



Graduate Theses, Dissertations, and Problem Reports

2004

Feature-level fusion in multimodal biometrics

Rohin K. Govindarajan
West Virginia University

Follow this and additional works at: <https://researchrepository.wvu.edu/etd>

Recommended Citation

Govindarajan, Rohin K., "Feature-level fusion in multimodal biometrics" (2004). *Graduate Theses, Dissertations, and Problem Reports*. 1489.
<https://researchrepository.wvu.edu/etd/1489>

This Thesis is protected by copyright and/or related rights. It has been brought to you by the The Research Repository @ WVU with permission from the rights-holder(s). You are free to use this Thesis in any way that is permitted by the copyright and related rights legislation that applies to your use. For other uses you must obtain permission from the rights-holder(s) directly, unless additional rights are indicated by a Creative Commons license in the record and/ or on the work itself. This Thesis has been accepted for inclusion in WVU Graduate Theses, Dissertations, and Problem Reports collection by an authorized administrator of The Research Repository @ WVU. For more information, please contact researchrepository@mail.wvu.edu.

FEATURE LEVEL FUSION IN MULTIMODAL BIOMETRICS

Rohin K. Govindarajan

A THESIS

submitted to the College of Engineering and Mineral Resources at West Virginia University in
partial fulfillment of the requirements for the degree of

MASTER OF SCIENCE in COMPUTER SCIENCE

Dr. Arun Abraham Ross, Chair

Dr. Lawrence Hornak

Dr. Stephanie Schuckers

Lane Department Of Computer Science and Electrical Engineering

West Virginia University

Morgantown, West Virginia

2004

Keywords: Feature level fusion, multimodal biometrics, biometrics, hand geometry, facial recognition

© Copyright 2004 by Rohin K. Govindarajan

All Rights Reserved

FEATURE LEVEL FUSION IN MULTIMODAL BIOMETRICS

Rohin K. Govindarajan

Abstract

Multimodal biometric systems utilize the evidence presented by multiple biometric modalities (e.g., face and fingerprint, multiple fingers of a user, multiple impressions of a single finger, etc.) in order to determine or verify the identity of an individual. Information from multiple sources can be consolidated in three distinct levels [1] : (i) feature set level; (ii) match score level; and (iii) decision level. While fusion at the match score and decision levels have been extensively studied in the literature, fusion at the feature level is a relatively understudied problem. A novel technique to perform fusion at the feature level by considering two biometric modalities - face and hand geometry, is presented in this paper. Also, a new distance metric conscripted as the Thresholded Absolute Distance (TAD) is used to help reinforce the system's robustness towards noise. Finally, two techniques are proposed to consolidate information available after match score fusion, with that obtained after feature set fusion. These techniques further enhance the performance of the multimodal biometric system and help find an approximate upper bound on its performance. Results indicate that the proposed techniques can lead to substantial improvement in multimodal matching abilities.

Acknowledgements

I am honored to be the first student graduating under my advisor Dr. Arun Abraham Ross. He is an exceptionally good teacher and a very motivated and spirited researcher. He has been my advisor, teacher, friend, philosopher and guide during the last one year. I wish to thank him profusely for taking the pain to spend long hours with me, discussing the concepts till I really got a firm grasp of them. I learnt from him the true meaning of hard work, sincerity and dedication. I will remain indebted to him, not only for making my masters a wonderful experience but also for the principles and values I gathered from him. Dr. Ross, thank you for everything!

My heartfelt thanks to Dr. Lawrence Hornak, for all the help, support and guidance he provided me in the last two years. He has played a very crucial role in making my masters a memorable experience. I have been deeply touched by his genuine care and concern towards his students.

I wish to thank Dr. Stephanie Schuckers and Dr. Bojan Cukic; for their unconditional support and valuable advice. I really enjoyed working with them.

My experience at the biomedical signal analysis lab was a wonderful one. I was fortunate to work with a number of extremely talented and highly motivated individuals. Our Research team was almost a family, sharing our happiness, helping each other during hard times, providing useful criticism and having fun. I wish to thank Sujan Parathasaradhi for all the support he gave me through my stay at the BIOSAL. I wish to thank Simona Crihalmeanu, Pisut Raphishak for their advice and help especially when I was working with Oracle and Matlab. I found good friends in Jidnya Shah and Sarvesh Maktal and spent some memorable moments in the lab with

them. I am grateful to them for carefully reading my thesis and helping me improve it with their suggestions. I will always remember Christopher Boyce, Reza Derakshani, Kelly Smith and Matthew Monaco for the fun we had together.

I wish to acknowledge the help and support provided by Dr. George Trapp, Dr. Ray Morehead, Mr. Grant Norman and Mr. Chris Randall during my tenure as a graduate assistant in the CSEE department.

Last but not the least, I wish to thank my family for their continued guidance and support.

It is to all these wonderful people that I dedicate this thesis to.

