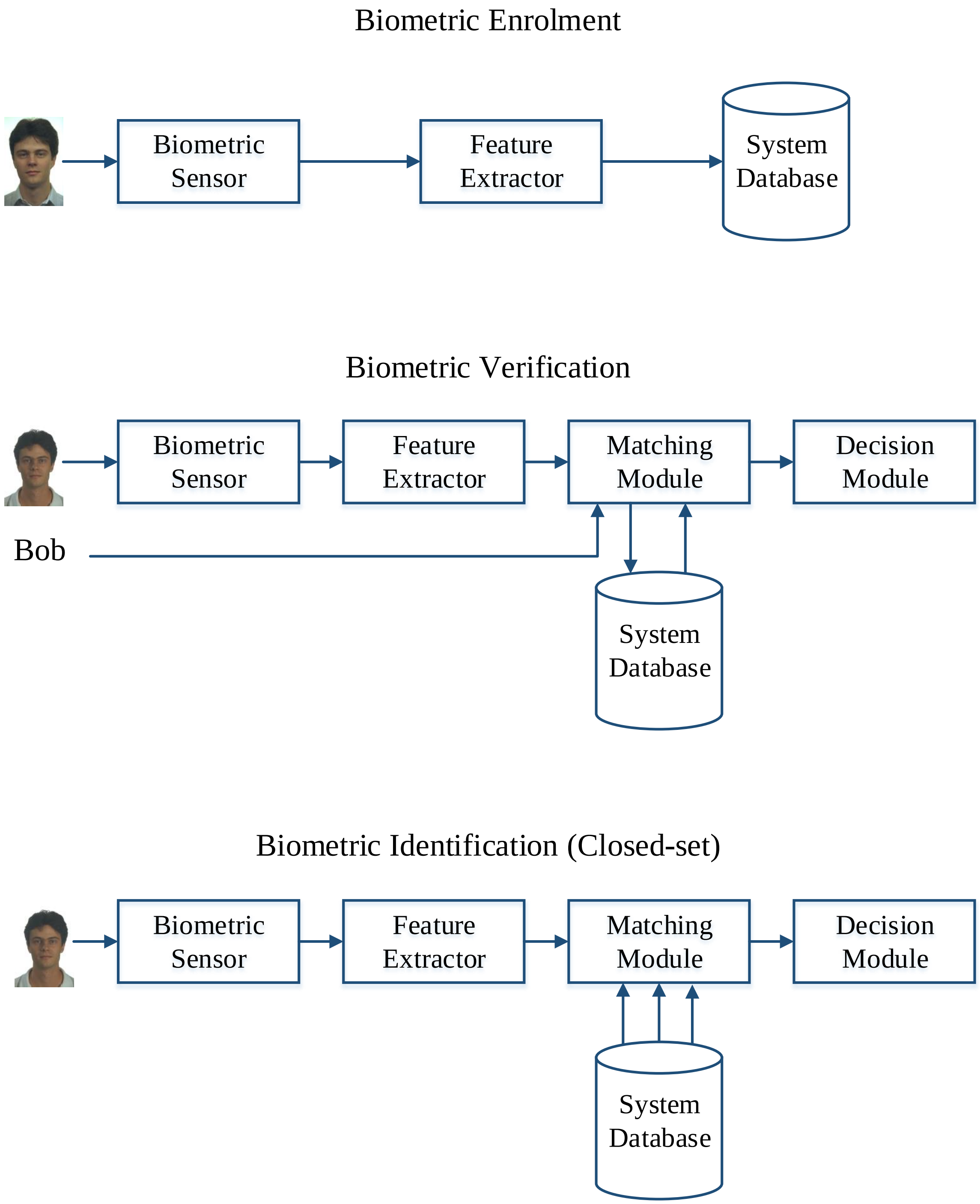


Figure 2.1: The enrollment, verification and identification process in a biometric system [1].

multimodal biometric systems take a step further and try to challenge the user by asking different subsets of biometrics at the identification time [1].

2.3 Information Sources for Multimodal Biometric Systems

Multimodal biometric systems utilize multiple sources of information to identify individuals [19]. The two important design considerations in a multimodal biometric system are the decision on the information sources and the fusion method to consolidate the information [1]. In this section different information sources are introduced and the different fusion methods are covered in the following sections. Based on the information sources, there are six different architectures for multimodal biometric systems [1]. These configurations are as follows [1]:

Multiple sensors - one biometric: These systems capture information about a single biometric using different sensors to get different representations of the biometric. For example, capturing the biometric with 2D, 3D, and X-ray cameras. If a user lacks that specific biometric (non-universality), this type of system would not be usable.

Multiple instances - one biometric: In this category, biometric systems use multiple instances of one biometric to make a recognition decision. For example, the image of retina from both right and left eyes are captured. These systems are efficient since they only need one type of sensor and feature extraction algorithm, while they still suffer from the same issues of correlated biometrics and non-universality.

Multiple algorithms - one biometric: These systems use multiple algorithms to extract features and match one biometric. For example, face matching using eigenfaces, geometry-based methods and dynamic link architecture. These systems can address the issue of correlated biometrics by selection algorithms which produce uncorrelated feature spaces. These systems still suffer from the non-universality issue.

Multiple samples with single sensor - one biometric: These systems capture multiple samples of a single biometric using the same sensor. For example, taking pictures of face with different facial expressions and then using them to create a composite face image.

Multiple biometric: These systems utilize multiple biometrics to recognize users. For example, the proposed system in this thesis uses three different biometrics, namely, face, iris, and ear. These systems are more difficult and expensive to deploy, since they need different sensors for each biometric and also different algorithms to match those biometrics [20]. On the other hand, these systems are able to provide a higher recognition rate and address the non-universality issue.

Hybrid systems: These systems make use of more than one of the mentioned architectures to provide a robust identification. For example, a multimodal system may uses three different biometrics and for each biometric, it may use multiple algorithms for matching.

2.4 Fusion for Multimodal Biometric Systems

Fusion is defined as [21]: "An information process that associates, correlates and combines data and information from single or multiple sensors or sources to achieve refined estimates of parameters, characteristics, events and behaviors". A fusion method should be able to recognize the part of information that is reliable [22]. Different disciplines such as signal and image processing [23], data mining [24], Forex trading [25], etc. use fusion techniques, so that information fusion is now recognized as a stand alone research area.

Multimodal biometric systems also require the fusion of information provided from different sources. Fusion approaches can be categorized into pre-mapping and post-mapping techniques [26]. As Figure 2.2 demonstrates, sensor level and feature level fusions are the two subcategories of the pre-mapping, while match score, rank, and decision level fusions are subcategories of post-mapping.

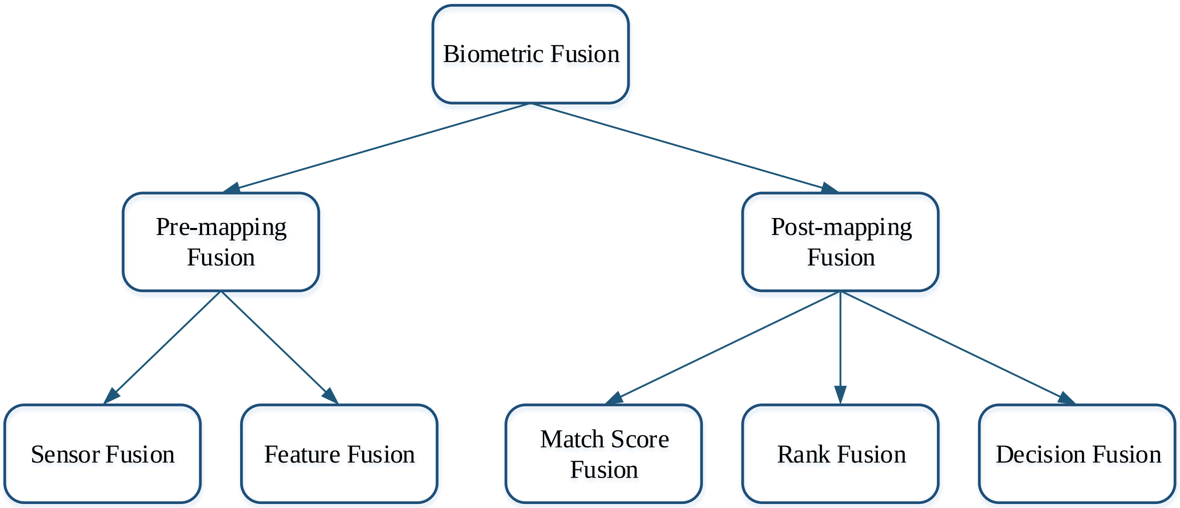


Figure 2.2: Multimodal biometric fusions classification [2].

2.4.1 Pre-Mapping Fusion

In pre-mapping, fusion occurs before matching the data from multiple sources. The data at this stage are rich in information, since no feature extraction or dimensionality reduction have been applied to them. On the other hand, there are some implementation problems, such as complex feature extraction and matcher design, that are associated with this category [27]. Sensor and feature level fusions are in this category.

Sensor Level Fusion

In sensor level fusion, raw data from sensors consolidate together before applying any feature extraction [1]. In one research [28], 2D face images and 3D face range data (different sensors) are consolidated to create a new 3D representation of the face. They used a probabilistic graphical model for the classification. Another project [29], combined multiple faces captured from a single camera using a mosaic method in order to enhance the recognition rate. In another research [30], the sensor data from the face and palm-print was fused by particle swarm optimization. The Kernel Direct Discriminant Analysis features were extracted from the fused data and the nearest neighbour classifier was used for their classification. In this research, the recognition performance was tested against score level fusion and also using different optimizations like genetic algorithm.

Feature Level Fusion

Feature level fusion consolidates the extracted feature points to create an extended feature points representation. This level of fusion still contains rich amount of information about the acquired data from the sensors and they are expected to provide better results [1]. For example, the hand geometry features are consolidated with PCA features from face and created a new feature space with higher number of dimensions [31].

In research by Feng et al. [32], face and palm-print were fused at the feature level using PCA and ICA features. Their results in a validation framework were an indicator of superiority of ICA in feature level fusion. In 2010, Rattani et al. [33] concatenated normalized features from face and fingerprint and then used dimensionality reduction techniques to address the problem of high dimensional feature space. They compared the recognition accuracy against match score level fusion. In recent research [34], face and iris were fused at the feature level using a new method based on minimum spanning tree. The comparison of their proposed method with traditional feature extractions like PCA, 2DPCA, and KPCA was an indicator of a better recognition result.

There are several drawbacks in using this level of fusion. First, the high-dimensional feature space created by fusing all the feature spaces will cause the “curse of dimensionality” problem. Second, since the features are coming from different feature spaces, normalization is required to alleviate the effect of significant range difference between feature spaces. Third, most commercial biometric systems do not allow access to features, which makes the deployment of this level of fusion impossible [31].

2.4.2 Post-Mapping Fusion

Post-mapping fusions refer to those fusion techniques that fuse the results obtained by different matchers. For each test query, biometric matchers provide a list of identities based on their similarity to the test query. Based on the nature of the list provided by the matcher, there are three different levels of fusion, namely, score level, rank level, and decision level. From score level to decision level, the amount of information reaching the fusion module decreases. In this section, I introduce these levels of fusion.

Match Score Level Fusion

In score level, each matcher provides a list of match scores associated with each identity, which represent the similarity of identities to the test query. This list is called the score list. Match score fusions do not restrict the scenario of multibiometric systems, for example, it can be used in case of multiple instances of a biometric or different biometrics from different sensors [19].

Match score fusion can be done by applying mathematical operations like summation or multiplication on the scores from different matchers. Since scores are generated from different modalities or different matchers, normalization of scores is an essential step before fusion. The normalization is time consuming and at the same time, the inappropriate selection of normalization would result in non-acceptable recognition results [1].

Hong and Jian [19], used face and fingerprint data in a match score fusion scenario. Their experiment on a public domain face database and the MSU fingerprint database [35] illustrated the superiority of score level fusion to using single biometrics.

Jian et al. [36] used different score level fusion techniques for fusing face, fingerprint and hand geometry. They normalized the scores from biometric matchers using seven different techniques and tested the sum-rule, max-rule, and min-rule score fusion methods. In all the cases the score level fusion resulted in a better performance except MAD normalization method.

In 2010, He et al. [37] evaluated the performance of sum-rule and Support Vector Machine (SVM) in the score fusion of fingerprint, face, and finger vein. They noticed that the performance of sum-rule is highly dependent on the selected normalization method.

Decision Level Fusion

The decision level fusion approaches are used in cases that each matcher only provides the final result. In the verification mode the final result is either accept or reject and in identification is the most similar identity to the query. Logical operators like “AND” and “OR” rules, decision table, Bayesian decision, and majority voting can be used to fuse matchers results and make the final decision [1]. Since “AND” and “OR” rules fusion methods have high False Reject Rate (FRR) and False Accept Rate (FAR), they are rarely used in real applications. The two common approaches for decision level fusion are majority voting and weighted majority voting, which are more reliable [1]. Chatzis et al. [38] proposed a clustering algorithm based on fuzzy k-mean, fuzzy vector quantization, and median radial basis function network for decision level fusion of voice and face. The comparison of their proposed methods with OR, AND, and k-mean showed that median radial basis function network performs better in decision level fusion, especially when the number of modalities is two.

Rank Level Fusion

Rank level fusion is used when the output of each biometric matcher is a ranking of identities in the database [1]. This list of identities, which is sorted based on their similarity to the test query, is called ranked list. The highest rank is associated with the identity that is the most similar to the test query. There are some biometric matchers that only provide a ranking of identities as the output [39]. Additionally, sometimes scores provided by different multimodal systems are not suitable for fusion and converting the scores to ranked lists and applying rank level fusion is more suitable [39]. The rank fusion approaches take the ranked lists from different biometric matchers and create a single ranked list by consolidating those.

Rank fusion has been used in different research areas such as social voting theory [40], collaborative filtering [41], bioinformatics [42], information retrieval [43], and documents ranking [44]. Recently, rank fusion has drawn researchers' attention to its application in multimodal biometrics [8, 45, 46].

In research in 2010 [39], palmprint from two different biometrics databases were used for multimodal rank fusion. The authors applied Borda count, logistic regression, maximum rank and nonlinear weighted ranking for the rank fusion of biometrics matchers outcome. Their experimental results revealed that the nonlinear weighted ranking method has a better capacity in improving the recognition performance.

Monwar et al. [47] suggested using a fuzzy rule inference system to multimodal rank fusion. They compared the proposed fuzzy rank fusion system with other rank level approaches as well as score level and decision level methods. Their experimental outcome showed not only a better recognition result, but also a better system response time.

In 2009, Abaza and Ross [48] introduced an approach for quality based rank level fusion. Their approach enhanced the system performance in case of low quality data and weak classifiers. Their experimental results showed a notable performance improvement with the proposed fusion approach. Marasco et al. [49] did an analysis of stability of rank level fusion in the presence of low quality biometric data. Their study with rank and score level fusion of low quality face data and synthetically degraded fingerprints showed that rank level fusion has a better performance in case of small degradations, while both rank and score will not perform well with a great amount of degradations. Alam et al. [50] proposed a quality measure that does not require previous modeling of environmental noise. Their method used the deviation of score data from their mean to calculate a confidence measure and then they used this confidence measure in the rank fusion of face and voice biometrics. Their method showed a better performance in comparison with Borda count and highest rank fusion methods. Since in some situation in rank fusion, the score data is not available, their method is not applicable to all the rank level fusion systems.

Rank level fusion is still a new approach for multimodal biometric systems. Previous researches on rank level fusion have not approached the problem of finding the best biometric matchers for each specific test query. Moreover, improvement of biometric systems to achieve higher recognition rates is an important priority for high security applications. This thesis addresses these issues by the means of fusion techniques based on resemblance probability distributions.

2.5 Description of Well-known Rank Level Fusion Methods

The concentration of this thesis is on the rank level fusion. The reason behind this concentration is that in most biometric systems the match score is not available [39] and they only provide rank information. On the other hand, the match score provided by biometric matchers are not always suitable for fusion [1]. The rank level methods are also not as abstract as decision level approaches and they have more information available for fusion. Rank level fusion is a relatively new multimodal biometric fusion approach that still has the capacity for more research.

Three of the well-known rank level fusion approaches are highest rank, Borda count, and logistic regression [1]. This thesis uses these fusion methods as the basis for fusion. This section describes these methods.

Suppose X as the test query that its identity is going to be recognized between n identities $\{id_1, id_2, ..., id_n\}$ registered in the system. There are n_b different biometrics (matchers) and the fusion module should fuse the results of matchers.

2.5.1 Highest Rank

In highest rank fusion, each identity is assigned the highest rank (minimum of the rank) among different ranked lists, a.k.a. biometric matchers. The fusion rank for identity i using highest rank method is calculated as [1]:

$$s_i = \min_{j=1}^{n_b} r_{j,i} \tag{2.1}$$

where $r_{j,i}$ is the rank of user i in the ranked list of biometric j and s_i is the consolidation rank from different ranked lists for identity i. The fusion ranked list is created by sorting of s_i increasingly. If ties happen between the ranks of identities, they will be randomly broken to create a linear ordering of identities. This fusion method is suitable for scenarios that the number of ranked lists are few and the number of identities is large. Highest rank fusion utilizes the strength of each biometric matcher [51].

2.5.2 Borda Count

The Borda count sums over the rank of each identity in all the ranked lists. The rank of identity i is calculated as [1]:

$$s_i = \sum_{j=1}^{n_b} r_{j,i} \tag{2.2}$$

where $r_{j,i}$ is the rank of user i in the ranked list of biometric j and s_i is the consolidation rank from different ranked lists for identity i. The final ranked list is created by sorting s_i , $i = 1, ..., n$ in an increasing order. Borda count is known as an unsupervised voting method, which means it does not consider the performance of the matchers and treats them all equally.

2.5.3 Logistic Regression

In Borda count, all ranked lists from matchers are treated equally for the fusion. Although, in reality all the matchers do not have the same discrimination ability. Logistic regression is basically the generalized version of the Borda count method. It does a weighted sum over the ranks from different matchers. For the user i, the fusion rank using logistic regression is calculated as [1]:

$$s_i = \sum_{j=1}^{n_b} w_j r_{j,i} \tag{2.3}$$

The weight w_j is a measure of matcher j performance. Determining the value of weights requires a training phase in advance.

2.6 Motivations

The need for higher security has always been a concern for society. Higher security for biometric systems can be provided by higher recognition rate. This goal can be achieved by designing better unimodal biometric matchers and also better performing fusion modules.

The dynamic quality assessment of matchers has been done based on the score information previously. The score information is not always available and some biometric matchers only provide rank information. It is important to devise methods to find the quality of matchers based on rank information.

Finding the best performing biometrics for each individual query is an important factor in identification rate of the biometric system. For example, it is known that face is a better performing biometric than ear in general cases. For distinguishing identical twins, the ear might be a better biometric though. The similarity between biometrics of different individuals is common and it is important to find best performing biometrics for each query to the system.

This thesis addresses these needs by incorporating information from distribution of users' biometric in the feature space, using this information to improve the ranked lists confidence and fusing the best performing biometrics for each test query.

2.7 Chapter Summary

This chapter explained biometric systems and their components. Multimodal biometric systems were introduced to enhance the recognition rate and the security of unimodal systems as well as addressing the non-universality problem. Information fusion is an important part of a multimodal biometric system. Different levels of information fusion were presented and post-mapping fusions were explained in more details by providing a review of previous researches in this field.

Chapter 3

ARCHITECTURE DEVELOPMENT OF THE MULTIMODAL BIOMETRIC SYSTEM

In this chapter, the proposed architecture of the multimodal biometric system based on resemblance probability distributions is introduced. The developed system utilizes frontal face, ear, and iris as biometrics and then applies the rank level fusion for decision making. Profile face is also used instead of ear to examine the effect of correlating the biometrics (frontal and profile face) on the system's performance. This chapter starts with an overview of the proposed multimodal biometric system and continues by introducing biometric algorithms for matching faces (frontal/profile), ears, and irises. At the end, an introduction to the concept of Resemblance Probability Distributions (RPD) is given.

The proper selection of biometrics is an essential task in any multimodal biometric system. There is no single biometric which is the best for all the applications and requirements. The selection of biometrics should be based on the type of the system operation (identification/verification), perceived risks, types of users, and specific requirements for security [52]. Since each biometric has its own advantages and disadvantages, a single biometric is not always able to satisfy all the requirements [52].

One of objectives of this thesis is to study the effect of resemblance probability distributions utilization for rank level fusion. For this purpose, the frontal face, the ear, and the iris are selected as main biometrics. Profile face is also used for observing the effect of correlation between the biometrics. All these biometrics are from the facial area of the human body which is easy and convenient for data acquisition [19]. Also, there are effective indexing and comparison methods for these biometrics, that is why I have chosen them for my multimodal biometric system.

Although rank level fusion has been extensively studied in other fields, such as voting theory, distributed database, collaborative filtering, and bioinformatics [53] [54] [41] [42], there are few works that studied it in the context of the multimodal biometric systems [8] [45] [48]. In identification systems where the only output of unimodal biometric matcher is a relative ranking of identities, rank level fusion is the only feasible option for consolidation of biometric information.

In my research, I have introduced *Resemblance Probability Distributions (RPD)* as a representation of the users' distribution in the feature space. I have developed two methods, namely *Ranked List Reinforcement* (RLR) and *Confidence-Based Ranked List Selection* (CBRLS), to utilize resemblance probability distributions to improve the recognition rate of a rank level fusion method. The main benefit of the proposed methods based on resemblance probability distribution is that they can recover the information about the performance of individual biometric matchers, which is usually lost due to the relative ranking of identities in a typical rank level system.

This chapter starts with an overview of the multimodal biometric system for rank level fusion that deploys resemblance probability distributions. Then, it looks closely at conventional unimodal biometric matchers for face (frontal/profile), ear, and iris as the building blocks of a multimodal system. It continues by providing an overview of a unimodal matcher that extracts resemblance probability distribution from the feature space of a biometric.

3.1 System Overview for Rank Level Fusion

Every multimodal biometric system that operates in identification mode consists of three important modules: *enrollment*, *identification*, and *system database*. These three modules are demonstrated in Figure 3.1 for the proposed multimodal biometric system based on resemblance probability distributions. This multimodal biometric system works with three biometrics, but in general it can operate with more biometrics.

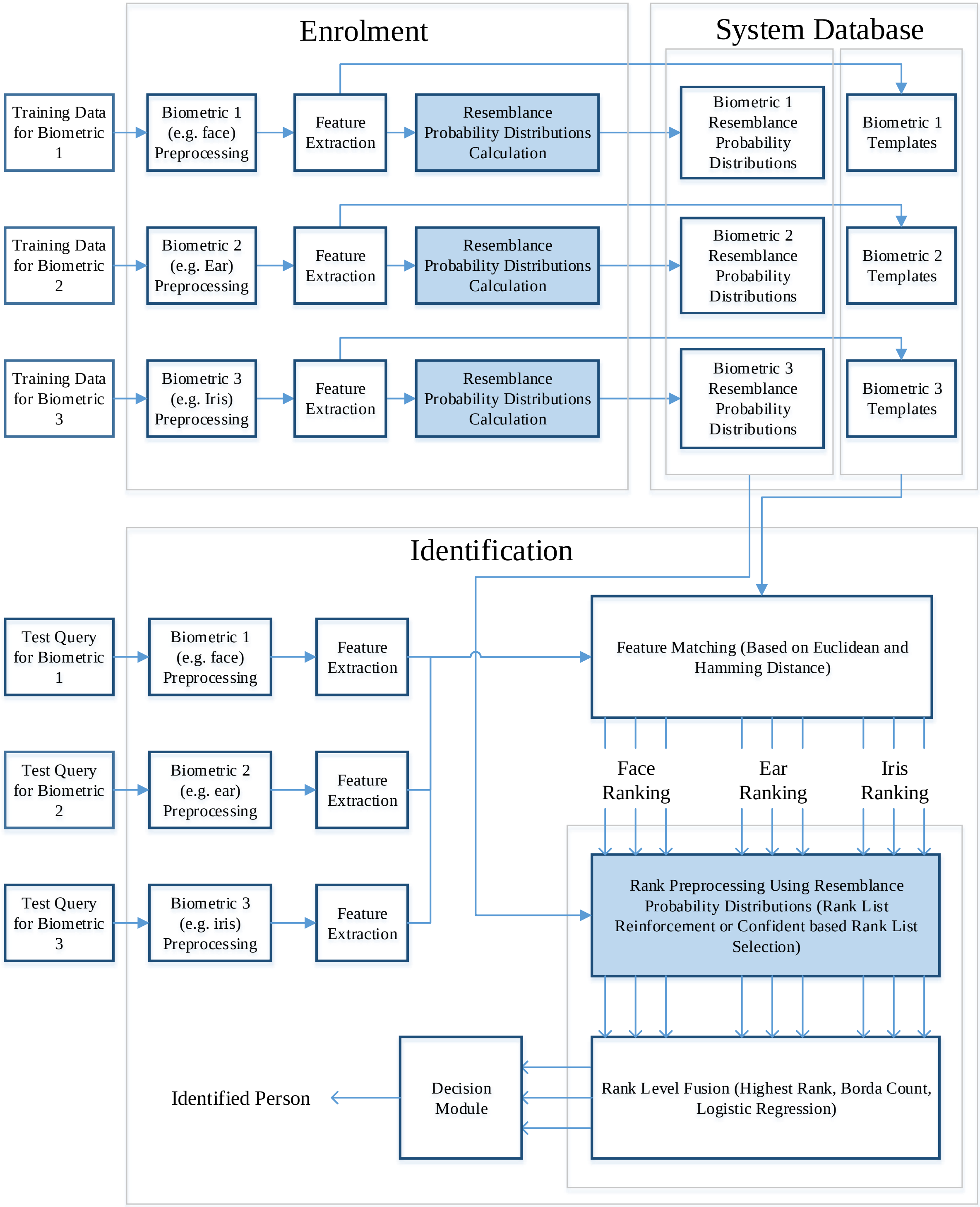

Enrolment
System Database
Training Data for Biometric 1
Biometric 1 (e.g. face) Preprocessing
Feature Extraction
Resemblance Probability Distributions Calculation
Biometric 1 Resemblance Probability Distributions
Biometric 1 Templates
Training Data for Biometric 2
Biometric 2 (e.g. Ear) Preprocessing
Feature Extraction
Resemblance Probability Distributions Calculation
Biometric 2 Resemblance Probability Distributions
Biometric 2 Templates
Training Data for Biometric 3
Biometric 3 (e.g. Iris) Preprocessing
Feature Extraction
Resemblance Probability Distributions Calculation
Biometric 3 Resemblance Probability Distributions
Biometric 3 Templates
Identification
Test Query for Biometric 1
Biometric 1 (e.g. face) Preprocessing
Feature Extraction
Test Query for Biometric 2
Biometric 2 (e.g. ear) Preprocessing
Feature Extraction
Test Query for Biometric 3
Biometric 3 (e.g. iris) Preprocessing
Feature Extraction
Feature Matching (Based on Euclidean and Hamming Distance)
Face Ranking
Ear Ranking
Iris Ranking
Rank Preprocessing Using Resemblance Probability Distributions (Rank List Reinforcement or Confident based Rank List Selection)
Rank Level Fusion (Highest Rank, Borda Count, Logistic Regression)
Decision Module
Identified Person

Figure 3.1: The proposed multimodal biometric system based on resemblance probability distributions for rank level fusion.

In Figure 3.1, during the enrollment, specific biometric samples of users are presented to the system as images. The biometrics that are used for this system are face, ear, and iris, but the system can operate with any other biometric as long as a proper feature extraction module is utilized. For better validation, we also utilized profile face as an alternative to ear to test the effect of correlated biometrics. The acquired biometric samples pass through some preprocessing (if needed) for illumination correlation and localization (for example, iris localization using Hough transform). Enrollment module extracts representative features from these images in order to make it possible to compare them against each other. The extracted features create a D-dimensional feature space, where every biometric sample resides as a point. Resemblance probability distributions capture the resemblance of each user's biometric samples to all the other users' samples in this feature space. All the resemblance probability distributions for each biometric can represent the distribution of users in the feature space. Figure 3.2 represents the distribution of users' faces in the feature space using the first three Fisherfaces.