Contents

1	Biometrics	1
1.1	Introduction	1
1.2	Characteristics of a good biometric	4
1.3	Limitations of unimodal biometric systems	6
1.4	Multimodal biometrics	10
1.4.1	Introduction to multimodal biometrics	10
1.4.2	Decision Level Fusion	11
1.4.3	Match Score Level Fusion	12
1.4.4	Feature Level Fusion	13
1.5	Hand Geometry as a Biometric	15
1.5.1	Advantages	15
1.5.2	Disadvantages	17
1.6	Face as a biometric	17
1.6.1	Advantages	18
1.6.2	Disadvantages	19

2	Feature level fusion in biometrics	20
2.1	Introduction	20
2.2	Advantages and disadvantages of feature level fusion	22
2.3	Data preprocessing in feature level fusion	26
2.3.1	Dimensionality Reduction:	27
2.3.2	Feature Normalization:	33
2.4	Distance measures	39
2.5	Feature level fusion	47
3	Synthesizing information across fusion levels	53
3.1	Introduction	53
3.1.1	The selective feedback scheme	54
3.1.2	The exhaustive fusion schemes	57
4	Biometrics with group consensus	61
4.1	Introduction	61
4.2	Biometrics with group consensus	64
4.3	The different levels of fusion in a Multi-user biometric system	66
4.3.1	Feature level fusion	66
4.3.2	Match score level fusion	69
4.3.3	Decision level fusion	70
4.4	Modes of operation in a MUB system	71

4.4.1	Serial operation mode	72
4.4.2	Parallel operation mode	73
4.5	Experiments	75
4.5.1	Data preprocessing	75
4.5.2	Distance Measure	75
4.5.3	Preliminary Experiments	76
4.6	Multi-user multimodal biometrics	79
4.7	Conclusion & Future Work	80
4.8	Future work	81
5	Multimodal biometric Databases	83
5.1	Introduction	83
5.2	Multimodal biometric databases	85
5.2.1	Limitation of these existing multimodal biometric databases	87
5.3	System Description	87
5.3.1	System Features	88
5.4	Limitations	95
5.4.1	Data restricted to 2D information	96
5.4.2	Data Acquisition is driven by research requirements	97
6	Summary and future work	98

List of Figures

1.1	Some of the popular biometric modalities used for authentication.	2
1.2	A biometric system may be divided into 4 different logical modules viz., (a) The sensor module (b) The feature module (c) The match module (d) The decision module.	3
1.3	The flow of information in a multimodal biometric system.	10
1.4	Decision level fused multimodal biometric system.	12
1.5	Match level fused multimodal biometric system.	13
1.6	Feature level fused multimodal biometric system.	14
2.1	The flow of information in a feature level fused multimodal biometric system. . .	21
2.2	The performance of match level and feature level fusion using MSU hand and face data. The performance of feature level fusion is only as good as the weakest biometric.	23

2.3	The performance of match level and feature level fusion schemes using COTS hand and MSU face data. The performance of feature level fusion is much lower than that of match level fusion.	24
2.4	The incompatibility problem in feature level fusion; the fingerprint template is incompatible with that of face and hand geometry.	25
2.5	Performance of a face recognition system as a function of the number of features. The EER initially reduces with the number of features, reaches a minimum, and then starts increasing.	26
2.6	Forward selection on MSU Hand Geometry data.	32
2.7	Forward selection on MSU Face data.	33
2.8	Forward selection on COTS Hand data.	34
2.9	Forward selection on MSU Hand-Face feature level fused data.	35
2.10	Forward selection on COTS Hand and MSU Face feature level fused data.	36
2.11	The effect of minmax normalization on MSU Hand, MSU Face and COTS Hand.	37
2.12	The effect of MAD normalization on MSU Hand, MSU Face and COTS Hand.	39
2.13	The comparison of the performance of MSU hand geometry data without feature selection using Euclidean distance and TAD.	41
2.14	The comparison of the performance of MSU face geometry data without feature selection using Euclidean distance and TAD.	42
2.15	The comparison of the performance of MSU hand + MSU face FLF geometry data without feature selection using Euclidean distance and TAD.	43

2.16	The comparison of the performance of MSU hand + MSU face FLF geometry data with feature selection using Euclidean distance and TAD.	44
2.17	The genuine and imposter score distribution in a hand geometry system.	45
2.18	The reasons for error in a hand geometry system.	45
2.19	The reason for a bad genuine score is due to a small subset of features (highlighted) while an imposter score is due to the overall effect of all features. .	46
2.20	Feature level fusion in multimodal biometric systems.	48
2.21	Case I : Comparison of match level fusion and feature level fusion when consolidating information pertaining to weak classifiers.	49
2.22	Comparison of match level fusion as opposed to feature level fusion while consolidating information from a strong classifier and a weak classifier.	51
2.23	The effect of noise on feature level fusion and match level fusion.	52
3.1	The motivation for the selective feedback technique is the existence of the 'critical' region where a decision cannot be made with 100% certainty without the availability of some extra information.	55
3.2	This feedback technique works by employing match level fusion as the primary scheme and obtaining feedback from the feature fusion level when the score falls in the critical region.	56
3.3	The feedback technique results in approximately 5% improvement in the performance of the system across all thresholds.	57

3.4	The exhaustive fusion technique aims at high performance gain and hence is relatively more computationally complex than the feedback technique.	58
3.5	The exhaustive fusion technique results in up to approximately 10% improvement in the performance of the system across all thresholds.	59
3.6	The exhaustive fusion technique results in up to approximately 10-15% improvement in the performance of the system across all thresholds.	60
4.1	Usage of multiple keys to access a secure resource.	62
4.2	A multi-user biometric system is more secure than a conventional biometric system.	64
4.3	A multi-user approach which combines the biometric of two or more persons. . .	65
4.4	Feature level fusion in MUB systems.	68
4.5	Match score level fusion in MUB systems.	71
4.6	Decision level fusion in MUB systems.	72
4.7	Serial mode of operation in a MUB systems.	73
4.8	Parallel mode of operation in a MUB systems.	74
4.9	Final Data Collection Count	74
4.10	The feature level fusion outperforms match level fusion in MUB-2 hand systems constructed in the DISJOINT mode.	77
4.11	The feature level fusion outperforms match level fusion in MUB-2 face systems constructed in the DISJOINT mode.	78
4.12	The feature level fusion outperforms match level fusion in MUB-2 hand systems constructed in the OVERLAP mode.	79

4.13	The performance of feature level fusion is better than that of match level fusion in MUB-2 face systems constructed in the OVERLAP mode.	80
4.14	The performance of the MUB system increases as the number of people being fused increases, reaches a maximum and then starts to deteriorate.	81
5.1	An overall view of the dataflow to and from the database to be developed.	88
5.2	Data collected at different places are stored in one central repository, located in WVU.	89
5.3	The data acquisition and storage process.	90
5.4	The fingerprint liveness data that will be stored in the system.	92
5.5	Research on template aging is being greatly hampered due to the non-availability of sufficient data. This problem will be addressed in this data collection effort. . .	93
5.6	Data reuse is also a major advantage of this system. The data output of one research project can be used as input in another project.	94
5.7	An elaborate security mechanism will be developed to safeguard the sensitive biometric data.	96

List of Tables

1.1	A summary of different multimodal biometric systems [25] [26].	9
-----	--	---

Chapter 1

Biometrics

1.1 Introduction

Over the years, user authentication has become an inseparable part of all transactions involving human computer interaction. Most conventional modes of authentication are based on ‘what we know’ (e.g; passwords) and/or ‘what we have’ (e.g., ID Card). Biometrics brings in stronger authentication capabilities by adding a third factor - ‘what we are’ (based on our innate physiological or behavioral characteristics like fingerprint, iris, etc.) with the traditional components [11]. Reasonable cost of deployment, reduced size of sensors, increased accuracy of matching algorithms and the ease of use have now made biometrics a very attractive alternative in the field of security and information assurance [11] [12].

A biometric identifier or trait or attribute can be formally defined as a behavioral or a physiological characteristic of an individual, which can be used to authenticate his/her identity

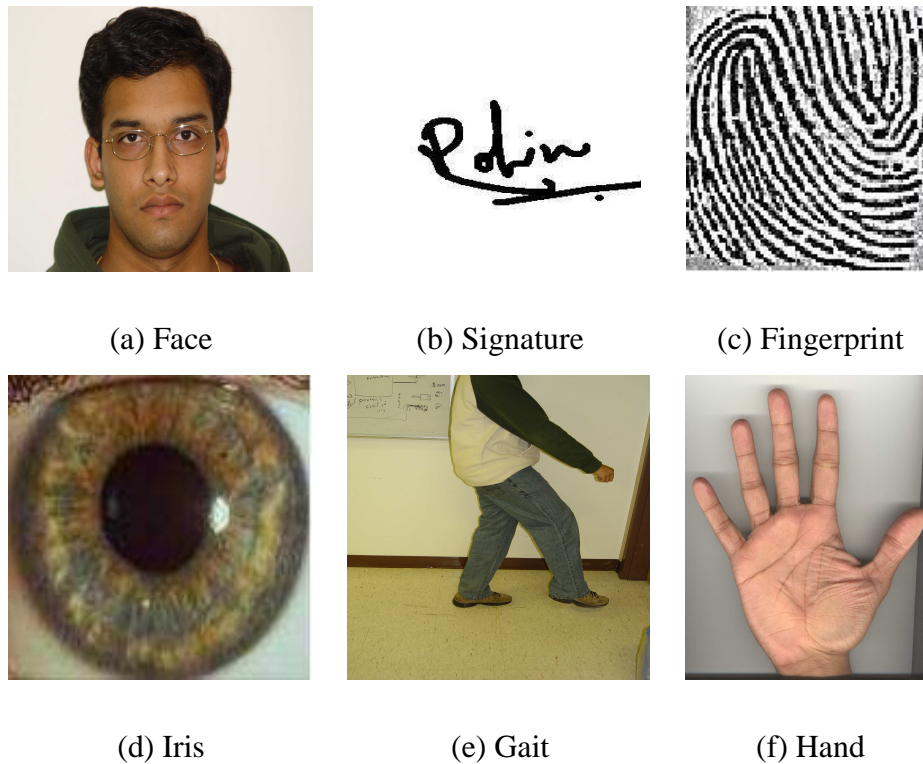


Figure 1.1: Some of the popular biometric modalities used for authentication.

with a certain degree of confidence. Biometric systems have been broadly classified into two categories depending on the number of biometric modalities required to perform authentication [11] [12]. These are:

1. **Unimodal biometric systems** : A unimodal biometric system is one that utilizes the information obtained from a single biometric trait in order to authenticate an individual.
2. **Multi-modal biometric systems**: A multimodal biometric (MB) system is one that utilizes information from multiple cues (multiple modalities or multiple processing techniques or both) to authenticate a user. This fusion of information can occur at the different logical modules (shown in Figure 1.2) of a biometric system.