Fisher image projection is used for extraction of features from face (frontal / profile) and ear. It creates a more compact representation of images, and thus we are able to discriminate better between different users' biometric samples. It is robust to illumination change, occlusion of biometric samples (for example, hair occluding ear), shifting, background noise and image scaling [55]. Iris code is extracted from the iris by utilizing 2D Gabor filter [56] as a comparable template for comparing irises with each other.

The extracted features from the samples and the resemblance probability distributions of each user's biometrics are stored in a database alongside with the identity of the user they belong to. This database is the reference for the identification module to compare queries with the registered users and determine their identity.

The identification module extracts the same features as the enrollment module from each test query. It compares the extracted features of the test query to all the registered users in

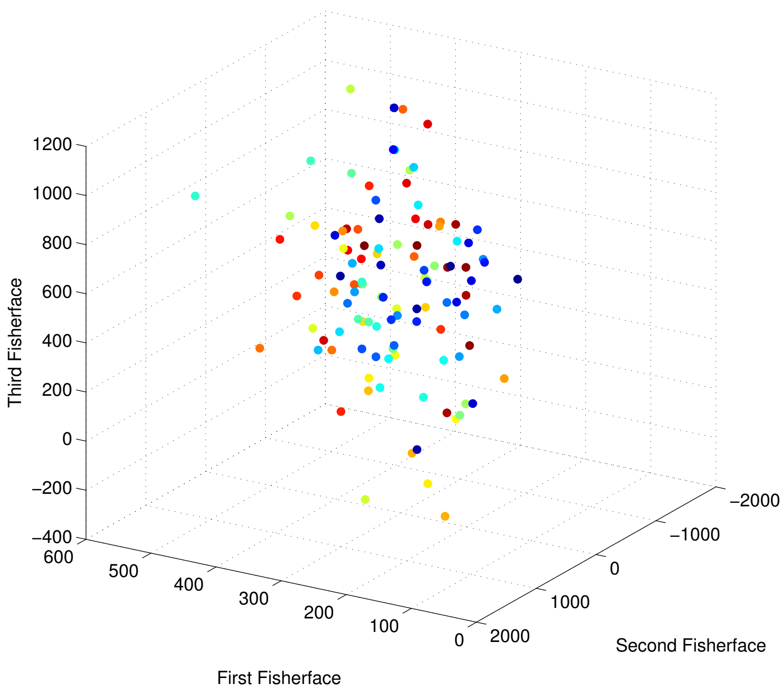
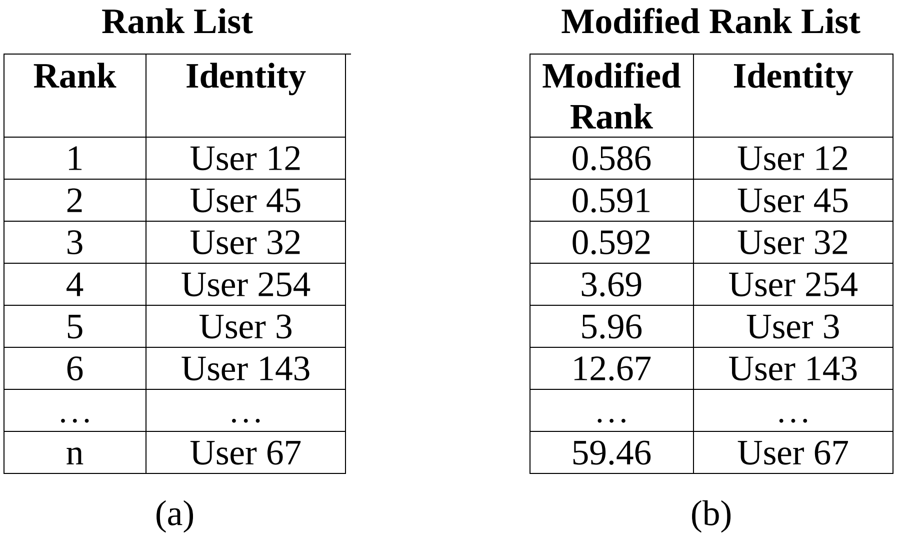


Figure 3.2: Demonstration of feature space for 113 faces of FERET database [3] using the first three Fisherfaces. Each color represents a user.

the database. This comparison can be done in different forms depending on the biometric and the type of extracted features. For measuring the similarity of extracted features for the face (frontal / profile) and the ear, the Euclidean distance between the features of the test query and registered users is used. For iris, the Hamming distance [57] between the generated iris codes is used. For each biometric, the feature matching provides a list of users that are ranked according to their similarity to the test query. These lists are called ranked lists. Figure 3.3 (a) represents a ranked list for n users.

Unlike conventional multimodal systems, the proposed system uses the resemblance probability distribution to modify the ranked lists. The modification reinforces the ranks by the similarity of different biometric ranked list and resemblance probability distributions of each user. After the ranked list modification, any rank level fusion algorithm can be used to fuse the list of different biometrics and find the final decision about the identity of the test query. Figure 3.3 (b) represents a modified ranked list for n users.



Rank List

Rank	Identity
1	User 12
2	User 45
3	User 32
4	User 254
5	User 3
6	User 143
…	…
n	User 67

(a)

Modified Rank List

Modified Rank	Identity
0.586	User 12
0.591	User 45
0.592	User 32
3.69	User 254
5.96	User 3
12.67	User 143
…	…
59.46	User 67

(b)

Figure 3.3: ranked list (a) and modified ranked list (b) for a test image of a biometric with n users. Unlike modified ranked list, the ranked list considers that the distance between each user and its immediate neighbor is one. This abstraction hides the actual distribution of users.

Although the system in Figure 3.1 responds in real time for each test query, in order to accelerate the system response time, another architecture is detailed in Figure 3.4. It has been observed that users who are in close distance in the feature space possess similar resemblance probability distributions. This architecture benefits from this similarity and clusters the users. Each cluster consists of users who have similar resemblance probability distributions. For each cluster, only a single resemblance probability distribution is stored in the database and during the identification, a fewer number of resemblance probability distributions are used for ranked list modification. The response time of the architecture in Figure 3.4 is thus decreased by using clustering.

The next section walks through the conventional unimodal biometric matchers for the face (frontal / profile), the ear and the iris. The feature extraction and similarity measure between the extracted features are detailed in that section.

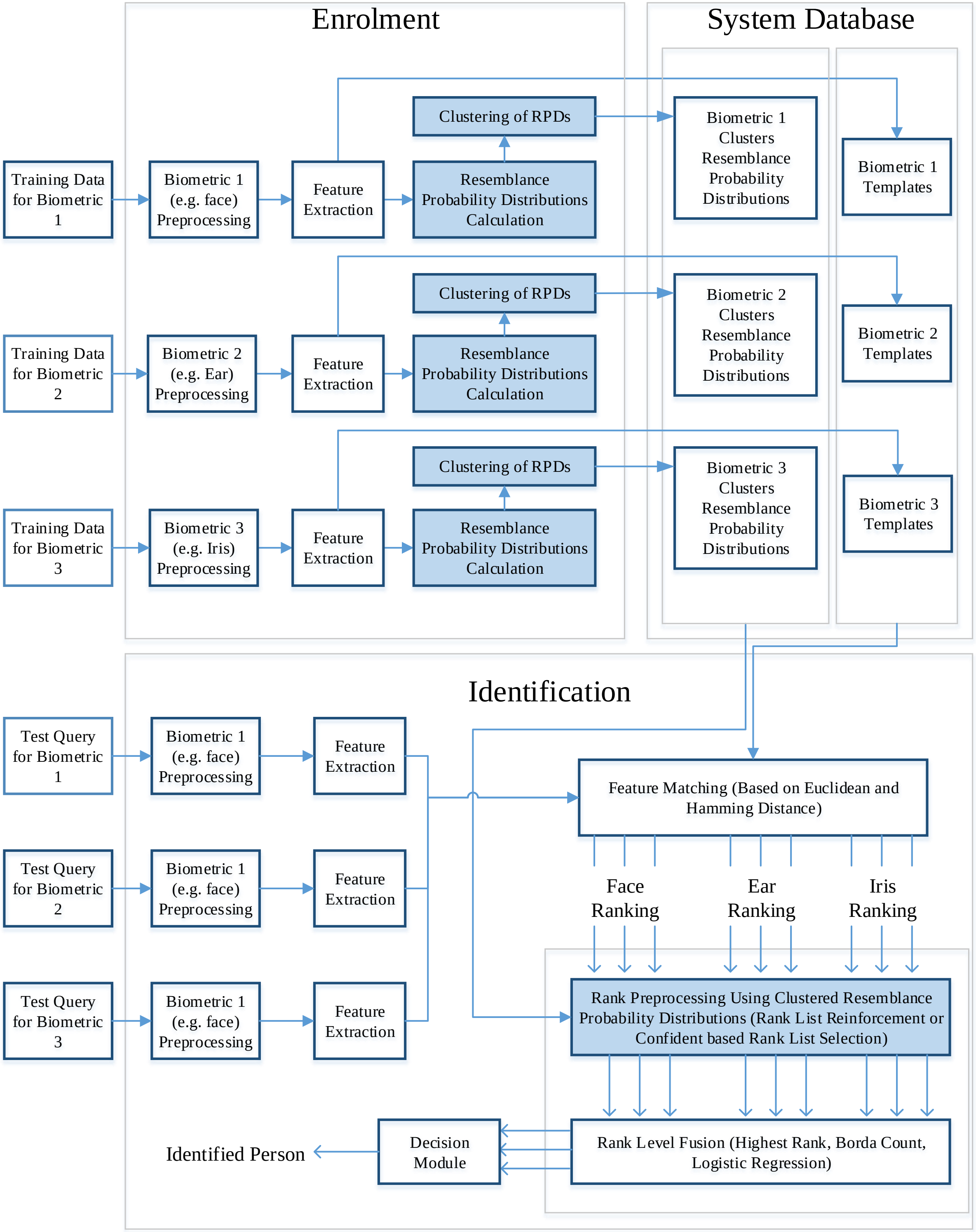

Enrolment
System Database
Training Data for Biometric 1
Biometric 1 (e.g. face) Preprocessing
Feature Extraction
Resemblance Probability Distributions Calculation
Clustering of RPDs
Biometric 1 Clusters Resemblance Probability Distributions
Biometric 1 Templates
Training Data for Biometric 2
Biometric 2 (e.g. Ear) Preprocessing
Feature Extraction
Resemblance Probability Distributions Calculation
Clustering of RPDs
Biometric 2 Clusters Resemblance Probability Distributions
Biometric 2 Templates
Training Data for Biometric 3
Biometric 3 (e.g. Iris) Preprocessing
Feature Extraction
Resemblance Probability Distributions Calculation
Clustering of RPDs
Biometric 3 Clusters Resemblance Probability Distributions
Biometric 3 Templates
Identification
Test Query for Biometric 1
Biometric 1 (e.g. face) Preprocessing
Feature Extraction
Test Query for Biometric 2
Biometric 1 (e.g. face) Preprocessing
Feature Extraction
Test Query for Biometric 3
Biometric 1 (e.g. face) Preprocessing
Feature Extraction
Feature Matching (Based on Euclidean and Hamming Distance)
Face Ranking
Ear Ranking
Iris Ranking
Rank Preprocessing Using Clustered Resemblance Probability Distributions (Rank List Reinforcement or Confident based Rank List Selection)
Rank Level Fusion (Highest Rank, Borda Count, Logistic Regression)
Decision Module
Identified Person

Figure 3.4: The proposed multimodal biometric system based on clustered resemblance probability distributions for rank level fusion.

3.2 Unimodal Matchers

A multimodal biometric system is basically a combination of some unimodal biometric matchers. The unimodal matchers' performance has a substantial effect on the whole performance of the multimodal system. In this section, each of the unimodal matchers for the face (frontal / profile), the ear, and the iris are described. Fisher's linear discriminant analysis is used for feature extraction of the face and ear. The Euclidean distance is used to compare features of the face and the ear biometric. The iris code is used as a feature for iris samples and Hamming distance between them is used as a similarity measure. Although unimodal biometric matchers introduced here do not extract Resemblance Probability Distributions (RPD), it is important to introduce them as the building blocks, so that the RPD module will be added to them later. At the end of this chapter, the overview of a single biometric matcher that uses RPDs is discussed and its implementation is detailed in the next chapter.

3.2.1 Frontal Face Matcher

The face matcher responsibility is to recognize users based on their faces. First, the face matcher is trained by different face image samples for each user. At the identification stage, a test face query image is presented to the face matcher and it provides a list of users sorted based on their similarity to the test query. The face matcher needs to extract some features from face images in order to compare faces. There are two major approaches for feature extraction from intensity face images [58]. The feature-based (structural) face recognition methods consider the relative distance of facial elements and extract local features from them. Examples of feature-based methods are geometry-based methods [59] [60], dynamic link architecture [61] [62], and Convolution Neural Network [63]. The second approach is based on holistic methods. This approach takes the whole face image as their input and extracts some representative features from the whole face image. Successful examples of holistic approach are Eigenfaces [64] and Fisherface [55] methods.

Among different feature extraction methods, Fisherface is the most popular due to its robustness to background noise, scaling, occlusion, illumination changes, and various facial expressions [55]. Fisherface is a combination of Principal Component Analysis (PCA) [65] and Linear Discriminant Analysis (LDA) [66]. The idea behind PCA is to create a transformation matrix to transform the data to a subspace which compresses the data with minimum loss in the standard deviation. PCA maintains the standard deviation of data points by considering the spread of data in feature space and finding new dimensions that the data has the highest standard deviation along them. In other words, PCA maximizes the scatter matrix for training face images. The drawback of PCA is that it does not consider the class of data points while maximizing the scatter matrix for them.

Fisherface is a combination of PCA and LDA which is also called Fisher LDA or FLDA. It benefits form the available class labels to provide a better discrimination between different users. Unlike PCA, FLDA attempts to find a projection that maximizes the scatter between different users while minimizing the scatter between the sample faces of each user. In the FLDA feature space, samples of each user are close to each other while different users are apart. The FLDA transformation matrix is calculated using standard methods [64] and [55], which is summarized in the rest of this subsection.

The FLDA transformation matrix is calculated based on the training data. Each training face image is converted to a vector as illustrated in Figure 3.5. Training face matrix that consists of multiple face vectors for each user is formed as [55]:

$$Training \quad matrix = [s_1^{u_1}...s_{m_{u_1}}^{u_1} \quad s_1^{u_2}...s_{m_{u_2}}^{u_2} \quad ...... \quad s_1^{u_n}...s_{m_{u_n}}^{u_n}] \tag{3.1}$$

where $s_j^{u_i}$ is a vector representation of jth face sample of user u_i. m_{u_i} is the number of training samples for user u_i and n is the total number of users.

The between-class scatter matrix S_B and within-class scatter matrix S_W are defined as [55]:

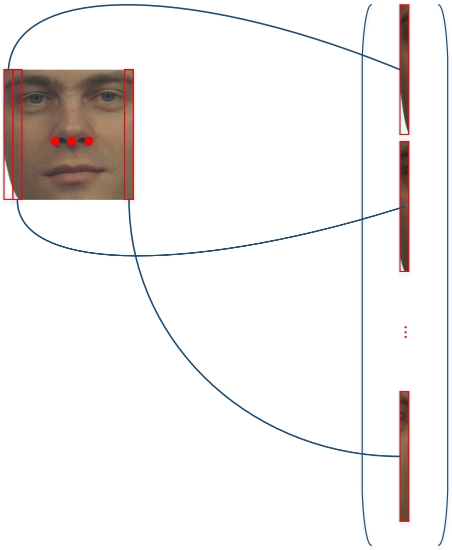


Figure 3.5: The vectorization process of face images. Columns of the face image stacks over each other to create a vector.

$$S_B = \sum_{i=1}^{n} m_{u_i} (\Psi_i - \Psi)(\Psi_i - \Psi)^T \tag{3.2}$$

$$S_W = \sum_{i=1}^{n} S_i \tag{3.3}$$

where Ψ is the arithmetic average of all the face vectors in the training set and Ψ_i is the average of each user's face vectors. The average value of each user's face vectors is used for inner class variation calculation to understand how much faces of a specific user can vary. S_B represents an average deviation of each user's average face vector from the average of all the users'. S_i which is the scatter of user i is defined as [55]:

$$S_i = \sum_{j=1}^{m_{u_i}} (s_j^{u_i} - \Psi_i)(s_j^{u_i} - \Psi_i)^T \tag{3.4}$$

The within-class scatter S_W shows an average deviation of all the users' face vectors from their own average face vectors. The deviation of all the face vectors from the average face vector of all users is called the total scatter matrix, which is defined as [55]:

$$S_T = \sum_{i=1}^{n} \sum_{j=1}^{m_{u_i}} (s_j^{u_i} - \Psi)(s_j^{u_i} - \Psi)^T \tag{3.5}$$

Fisher's Linear Discriminant Analysis (FLDA) tries to project the data to a subspace that increases the between-class scatter and decreases the within-class scatter. To obtain this objective, the projection that maximizes the fraction of between-class scatter to within-class scatter is needed. Mathematically speaking, the optimal projection W_{opt} is defined as [55]:

$$W_{opt} = \arg\max_{W} J(W) \tag{3.6}$$

The discriminant power $J(W)$ is defined as [55]:

$$J(W) = \left| \frac{W_T.S_B.W}{W_T.S_W.W} \right| \tag{3.7}$$

Maximizing the discriminant power J with respect to W will lead to finding a projection W_{opt} that satisfies the maximization and minimization of between-class and within-class scatters respectively. Combining equation 3.6 and 3.7 leads to the full description of the function that is needed to be optimized [55]:

$$W_{opt} = \arg\max_{W} \left| \frac{W_T.S_B.W}{W_T.S_W.W} \right| = [w_1 \quad w_2 \quad ... \quad w_p] \tag{3.8}$$

where $\{w_1, w_2, ..., w_p\}$ is the set of eigenvectors of S_W and S_B corresponding to p largest eigenvalues $\{\lambda_1, \lambda_2, ..., \lambda_p\}$. The optimization can be solved by the solution for the generalized eigenvalue problem [55]:

$$S_B w_i = \lambda_i S_W w_i, \qquad i = 1, ..., p \tag{3.9}$$

The maximum number of non-zero eigenvalues is n-1 where n is the number of users. So the maximum value for p is n-1.

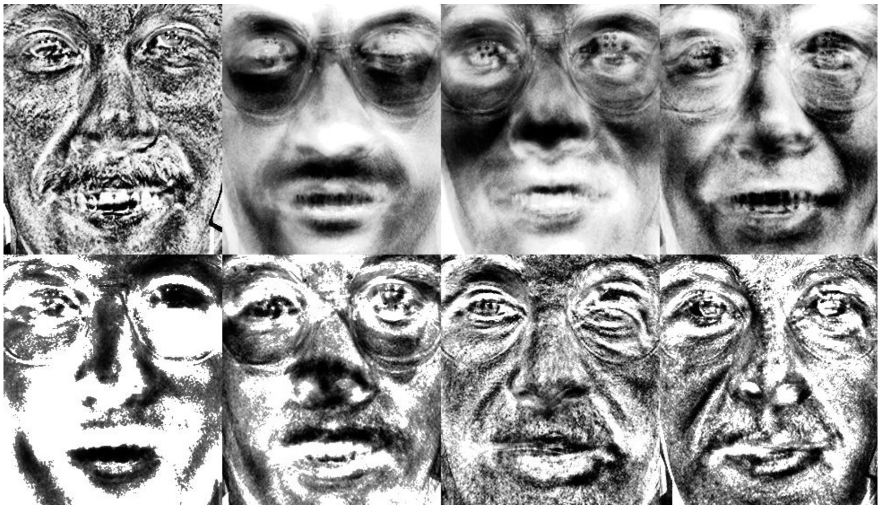


Figure 3.6: Fisherfaces based on some images from FERET database [3].

After solving the generalized eigenvalue equation 3.9, $W_{opt} = [w_{opt1}, w_{opt2}, ..., w_{optp}]$ will be the transformation matrix for FLDA space. The transformation of face vectors to the FLDA space can be done by [55]:

$$pr(\Phi_j^{u_i}) = W_{opt}^T . \Phi_j^{u_i} \tag{3.10}$$

where Φ_i is the difference of face vector $s_j^{u_i}$ and all the users' average face vector Ψ as follows [55]:

$$\Phi_j^{u_i} = s_j^{u_i} - \Psi \tag{3.11}$$

The projected faces to the FLDA space are called Fisherfaces and have lower number of dimensions in comparison with the original face vectors. The training of the face matcher is done by projecting all the sample images of each user to the FLDA space. Figure 3.6 presents Fisherfaces created based on some images from FERET database [3].

The identification module of the face matcher requires to determine a list of identities based on their similarities to a new test face query. To fulfill this goal, the test query image needs to be converted to a vector and then projected to the FLDA space using the W_{opt} projection matrix. At first, the test face query vector $face_t$ is subtracted from the average face vector of training set using equation 3.11 to obtain Φ_t. For the mean subtracted test

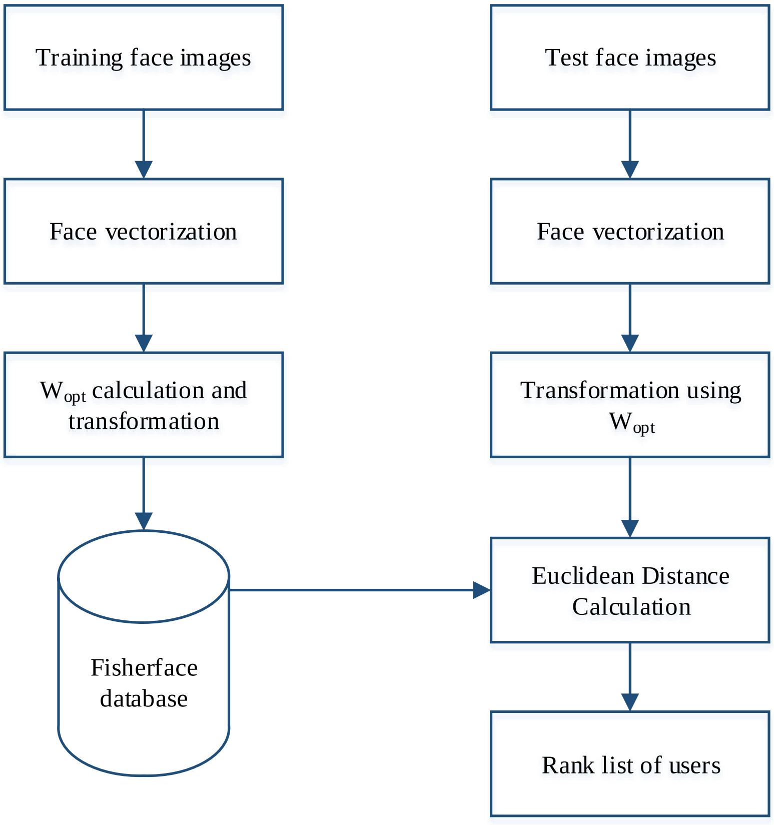


Figure 3.7: Flowchart of the face matcher based on FLDA (Adapted from [2]).

face query vector Φ_t the projection is calculated as follows [55]:

$$pr(\Phi_t) = W_{opt}^T . \Phi_t \tag{3.12}$$

The similarity of the projected test face query to the training faces in the FLDA space is calculated using the Euclidean distance. The distance of the test face query from each user's faces in the training set is calculated as:

$$D(face_t, u_i) = \sqrt{\sum_{j=1}^{m_{u_i}} [pr(\Phi_t) - pr(\Phi_j^{u_i}))(pr(\Phi_t) - pr(\Phi_j^{u_i}))^T} \tag{3.13}$$

The ranked list is created by ascending sorting of the identities based on their distances to the queried face. Figure 3.7 presents the flowchart of the face matcher based on Fisherface.

3.2.2 Profile Face Matcher

The only difference between the profile and the frontal face is the angle of image acquisition. The profile face matcher is essentially the same as the frontal face matcher. For the profile face, first the image is localized and then the transformation matrix is created. All the profile face images are transformed into the FLDA space. During the identification, a ranked list of users based on their similarity to the queried test profile face is created using the same approach that is explained for the frontal face.

3.2.3 Ear Matcher

Human ear contains a rich structure that makes it a good choice for identification. Despite the fact that humans are not capable of distinguishing between ears [67], studies on PCA based face and ear recognition showed that the ear has the same discriminative capability as the face [68].

Ear databases that are selected for testing the proposed multimodal biometric system are not acquired in same illumination. The Fisher's linear discriminant analysis [55] is robust to illumination change. Some research [2] suggested using the same approach as Fisherface for the ear biometric, which is called Fisherear. In this approach, ears are projected into the FLDA space and the Euclidean distance is used to find the similarity of the two Fisherears.

The first step is the conversion of ear images to ear vectors, which can be done using the same approach that is demonstrated in Figure 3.5 for faces. After this conversion, the within-class scatter S_B, the between-class scatter S_B, and the total scatter S_T matrices are created based on the training matrix for the ears. The optimum transformation matrix W_{opt} is calculated by solving the generalized eigenvalue problem for equation 3.8 [2].

All training ear vectors are projected into the FLDA space using equation 3.10 and 3.11. Figure 3.8 shows some samples of ear from USTB database [4] and the corresponding Fisherears are shown in Figure 3.9.

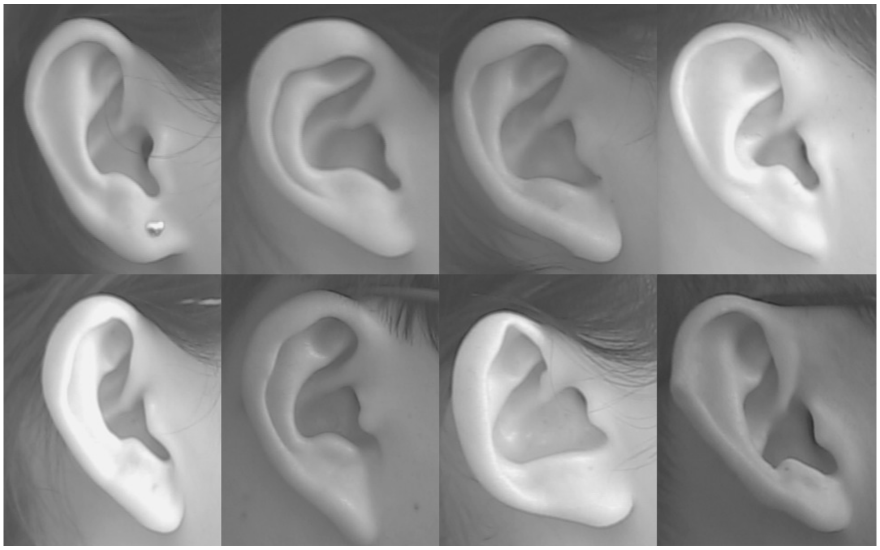


Figure 3.8: Examples of ears from USTB database [4].

Each Fisherear is a point in the FLDA space and their similarities are computable using Euclidean distance. For any test ear image, first the image is converted to a vector and then it is projected into FLDA space using equation 3.12. The distance from the test ear to each class in the FLDA space is calculated using equation 3.13. The ranked list is created by ascending sorting of identities based on their distance to the test ear.

3.2.4 Iris Matcher

Iris is a muscular part of the eye that controls the amount of light entering the pupil [69]. Because of its detailed structure, it has very distinctive features, such as ridges, rings, arching ligaments, and a zigzag collarette, for human identification [69]. Iris is a planar surface that is robust to viewing angle and change of view only causes affine transformation to its structure. The non-affine transformation caused by dilation of the iris is also reversible.

The first step for creating an iris matcher is the iris localization in an eye image. Since iris has a circular shape, its location and boundary can be localized using circle Hough transform [70]. The circle Hough transform uses a voting scheme to detect circles in images. The robustness of Hough transform to partial occlusion makes it ideal for iris localization, since some part of iris might be occluded by eyelid. Figure 3.10 describes the process of iris

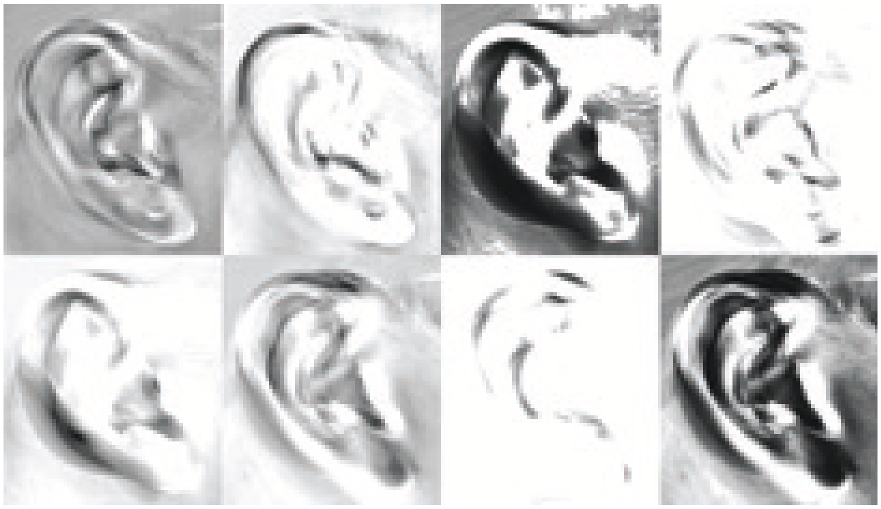


Figure 3.9: Fisherears corresponding to ear in figure 3.8.

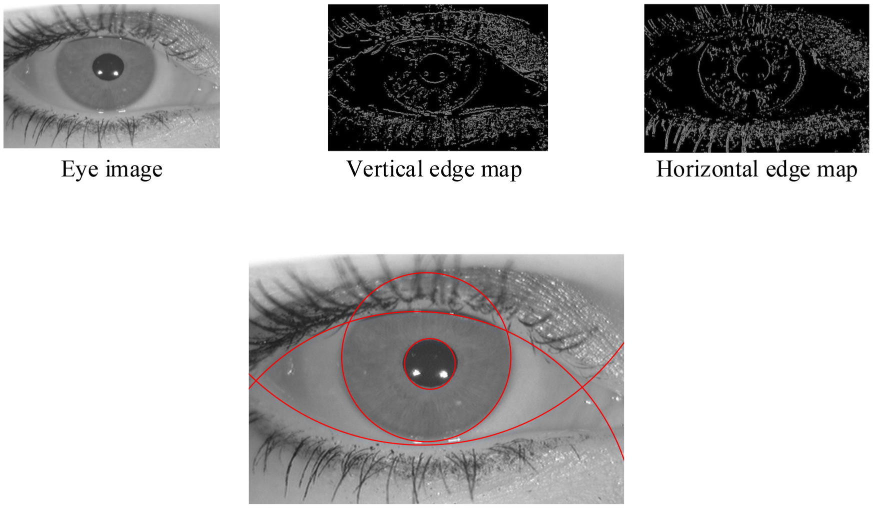
localization that is suggested by Wildes [71]. In order to apply circle Hough transform, eye image needs to be converted to an edge map. In Figure 3.10, the eyelid and the pupil edges are the strongest edges in the horizontal edge map of the image. Applying the circle Hough transform on this horizontal edge map results in localization of eyelids and the pupil. The vertical edge map contains the edges of the outer boundary of the iris. The area of the iris that is occluded by eyelid is considered as noise and a noise mask is created to exclude this part.

The *homogeneous rubber sheet model* is used for transforming pixels from an iris region to a polar coordinate [5]. Figure 3.11 illustrates the process of homogeneous rubber sheet model where each pixel from the Cartesian location (x, y) is transformed to (r, θ), where r is in the range of $[0, 1]$ and θ is in $[0, 2\pi]$. This mapping is done as [72]:

$$I(x(r,\theta), y(r,\theta)) \longrightarrow I(r,\theta) \tag{3.14}$$

with,

$$x(r,\theta) = (l-r)x_p(\theta) + rx_i(\theta) \tag{3.15}$$



Eye image

Vertical edge map

Horizontal edge map

Iris localization using circle Hough transform

Figure 3.10: The process of iris localization using edge maps and circle Hough transform.

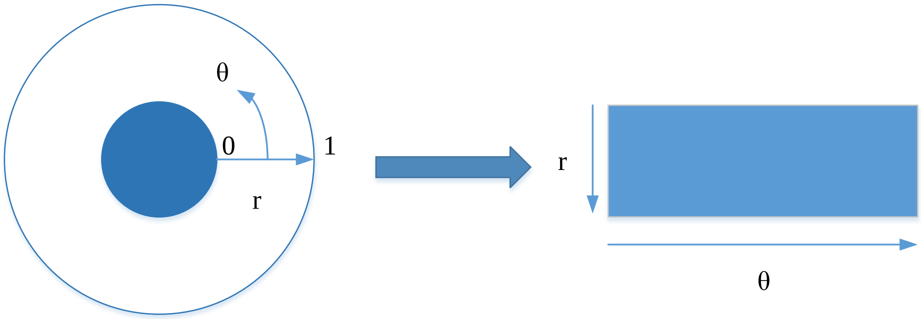


Figure 3.11: The homogeneous rubber sheet model [5].

$$y(r,\theta) = (l - r)y_p(\theta) + ry_i(\theta) \tag{3.16}$$

where for the iris region $I(x,y)$ the coordinates (x,y) and (r,θ) are the Cartesian pixel coordinates and corresponding normalized polar coordinates. (x_p,y_p) and (x_i,y_i) are the center location of pupil and iris circles along θ direction.

The iris code is the extracted features from the iris normalized rubber sheet, which is calculated using a 2-D Gabor filter as follows [69]:

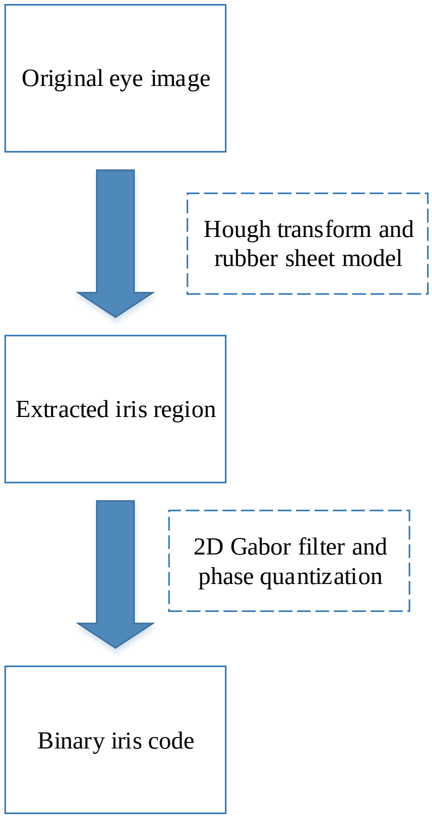

Original eye image
Hough transform and rubber sheet model
Extracted iris region
2D Gabor filter and phase quantization
Binary iris code

Figure 3.12: The process of iris code generation [2].

$$h_{\{Re,Im\}} = sgn_{\{Re,Im\}} \int_{\rho} \int_{\phi} I(\rho,\phi) e^{-i\omega(\theta_0,\phi)} e^{-(r_0-\rho)^2/\alpha^2} e^{-(\theta_0-\phi)^2/\beta^2} \rho d\rho d\phi \tag{3.17}$$

where $I(\rho,\phi)$ is the iris in polar coordinate, α and β are effective width and length of the Gabor wavelet, ω is the Gabor wavelet frequency and r_0 and θ_0 are the center coordinate of the region that equation 3.17 calculates. $h_{\{Re,Im\}}$ is a binary complex number that the value of its real and imaginary parts can be either 0 or 1. These values are determined by the sign of the two dimensional integral over ρ and ϕ in equation 3.17. Figure 3.12 summarizes the process of iris code generation.

The iris code consists of binary numbers. The distance between two binary numbers can be calculated using Hamming distance (HD) [57]. The distance between two iris codes is calculated as follows [69]:

$$HD = \frac{\parallel C_A \oplus C_B \cap M_A \cap M_B \parallel}{\parallel M_A \oplus M_B \parallel} \tag{3.18}$$

where C_A and C_B are iris codes for image A and B and M_A and M_B are their corresponding noise masks. The $\oplus$ and $\cap$ are XOR and AND operators. $\parallel x \parallel$ means the number of non-zero bits in the bit vector x.

Based on the Hamming distance, every test iris image can be compared against other users in the database and the ranked list of identities can be created in the same way as the face and ear biometric.

3.3 Biometric Matcher with Resemblance Probability Distribution

The main contribution of this thesis is the introduction of resemblance probability distributions and deploying them for rank level fusion in multimodal biometric systems. For the sake of simplicity, there were no module for resemblance probability extraction in the biometric matchers introduced for the face, the ear, and the iris. This section introduces the architecture of a single matcher with resemblance probability distribution and the next chapter will provide more details on its realization.

Resemblance probability distribution (RPD) for each user represents the similarity of that user to all the other users. This information can be extracted from the feature space of the training data. Figure 3.13 illustrates the architecture of a single biometric matcher with the RPDs extraction module. After creating the feature space from the training data, the RPD module uses that information for creating the RPDs for all users in the training set. The RPDs are stored in the database alongside the extracted features. During the ranked list creation, the system solely uses the extracted features and does not use RPDs. RPDs are used after the creation of ranked lists by all the unimodal matchers to modify the ranked lists to improve the recognition.

The details of the RPDs extraction and its utilization for ranked list modification is

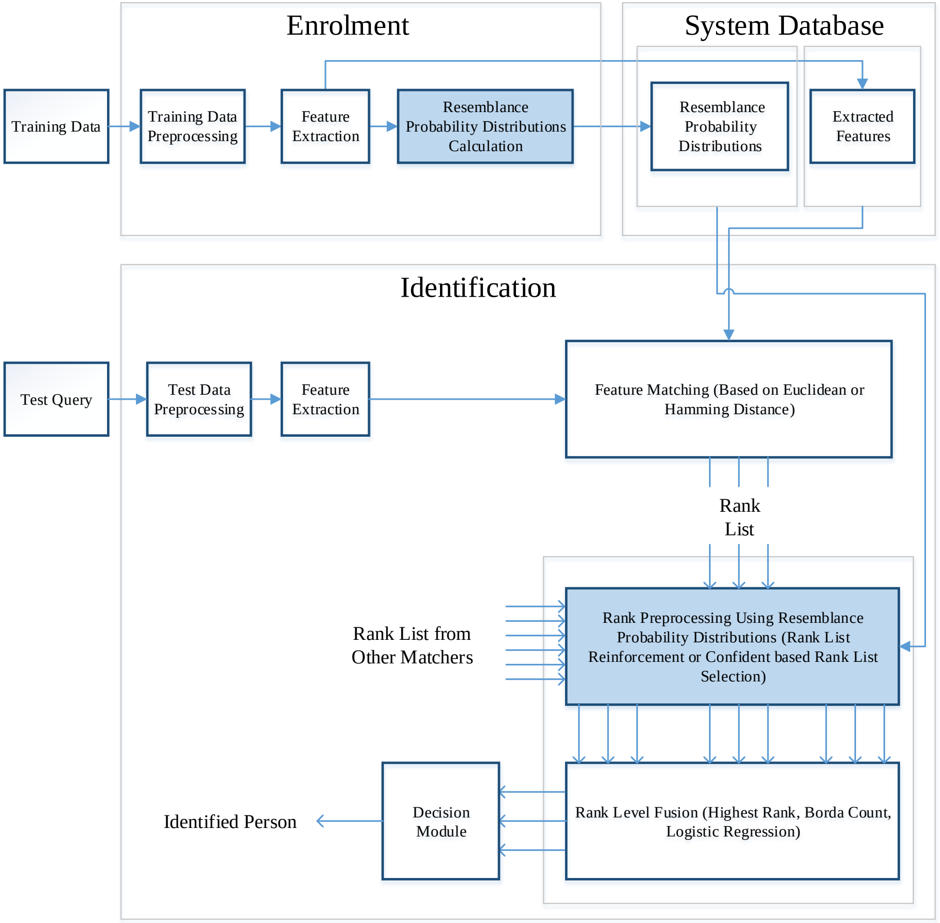

Enrolment
System Database
Training Data
Training Data Preprocessing
Feature Extraction
Resemblance Probability Distributions Calculation
Resemblance Probability Distributions
Extracted Features
Identification
Test Query
Test Data Preprocessing
Feature Extraction
Feature Matching (Based on Euclidean or Hamming Distance)
Rank List
Rank List from Other Matchers
Rank Preprocessing Using Resemblance Probability Distributions (Rank List Reinforcement or Confident based Rank List Selection)
Identified Person
Decision Module
Rank Level Fusion (Highest Rank, Borda Count, Logistic Regression)

Figure 3.13: Architecture of a unimodal biometric matcher with resemblance probability distribution modules.

explained in the next chapter.

3.4 Chapter Summary

This chapter introduced the overall architecture of the multimodal biometric system using the novel concept of resemblance probability distributions. The resemblance probability distribution is able to recover information about the performance of each biometric matcher for each test query. The chapter also introduced the novel approach to cluster the users in order to benefit from the similarities of resemblance probability distributions for a faster response time. It provided reasons behind selection of face (frontal / profile), ear, and iris for this system. The conventional unimodal matchers for face, ear, and iris were designed. For face and ear, Fisherface and Fisherear approaches were used for feature extraction and Euclidean distance was used for comparing different faces and ears. For iris, Hough transform was used for localization and Gabor filter for feature extraction. Hamming distance was used as a distance measure between different irises. At the end, the architecture for conventional unimodal matchers was extended to contain the module for resemblance probability distribution.

Chapter 4

PROPOSED CONFIDENCE-BASED RANK LEVEL FUSION

In biometric systems, after registering the users using the training data, the system is ready to specify the identity of new samples of the registered users. These new samples are called test queries. The goal of the biometric system is to recognize the user to whom the test query belongs. In multimodal biometric systems that operate using the rank level fusion model, each biometric matcher creates a ranked list of users identity for each test query. A ranked list is a relative ordering of possible users identity based on the similarity to the test query [1]. In the ranked list, the probability of each identity being the identity of the test query is not specified. The only available information is the ranking, i.e. 1, 2, 3, 4 and so on. In the ranked list, the identity with the rank r has a higher probability to be the actual identity of the test query than the identity with the rank $r+1$. Since ranked list only contains the ranking of identities, the information about the probability of each identity being the actual identity of the test query is abstracted as ranking. This abstraction of probabilities conceals the accuracy of the matchers for each test query. In this thesis, I proposed an approach to improve the confidence of rank list based on information from the distribution of users' biometrics in the feature space. Figure 4.1 demonstrates the general overview of this system.

This chapter introduces the notion of Resemblance Probability Distribution (RPD) to retain the lost information due to the abstraction probabilities in the ranked lists and uses this information to obtain a higher recognition rate. Ranked list reinforcement (RLR) and confidence-based ranked list selection (CBRLS) are two new rank fusion methods based on the idea of resemblance probability distributions. At the end of this chapter, the notion of

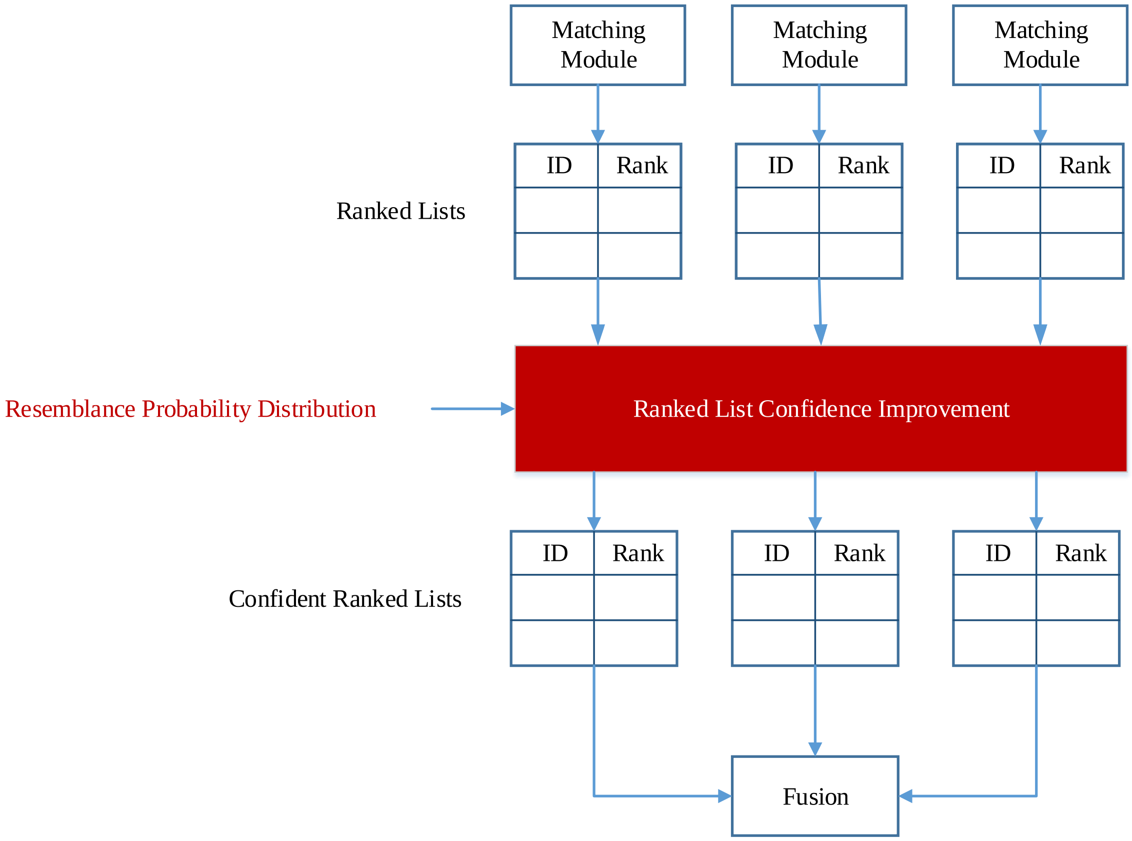


Figure 4.1: Overview of the system to improve the confidence of ranked lists. The confidence improvement is a layer between the biometric matchers and the fusion module takes ranked lists as inputs and provide more confidence ranked lists as the output.

RPD is generalized to clusters of users in order to accelerate the fusion module's decision making process.

4.1 Resemblance Probability Distributions

A Resemblance Probability Distribution (RPD) essentially represents the probability of each user being classified as all enrolled users to the system. The resemblance probability distributions provide the system with an insight on how probable is the misclassification of each user's biometrics with other users' biometrics and also how probable is the correct classification of each user. RPDs are beneficial for rank level fusion, since for each test query, RPDs dynamically retain the information about the performance of each matcher. The utilization of these performance measures helps the fusion module to consolidate the ranked lists with a higher confidence and results in a more accurate recognition of the test query's identity.

In order to formally introduce the resemblance probability distribution, it is essential to provide a definition for the distance from one user to another. Suppose that there are n registered users $U = \{u_1, ..., u_n\}$ and the multimodal biometric system works with n_b biometrics, namely $B = \{b_1, ..., b_{n_b}\}$. For any biometric b_j of user u_i, consider there are m ($m > 1$) training samples $S^{u_i,b_j} = \{s_1^{u_i,b_j}, ..., s_m^{u_i,b_j}\}$. Feature points extracted from S^{u_i,b_j} are $F_{S^{u_i,b_j}} = \{f_{s_1^{u_i,b_j}}, ..., f_{s_m^{u_i,b_j}}\}$. I define the distance from the user u_i to $u_{i'}$ for biometric b_j as follows:

$$D_{b_j}(u_i, u_{i'}) = \begin{cases} 1/m \sum_{k=1}^{m} \min_{l \in \{1,...,m\}} \|(f_{s_k^{u_i,b_j}} - f_{s_l^{u_{i'},b_j}})\|, & \text{if } i \neq i^{'} \\ 1/m \sum_{k=1}^{m} \min_{l \in \{1,...,m\}-\{k\}} \|(f_{s_k^{u_i,b_j}} - f_{s_l^{u_{i'},b_j}})\|, & \text{if } i = i^{'} \end{cases} \tag{4.1}$$

where $\|(f_{s_k^{u_i,b_j}} - f_{s_l^{u_{i'},b_j}})\|$ is the magnitude of the difference vector $(f_{s_k^{u_i,b_j}} - f_{s_l^{u_{i'},b_j}})$. The first part of equation 4.1 defines the distance of the user u_i from the user $u_{i'}$ $(i \neq i^{'})$ as an average of the minimum distances from samples feature points of u_i to $u_{i'}$. As figure 4.2 demonstrates, the distance from user u_i to user $u_{i'}$ $(i \neq i^{'})$ is calculated by considering the feature point of each biometric sample of user u_i and finding the feature point of the user $u_{i'}$ that is in the closest distance to it. The average of all these minimum distances is the distance from u_i to $u_{i'}$. As it can be inferred from the definition, the distance from user u_i to $u_{i'}$ is not necessarily the same as the distance from user $u_{i'}$ to u_i. Figure 4.3 elaborates the underlying reason for this dissimilarity. In figure 4.3, the user u_i has a dense distribution of feature points with a small variance, while user $u_{i'}$ feature points are more sparsely distributed and they have an overlap with user u_i. As it is obvious from the distributions, it is more probable to misclassify user u_i as user $u_{i'}$ while there is a lower probability for user $u_{i'}$ to be misclassified as user u_i. The second part of equation 4.1 defines the distance of user u_i from

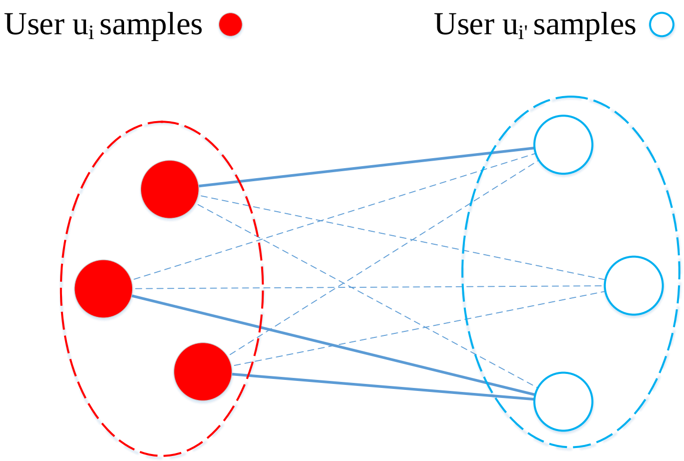


Figure 4.2: The lines represent the distances of user u_i feature points from user $u_{i'}$'s. The solid lines are the shortest distance to reach user $u_{i'}$ from user u_i feature points. Distance from user u_i to user $u_{i'}$ is the average of these minimum distances.

itself as the average of distances from each sample's feature point of user u_i to the closest sample's feature point of the same user.

Suppose D_{u_i,b_j} is a vector representing the distances from user u_i for biometric b_j to all the users (including itself). D_{u_i,b_j} can be transformed to a similarity measure by subtracting all the distances from the maximum value in the vector D_{u_i,b_j}. I define the resemblance probability distribution of user u_i as follows:

$$PRD(u_i) = \frac{\max\left(D_{u_i,b_j}\right) \times \vec{1}_n - D_{u_i,b_j}}{\|\max\left(D_{u_i,b_j}\right) \times \vec{1}_n - D_{u_i,b_j}\|} \tag{4.2}$$

where $\vec{1}_n$ is a vector of ones with size n and $\|\max\left(D_{u_i,b_j}\right) \times \vec{1}_n - D_{u_i,b_j}\|$ is the magnitude of $(\max\left(D_{u_i,b_j}\right) \times \vec{1}_n - D_{u_i,b_j})$. Formula 4.2 calculates the normalized similarity of u_i to all the users (including itself). The resemblance probability distribution of each user shows the distribution of all the users in relation to that user. Algorithm 1 demonstrates the process of creating RPDs for all users. For each biometric, the algorithm iterates through all users, calculates the distance of that user to all the users, and finally calculates the resemblance probability distribution of that user. RPDs for all the users represent the distribution of the

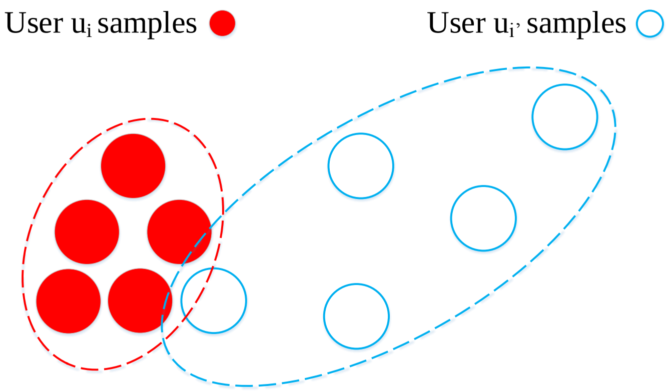
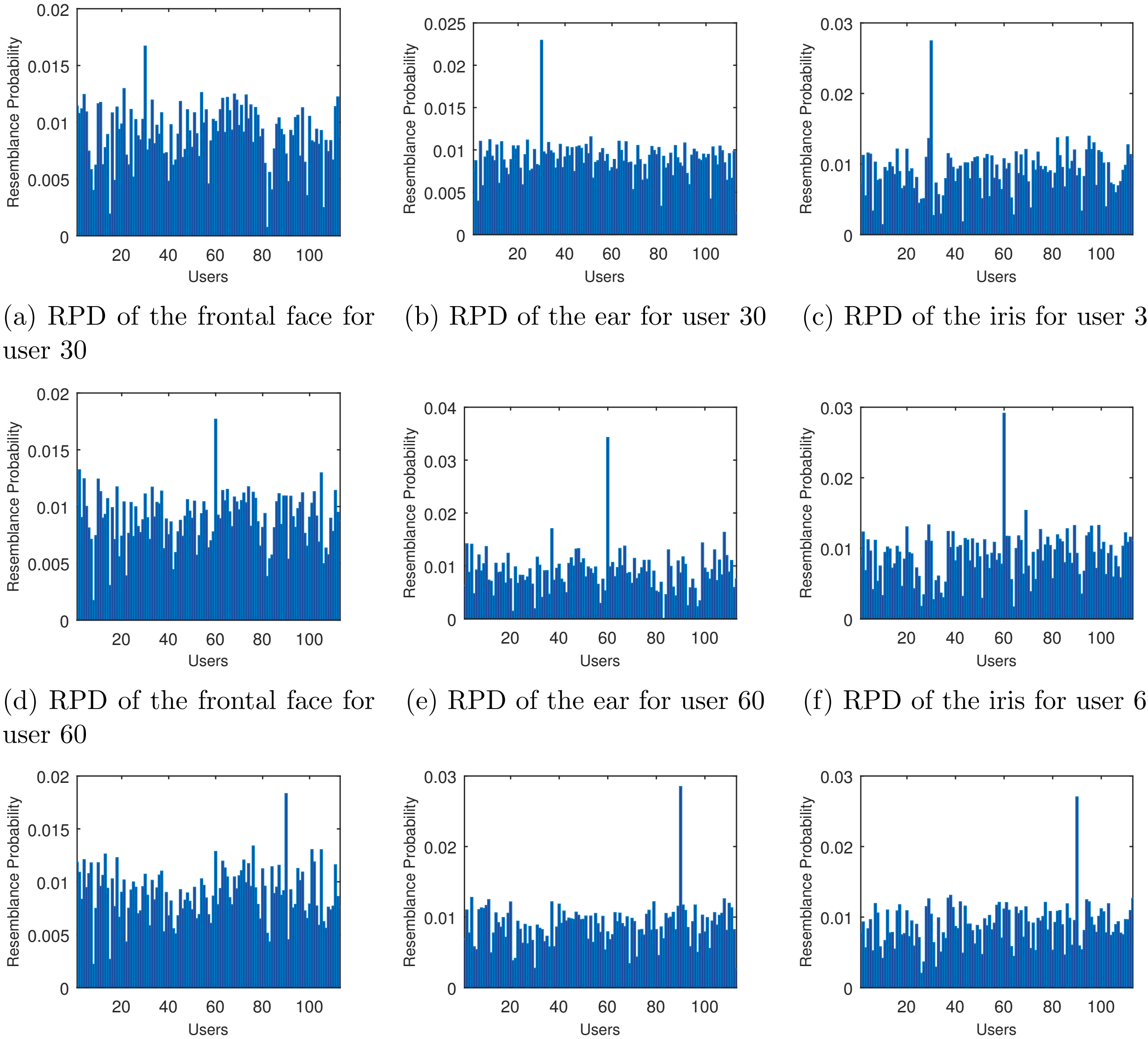


Figure 4.3: An example of densely distributed feature points for user u_i beside a more spread distribution of feature points for user $u_{i'}$ for the same biometric. It is more probable to misclassify user u_i with user $u_{i'}$ while there is a less probability for user $u_{i'}$ to be misclassified as user u_i. This example illustrates the reason behind the dissimilarity of distance from user u_i to $u_{i'}$ and user $u_{i'}$ to u_i.

users in the feature space. Figure 4.4 demonstrates the resemblance probability distributions for three biometrics of three users. For each biometric, the resemblance probability distributions of different users are not identical, which demonstrates the fact that different users' feature points reside in various locations in the feature space. Across different biometrics of the same user, each resemblance probability distribution has its own characteristics, which demonstrates the independence of different biometrics. The only similarity of resemblance probability distributions of the same user is that for all the biometrics the highest value is for that user, which is the indicator of the high similarity of the user to itself.