Biometric systems that use multiple processing techniques on the same modality are often classified as being unimodal. Both unimodal and multimodal biometric systems are explained in detail in sections 1.3 and 1.4 of this chapter.

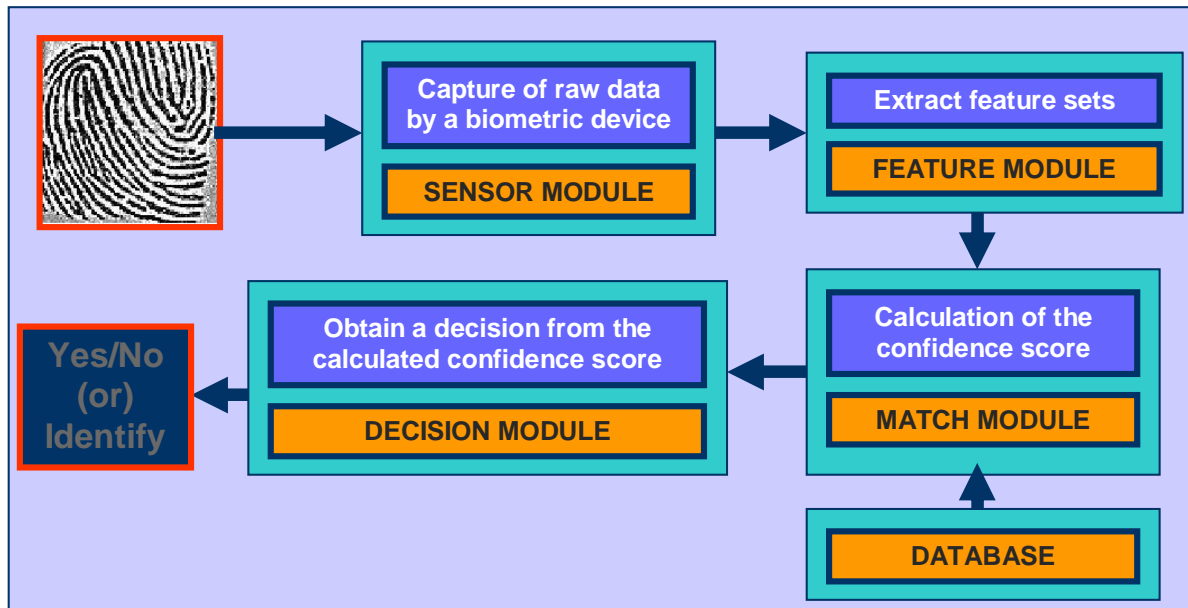


Figure 1.2: A biometric system may be divided into 4 different logical modules viz., (a) The sensor module (b) The feature module (c) The match module (d) The decision module.

It is essential to know and interpret the terminology used while describing a biometric system in order to understand this thesis better. Some of key words frequently used in this thesis are given below:

1. **Template/feature set:** The compact mathematical representation of a person's biometric information that is stored in a computer is called a template.

2. **Enrollment:** The process of capturing and storing the biometric information of a individual in order to authenticate them later is called as enrollment.
3. **Verification:** Verification means authenticating a users identity by comparing his biometric template with their own pre-stored biometric template (1 to 1 matching) captured during their enrollment into the system.
4. **Identification:** Identification would involve determining a persons identity by comparing his biometric template with all (1 to many matching) the templates in the database.
5. **Authentication:** The process of confirming, rejecting or establishing (both verification and identification) is commonly called as authentication.

1.2 Characteristics of a good biometric

Each biometric trait has its own advantages and drawbacks making it extremely good for certain applications, population groups or environmental conditions, and totally unsuitable for others. For example, iris recognition using infrared illumination might not work very well in poor illumination. Similarly fingerprints might not work when the perspiration content of the finger is high or when it is covered with dirt and grease. It is difficult to envision an 'ideal' biometric which does not have any drawbacks and hence works perfectly well under all possible conditions. The discussion in this section is intended to help us understand the drawbacks in current biometric systems and identify key areas in which improvements can be made. It will also help us understand the need to employ a multimodal biometric system as opposed to a unimodal one.

A few of the requirements that the above mentioned ‘ideal’ modality would need to satisfy are listed below [34]:

1. **Universality:** Every human must have the biometric trait, i.e. the biometric in consideration should be present in all users of the system and perform effectively in all population groups. For example, a fingerprint system might not perform well on a target population comprising of manual laborers because the ridge information necessary for fingerprint recognition may be damaged or affected. A hand geometry system may be more relevant in such a scenario.
2. **Uniqueness:** The attribute should not only be inseparable from the individual, but it should be unique across the target population.
3. **Permanence:** The biometric attribute under consideration must not change over time, i.e. it must be temporally invariant. The attribute should not be subject to significant differences based on age or altered due to a disease.
4. **Collectability:** It must be easy to acquire the biometric data. Extensive user cooperation should not be required. The biometric trait itself or its collection process should not intimidate the public. The system should be easy to interact with and have broad public acceptance.
5. **Tamper resistant:** The attribute should be difficult to manipulate and robust to spoofing attempts. The less reproducible the attribute, the more secure it is.

6. **Cost effectiveness:** The hardware and software needed to identify, collect and match the biometric should be inexpensive and easily available.
7. **Small template size:** The feature set extracted from the biometric trait should be small in size and, hence, easy to store and use.
8. **Small FRR and FAR:** The biometric system should have small False Reject Rates (FRR) and small False Accept Rates (FAR). FAR is defined as the frequency with which an imposter is incorrectly identified to be a valid enrolled user. FRR is the percentage of attempts when a genuine user is incorrectly rejected by the system as an impostor.

No single biometric system commercially available in the market today satisfies all the above criteria. It is safe to predict that it would be impossible to find a single biometric attribute which can satisfy all the above mentioned criteria. Therefore it would be instructive to combine one or more existing biometrics in order to create a 'good' and 'strong' biometric identifier. This fusion of the discriminatory information pertaining to different biometric cues constitutes the science of multimodal biometrics. The limitations of a unimodal biometric system are enumerated in the next section in order to better justify the need for a multimodal biometric system [13] [14].

1.3 Limitations of unimodal biometric systems

Biometric systems employing a single biometric modality for the purpose of identification or authentication are termed as unimodal biometric systems. Unimodal systems face many limitations while operating in real world conditions and are not as secure and infallible as they are

expected to be. A detailed discussion about these drawbacks would help us better understand the motivation behind multimodal biometrics. Some of the problems in unimodal biometric systems have been discussed by Ross and Jain [14] and are summarized below:

1. **Error rates and performance:** Every biometric modality has an upper bound on performance (or lower bound on its error rates) due to its inherent characteristics even when operating in a constrained environment. The performance of the system can only be as good as that of the biometric trait itself. The three main kinds of errors that are used to measure the performance of a biometric system are the False Accept Rate (FAR), False Reject Rate (FRR) and the Failure to acquire (FTA). It is very difficult to minimize all the three errors at the same time. An effort to reduce one error might increase the other.
2. **Noise in real world data:** Users working in coal mines or factories would tend to have bad fingerprints because their fingers are likely to have cuts and bruises. Factors such as these contribute to the noise in real world biometric data. Similarly an extra ring or a band-aid on a finger may be considered to be noise in a hand geometry system while background voices can contribute to noise in a speaker recognition system. These noises might result in a genuine user being rejected by the system. Such factors are many times ignored in tests conducted under laboratory conditions and, hence, the true performance of the biometric cannot be correctly assessed.
3. **Intra-class and inter-class variations:** An ideal biometric trait should exhibit significant variation between different users (inter-class variation) while exhibiting minimal variations during multiple presentations by the same user (intra-class variation). This is very difficult

to be realized using a single biometric modality due to inherent limitations and real world constraints like environmental conditions, user co-operation, etc. High performance biometrics like iris and retina recognition that have high inter-class and low intra-class variations may suffer from high failure to acquire (FTA) rates [35].

4. **Non-universality**:- The term ‘non-universality’ can be interpreted in two ways, (a) the failure of a biometric trait to be present in the entire user population, thereby preventing a subset of users from being enrolled and (b) the inability of a biometric system to work well under all environmental conditions or applications. In the first case it may be due to the absence of the biometric trait as a result of dismemberment or inferior quality of the trait that prevents it from being enrolled (e.g., it has been shown that approximately 4% of the fingerprints cannot be successfully enrolled). In the second case it could be due to the environmental conditions that prevent the system from capturing the biometric in a proper manner (e.g., face recognition system installed outdoors might fail if the weather is very foggy [36]).
5. **Spoofing**: It can be defined as intentionally cheating the system in order to make it accept an artificially prepared biometric as a true biometric. For example, video recordings of a user’s face can be played on a laptop and presented before a facial recognition camera; iris images of very high quality (2400 x 1200) may be used to fool an iris camera; artificial fingerprints can be made using gelatin, playdoh, etc [36].

One of the obvious solution to the problems enumerated above, is the use of multiple biometric traits in order to authenticate a claimed identity or perform identification. Such systems

Author & Year	Biometric Modalities	Level of fusion
A. Kumar and D. Zhang 2003 [25]	Face, Palm	match score
A. Kumar, et al. 2003 [24]	Palm, Hand	match score, feature level
Y. Wang, et al. 2003 [15]	Face, Iris	match score
K. Chang, et al. 2003 [16]	Face, Ear	feature level
G. Shakhnarovich and T. Darrell 2002 [17]	Face, Gait	match score
A. Ross and A. Jain 2001 [1]	Face, Hand, Finger	match score
R. Frischholz and U. Dieckmann 2000 [18]	Face, Voice, Lip	match score
S. Ben-Yacoub 1999 [19]	Face, Voice	match score
L. Hong and A. Jain 1998 [20]	Face, Finger	match score
E. Bigun, et al. 1997 [21]	Face, Voice	match score
J. Kittler, et al. 1997 [22]	Face, Voice	match score
R. Brunelli and D. Falavigna 1995 [23]	Face, Voice	match score

Table 1.1: A summary of different multimodal biometric systems [25] [26].

are called as multimodal biometric systems. A multimodal biometric system is also able to meet the stringent performance needs in commercial applications while also providing better performance and lower error rates [13] [14]. Some of the multimodal biometric systems discussed in the literature have been summarized in Table 1.1.