Algorithm 1 Calculation of resemblance probability distributions for all the users. Range of i and j are the natural numbers in $[1, n]$ and $[1, n_b]$.

```
for each biometric $b_j$ do
    for each user $u_i$ do
        for each user $u_{i'}$ do
            Calculate $D_{b_j}(u_i, u_{i'})$ using equation 4.1
        end
        Calculate the resemblance probability of $u_i$ using equation 4.2
    end
end
```



(a) RPD of the frontal face for user 30

(b) RPD of the ear for user 30

(c) RPD of the iris for user 30

(d) RPD of the frontal face for user 60

(e) RPD of the ear for user 60

(f) RPD of the iris for user 60

(g) RPD of the frontal face for user 90

(h) RPD of the ear for user 90

(i) RPD of the iris for user 90

Figure 4.4: Resemblance probability distributions (RPDs) for three biometrics of three users. Each sub-figure represents the resemblance probability distribution of a specific biometric for a specific user. The horizontal axis of each sub-figure represents all the registered users in the system and the vertical axis shows the similarity of that user to the user that the resemblance probability distribution belongs to.

The resemblance probability is able to capture the valuable information about the distribution of the users in the feature space, and inform the other modules of a multimodal biometric system about it. This information creates a model of the *users' neighborhood* in the feature space. The neighborhood information is important since each user might be misclassified as one of its immediate neighbors during the identification process. The advance knowledge about the probable misclassification of each user's biometrics will provide the system with more evidences about the actual identity of the user. In the next section, two possible utilizations of resemblance probability distributions for rank level fusion are introduced.

4.2 Proposed Resemblance Probability Distribution-Based Fusion Methods

The resemblance probability distributions capture the valuable information about the neighborhood of each user and provide this information to the rank fusion module. The input for the rank fusion module is the relative ranking of identities, that is based on the decision of matchers about the actual identity of the test query. A ranked list considers that the distance between consecutive identities is one. This abstraction hides the actual distribution of identities in the ranked list and might lead to a lower fusion's accuracy (chapter 3, figure 3.3). The resemblance probability distributions provide the *neighborhood information* to the ranked lists, which results in a better recognition rate. In this section, two fusion methods based on resemblance probability distributions, namely *Ranked List Reinforcement* (RLR) and *Confidence-Based Ranked List Selection* (CBRLS), are proposed. Then, the resemblance probability distribution is generalized for clusters of users to accelerate the two proposed fusion methods.

4.2.1 Ranked List Reinforcement Method for Rank Fusion

It is probable that in a ranked list, the matcher ranks the neighbors of the actual identity of a test query in the feature space higher than the actual identity. This problem occurs mostly when there is a large inter-class similarity between users. In the case of high inter-class similarity, the similarity of neighbor users to each other is high. Since the ranked list does not provide the actual similarity of users to the test query, it is not possible to detect the misclassifications due to high inter-class similarity.

Resemblance probability distribution can be added to the multimodal biometric system to address the issue of large inter-class similarity. The ranked list reinforcement is a reordering of the ranked list based on the similarity of resemblance probability distributions with the ranked lists. Figure 4.5 demonstrates an overview of the fusion system that uses the ranked list reinforcement prior to fusion. The idea behind ranked list reinforcement is based on a high similarity of all the resemblance probabilities of the actual identity of the test query with their corresponding ranked lists. The similarity value is used to boost the actual identity's rank and lower the other identities' in the ranked list. The reinforced ranked lists then can be fused using any rank level fusion method to obtain a higher recognition rate.

Since the standard deviations of ranked lists and resemblance probability distributions are finite and non zeros (considering that extracted features are distinctive), Pearson correlation [73] can be considered as a similarity measure of ranked lists and resemblance probability distributions. Suppose that RL^{b_j} is a vector, which contains a ranking of users sorted based on their identities for the biometric b_j and $RPD_{u_i}^{b_j}$ is the resemblance probability distribution of user u_i for the same biometric b_j. $RL^{b_j}(u_k)$ and $RPD_{u_i}^{b_j}(u_k)$, where $k = 1, 2, ..., n$, are the rank of user u_k in the ranked list RL^{b_j} and the resemblance probability of user u_i to user u_k respectively. Since in the ranked list the lower the value of the rank, the higher its similarity to the actual identity, the RPD is subtracted from 1 to make it compatible for correlation analysis with the ranked list. The Pearson correlation between RL^{b_j} and $(\vec{1}_n - RPD_{u_i}^{b_j})$ can

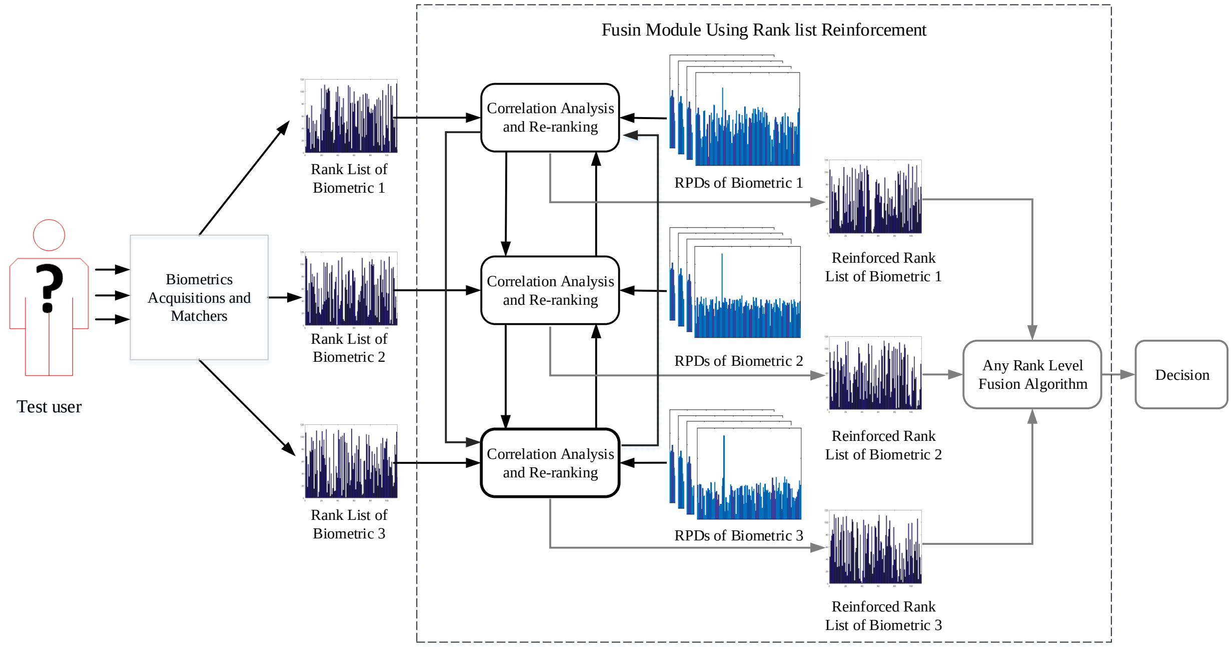

Fusin Module Using Rank list Reinforcement
Test user
Biometrics Acquisitions and Matchers
Rank List of Biometric 1
Rank List of Biometric 2
Rank List of Biometric 3
Correlation Analysis and Re-ranking
Correlation Analysis and Re-ranking
Correlation Analysis and Re-ranking
RPDs of Biometric 1
RPDs of Biometric 2
RPDs of Biometric 3
Reinforced Rank List of Biometric 1
Reinforced Rank List of Biometric 2
Reinforced Rank List of Biometric 3
Any Rank Level Fusion Algorithm
Decision

Figure 4.5: Flowchart of ranked list reinforcement (RLR) using resemblance probability distributions (RPDs).

be estimated using sample correlation coefficient as follows [73]:

$$corr(RL^{b_j}, (\vec{1}_n - RPD^{b_j}_{u_i})) = \frac{\sum_{k=1}^{n}((RL^{b_j}(u_k) - \overline{RL^{b_j}})((\vec{1}_n - RPD^{b_j}_{u_i}(u_k)) - (\overline{\vec{1}_n - RPD^{b_j}_{u_i}}))}{\sqrt{\sum_{k=1}^{n}(RL^{b_j}(u_k) - \overline{RL^{b_j}}) \sum_{k=1}^{n}((\vec{1}_n - RPD^{b_j}_{u_i}(u_k)) - (\overline{\vec{1}_n - RPD^{b_j}_{u_i}}))}} \tag{4.3}$$

where $\overline{RL^{b_j}}$ and $(\overline{\vec{1}_n - RPD^{b_j}_{u_i}})$ are average values of the ranked list RL^{b_j} and $(\vec{1}_n - RPD^{b_j}_{u_i})$. The value of Pearson correlation is in range $[-1, 1]$. The value is 1 when both the ranked list and $(\vec{1}_n - RPD)$ are correlated. It is -1 when they are inversely correlated and zero when there is no correlation between them. The value of correlation can be any other real number in range $[-1, 1]$ based on the degree of correlation between the ranked list and $(\vec{1}_n - RPD)$.

Since both resemblance probability distributions and ranked lists are calculated from the same feature space, the ranked list of each user should be similar to the $(\vec{1}_n - RPD)$ of that user and its neighbors in the feature space. In case of uncorrelated biometrics, the neighbors

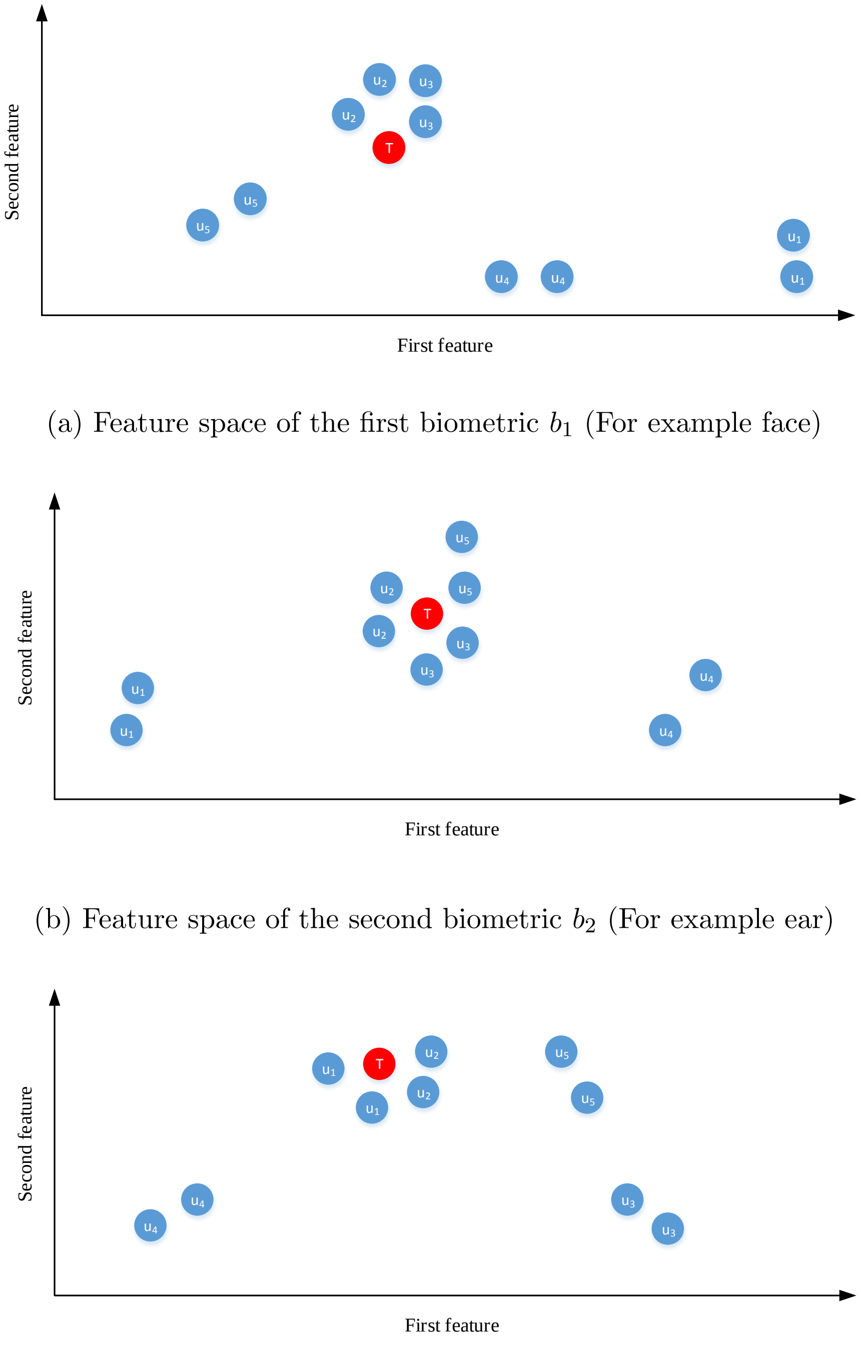
Algorithm 2 ranked list reinforcement for a multimodal system with n_b different biometrics.

```
for each ranked list $RL_{b_j}$ do
    for each user $u_i$ do
        $RRL_{b_j}(u_i) = RL_{b_j}(u_i) \times \sum_{k=1}^{n_b}(\vec{1}_n - corr(LR_{b_k}, (\vec{1}_n - RPD^{b_k}_{u_i})))$
    end
end
```

of each user are not the same across different biometrics. In an ideal case, the correlation between the ranked lists of different biometric and $(\vec{1}_n - RPD)$ of the actual identity of the test query should be close to 1. Since the neighbors of each user are not the same across different biometrics, if there is a high correlation between the $(\vec{1}_n - RPD)$ of the actual identity's neighbor and the one of the ranked lists, the correlation is expected to be small for other ranked lists.

Based on this idea, algorithm 2 reinforces the rank of each identity (user) for each biometric by considering the Pearson correlation between that user's resemblance probability distributions and the ranked lists of all biometrics. The reinforced rank of each identity (user) for each biometric is calculated by considering its current rank and the similarity of that user's RPDs with ranked lists of corresponding biometrics.

Figure 4.6 provides an example of three 2D feature spaces for three biometrics of five users. In this figure, the samples for user u_2 are close to samples of other users. The system is asked to determine the identity of the test query T of user u_2, which is demonstrated with a red circle in the three biometrics' feature spaces. Figure 4.7 shows the result of Borda count rank fusion for the ranked lists created for the test query T. In the result of the Borda count, the lowest rank is 7 for both users 2 and 5. The Borda count rank level fusion is not able to distinguish between these two users. Figure 4.8 demonstrates the result of ranked list reinforcement for the same ranked lists. The reinforced ranked list for each biometric is more accurate and user u_2 is the first rank in all of them. The fusion of reinforced ranked lists using Borda count has user u_2 with a lowest rank. Moreover, the gap between the first

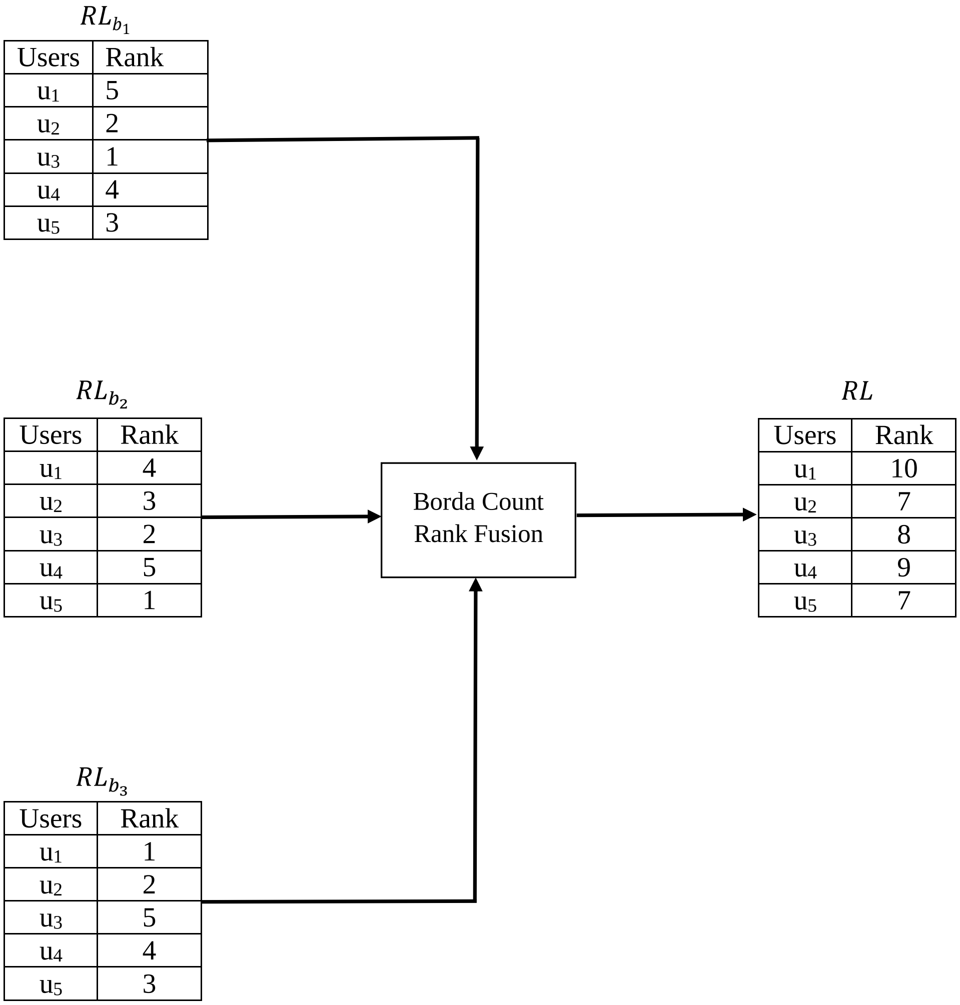


(a) Feature space of the first biometric b_1 (For example face)

(b) Feature space of the second biometric b_2 (For example ear)

(c) Feature space of the third biometric b_3 (For example iris)

Figure 4.6: Example of a 2D feature space for three biometrics of five users. For each user, there are two training samples per each biometric, which are represented by blue circles. A test query T of user u_2 is also represented by a red circle among the training samples.



RL_{b_1}

Users	Rank
u1	5
u2	2
u3	1
u4	4
u5	3

RL_{b_2}

Users	Rank
u1	4
u2	3
u3	2
u4	5
u5	1

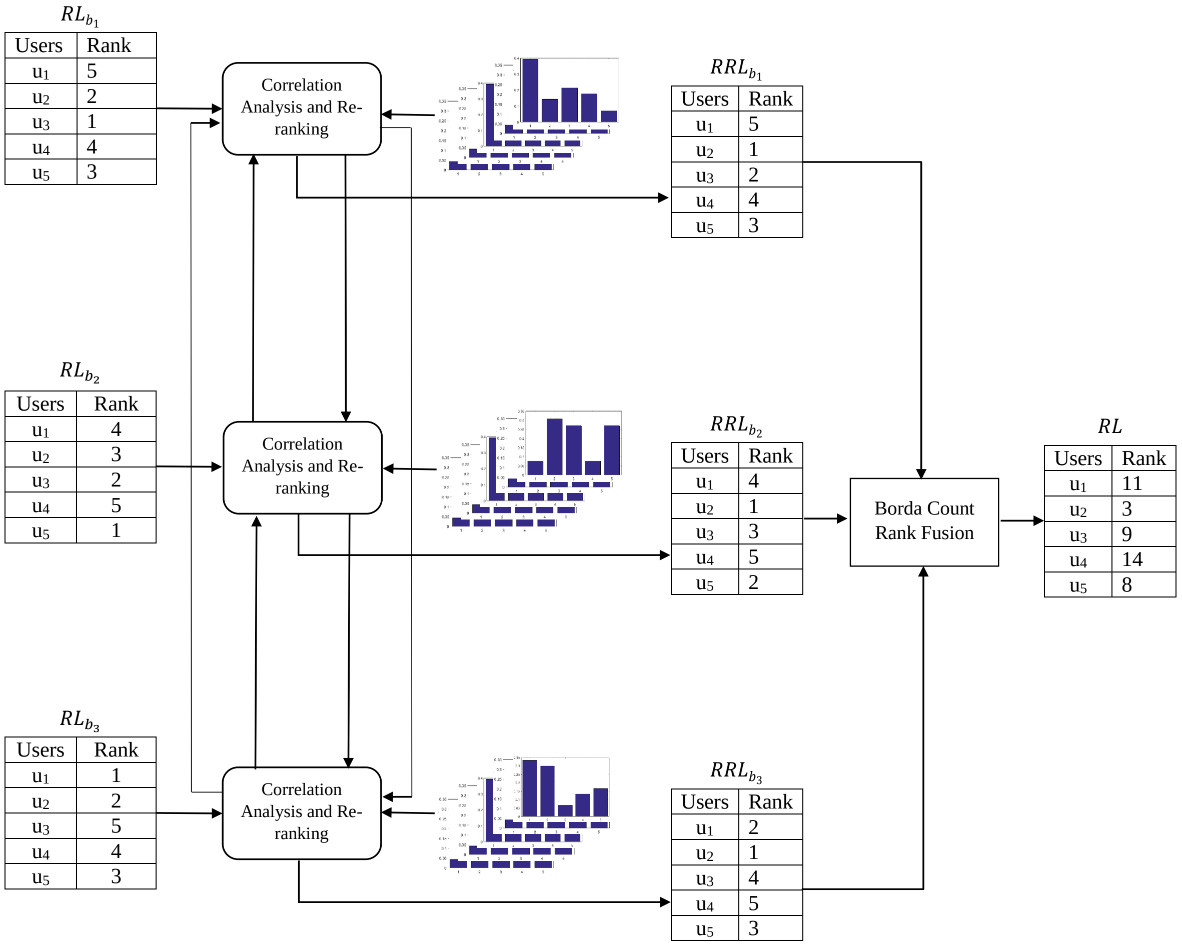
RL_{b_3}

Users	Rank
u1	1
u2	2
u3	5
u4	4
u5	3

RL

Users	Rank
u1	10
u2	7
u3	8
u4	9
u5	7

Figure 4.7: Borda count fusion of ranked lists for the test query in figure 4.6. Borda count is unable to distinguish between users u_2 and user u_5



RL_{b_1}

Users	Rank
u1	5
u2	2
u3	1
u4	4
u5	3

RL_{b_2}

Users	Rank
u1	4
u2	3
u3	2
u4	5
u5	1

RL_{b_3}

Users	Rank
u1	1
u2	2
u3	5
u4	4
u5	3

RRL_{b_1}

Users	Rank
u1	5
u2	1
u3	2
u4	4
u5	3

RRL_{b_2}

Users	Rank
u1	4
u2	1
u3	3
u4	5
u5	2

RRL_{b_3}

Users	Rank
u1	2
u2	1
u3	4
u4	5
u5	3

RL

Users	Rank
u1	11
u2	3
u3	9
u4	14
u5	8

Correlation Analysis and Re-ranking
Correlation Analysis and Re-ranking
Correlation Analysis and Re-ranking
Borda Count Rank Fusion

Figure 4.8: The Borda count fusion of reinforced ranked lists for the test query in figure 4.6. The fusion based on reinforced ranked lists is able to correctly rank user u_2 at the first rank.

lowest rank (rank 3 for user u_2) and the second lowest rank (rank 8 for user u_5) is large, which represents a large confidence margin.

ranked list reinforcement exploits the information from all the biometrics' ranked lists to provide a higher accuracy for each ranked list. Any rank level fusion can be used to fuse the reinforced ranked lists. In chapter 6, reinforced ranked lists are fused using three different rank level fusions to show the advantage of reinforcement.

4.2.2 Confidence-Based Ranked List Selection

The second proposed approach that uses resemblance probability distributions in the rank fusion is the *confidence-based ranked list selection* (CBRLS). It would be beneficial for a fusion module to know about the performance of each matcher in order to use the results from the well performing matchers. This task can be done in a global or a local manner. The global approaches, such as logistic regression [1], test each biometric matcher prior to the real world implementation to come with a measure of their performance. They use this performance measure as a factor in the fusion methods to put more attention toward biometric matchers with higher recognition rates.

The fact that a biometric matcher does not perform the same for all the users draws my attention toward considering a local performance measurement. The assumption here is that a biometric has different discriminability for different users registered in the system. For example, consider a case when a person has a unique face, so that its feature points are at a far distance from the whole population in the database. The face matcher is able to recognize this person with a very high confidence. For identical twins, however, the face matcher is likely to misclassify their faces. This will result in a low recognition rate for identical twins. Figure 4.9 provides an example for this fact. This figure shows two eigenvectors with the largest eigenvalues of the extracted features from faces and ears of 20 users. Ear biometric cannot distinguish between user 8, 13, and 5 with a high confidence, while face can provide a higher confidence in their recognition. On the other hand, face biometric has a low confidence to distinguish user 3 from 19 while in ear biometric user 3 is perfectly separated from the rest of the population.

Although it is possible to come up with a prior local measure of matcher's performance for each individual user, it is impossible to use this measure at the time of identification, since the identity is not known yet. My focus is to introduce a measure of confidence for ranked lists provided by each matcher, that is adaptive to the test query. For each query, a series of ranked lists are adaptively selected to provide the highest confidence in the final decision.

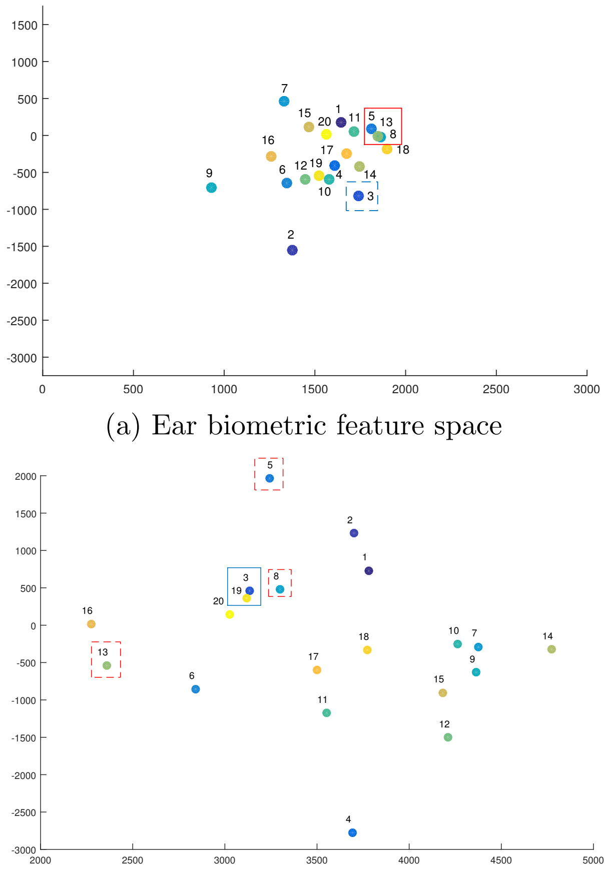
In the next subsections, I will talk about the confidence of a matcher that works on score level, then propose an approach to convert a ranked list to a pseudo-score list and finally introduce the novel confidence-based ranked list selection approach.

Confidence of a Matcher

This section proposes an approach to measure the confidence of a matcher that outputs the similarity of the test query to users (identities) as scores. Before going further, it is essential to define the meaning of confidence in this context. Here, confidence is defined as the ability of a matcher to distinguish between all the possible identities for a test query. The confidence of a matcher for each test query provides a measurement of how probable is that the current test query will be misclassified with other identities rather than its actual identity. More formally, if the resulted score list from a matcher was normalized to a probability distribution P, the confidence of the discrete probability distribution P is defined as:

$$CM(P) = \sum_{i=1}^{n-1} e^{\frac{-(i-1)^2}{n}} (SortedP_i^j - SortedP_{i+1}^j) \tag{4.4}$$

where n is the number of registered users in the systems and $SortedP$ is the descending sorted discrete probability distribution P. The distance between each normalized score and its consecutive normalized score in the sorted normalized score list is called the *confidence margin.* Formula 4.4 follows my definition of confidence and measures a weighted average of confidence margins. The confidence margins are weighted using a Gaussian function. The



(a) Ear biometric feature space

(b) Face biometric feature space

Figure 4.9: Discriminability of features extracted from face and ear of 20 users based on their two eigenvectors with the largest eigenvalues. Each circle represents a training sample of users. The number beside each circle is the user's identity that each sample belongs to. The samples in solid rectangles are the samples of users that cannot be distinguished with a high confidence. The dashed rectangles represents the same users in the feature space of another biometric, which can be distinguished with a high confidence.

reason behind using a Gaussian function is that it is more important to have a large margin between identities at the begining of the sorted normalized score list because they have a higher probability to be the actual identity of the test query.

The normalized score list has its highest confidence in the case that one identity has the probability of 1 and the rest have the probability of 0. In this case, the confidence based on formula 4.4 is 1. If the probability distribution has the same value for all the identities, it means that the matcher cannot distinguish between different identities. In the case of a uniform distribution, the confidence value is 0 and it shows the inability of the matcher to make a correct decision.

Ranked List Conversion to Pseudo-Score List

Using ranked list to calculate the confidence will result in the same confidence value for all the matchers, since the differences of consecutive ranks (confidence margins) are always one. In order to facilitate the calculation of confidence, there is a need to retrieve the score information.

Algorithm 3 demonstrates the process of pseudo-score retrieval. The pseudo-score of each user (identity) is calculated by multiplying the rank of the user (identity) by the correlation between that user's $(\vec{1}_n - RPD)$ and the ranked list. The resulting pseudo-scores are real numbers that have information about the distribution of users in the feature space and the matcher's ranking of identities for the test query. In the case that two users are really close in the feature space, they should have a close rank. On the other hand, since the two users are close in the feature space, their resemblance probability distributions should be similar as well. The correlation of the RPDs of those users and the ranked list results in close correlation values. As the result of close ranks and correlation values, the pseudo-scores of those users will have values with a small confidence margin, which is an indicator of the matcher's inability to distinguish between them.

Algorithm 3 The process of creating the pseudo-score list from ranked list containing N users using resemblance probability distributions.

```
for each ranked list $RL_{b_j}$ do
    for each user $u_i$ do
        $PseudoScore_{b_j}(u_i) = (N - RL_{b_j}(u_i) + 1) \times (corr(LR_{b_j}, (\vec{1}_n - RPD^{b_j}_{u_i})))$
    end
end
```

Cascade of Ranked Lists

The confidence of matchers provides a criteria to adaptively select ranked lists based on their performance for each query. It is important to use the outcome of all the matchers and at the same time, accent matchers that perform better for each specific query.

Cascade of Ranked Lists is the novel approach to utilize the confidence in order to select a set of well-performed matchers that work in sequence and result in the ranked lists with high confidence values. Figure 4.10 demonstrates the flowchart of the confidence-based ranked list selection for rank fusion. In this flowchart, it is considered that the number of biometrics is three, although there is no limitation on more biometrics. The process starts with converting the ranked list of each biometric to pseudo-scores using algorithm 3. The pseudo-scores are sorted in a descending order so that the high score identities are at the top of the list and low scores are at the bottom. In order to calculate the confidence, I need to convert pseudo-score lists to discrete probability distributions. This can be done as:

$$NPseudoScore_{b_j} = \frac{PseudoScore_{b_j} - min(PseudoScore_{b_j}) \times \vec{1}_n}{\|PseudoScore_{b_j} - min(PseudoScore_{b_j}) \times \vec{1}_n\|} \tag{4.5}$$

The confidence of each normalized sorted pseudo-score list can be calculated using equation 4.4. For each pseudo-score list, the k first high score users are selected based on the confidence value of that list as follows:

$$k = \max\{(1 - CM)(N_l - 1) + 1, k_{min}\} \tag{4.6}$$

where CM is the confidence of the list and k_{min} is the minimum required number of users in each list. In the case that confidence of the list is zero and it cannot distinguish between users, k will be equal to N_l, which is the total number of users that are in the current state of the list. In case that the value calculated by $(1 - CM)(N_l - 1) + 1$ is less than k_{min}, k will be equal to k_{min} to insure that the list size will not drop below a certain threshold. The reason behind using k_{min} is to preserve a minimum list size in order to avoid any users lost

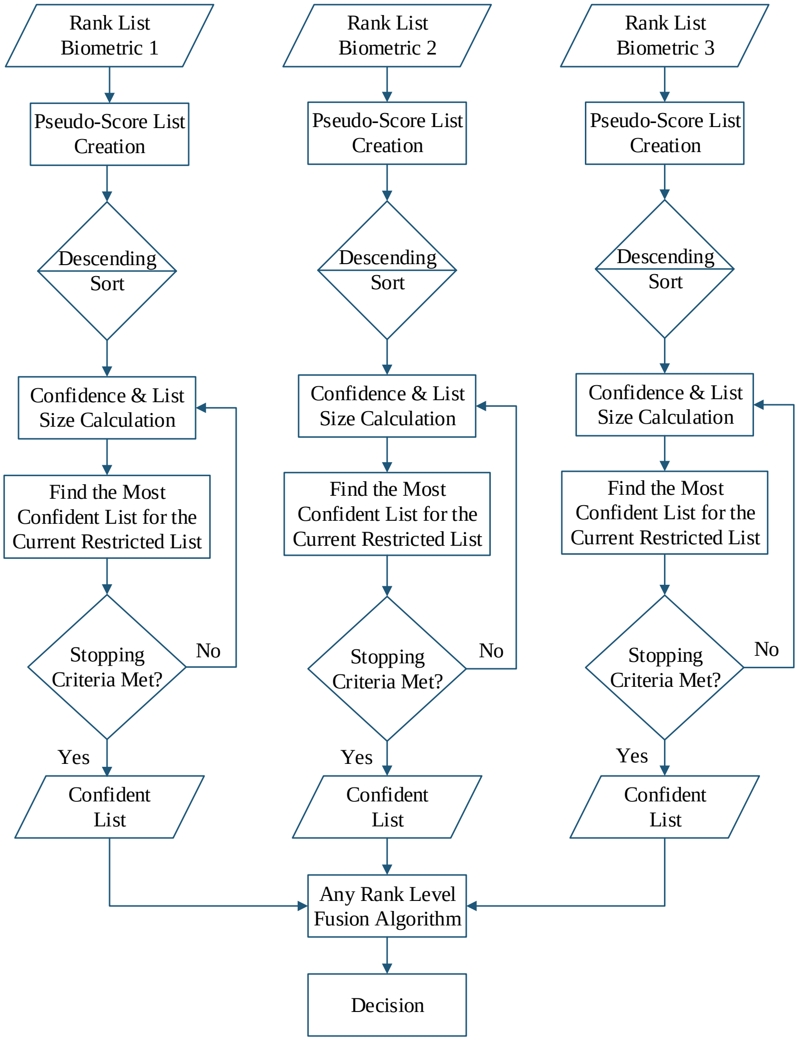


Figure 4.10: Flowchart of the confidence-based ranked list selection (CBRLS) approach.

due to inaccuracy of confidence calculation. The k first high score users of each list form another list, which is called the *restricted list*.

For each restricted list, the system searches to find the matcher that provides the highest confidence for the remaining identities in the list. To accomplish this task, for any restricted list L_{b_j}, the pseudo-scores for the identities in L_{b_j} are selected from all the other lists $L_{b_{j'}}$ and the confidence value is calculated for them to find the matcher that provides the highest confidence for the identities in the restricted list L_{b_j}. The pseudo-scores from the matcher that has the highest confidence for the identities in restricted list L_{b_j} are replaced with the original pseudo scores.

This process continues for all the matchers, until there are no other changes in the restricted lists. In this state, all the lists have reached their highest confidence. In order to fuse these restricted lists, it is required to convert them back to ranked lists by assigning ranks based on the pseudo-score values. Fusion also requires that all the ranked lists have the ranking for same identities. Due to elimination of some users in the process of restricted list creation, the users in the lists are not identical. To address this problem, the list alignment is preformed to add the missing users to each list. The added users will have the rank equal to the size of the initial list plus one.

Figure 4.11 provides an example of three 2D feature spaces for three biometrics of five users. In this figure, the samples for user u_1 are close to samples of other users in the feature spaces for biometrics b_1 and b_2. The samples of user u_1 are perfectly separated from the other users' samples in feature space of biometric b_3. The system is asked to determine the identity of the test query T of user u_1, which is demonstrated with a red circle in the three biometrics' feature spaces. Figure 4.12 shows the Borda count rank fusion for the ranked lists created for the test query T. In the result of the Borda count, the lowest rank is 7 for both users u_1 and u_2. The Borda count rank level fusion is not able to distinguish between these two users. Figure 4.13 demonstrates the result of confidence-based ranked list selection for the same ranked lists. After conversion of ranked lists to pseudo-score lists, the confidence measures show that biometrics b_1 and b_2 are not as confident as biometric b_3 in the ranking of users. After creating the restricted lists based on the value of k for each pseudo-score list, the matcher that provides the highest confidence for each restricted list is selected. In this example, the matcher for biometric b_3 provides the highest confidence for all the restricted lists. So the values of the pseudo-scores in each restricted list are replaced by values suggested by pseudo-scores of biometric b_3. The confidence measure for each modified pseudo-score list is calculated and the number of remaining users in the restricted lists is determined. In this example, after this stage, all the restricted lists have reached their highest confidence. In order to fuse these restricted lists, it is required to convert them back to ranked list by assigning ranks based on the scores. Since the users in all the lists are not identical, the list alignment is preformed to add the missing users to each list. The reinforced ranked list for each biometric is more accurate and user u_2 is given the first rank in all of them. The fusion of reinforced ranked lists using Borda count rank level fusion method has user u_2 with a lowest rank. Moreover, the gap with the first lowest rank (rank 3 for user u_2) and the second lowest rank (rank 8 for user u_5) is large, which represents a large confidence margin.

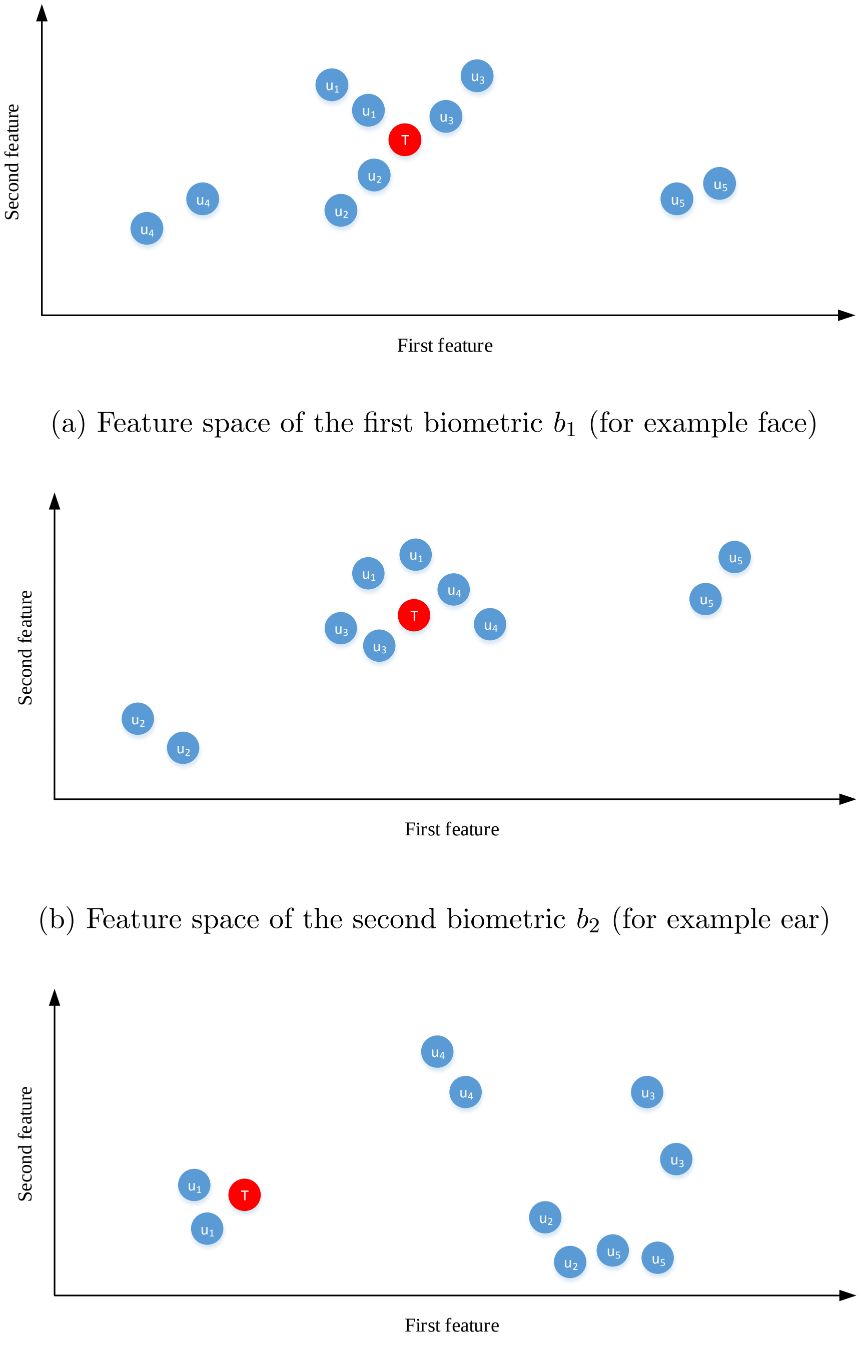
4.2.3 Clustering of Users for Confidence-Based Rank Fusion

Rank reinforcement and confidence-based ranked list selection both utilize resemblance probability distributions to enhance the recognition rate. The fact that resemblance probability distributions of neighbor users possess a high degree of similarity is neglected by both of these methods. The similarity between neighboring users can be utilized to reduce the computational complexity of the system and enhance its response time. In this section, the novel idea of clustering of the users based on the similarity of their resemblance probability distributions and adaptation of rank reinforcement and confidence-based ranked list selection for clusters of users are introduced.

User Clustering Based on Resemblance Probability Distributions

Clustering is defined as “partitioning a set of objects into relatively homogeneous subsets based on inter-objects similarities” [74]. Based on the definition, there are two fundamental steps in clustering: Defining the similarity measure and choosing a clustering (partitioning) approach.

The clustering of users should be based on how informative their resemblance probability distributions are with respect to others. Pearson correlation coefficient [73] can be used to find the similarity of resemblance probability distributions. The higher the correlation value

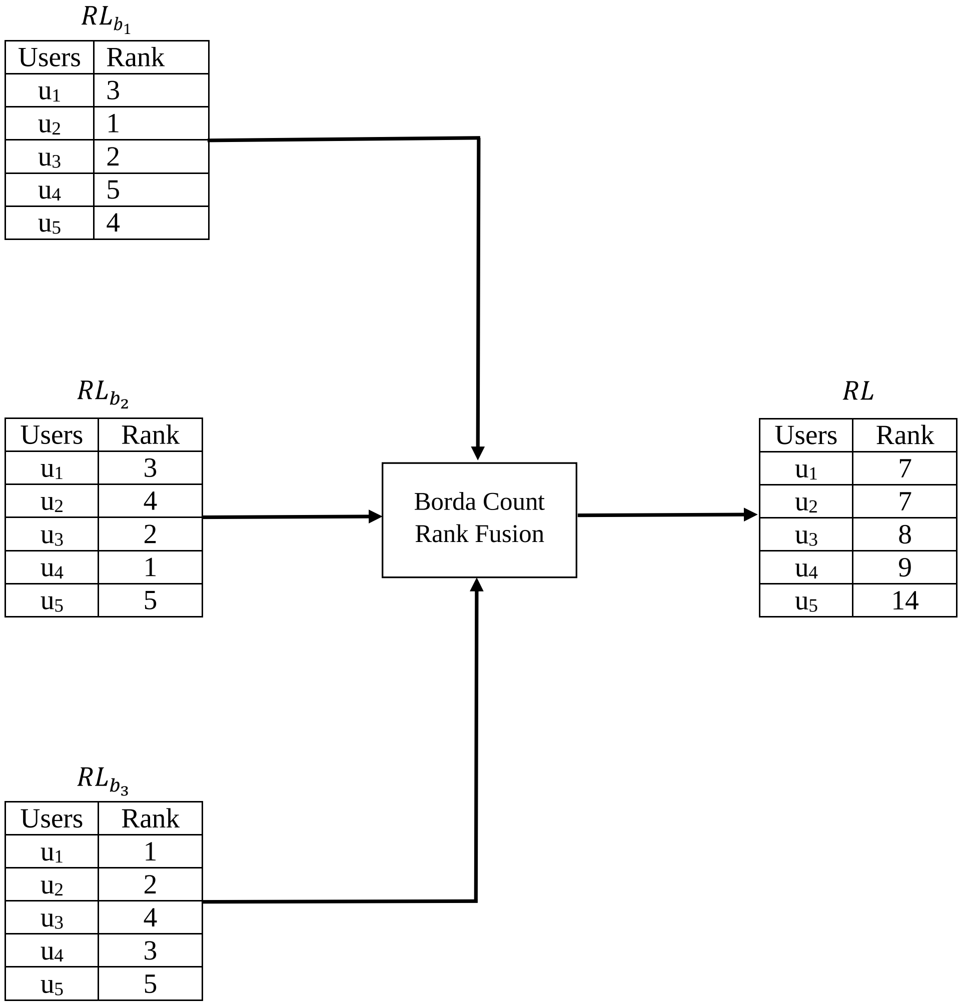


(a) Feature space of the first biometric b_1 (for example face)

(b) Feature space of the second biometric b_2 (for example ear)

(c) Feature space of the third biometric b_3 (for example iris)

Figure 4.11: Example of a 2D feature space for three biometrics of five users. For each user, there are two training samples per each biometric, which are represented by blue circles. A test query T of user u_2 is also represented by a red circle among the training samples.



RL_{b_1}

Users	Rank
u_1	3
u_2	1
u_3	2
u_4	5
u_5	4

RL_{b_2}

Users	Rank
u_1	3
u_2	4
u_3	2
u_4	1
u_5	5

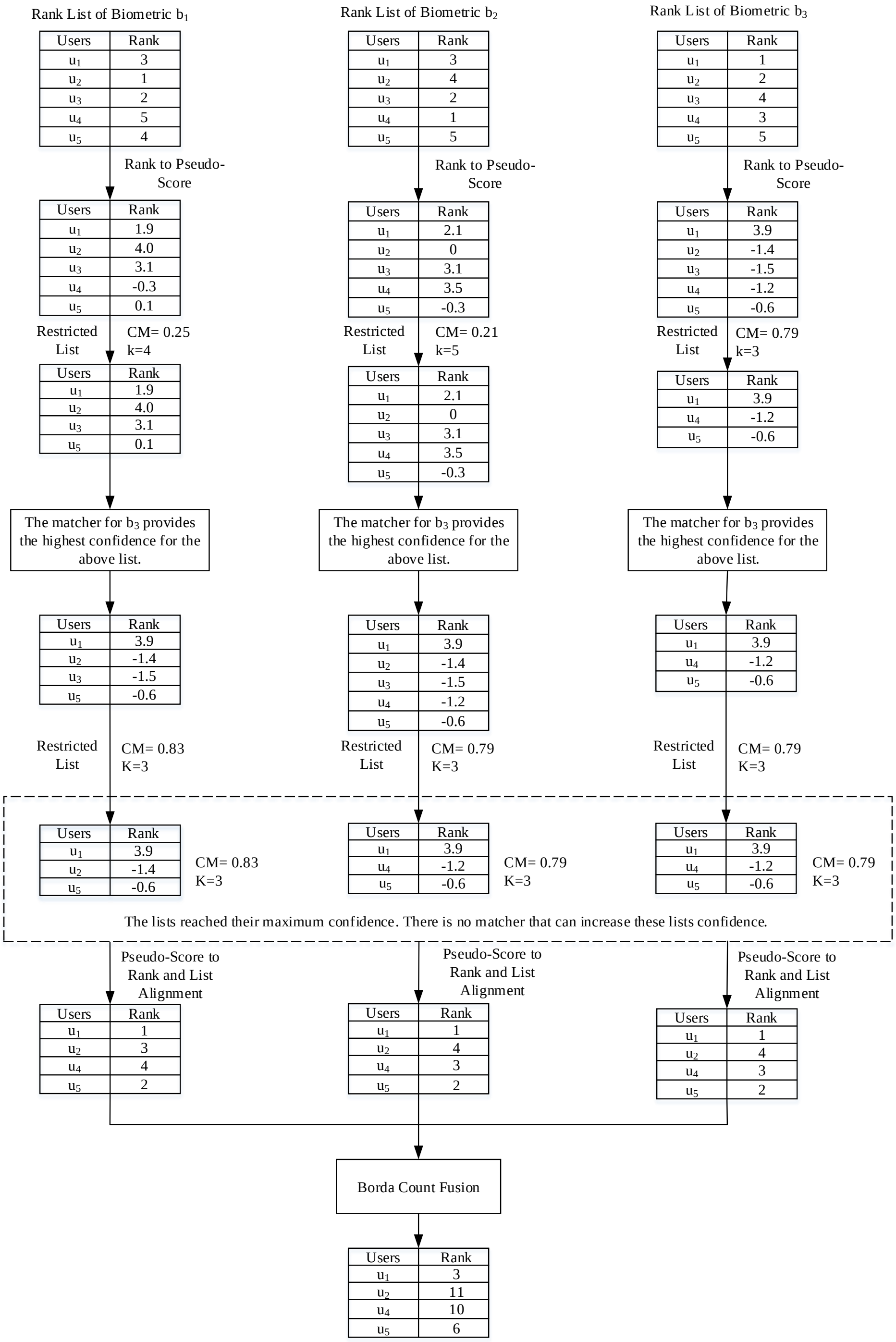
RL_{b_3}

Users	Rank
u_1	1
u_2	2
u_3	4
u_4	3
u_5	5

RL

Users	Rank
u_1	7
u_2	7
u_3	8
u_4	9
u_5	14

Figure 4.12: Borda count fusion of ranked lists for the test query in figure 4.11. Borda count is unable to distinguish between users u_1 and user u_2


Rank List of Biometric b_1
Rank List of Biometric b_2
Rank List of Biometric b_3
Rank to Pseudo-Score
Restricted List
CM= 0.25
k=4
CM= 0.21
k=5
CM= 0.79
k=3
The matcher for b_3 provides the highest confidence for the above list.
CM= 0.83
K=3
CM= 0.79
K=3
The lists reached their maximum confidence. There is no matcher that can increase these lists confidence.
Pseudo-Score to Rank and List Alignment
Borda Count Fusion

Rank List of Biometric b_1

Users	Rank
u_1	3
u_2	1
u_3	2
u_4	5
u_5	4

Rank List of Biometric b_2

Users	Rank
u_1	3
u_2	4
u_3	2
u_4	1
u_5	5

Rank List of Biometric b_3

Users	Rank
u_1	1
u_2	2
u_3	4
u_4	3
u_5	5

Rank to Pseudo-Score

Users	Rank
u_1	1.9
u_2	4.0
u_3	3.1
u_4	-0.3
u_5	0.1

Users	Rank
u_1	2.1
u_2	0
u_3	3.1
u_4	3.5
u_5	-0.3

Users	Rank
u_1	3.9
u_2	-1.4
u_3	-1.5
u_4	-1.2
u_5	-0.6

Restricted List

Users	Rank
u_1	1.9
u_2	4.0
u_3	3.1
u_5	0.1

Users	Rank
u_1	2.1
u_2	0
u_3	3.1
u_4	3.5
u_5	-0.3

Users	Rank
u_1	3.9
u_4	-1.2
u_5	-0.6

The matcher for b_3 provides the highest confidence for the above list.

Users	Rank
u_1	3.9
u_2	-1.4
u_3	-1.5
u_5	-0.6

Users	Rank
u_1	3.9
u_2	-1.4
u_3	-1.5
u_4	-1.2
u_5	-0.6

Users	Rank
u_1	3.9
u_4	-1.2
u_5	-0.6

Restricted List

Users	Rank
u_1	3.9
u_2	-1.4
u_5	-0.6

Users	Rank
u_1	3.9
u_4	-1.2
u_5	-0.6

Users	Rank
u_1	3.9
u_4	-1.2
u_5	-0.6

Pseudo-Score to Rank and List Alignment

Users	Rank
u_1	1
u_2	3
u_4	4
u_5	2

Users	Rank
u_1	1
u_2	4
u_4	3
u_5	2

Users	Rank
u_1	1
u_2	4
u_4	3
u_5	2

Borda Count Fusion

Users	Rank
u_1	3
u_2	11
u_4	10
u_5	6

Figure 4.13: Confidence-based ranked list selection (CBRLS) approach for fusion of the ranked lists of the test query in figure 4.11. The fusion based on CBRLS is able to correctly rank user u_1 at the first rank with a high confidence margin.

between two distributions, the more redundancy between them and they relatively provide the same information. The correlation between the two resemblance probability distribution $RPD^{b_j}_{u_i}$ and $RPD^{b_j}_{u_{i'}}$ is defined as [73]:

$$corr(RPD^{b_j}_{u_i}, RPD^{b_j}_{u_{i'}}) = \frac{\sum_{k=1}^{n}((RPD^{b_j}_{u_i}(u_k) - \overline{RPD^{b_j}_{u_i}})(RPD^{b_j}_{u_{i'}}(u_k) - \overline{RPD^{b_j}_{u_{i'}}})}{\sqrt{\sum_{k=1}^{n}(RPD^{b_j}_{u_i}(u_k) - \overline{RPD^{b_j}_{u_i}}) \sum_{k=1}^{n}(RPD^{b_j}_{u_{i'}}(u_k) - \overline{RPD^{b_j}_{u_{i'}}})}} \tag{4.7}$$

This correlation value is considered as the similarity measure between $RPDs$.

Clustering algorithms can be divided into two main categories: hierarchical and partitional. A complete review of different clustering algorithms can be found in [75]. In contrast to hierarchical clustering, partitional clustering algorithms require the specification of the number of clusters [75], which is not available in this application. In partitional clustering, a criterion is optimized to find the optimum grouping of objects. Since the combinatorial search of the all possible assignments is computationally expensive, in practice, a local optimization is performed several times with different initial settings and the best result is kept as the final clustering. Since hierarchical clustering does not require to know the number of clusters in advance and also provides a more robust output than the partitional approach, it is selected for clustering the users.