1.4 Multimodal biometrics

1.4.1 Introduction to multimodal biometrics

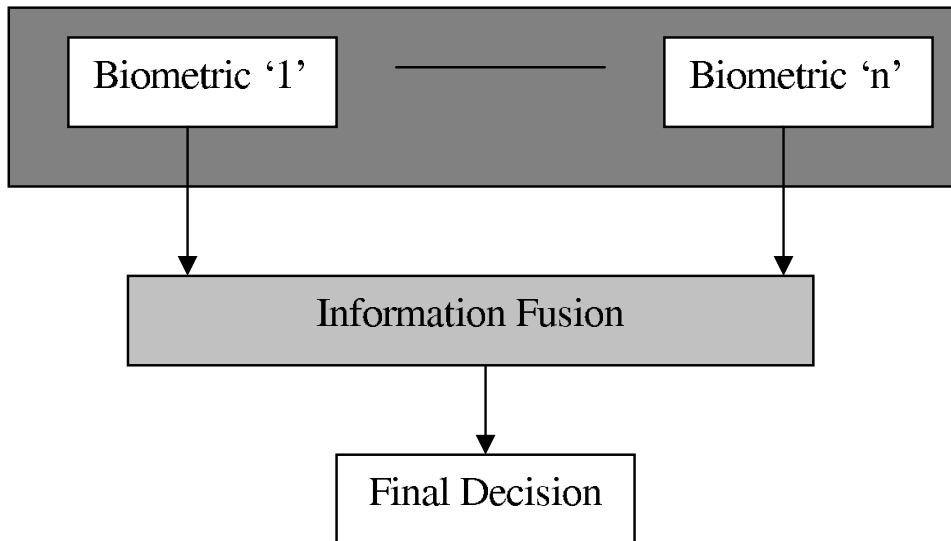


Figure 1.3: The flow of information in a multimodal biometric system.

When the evidence required for performing authentication is derived from two or more biometric traits, or from independent decisions or scores resulting from processing a single biometric trait in multiple ways, then such a system is called a multimodal biometric system. Hence the term multimodal biometrics has a very broad meaning and can be interpreted in numerous ways depending on the source of the cues used for authentication. Hong, Jain and Pankanti [27] have shown that multimodal biometric systems have better accuracy and reliability than single biometric systems while compromising on time for authentication, storage space and extra hardware/software. Integrating the classification abilities of multiple biometric modalities can surpass the upper bounds on performance imposed by a unimodal system. The probability

of multiple biometric modalities being affected by noise or getting spoofed simultaneously is considerably less compared to a unimodal biometric system. Similarly the probability of a person experiencing the FTE (Failure to Enroll) / FTA (Failure to Accept) problem in all available biometrics is relatively small. The fusion of multiple pieces of evidence in a multimodal biometric system can occur at various levels viz., the decision module level, match score level and the feature set level [1]. Each technique has its own advantages and drawbacks as explained in the subsequent subsections.

1.4.2 Decision Level Fusion

Decision level fusion in multimodal biometric systems would involve integrating the results emerging from the decision modules of each constituent modality. A number of methods like majority voting [28], behavior knowledge space [29], and weighted voting based on Dempster-Shafer theory of evidence [30] can be used in order to converge on a final decision. This level of fusion is the simplest to implement of all the three available methods. But unfortunately this method of fusion suffers from several problems. The different component biometric systems would be very loosely coupled as they are connected at the highest (decision) layer. This makes the system very rigid and, hence, in most cases does not provide a substantial increase in performance [1].