The pseudo-code for agglomerative hierarchical clustering [75] is given in algorithm 4. At the beginning, the algorithm assigns each data point to a singleton cluster. The distance between each pair of clusters is calculated and the two clusters that have the least distance are merged and form a new cluster. This process continues until all the clusters merge and form a single cluster containing all the data points. The process of hierarchical clustering can be shown using a dendrogram as an interpretable visual representation. Figure 4.14 demonstrates ten hypothetical data points in a 2D feature space and the dendrogram of their hierarchical clustering. Each level in the dendrogram is a clustering of data points. The clusters in the lower levels of dendrogram have the most similarity between their data

Algorithm 4 Agglomerative hierarchical clustering [75].

```
Consider each data point as a singleton cluster.
while there is more that one cluster do
    Calculate the distance between each pair of clusters.
    Merge the pair that has the lowest distance.
end
```

points.

In the hierarchical clustering, the measurement of distance between two clusters can be calculated using three major approaches: single-linkage, complete-linkage, and group-average [75]. In single-linkage, the distance between two clusters G and H is [75]:

$$d_{sl} = min_{i \in G, j \in H} d_{i,j} \tag{4.8}$$

where $d_{i,j}$ is the distance between two data points i and j. Single-linkage make the chaining effect which results in early merging of clusters. Complete-linkage distance of two clusters G and H is calculated as [75]:

$$d_{cl} = max_{i \in G, j \in H} d_{i,j} \tag{4.9}$$

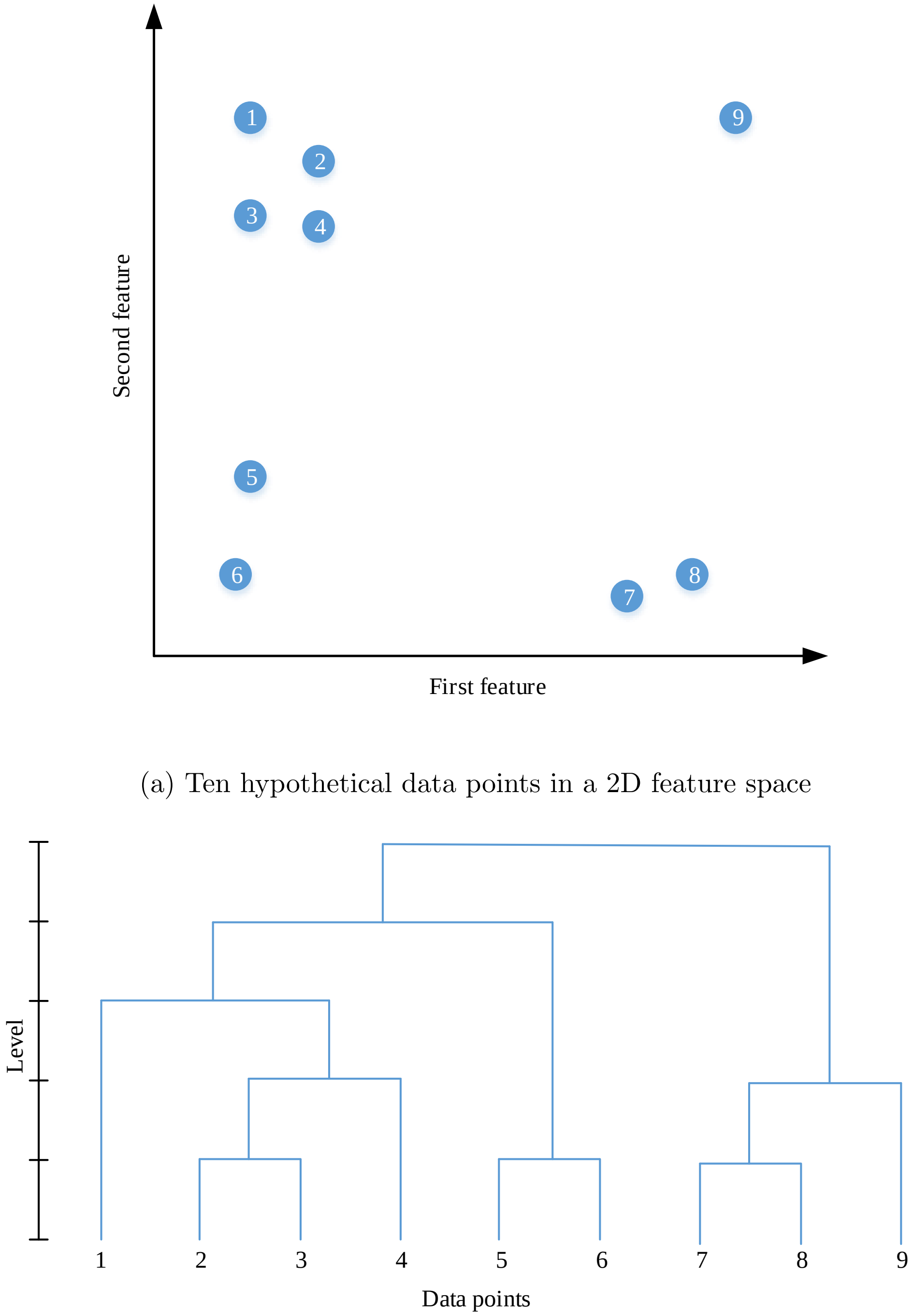
Complete linkage creates dense clusters, although it might result in late merging of clusters due to outliers. Group-average distance is defined as [75]:

$$d_{ga} = \frac{1}{N_G N_H} \sum_{i \in G, j \in H} d_{i,j} \tag{4.10}$$

where N_G and N_H are the cardinality of clusters G and H. Group average is a compromise between the complete-linkage and single-linkage.

Since hierarchical clustering with group average distance prevents from chaining and late merging and also provide relatively dense clusters, for each biometric, the users are clustered using this clustering approach.

Clustering of users reduces the system capability to distinguish between users in the same cluster, especially when there is a high correlation between biometrics, which results in



(a) Ten hypothetical data points in a 2D feature space

(b) Dendrogram of clustering the hypothetical data points in (a)

Figure 4.14: Example of clustering ten hypothetical data points in a 2D feature space using hierarchical clustering considering the group-average as the distance of two clusters and the resulting dendrogram.

similar clusters of users for different biometrics. The fewer number of clusters will decrease the time complexity of fusion, although it can reduce the recognition rate at the same time. In this case, there is a trade-off between the recognition rate and the time complexity of the system. The optimum number of clusters should be selected based on the application and the importance of recognition rate and the response time. The experimental results in chapter 5 will elaborate more about this trade-off.

Resemblance Probability Distributions for Clusters

As a result of hierarchical clustering, users will be grouped into non-overlapping clusters. Since users in each cluster have similar resemblance probability distributions, a single distribution can be used for all the users in a cluster. The resemblance probability distribution for each cluster shows the probability of classification of that cluster as all clusters.

It can be considered that each cluster is a super-user that contains users with similar RPDs. The distance from super-user su_i to $su_{i'}$ is calculated using the following formula, which is similar to the distance between the ordinary users in formula 4.1:

$$D_{b_j}(su_i, su_{i'}) = \begin{cases} 1/m_i \sum_{k=1}^{m_i} \min_{l\in\{1,\ldots,m_{i'}\}} \|(f_{s_k^{su_i,b_j}} - f_{s_l^{su_{i'},b_j}})\|, & \text{if } i \neq i' \\ 1/m_i \sum_{k=1}^{m_i} \min_{l\in\{1,\ldots,m_{i'}\}-\{k\}} \|(f_{s_k^{su_i,b_j}} - f_{s_l^{su_{i'},b_j}}\|, & \text{if } i = i' \end{cases} \tag{4.11}$$

where m_i and $m_{i'}$ are the number of samples in super-users su_i and $su_{i'}$ and $\|(f_{s_k^{u_i,b_j}} - f_{s_l^{u_{i'},b_j}})\|$ is the magnitude of the difference feature vector $(f_{s_k^{u_i,b_j}} - f_{s_l^{u_{i'},b_j}})$. In this formula, for all the samples of all the users in a super-user, the average of minimum distances to the samples in all the super-user is calculated.

The resemblance probability distribution for all super-user can be calculated using algorithm 5. The difference between Algorithm 1 and 5 is that Algorithm 5 iterates through the samples in super-users and use the distance measure of super-users.

Algorithm 5 Calculation of resemblance probability distributions for the super-users. i varies between 1 and number of super-users and j is in the range of $[1, n_b]$.

```
for each biometric $b_j$ do
    for each super-user $u_i$ do
        for each super-user $u_{i'}$ do
            Calculate $D_{b_j}(su_i, su_{i'})$ using equation 4.11
        end
        Calculate the resemblance probability of $su_i$ using equation 4.2
    end
end
```

Confidence-Based Rank Fusion Using Clusters

The most important part in adaptation of both rank reinforcement and confidence-based ranked list selection is the calculation of correlation between ranked lists and super-users' resemblance probability distributions. The issue is that ranked lists and super-users' resemblance probability distributions do not have the same dimensions and it is not possible to calculate the correlation between them. To fix this, the ranked list of users needs to be converted to the ranked list of super-users. The rank of a super-user su_i for biometric b_j is calculated as follows:

$$RLSU_{b_j}(su_i) = \sum_{u \in su_i} RL_{b_j}(u) \tag{4.12}$$

In formula 4.12, the rank of users that are in the same cluster are summed to form a rank for the super-user. Now the super-users' ranked list and resemblance probability distributions have the same dimensions.

Both ranked list rank reinforcement and confidence-based ranked list selection methods requires the calculation of the Pearson correlation. In the clustering approach, the correlation for all the super-users' resemblance probability distributions and all the super-users' ranked lists can be calculated once. Then, a hash table is created that maps each user to the correlation value of its super-user. In this case, there is no need to do the calculation for each individual users. Therefore, this reduction of calculation can considerably enhance the response time of the system.

The other parts of algorithms for ranked list reinforcement and confidence-based ranked list selection stay the same.

4.3 Chapter Summary

In this chapter, the notion of resemblance probability distribution is introduced as a way to represent the distribution of users in the feature space. The ranked list reinforcement and confidence-based ranked list selection are proposed as two fusion methods based on resemblance probability distributions. These two methods are discussed by providing detailed examples of their procedures. The ranked list reinforcement exploits the underlying distribution of users to address the problem of inter-class similarity and decrease the misclassification in ranked lists. The confidence-based ranked list selection also uses the users' distribution to calculate the matchers' confidence and then utilizes them to create high confidence ranked lists. These two methods are able to significantly increase the recognition rate of rank level fusion systems. At last, the idea of resemblance probability distribution is extended to clusters of users (super-user) to enhance the response time of algorithms that are based on resemblance probability distributions. These methods will be extensively tested and proven to be efficient in the next chapter.

Chapter 5

EXPERIMENTATION AND RESULTS

This chapter covers the implementation overview of the proposed multimodal system, the databases used for system performance validation and the experimental results for different scenarios. Four multimodal databases are used for the validation. The first two multimodal databases contain faces, ears, and irises from widely used databases for biometric, in order to evaluate the performance of the proposed system in general. The third multimodal database consists of frontal face, profile face, and iris in order to test the system performance in the case of correlated biometrics. The fourth database consists of users with similar biometrics to evaluate identification rate in this scenario and also show how confidence-based ranked list selection approach can handle this situation.

5.1 Implementation Overview

The proposed system is implemented in MATLAB R2014a on an Intel(R) Core(TM)2 Duo machine running Windows 7. The implemented system has a graphical user interface to select different databases for each biometric. Each database is divided into enrollment data and identification data to facilitate the process of training and testing. After database selection, the system creates a multimodal database using the selected biometric databases. For enrollment, the proper feature extractions are utilized for each biometric to obtain representative features from the training portion of the databases. Resemblance Probability Distributions (RPDs) are calculated using the similarity of extracted features for each user. The extracted features accompanied with resemblance probability distributions for each user are stored in the system's database. After enrollment, the system operates solely based on the extracted features and resemblance probability distributions calculated during the enrollment.

For testing the system performance, the identification portion of the data is used. The same features as enrollment are extracted from the identification data and the ranked lists are created. The system provides a drop-down menu to select between different rank level fusion approaches. After selecting the desired fusion approach, the recognition results are created as comma separated values (CSV) files in the “results” directory.

5.2 Experimental Data

Due to the effort required to create a multimodal biometric database, most multimodal biometric systems use virtual databases for their performance evaluation. A virtual multimodal database for three biometrics is created by selecting three users from each biometric database and considering this triple as a virtual user [1]. The assumption behind the virtual database creation is that different biometrics of a person are not dependent [76].

For iris, the CASIA Iris Image Database V4.0 (CASIA-IrisV4) is used [77]. This database consists of six subsets. In this thesis, two of these subsets are deployed for creating multimodal databases. The other four subsets are for far distance iris recognition and deformation of the iris due to pupil dilation, which are beyond the scope of this thesis. CASIA-Iris-Interval subset is captured by a close-up iris camera, which contains an array of NIR LED. This subset provides a detailed texture of irises for 249 users. CASIA-Iris-Syn contains 10,000 iris images of 1,000 subjects. The irises in this subset are synthesized from CASIA Iris Image Database V1.0 [78]. The iris images in CASIA-Iris-Syn look completely realistic and the statistics show the same performance for synthetic and genuine iris databases [78].

For ear, the USTB database from Ear Recognition Laboratory at University of Science and Technology Beijing is used [4]. This database contains 1276 ear images of 216 subjects, which are captured in different illuminations and orientations. All the subjects’ heads had a two-meter distance from the camera during the acquisition. In order to reduce the effect of illumination and orientation, a normalization technique is utilized [79]. In order to test the capability of the system, another ear database provided by Indian Institute of Technology (IIT) Delhi, which contains 793 images of 221 subjects is used [79]. This database is acquired from students and staff at IIT Delhi in an indoor environment.

Face images from the widely used Facial Recognition Technology (FERET) database [3] are utilized. In this database, there are 14,051 face images in 24 categories of 1199 subjects captured in different orientations and illumination conditions. Among the orientations, the frontal and profile faces are used for creation of multimodal databases. Another database used from the University of Essex, UK [80]. There are 3,059 face images of 153 subjects in front of a green curtain, which 20 of them are females and the rest are males. Images of each subject have a considerable expression change, which makes a high intra-class variation.

In order to completely test the system from different aspects, four multimodal databases are created. The first and second multimodal databases are created by using FERET (frontal faces) and Essex face recognition data for face, USTB and IIT for ear, and CASIA-Iris-Interval and CASIA-Iris-Syn for iris respectively. These two databases are created from widely used databases to test the system performance in general. The first and second multimodal databases contain 216 and 153 subjects and 17,280 and 9,792 test queries respectively. Figure 5.1 and 5.2 show snapshots of these multimodal databases. The third database uses frontal and profile faces from FERET for the first and second unimodal biometrics and CASIA-Iris-Interval for the third one. This database is created with the aim of testing the effect of correlated biometrics on the final identification rate of the system. The third multimodal database contains 249 subjects with 19,920 test queries. Figure 5.3 provides a snapshot of this database. The fourth database is created to test the capability of confidence-based ranked list selection approach in handling users with similar biometrics. The same unimodal databases as the first multimodal database are used in the creation of this one. In this database, the users are paired and then for each pair, one of their biometric is randomly (uniformly) selected. The extracted features of the selected biometric of the first

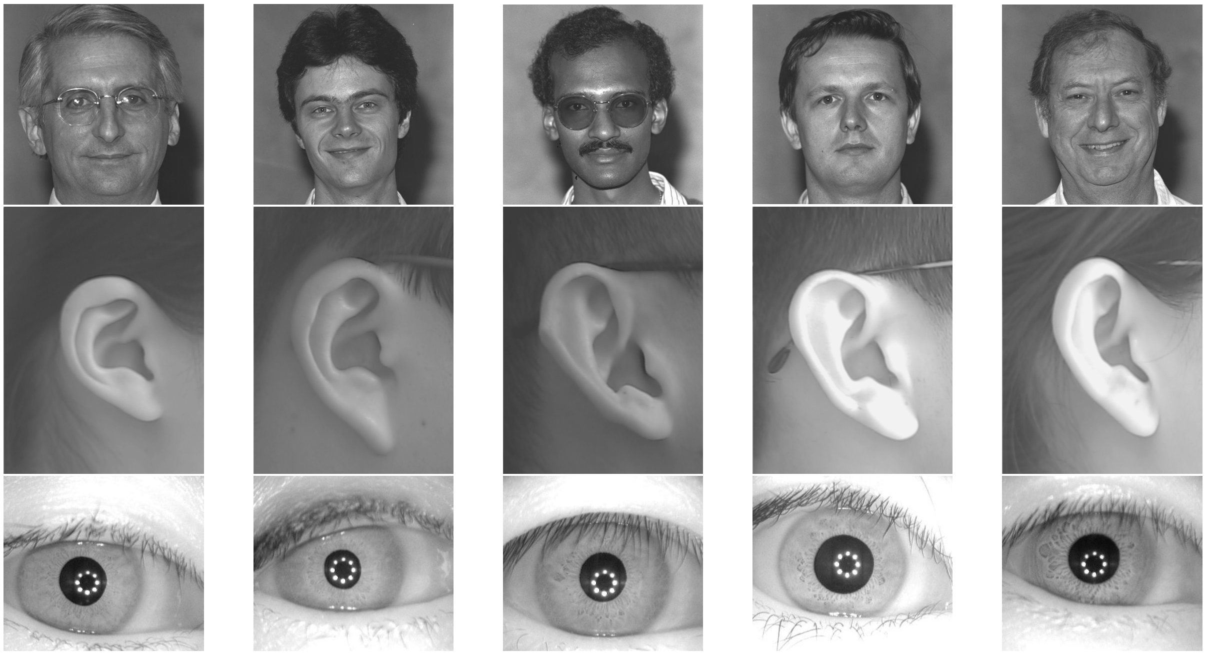


Figure 5.1: First multimodal database created from face images from FERET, ear from USTB, and iris from CASIA-Iris-Interval. The database contains 216 users and 17,280 test queries.

user in the pair are cloned for the second user, so that both of them have the same data for that biometric. This database has 216 subjects and there are 17,280 test queries to test the performance of fusion methods. A snapshot of this database is provided in figure 5.4. Table 5.1 shows the unimodal databases used in each of the four multimodal database.

Table 5.1: The four multimodal databases used for testing the system.

	FERET	FERET	Essex	USTB	IIT	CASIA	CASIA
	(frontal)	(profile)				Internal	Syn
1st multimodal database	✓			✓		✓	
2nd multimodal database			✓		✓		✓
3rd multimodal database	✓	✓				✓	
4th multimodal database	✓			✓		✓	

5.3 Experimental Results

The goal of the experiment is to test the superiority of proposed approaches for biometric rank fusion. This section first analyzes the correlation of different unimodal biometric

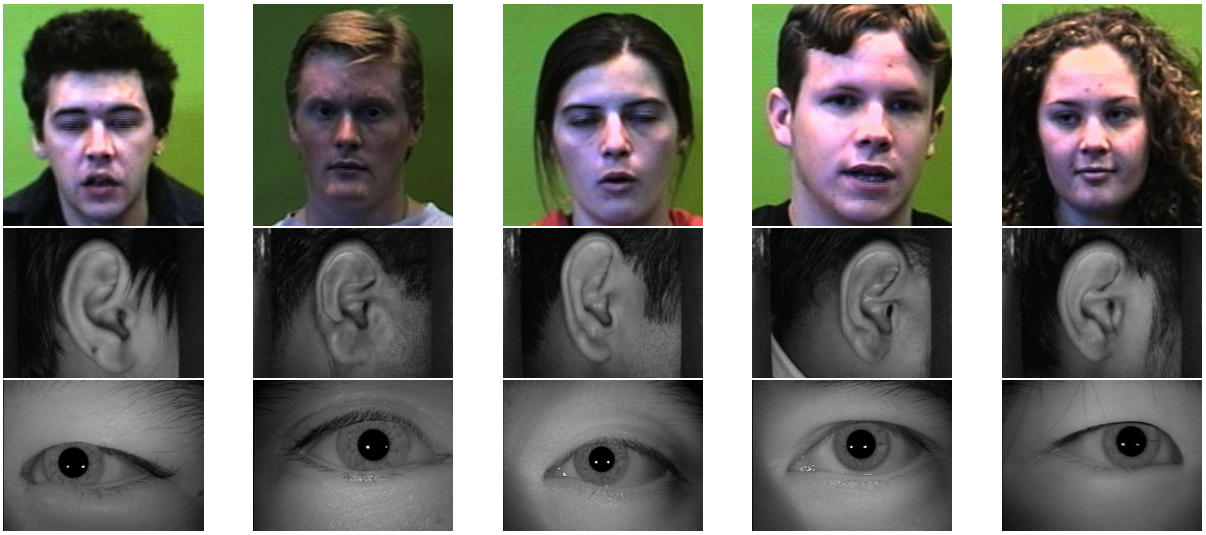


Figure 5.2: Second multimodal database created from face images from Essex face recognition data, ear from IIT database, and iris from CASIA-Iris-Syn. The database contains 153 users and 9,792 test queries.

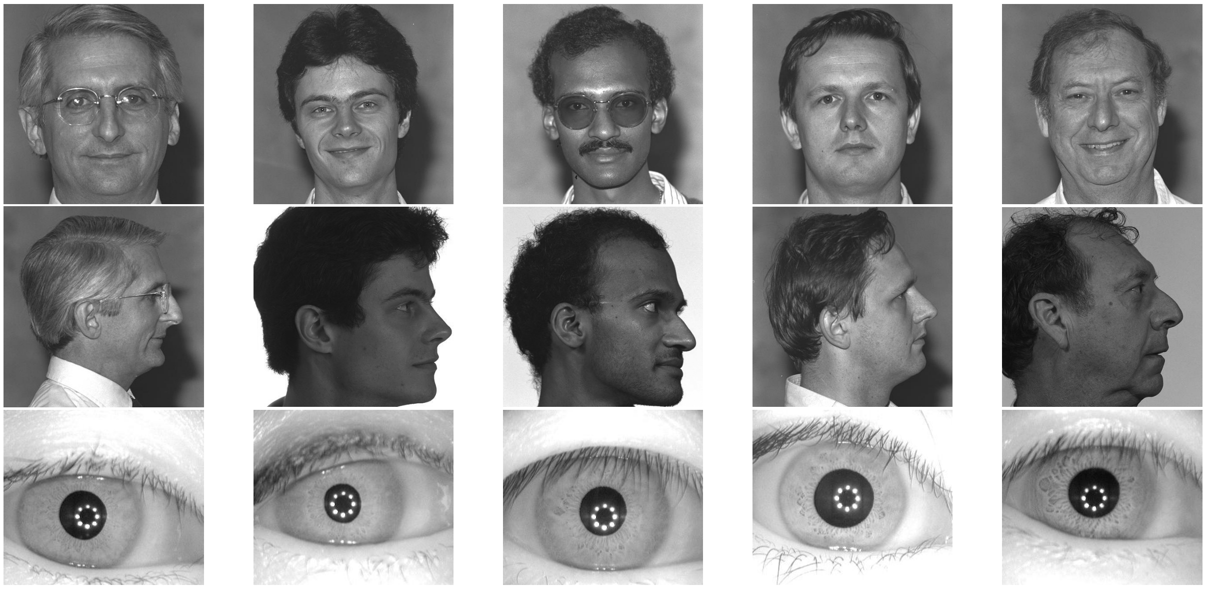


Figure 5.3: Third multimodal database created from frontal and profile face images from FERET and irises from CASIA-Iris-Interval. The database contains 249 users and 19,920 test queries.

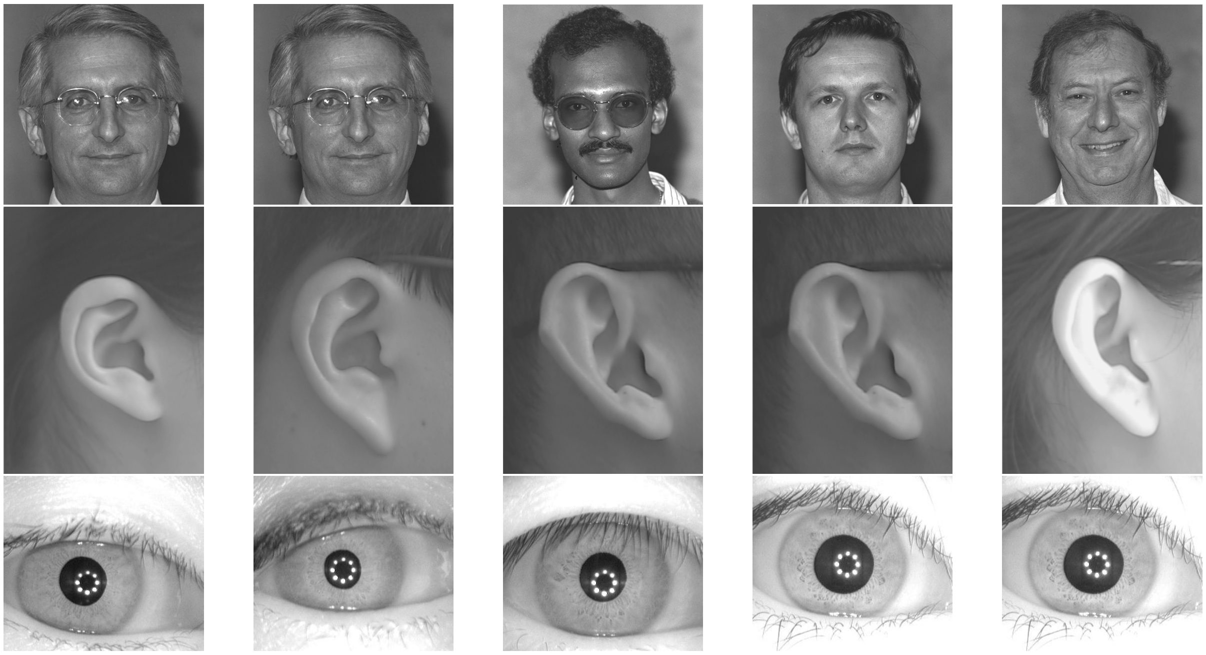


Figure 5.4: Fourth multimodal database created from face images from FERET, ear from USTB, and iris from CASIA-Iris-Interval. In this database each subject shares the same biometric with another subject. The database contains 216 users and 17,280 test queries.

databases that are used in the creation of multimodal databases. Then, it continues by testing the hypothesis that ranked list reinforcement and confidence-based ranked list selection methods are built upon. In order to verify the performance of the proposed methods from different aspects, the identification rate of the system is tested using four multimodal biometric databases.

5.3.1 Correlation Analysis of Unimodal Biometric Databases

The ability of a multimodal biometric system in providing a high identification rate is dependent on the correlation between unimodal biometrics. Uncorrelated biometrics will provide the multimodal system with information that can be inferred to obtain a higher identification rate. Table 5.2 demonstrates the correlation between unimodal biometrics that are used in the four multimodal databases. The correlation value can vary between 1 and -1. The higher the correlation value is, the more correlated the two databases are. The highest correlation among unimodal databases is between frontal and profile faces from FERET database, which is 0.6678. This high correlation value was expected, since the frontal and profile faces in FERET are captured from the same users. CASIA Internal also has a high correlation with FERET (both frontal and profile). The correlation values between the other databases are small.

Table 5.2: The average Pearson correlation between ranked lists created from the test queries of unimodal biometric databases. The value only provided for unimodal databases that are used together in a multimodal database.

	FERET (frontal)	FERET (profile)	Essex	USTB	IIT	CASIA Internal	CASIA Syn
FERET (frontal)	1						
FERET (profile)	0.6678	1					
Essex	-	-	1				
USTB	0.0128	-	-0.0036	1			
IIT	-	-	0.0244	0.1029	1		
CASIA Internal	0.3143	0.3275	-0.0434	0.2951	0.2172	1	
CASIA Syn	-	-	0.0152	0.1081	0.0984	0.0864	1

5.3.2 Correlation Analysis of Ranked Lists and Resemblance Probability Distributions

The performance of the ranked list reinforcement method is dependent on the correlation of the ranked lists and the resemblance probability distributions (RPD) of the actual identity of the test query. If the correlation between the ranked list and $\vec{1}_n - RPD$ of the actual identity of the test query is high for all the biometrics, then the actual identity has a better chance to move higher in the reinforced ranked lists. Table 5.3 shows the average correlation value between the ranked lists created for all test queries and $\vec{1}_n - RPD$s of the actual identity of each test query. As table 5.3 demonstrates, in most cases the correlation value is higher than 0.9, which is an indicator of a high similarity between the ranked lists and $\vec{1}_n - RPD$ of the actual identity of the test queries.

Table 5.3: The average Pearson correlation of ranked lists created for test queries of databases and $\vec{1}_n - RPD$s of the actual identities of the test queries.

	Biometrics			
Databases	Face (frontal)	Face (profile)	Ear	Iris
First multimodal database	0.9127	-	0.9382	0.9462
Second multimodal database	0.8936	-	0.9268	0.9396
Third multimodal database	0.9254	0.9246	-	0.9431
fourth multimodal database	0.9185	-	0.9197	0.9361

5.3.3 Similarity of Pseudo-Scores to Match Scores

The performance of the confidence-based ranked list selection approach is highly dependent on the pseudo-scores. The high similarity of the pseudo-scores to the underlying match scores that ranked list is created upon results in a better confidence measure and performance for the ranked list selection. In order to verify the similarity of pseudo-scores and actual match scores, normalized root-mean-square deviation ($NRMSD$) is used [81]. $NRMSD$ is a measure that shows the difference between predicted values and actual values of a signal and it varies between 0 and 1. Table 5.4 shows the average of $NRMSD$ for the test queries of different biometrics in multimodal databases. In all cases, the average value of $NRMSD$ is less than 0.015, which shows a high similarity between the pseudo-scores and the actual match scores.

Table 5.4: The average of normalized root-mean-square deviation between pseudo-scores and normalized match scores for queries of each biometric in databases.

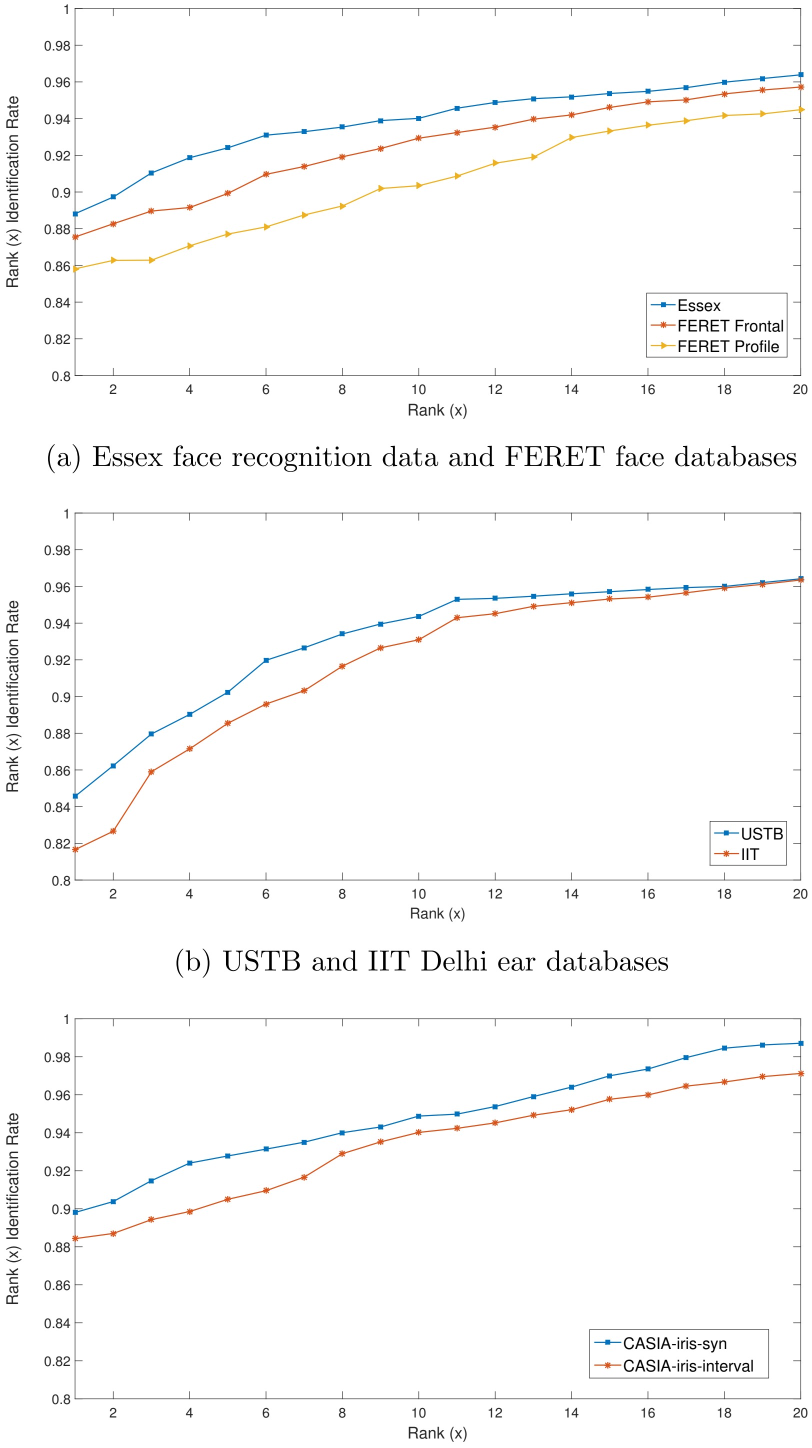
	Biometrics			
Databases	Face (frontal)	Face (profile)	Ear	Iris
First multimodal database	0.0144	-	0.0096	0.0127
Second multimodal database	0.0093	-	0.0112	0.0098
Third multimodal database	0.0096	0.0081	-	0.0115
fourth multimodal database	0.01391	-	0.0099	0.0109

5.3.4 Identification Rate Analysis of RLR and CBRLS

In order to evaluate the identification rate of the fusion methods, Cumulative Match Characteristic (CMC) curve [82] is employed. The CMC curve summarizes the identification rate of the system at different ranks. Rank x identification rate in CMC curve shows the proportion of times that the true identities of test queries were in the first n-top ranks of the fusion results.

The identification rate of each individual biometric is an important factor in the performance of the multimodal system. Moreover, it helps to grasp the effect of fusion on the identification rate. Figure 5.5 plotted the CMC curve for unimodal biometrics that are used in each multimodal database. Among the six unimodal biometric databases, CASIA-Iris-Syn has the highest first rank identification rate of 0.8980. The first rank identification rate for Essex face recognition data, CASIA Interval, FERET frontal, FERET profile, IIT, and USTB are 0.0.8881, 0.8843, 0.8754, 0.8581, 0.8456, and 0.8165, respectively.

Figure 5.6 demonstrates the identification rates of highest rank, Borda count, and logistic regression with and without using ranked list reinforcement (RLR) and confidence-based ranked list selection (CBRLS) by CMC curves for the first multimodal database. Ranked list reinforcement and confidence-based ranked list selection were able to increase the identification rates for all the tested fusion methods. In general, the confidence-based ranked list selection performed better. The reason is the attention to the performance of individual matchers for each test query and using the most confident ranked lists. The highest first rank identification rate (0.9881) is obtained by logistic regression with CBRLS. The second highest identification rate (0.9772) was for logistic regression with ranked list reinforcement. Borda count with CBRLS, Borda count with RLR, logistic regression, highest rank with CBRLS, highest rank with RLR, Borda count, and highest rank fusion were respectively the third to ninth place in the first rank identification rates. The reason behind the lower identification rate using highest rank and Borda count is that the unimodal biometrics in this multimodal



(a) Essex face recognition data and FERET face databases

(b) USTB and IIT Delhi ear databases

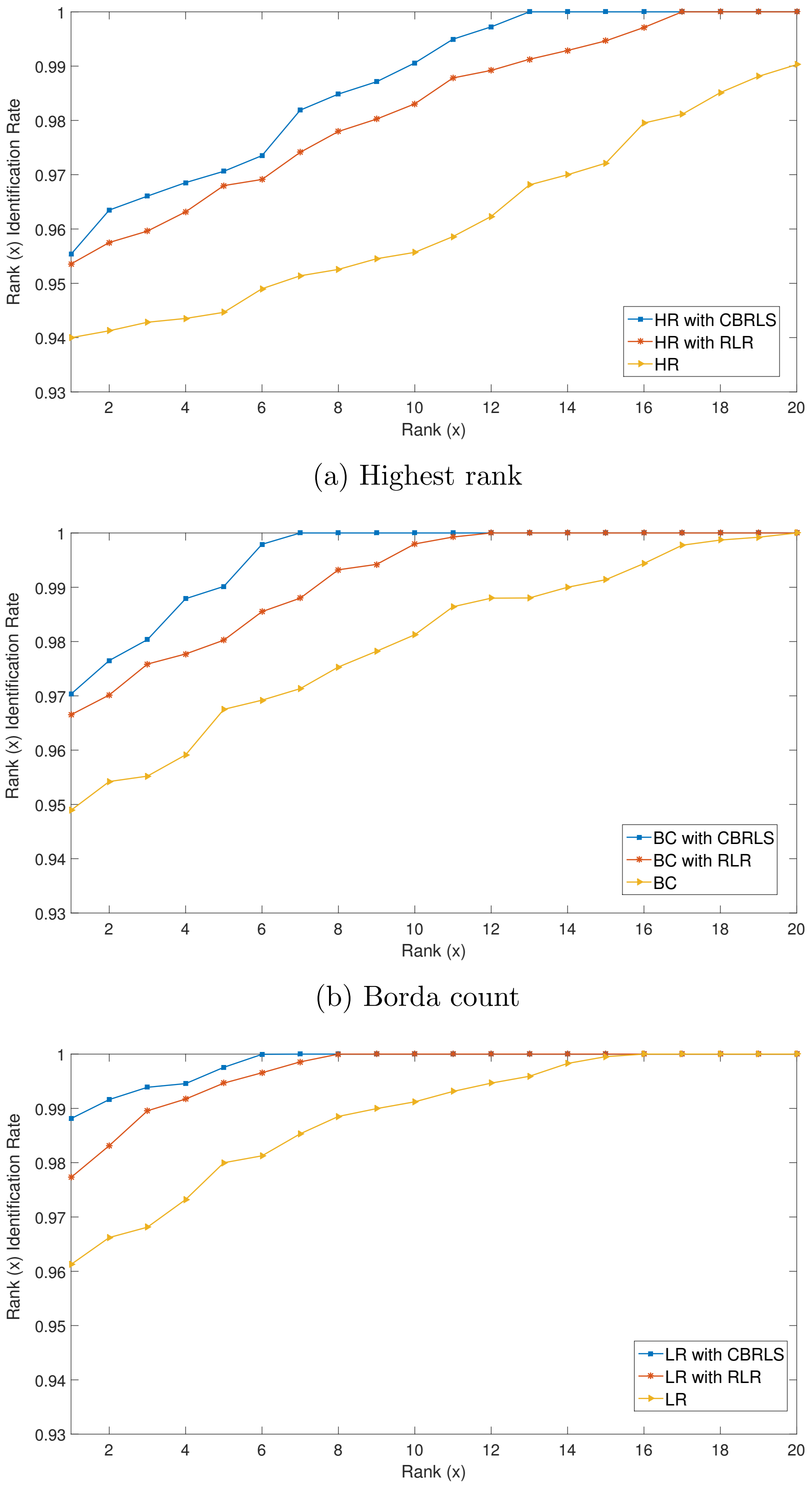
(c) CASIA-Iris-Interval and CASIA-Iris-Syn iris databases

Figure 5.5: CMC curves for unimodal biometrics used in creation of the multimodal databases.

database do not have the same identification rate. The inattention to the performance of each unimodal biometric matcher, resulted in a lower identification rate by highest rank and Borda count fusion. Moreover, CBRLS and RLR with logistic regression were able to reach 100% identification rate at rank 6 and 8 respectively, while logistic regression alone reached that point at rank 16.

In order to validate the ability of proposed methods to increase the identification rate, the second multimodal database, which consists of well-known unimodal databases, is used. Figure 5.7 demonstrates the CMC curves for highest rank (HR), Borda count (BC), and logistic regression (LR) with and without using ranked list reinforcement (RLR) and confidence-based ranked list selection (CBRLS). Similar to the results from the first database, the logistic regression with CBRLS provided the highest identification rate for all the ranks. Using RLR and CBRLS with highest rank, Borda count and logistic regression were able to increase the identification rate in all the cases. Comparing the CMC curves for different fusion methods demonstrates the ability of both RLR and CBRLS in improving the identification rate. The highest difference between the first rank identification rate of a fusion method with and without RLR and CBRLS are 0.0113 and 0.0181, which are for logistic regression fusion method. In addition, CBRLS and RLR with logistic regression were able to reach 100% identification rate at rank 7 and 8 respectively, while logistic regression alone reached that point at rank 13. The results from both figures 5.6 and 5.7 are an indicator of superiority of fusion using RLR and CBRLS.

Multimodal biometric systems are not able to obtain a high identification rate in the presence of correlated biometrics. The third multimodal database is selected in a way to have the highest correlation between its unimodal biometrics. As indicated in table 5.2, the correlation between FERET frontal and profile faces, FERET frontal face and CASIA Interval, and FERET profile and CASIA Interval are 0.6678, 0.3143, and 0.3275 respectively, which are the highest correlations among the unimodal databases in this experiment. Figure

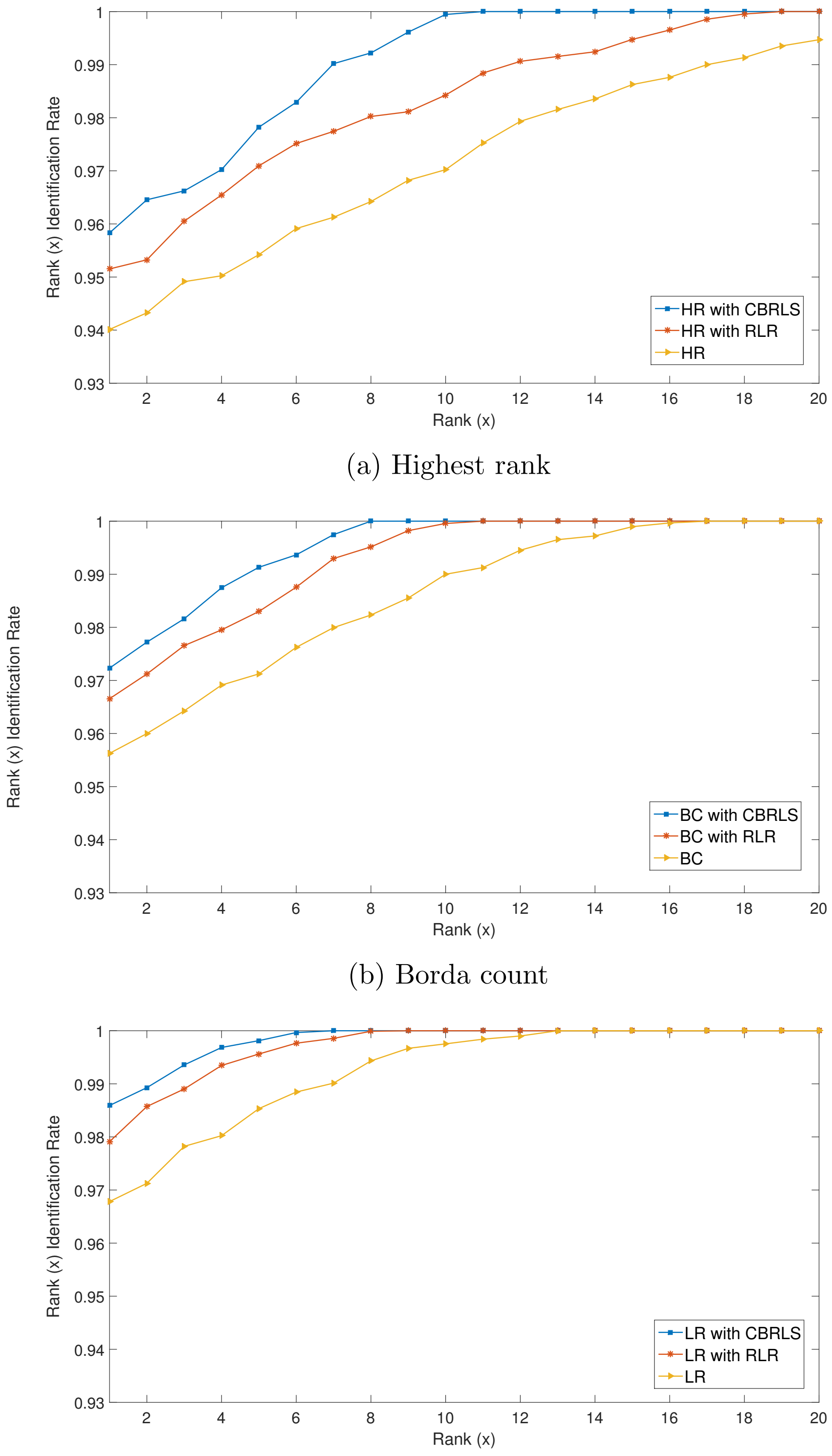


(a) Highest rank

(b) Borda count

(c) Logistic regression

Figure 5.6: CMC curves for highest rank, Borda count, and logistic regression fusion with and without ranked list reinforcement (RLR) and confidence-based classifier selection (CBRLS) on the first multimodal database.



(a) Highest rank

(b) Borda count

(c) Logistic regression

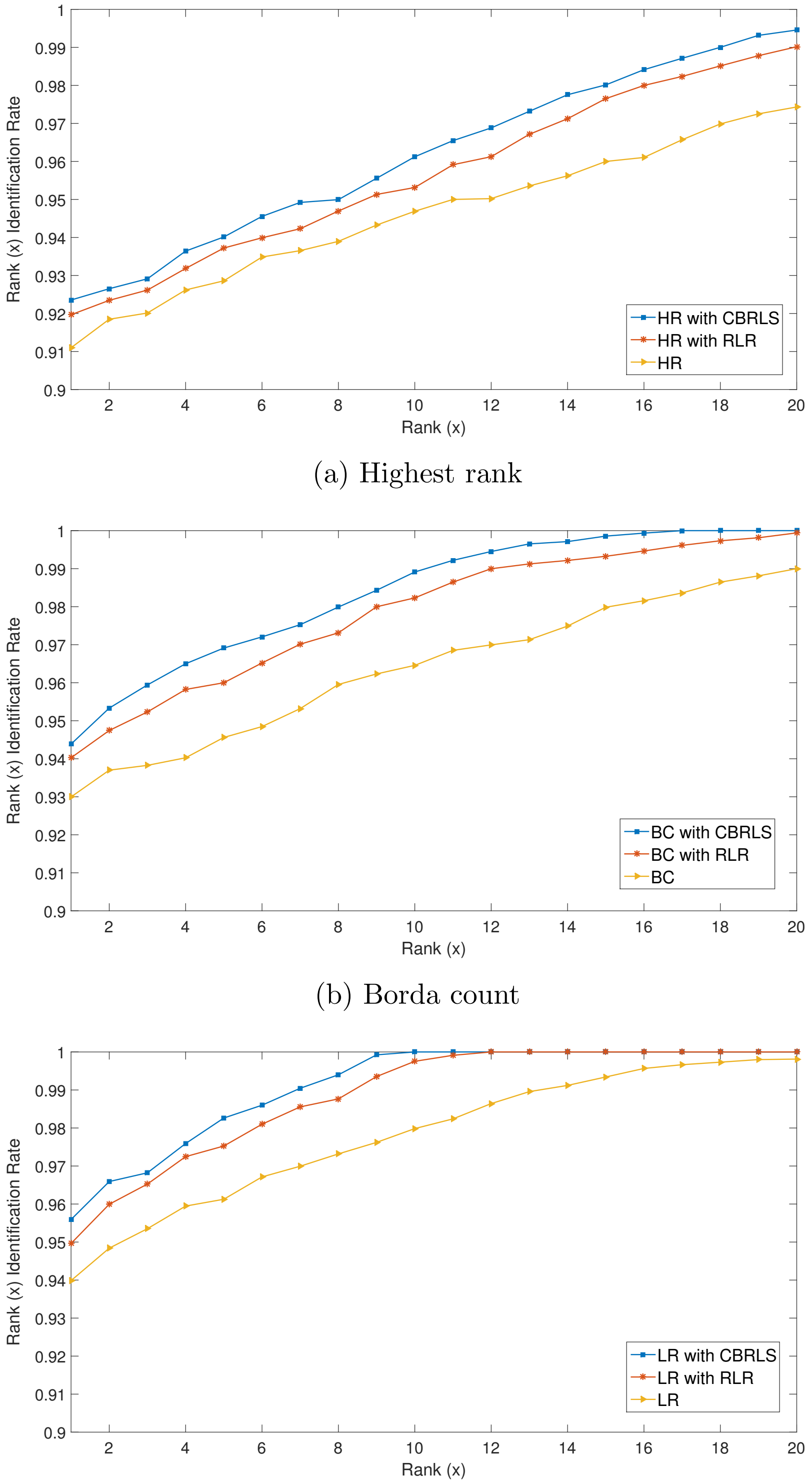
Figure 5.7: CMC curves for highest rank, Borda count, and logistic regression fusion with and without ranked list reinforcement (RLR) and confidence-based classifier selection (CBRLS) on the second multimodal database.

5.8 demonstrates the identification rates using CMC curves for highest rank, Borda count, and logistic regression with and without using RLR and CBRLS. The CMC curves show that in the presence of correlated biometrics, the multimodal system is not able to provide a high identification rate. Even though the identification rate for fusion methods are low, RLR and CBRLS are still able to provide a higher identification rate. The highest first rank identification rate obtained is 0.9559 for linear regression with CBRLS.

Confident-based ranked list selection (CBRLS) is superior in identifying the matchers which work better for each test query. To validate this superiority, the fourth database is used, which contains pairs of users with the same biometrics. Figure 5.9 demonstrates the identification rates for different ranks using CMC curves for highest rank, Borda count, and logistic regression fusions with and without using RLR and CBRLS. The results show that despite the difficulty of this database, fusion methods with CBRLS were able to maintain a high identification rate, while methods without CBRLS have lower first rank identification rates. The high gap between the identification rates of methods with CBRLS and others is due to a dynamic selection of ranked lists based on their confidence using CBRLS method. The highest obtained rank was for logistic regression with CBRLS, which is 0.95206. CBRLS with logistic regression increased the identification rate of the multimodal biometric system by 5.8% in cases of users with similar biometrics.

5.3.5 Analysis of RLR and CBRLS with Clustering

Clustering of users accelerates the identification process for fusion methods that use RLR and CBRLS. The cluster size is an important factor in this acceleration. Figure 5.10 shows the average identification response time of the fusion methods with RLR and CBRLS for different levels of cut in the dendrogram (different cluster sizes). First, second, and the third levels cut of the dendrogram provide the most reduction in the response time of the system. This reduction is due to the increase in the cluster sizes and decrease in the number of clusters.

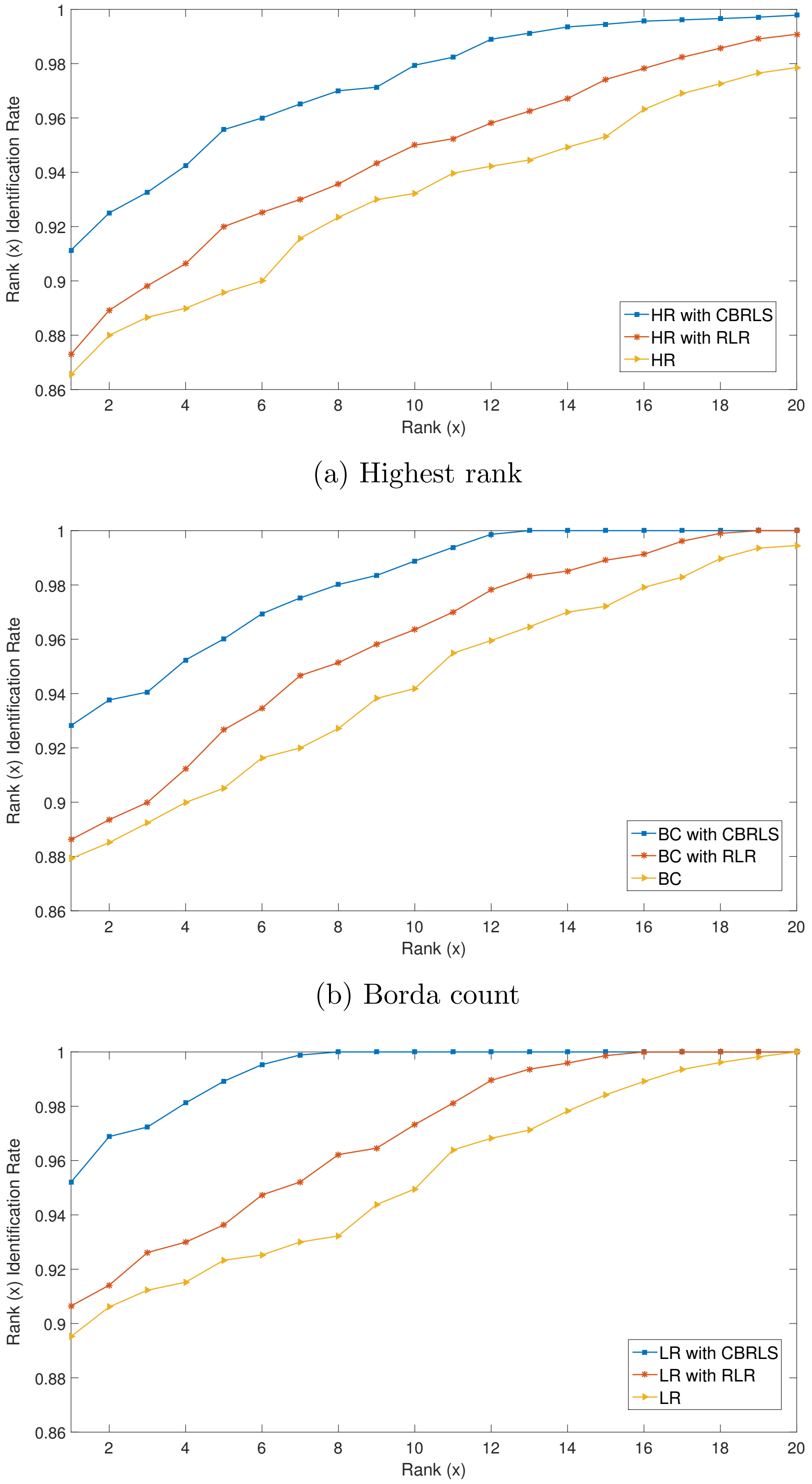


(a) Highest rank

(b) Borda count

(c) Logistic regression

Figure 5.8: CMC curves for highest rank, Borda count, and logistic regression fusion with and without ranked list reinforcement (RLR) and confidence-based classifier selection (CBRLS) on the third multimodal database.



(a) Highest rank

(b) Borda count

(c) Logistic regression

Figure 5.9: CMC curves for highest rank, Borda count, and logistic regression fusion with and without ranked list reinforcement (RLR) and confidence-based classifier selection (CBRLS) on the fourth multimodal database.