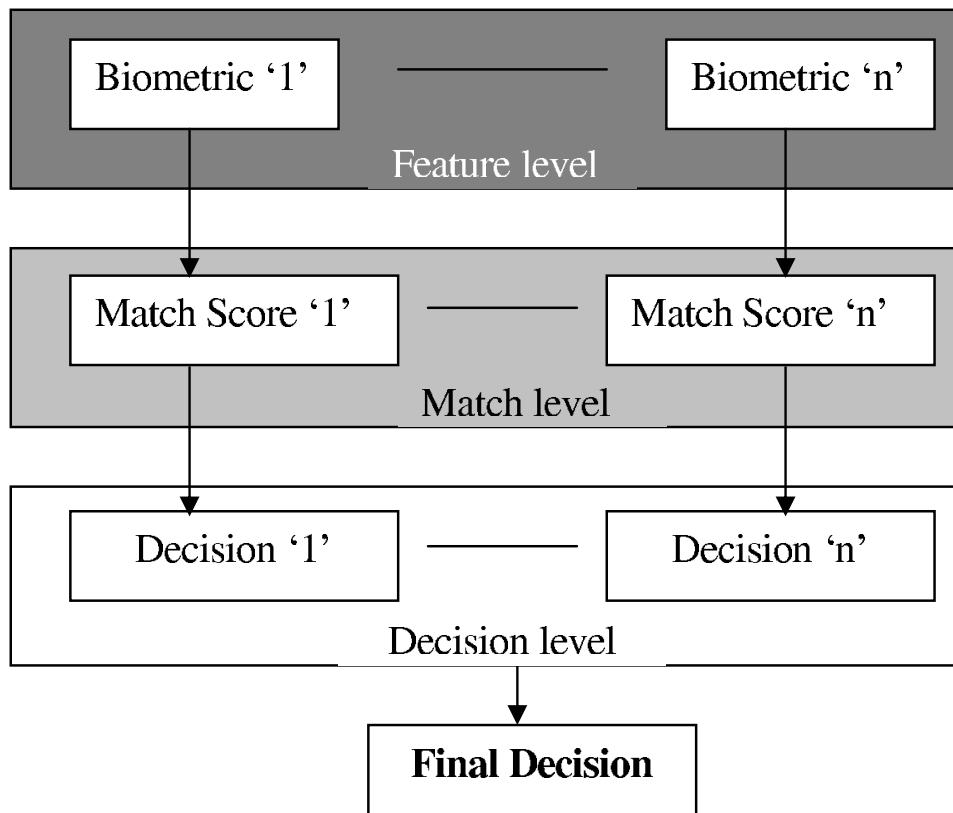


Figure 1.4: Decision level fused multimodal biometric system.

1.4.3 Match Score Level Fusion

This method of fusion involves the integration of the system at the match score level. This process would involve the integration of the different match scores generated from each of the component biometric modalities resulting in one consolidated match score. This match score is then used by the decision module. This system is moderately flexible and also fairly simple to implement. The match score can be consolidated in numerous ways like the max rule, min rule, sum rule, mean rule, median rule, etc [22]. The best rule suited for an application would be decided based on component biometric modalities and the environmental conditions under which they are required

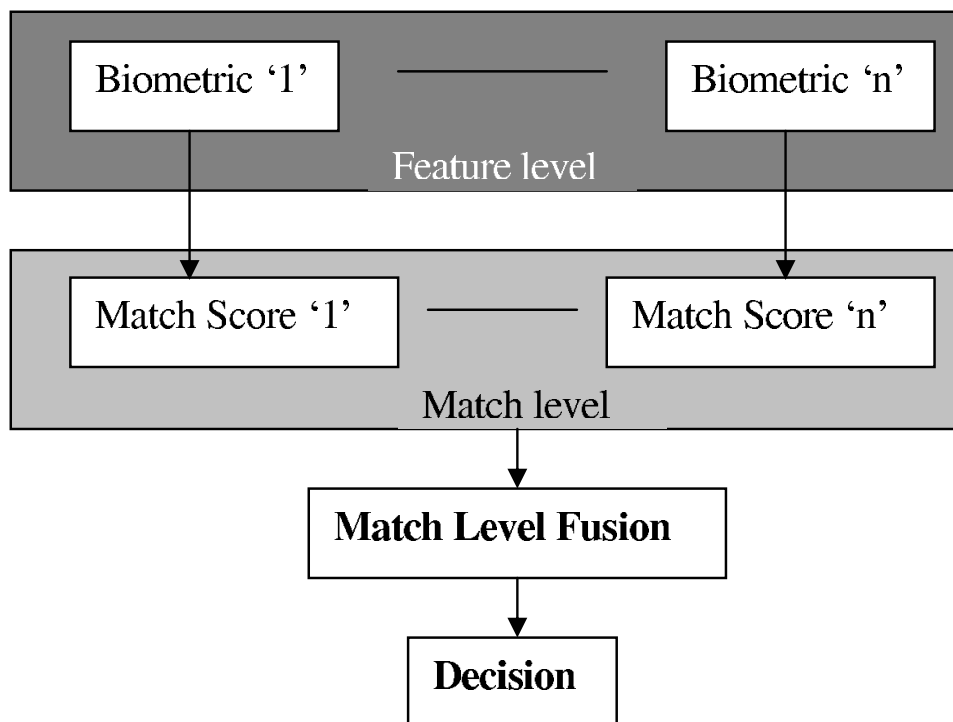


Figure 1.5: Match level fused multimodal biometric system.

to operate.

1.4.4 Feature Level Fusion

In this type of biometric fusion, the feature sets of each biometric trait are generated separately, and then fused together to produce a single multimodal biometric template. This template is then used as the input to the matcher to generate match scores, which is then fed to the decision making module. This is expected to be the best type of fusion because the feature sets constitute the richest source of information.