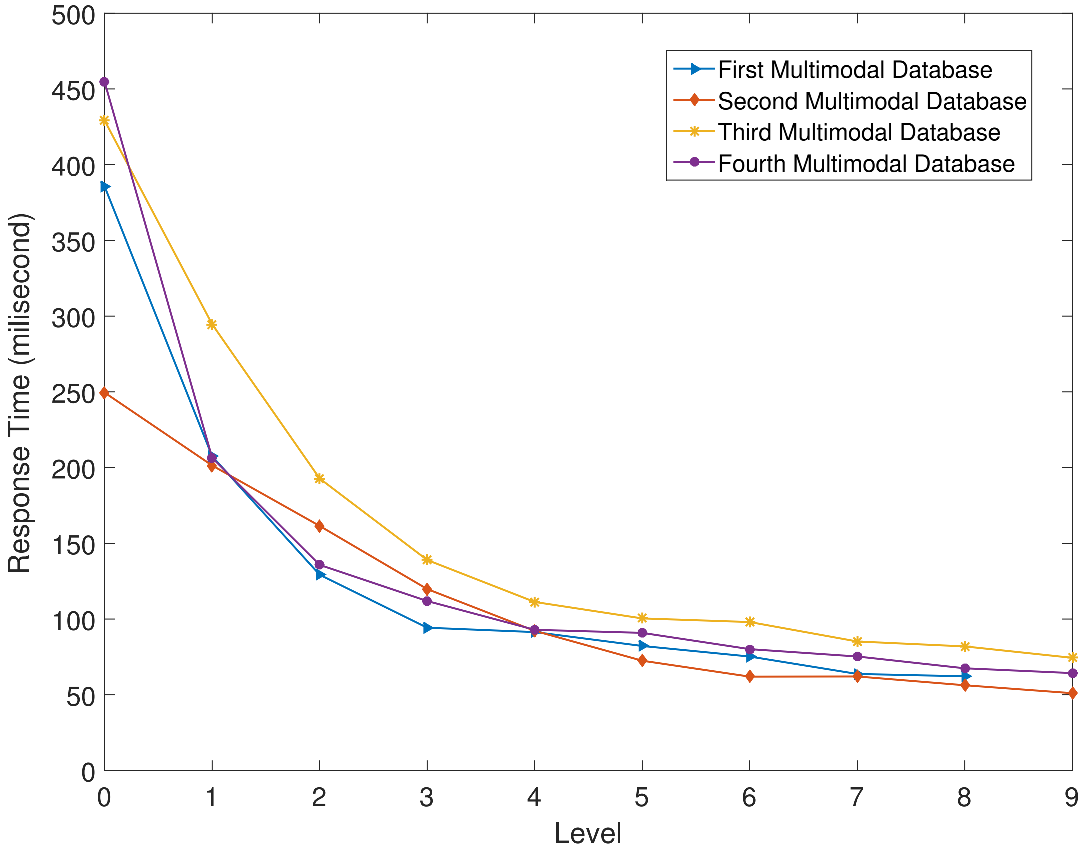
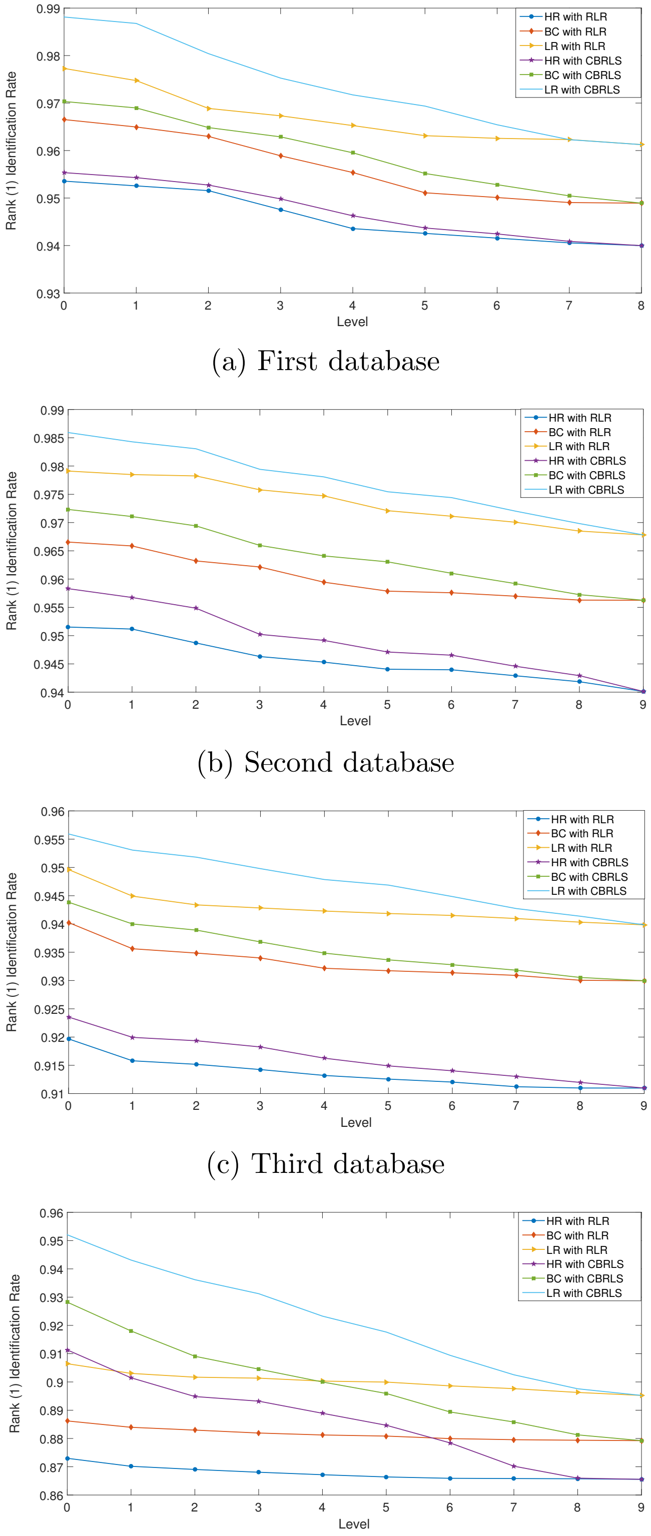


Figure 5.10: Average response time of the system for fusion methods that use RLR and CBRLS for different levels of cut in the dendrogram.



(a) First database

(b) Second database

(c) Third database

(d) Fourth database

Figure 5.11: First rank identification rate for cuts at different levels of dendrogram.

On the other hand, clustering of users decreases the system's ability to distinguish between users and it will cause a lower identification rate for large cluster sizes. Figure 5.11 shows this trade-off by demonstrating the first rank identification rates of fusions with RLR and CBRLS for the four databases for cuts at different levels of dendrogram. The value for the level zero is equal to first rank identification rate of fusion methods with RLR and CBRLS without clustering (cluster size of 1). The last level of cut in the dendrogram is considering all the users in one cluster. It basically is equal to not using RLR and CBRLS, which results in the same identification rate as fusion methods without RLR and CBRLS. Depending on the application and the required response time, and acceptable identification rate, the system administrator is able to decide on the proper clustering of the users.

5.4 Chapter Summary

This chapter provided different experimentation for analyzing the performance of ranked list reinforcement (RLR) and confidence-based ranked list selection approaches for multimodal biometric rank level fusion. Four different multimodal biometric databases were utilized to evaluate the system from different aspects. The first two multimodal databases were composed of well-known face, iris, and ear biometrics to test the system in general. The proposed fusion methods that used RLR and CBRLS produced higher identification rates. The third multimodal database was created from unimodal databases that had the highest correlation values. The identification rates of fusion methods for this database were lower than the others, although employing RLR and CBRLS helped the fusion methods to obtain higher identification rates. The fourth database contained users with the same biometric for one of their modalities. This database showed the superiority of CBRLS to handle the situations that two people have similar biometrics. In total, employment of RPDs in fusion was able to increase the identification rate of the multimodal biometric system by 2.9% in general cases and 5.8% in cases of users with similar biometrics.

Chapter 6

CONCLUSION AND FUTURE WORK

This chapter concludes this master thesis by providing the thesis summary, a summary of contribution attained in this research, conclusions and the possible direction for extending the contributions of this thesis and improvement of multimodal biometric systems.

6.1 Thesis Summary

Chapter 1 started with an introduction to biometric and its important in the current society. The key challenges in the design of a biometric system were discussed and then the contributions of this thesis alongside a brief methodology to address these challenges were presented.

Chapter 2 provided an overview of the biometric system and the advantages of using a multimodal biometric system. Different types of multimodal biometric systems were discussed. Then, information fusion was introduced as an important part of a multimodal biometric system. Advantages of different levels of fusion with a review of previous researches with emphasis on post-mapping fusions were provided. At the end of this chapter, highest rank, Borda count, and logistic regression were covered in more detail as well-known rank level fusion methods.

In Chapter 3, an overview of the multimodal biometric system for rank level fusion that deploys resemblance probability distributions were provided. Then, the chapter looked in detail to the conventional unimodal biometric matchers for face (frontal/profile), ear, and iris as the building blocks of a multimodal system. An overview of unimodal biometric matchers with ability to extract resemblance probability distribution were discussed.

Chapter 4 covered the proposed methodologies for confidence-based rank fusion. This chapter introduced the notion of Resemblance Probability Distribution (RPD) to retain the lost information due to abstraction in the ranked lists and used this information to obtain a higher recognition rate. Ranked List Reinforcement (RLR) and Confidence-Based Ranked List Selection (CBRLS) were the two new rank fusion methods based on the idea of resemblance probability distributions. In order to accelerate the fusion module, the notion of RPD was generalized to clusters of users.

Chapter 5 provided the implementation overview of the proposed multimodal system. It introduced different databases used for system performance validation in order to cover different scenarios for the system and then provided the experimental results for these databases. Four multimodal databases were used for the validation. The first two multimodal databases contained faces, ears, and irises from widely used databases for biometric, in order to evaluate the performance of the proposed system in general. The third multimodal database consisted of frontal face, profile face, and iris in order to test the system performance in the case of correlated biometrics. The fourth database consisted of users with similar biometrics to evaluate the recognition rate in this scenario and also showed how confidence-based ranked list selection approach can handle this situation. The experimental results for clustering of the users and its effect of the system response time and recognition rate were also provided at the end of this chapter.

6.2 Summary of Contributions

This section summarizes the contribution of this research to rank level fusion in multimodal biometric systems. The contributions of this thesis are as follows:

- This thesis introduced the notion of Resemblance Probability Distribution (RPD) as a supplementary information along with the ranked list of each biometric matcher to capture the distribution of users in the feature space. RPDs can be used to improve the recognition rate and accuracy of the system.

- The RPD was used in the new concept of ranked list reinforcement (RLR) for rank level fusion in multimodal biometric system. RLR is the reordering of rank list based on the information provided by RPD in order to result a rank list with a higher confidence level.

- The novel confidence-based ranked list selection (CBRLS) was also proposed based on RPDs. CBRLS is able to select biometric matchers dynamically based on their performance for any test query. CBRLS is able to address the problem of noisy data and inter-class similarity.

- This thesis also generalized the notion of RPDs to clusters of users and adapted the ranked list reinforcement and confidence-based ranked list selection approaches to operate on clusters. The clustering of users helped to accelerate the system response time.

This thesis also had the following experimental and development contributions:

- The effect of cluster size on the identification rate and also enhancement of the system's response time was evaluated.

- The effect of correlated biometrics e.g., frontal face, profile face, and ear and uncorrelated biometrics e.g. frontal face, ear, and iris has been studied to evaluate the performance of the proposed RPD based fusion techniques in this situation. The system also tested on database of users with similar biometrics to evaluate the ability of the proposed methods in recognizing the proper matchers for fusion.

- Unimodal biometric systems for frontal face, profile face, ear, and iris were developed.

- A multimodal biometric system with rank level fusion and the ability to use RPDs for ranked list reinforcement and confidence-based ranked list selection was developed.

6.3 Conclusions

In this master thesis, a new multimodal biometric system based on face, ear, and iris (all from facial area) was presented. In order to consolidate the recognition results from different matchers, two different fusion approaches were proposed. Both of the proposed fusion approaches were based on the idea of resemblance probability distribution, which is also a contribution of this thesis. The resemblance probability distribution is the distribution of users' biometrics in the feature space and this information can be used in order to improve the fusion process in multimodal systems. The rank list reinforcement method was introduced to enhance the rank lists from biometric matchers. It reorders the rank of users in the ranked list by the means of resemblance probability distributions. Confidence-based rank list selection (CBRLS) is another method proposed based on resemblance probability distributions. CBRLS is able to dynamically select ranked lists for different test queries based on the confidence level calculated using resemblance probability distributions. This thesis also generalized the notion of resemblance probability distributions to the clusters of users to enhance the response time of the multimodal biometric systems. The proposed approaches were tested using four different multimodal biometric databases. Both RLR and CBRLS provided high recognition rates on general biometric databases. In the presence of correlated biometrics, RLR and CBRLS was still able to improve the recognition rate. For the fourth database, which contained users with similar biometrics, CBRLS provided far better results than any other fusion methods. The outcomes of this research have been presented and published in high quality conferences, such as International Conference on Computational Science (ICCS), the IEEE international conference on Identity, Security and

Behavior Analysis (ISBA), and international conference of Computer Analysis of Images and Pattern (CAIP).

6.4 Future Work

In this work, I employed the RPDs to the multimodal biometric domain. However, RPDs can be used to improve the identification rate of any pattern recognition systems that consolidate information from different sources.

Testing the proposed system on a real multimodal biometric system is essential for the real world deployment of the system as a security application. The system's performance can be tested on a multimodal database, that all the modalities are collected from users in one session.

More research can be done in utilization of RPDs to increase the identification rate of biometric systems that works solely based on one biometric. These unimodal systems can then be used in a multimodal system to provide a higher identification rate.

Rank list reinforcement and confidence based rank list selection were two of the possible techniques for utilization of RPDs. Further research can be done on finding new approaches to utilize RPDs in fusion of information.

Finally, this research only investigated the utilization of resemblance probability distribution on rank level fusion. The effect of RPDs employment on other post-mapping fusion levels can be investigated.

Bibliography

[1] Arun A Ross, Karthik Nandakumar, and Anil K Jain. *Handbook of multibiometrics*, volume 6. Springer Science & Business Media, 2006.

[2] MD Monwar. *A Multimodal Biometric System Based on Rank Level Fusion*. PhD thesis, University of Calgary, 2500 University Dr NW, Calgary, 2013.

[3] P Jonathon Phillips, Harry Wechsler, Jeffery Huang, and Patrick J Rauss. The feret database and evaluation procedure for face-recognition algorithms. *Image and vision computing*, 16(5):295–306, 1998.

[4] USTB ear database, china. retrieved on september 21, 2014. http://www1.ustb.edu.cn/resb/en/index.htm.

[5] John G Daugman. High confidence visual recognition of persons by a test of statistical independence. *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, 15(11):1148–1161, 1993.

[6] Anil K Jain, Patrick Flynn, and Arun A Ross. *Handbook of biometrics*. Springer Science & Business Media, 2007.

[7] Ted Dunstone and Neil Yager. *Biometric system and data analysis: Design, evaluation, and data mining*. Springer Science & Business Media, 2008.

[8] Maruf Monwar and Marina L Gavrilova. Multimodal biometric system using rank-level fusion approach. *Systems, Man, and Cybernetics, Part B: Cybernetics, IEEE Transactions on*, 39(4):867–878, 2009.

[9] Yi Chen, Sarat C Dass, and Anil K Jain. Fingerprint quality indices for predicting authentication performance. In *Audio-and Video-Based Biometric Person Authentication*, pages 160–170. Springer, 2005.

[10] Umut Uludag, Arun Ross, and Anil Jain. Biometric template selection and update: a case study in fingerprints. *Pattern Recognition*, 37(7):1533–1542, 2004.

[11] Anil K Jain. Biometric recognition: how do i know who you are? In *Image Analysis and Processing–ICIAP 2005*, pages 19–26. Springer, 2005.

[12] Ruud Bolle. *Guide to biometrics.* Springer Science & Business Media, 2004.

[13] Hossein Talebi and Marina L Gavrilova. Prior resemblance probability of users for multimodal biometrics rank fusion. In *Identity, Security and Behavior Analysis (ISBA), 2015 IEEE International Conference on*, pages 1–7. IEEE, 2015.

[14] Hossein Talebi and Marina L Gavrilova. Confidence based rank level fusion for multimodal biometric systems. In *Computer Analysis of Images and Patterns*, pages 211–222. Springer, 2015.

[15] Davide Maltoni, Dario Maio, Anil K Jain, and Salil Prabhakar. *Handbook of fingerprint recognition.* Springer Science & Business Media, 2009.

[16] Anil K Jain and Stan Z Li. *Handbook of face recognition*, volume 1. Springer, 2005.

[17] Arun Ross and Anil K Jain. Multimodal biometrics: An overview. In *Signal Processing Conference, 2004 12th European*, pages 1221–1224. IEEE, 2004.

[18] Robert W Frischholz and Ulrich Dieckmann. Biold: a multimodal biometric identification system. *Computer*, 33(2):64–68, 2000.

[19] Lin Hong and Anil Jain. Integrating faces and fingerprints for personal identification. *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, 20(12):1295–1307, 1998.

[20] Mohamed Soltane, Noureddine Doghmane, and Noureddine Guersi. Face and speech based multi-modal biometric authentication. *International Journal of Advanced Science*

and Technology, 21(6):41–56, 2010.

[21] James Llinas, Christopher Bowman, Galina Rogova, Alan Steinberg, Ed Waltz, and Frank White. Revisiting the jdl data fusion model ii. Technical report, DTIC Document, 2004.

[22] Jana Kludas, Eric Bruno, and Stephane Marchand-Maillet. Information fusion in multimedia information retrieval. In *Adaptive Multimedia Retrieval: Retrieval, User, and Semantics*, pages 147–159. Springer, 2008.

[23] Valdimir S Petrović and Costas S Xydeas. Gradient-based multiresolution image fusion. *Image Processing, IEEE Transactions on*, 13(2):228–237, 2004.

[24] Vicenc Torra. *Information fusion in data mining*, volume 123. Springer, 2013.

[25] Hossein Talebi, Winsor Hoang, and Marina L Gavrilova. Multi-scale foreign exchange rates ensemble for classification of trends in forex market. *Procedia Computer Science*, 29:2065–2075, 2014.

[26] Conrad Sanderson and Kuldip K Paliwal. Information fusion for robust speaker verification. In *INTERSPEECH*, pages 755–758, 2001.

[27] Uwe M Bubeck. Multibiometric authentication. *Term Project CS, San Diego State University*, 574, 2003.

[28] Rein-Lien Hsu. *Face detection and modeling for recognition.* PhD thesis, Michigan State University, 2002.

[29] Xiaoming Liu and Tsuhan Chen. Geometry-assisted statistical modeling for face mosaicing. In *Image Processing, 2003. ICIP 2003. Proceedings. 2003 International Conference on*, volume 2, pages II–883. IEEE, 2003.

[30] R Raghavendra, Ashok Rao, and G Hemantha Kumar. Multisensor biometric evidence fusion of face and palmprint for person authentication using particle swarm optimisation (pso). *International Journal of Biometrics*, 2(1):19–33, 2009.

[31] Arun A Ross and Rohin Govindarajan. Feature level fusion of hand and face biometrics. In *Defense and Security*, pages 196–204. International Society for Optics and Photonics, 2005.

[32] Guiyu Feng, Kaifeng Dong, Dewen Hu, and David Zhang. When faces are combined with palmprints: a novel biometric fusion strategy. In *Biometric authentication*, pages 701–707. Springer, 2004.

[33] Ajita Rattani, Dakshina Ranjan Kisku, Manuele Bicego, and Massimo Tistarelli. Feature level fusion of face and fingerprint biometrics. In *Biometrics: Theory, Applications, and Systems, 2007. BTAS 2007. First IEEE International Conference on*, pages 1–6. IEEE, 2007.

[34] Dhiman Karmakar and CA Murthy. Generation of new points for training set and feature-level fusion in multimodal biometric identification. *Machine vision and applications*, 25(2):477–487, 2014.

[35] Anil Jain, Lin Hong, and Ruud Bolle. On-line fingerprint verification. *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, 19(4):302–314, 1997.

[36] Anil Jain, Karthik Nandakumar, and Arun Ross. Score normalization in multimodal biometric systems. *Pattern recognition*, 38(12):2270–2285, 2005.

[37] Mingxing He, Shi-Jinn Horng, Pingzhi Fan, Ray-Shine Run, Rong-Jian Chen, Jui-Lin Lai, Muhammad Khurram Khan, and Kevin Octavius Sentosa. Performance evaluation of score level fusion in multimodal biometric systems. *Pattern Recognition*, 43(5):1789–1800, 2010.

[38] Vassilios Chatzis, Adrian G Borş, and Ioannis Pitas. Multimodal decision-level fusion for person authentication. *Systems, Man and Cybernetics, Part A: Systems and Humans, IEEE Transactions on*, 29(6):674–680, 1999.

[39] Ajay Kumar and Sumit Shekhar. Palmprint recognition using rank level fusion. In *Image Processing (ICIP), 2010 17th IEEE International Conference on*, pages 3121–3124. IEEE, 2010.

[40] Mark Montague and Javed A Aslam. Condorcet fusion for improved retrieval. In *Proceedings of the eleventh international conference on Information and knowledge management*, pages 538–548. ACM, 2002.

[41] David M Pennock, Eric Horvitz, C Lee Giles, et al. Social choice theory and recommender systems: Analysis of the axiomatic foundations of collaborative filtering. In *AAAI/IAAI*, pages 729–734, 2000.

[42] Vasyl Pihur, Susmita Datta, and Somnath Datta. Finding cancer genes through meta-analysis of microarray experiments: Rank aggregation via the cross entropy algorithm. *Genomics*, 2008.

[43] Rabia Nuray and Fazli Can. Automatic ranking of information retrieval systems using data fusion. *Information Processing & Management*, 42(3):595–614, 2006.

[44] Mohamed Farah and Daniel Vanderpooten. An outranking approach for information retrieval. *Information Retrieval*, 11(4):315–334, 2008.

[45] Jay Bhatnagar, Ajay Kumar, and Nipun Saggar. A novel approach to improve biometric recognition using rank level fusion. In *Computer Vision and Pattern Recognition, 2007. CVPR'07. IEEE Conference on*, pages 1–6. IEEE, 2007.

[46] Ajay Kumar and Sumit Shekhar. Personal identification using multibiometrics rank-level fusion. *Systems, Man, and Cybernetics, Part C: Applications and Reviews, IEEE*

Transactions on, 41(5):743–752, 2011.

[47] Md Maruf Monwar, Marina Gavrilova, and Yingxu Wang. A novel fuzzy multimodal information fusion technology for human biometric traits identification. In *Cognitive Informatics & Cognitive Computing (ICCI* CC), 2011 10th IEEE International Conference on*, pages 112–119. IEEE, 2011.

[48] Ayman Abaza and Arun Ross. Quality based rank-level fusion in multibiometric systems. In *Biometrics: Theory, Applications, and Systems, 2009. BTAS'09. IEEE 3rd International Conference on*, pages 1–6. IEEE, 2009.

[49] Emanuela Marasco, Ayman Abaza, and Bojan Cukic. Why rank–level fusion? and what is the impact of image quality? *International Journal of Big Data Intelligence*, 2(2):106–116, 2015.

[50] Mohammad Rafiqul Alam, Mohammed Bennamoun, Roberto Togneri, and Ferdous Sohel. Confidence-based rank-level fusion for audio-visual person identification system. In *3rd International Conference on Pattern Recognition Applications and Methods*, pages 608–615, 2014.

[51] Stan Z Li. *Encyclopedia of Biometrics: I-Z.*, volume 1. Springer Science & Business Media, 2009.

[52] Chuck Wilson. *Vein pattern recognition: a privacy-enhancing biometric*. CRC press, 2010.

[53] Michel Truchon. An extension of the condorcet criterion and kemeny orders. *Cahier*, 9813, 1998.

[54] Ronald Fagin. Combining fuzzy information from multiple systems. In *Proceedings of the fifteenth ACM SIGACT-SIGMOD-SIGART symposium on Principles of database systems*, pages 216–226. ACM, 1996.

[55] Peter N. Belhumeur, João P Hespanha, and David Kriegman. Eigenfaces vs. fisherfaces: Recognition using class specific linear projection. *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, 19(7):711–720, 1997.

[56] Dennis Gabor. Theory of communication. part 1: The analysis of information. *Journal of the Institution of Electrical Engineers-Part III: Radio and Communication Engineering*, 93(26):429–441, 1946.

[57] Richard W Hamming. Error detecting and error correcting codes. *Bell System technical journal*, 29(2):147–160, 1950.

[58] Wenyi Zhao, Rama Chellappa, P Jonathon Phillips, and Azriel Rosenfeld. Face recognition: A literature survey. *Acm Computing Surveys (CSUR)*, 35(4):399–458, 2003.

[59] Ingemar J Cox, Joumana Ghosn, and Peter N Yianilos. Feature-based face recognition using mixture-distance. In *Computer Vision and Pattern Recognition, 1996. Proceedings CVPR'96, 1996 IEEE Computer Society Conference on*, pages 209–216. IEEE, 1996.

[60] BS Manjunath, Rama Chellappa, and Christoph von der Malsburg. A feature based approach to face recognition. In *Computer Vision and Pattern Recognition, 1992. Proceedings CVPR'92., 1992 IEEE Computer Society Conference on*, pages 373–378. IEEE, 1992.

[61] Kazunori Okada, Johannes Steffens, Thomas Maurer, Hai Hong, Egor Elagin, Hartmut Neven, and Christoph von der Malsburg. The bochum/usc face recognition system and how it fared in the feret phase iii test. In *Face Recognition*, pages 186–205. Springer, 1998.

[62] Laurenz Wiskott, J-M Fellous, N Kuiger, and Christoph Von Der Malsburg. Face recognition by elastic bunch graph matching. *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, 19(7):775–779, 1997.

[63] Steve Lawrence, C Lee Giles, Ah Chung Tsoi, and Andrew D Back. Face recognition: A convolutional neural-network approach. *Neural Networks, IEEE Transactions on*, 8(1):98–113, 1997.

[64] Matthew A Turk and Alex P Pentland. Face recognition using eigenfaces. In *Computer Vision and Pattern Recognition, 1991. Proceedings CVPR'91., IEEE Computer Society Conference on*, pages 586–591. IEEE, 1991.

[65] Ian Jolliffe. *Principal component analysis*. Wiley Online Library, 2002.

[66] Suresh Balakrishnama and Aravind Ganapathiraju. Linear discriminant analysis-a brief tutorial. *Institute for Signal and Information Processing*, 1998.

[67] Mark Burge and Wilhelm Burger. Ear biometrics. In *Biometrics*, pages 273–285. Springer, 1996.

[68] Kyong Chang, Kevin W Bowyer, Sudeep Sarkar, and Barnabas Victor. Comparison and combination of ear and face images in appearance-based biometrics. *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, 25(9):1160–1165, 2003.

[69] John Daugman. How iris recognition works. *Circuits and Systems for Video Technology, IEEE Transactions on*, 14(1):21–30, 2004.

[70] Paul VC Hough. Method and means for recognizing complex patterns. Technical report, 1962.

[71] Richard P Wildes. Iris recognition: an emerging biometric technology. *Proceedings of the IEEE*, 85(9):1348–1363, 1997.

[72] Libor Masek et al. *Recognition of human iris patterns for biometric identification*. PhD thesis, Masters thesis, University of Western Australia, 2003.

[73] Karl Pearson. Note on regression and inheritance in the case of two parents. *Proceedings of the Royal Society of London*, pages 240–242, 1895.

[74] Yun Wang. *Statistical Techniques for Network Security: Modern Statistically-Based Intrusion Detection and Protection: Modern Statistically-Based Intrusion Detection and Protection*. IGI Global, 2008.

[75] Anil K Jain, M Narasimha Murty, and Patrick J Flynn. Data clustering: a review. *ACM computing surveys (CSUR)*, 31(3):264–323, 1999.

[76] Marina L Gavrilova and Md Maruf Monwar. Fusing multiple matcher's outputs for secure human identification. *International Journal of Biometrics*, 1(3):329–348, 2009.

[77] CASIA. Casia iris database, 2015. [Online; Retrieved on May-2015, http://biometrics.idealtest.org/dbDetailForUser.do?id=4].

[78] Tieniu Tan, Zhaofeng He, and Zhenan Sun. Efficient and robust segmentation of noisy iris images for non-cooperative iris recognition. *Image and Vision Computing*, 28(2):223–230, 2010.

[79] Ajay Kumar and Chenye Wu. Automated human identification using ear imaging. *Pattern Recognition*, 45(3):956–968, 2012.

[80] University of essex face recognition data, 2015. [Online; accessed 21-April-2015, http://cswww.essex.ac.uk/mv/allfaces/].

[81] Rob J Hyndman and Anne B Koehler. Another look at measures of forecast accuracy. *International journal of forecasting*, 22(4):679–688, 2006.

[82] Hyeonjoon Moon and P Jonathon Phillips. Computational and performance aspects of pca-based face-recognition algorithms. *Perception-London*, 30(3):303–322, 2001.