This thesis involves a detailed study of the fusion of biometrics (Hand and Face) at the feature

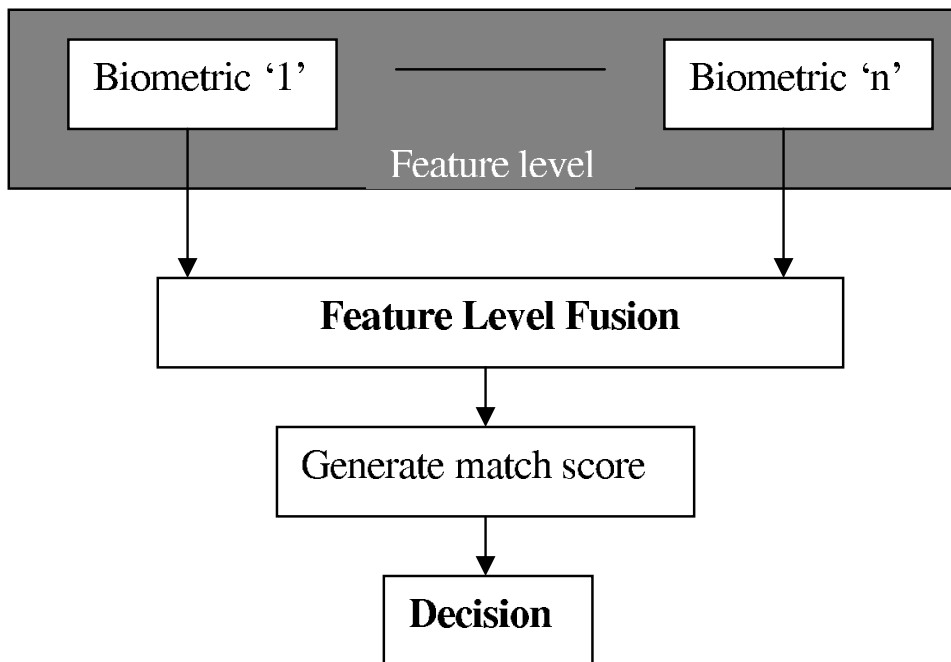


Figure 1.6: Feature level fused multimodal biometric system.

set level in contrast to the popular fusion schemes at the decision level and the match score level. It also involves an examination of various data normalization schemes and feature selection algorithms in order to optimize feature fusion. Further, techniques to perform multiuser fusion is studied for joint authentication in high security applications. The experiments pertaining to fusion conducted in this thesis are performed on the hand and face biometric data sets. The new algorithms developed in this thesis for comparing feature-fused templates are based on certain inherent characteristics of the data sets. Therefore, it is imperative to have a good understanding of their key characteristics, in order to better interpret the results presented in the subsequent chapters.

1.5 Hand Geometry as a Biometric

Hand geometry is one of the oldest biometrics and has been in commercial use for last two decades. It utilizes the geometric and physical characteristics of the hand for establishing identity (e.g., length of the fingers, width of the fingers, width of the palm, thickness of the hand etc.). Even though individual hand features have been found insufficient for identification, a collection of features can be reliably used for the verification of an individual's identity. Over the years this biometric has been carefully researched and refined. Apart from its various advantages, there exist some inherent disadvantages, due to the very nature of this biometric that cannot be overcome. The advantages and disadvantages of the biometric are discussed in detail below [11].

1.5.1 Advantages

1. Hand geometry recognition, along with fingerprint recognition has been around for a very long time and proven to be an extremely reliable technology.
2. It is been widely accepted to be one of the easiest to use and administer amongst all the biometric technologies that are commercially available today.
3. It has a very high user acceptance rate and user confidence compared with other invasive biometrics. This is very important in mass applications like the US-VISIT program (Immigration and border control applications), where other invasive biometrics (e.g., iris) may not be applicable.

4. Hand geometry recognition has worked in the most difficult environments, both indoor and outdoor [37]. In the case of an indoor environment, it has proved to be resistant to a fair amount of rough usage from end users, especially in large factory, warehouse, and retail settings. In the case of an outdoor environment, the technology has worked well in the most extreme of atmospheric climates, ranging from very hot to very cold (provided that certain modifications are done to the device in-order to adapt it to that particular environment).
5. The hand geometry is a very stable and reliable biometric because its physical characteristics, after a certain age, are invariant over time (except for conditions resulting from disease or accidents).
6. Hand geometry can be easily coupled with other biometric traits to produce better performing multimodal biometric systems.
7. The amount of data required to uniquely identify an individual using hand geometry is relatively small thus enabling it to be stored in smart cards.
8. Hand Geometry is also quite resistant to spoofing. The time and effort required to sufficiently spoof a person's hand is generally too great, especially when used in the verification mode. There has also been some liveness detection (spoofing countermeasures) designed for the hand geometry system. For example, pulse oximetry, where the oxygen content in the blood flowing through a persons hand is measured to determine liveness [38].

1.5.2 Disadvantages

1. The features that are identified from a human hand are only moderately unique. Therefore this restricts the usage of this technology only for verification purposes and cannot be used for identification. Therefore hand geometry is termed to be a ‘weak’ biometric, which in turn prevents its usage in high security applications. Other biometrics like fingerprint, iris etc. are termed to be ‘strong’ biometrics.
2. The size of a hand geometry system is considerably larger than that of most other biometric devices.
3. If the number of features recorded are less and if the population enrolled is large then there is a possibility of duplication.
4. The liveness detection measures are still mostly in their developmental stages and require considerable extra hardware.

Two different hand geometry data sets were used in this thesis. They are explained in detail in chapter 2.

1.6 Face as a biometric

The development of automatic facial recognition systems began in the late 80’s and commercial systems were made available in the 90’s. Currently this technology is receiving significant public attention as a tool for averting terrorist attacks and as a consequence, facial recognition has been

put to use in many law enforcement applications. Software has also been developed for other applications like computer networks and automated bank tellers that use this technology for user verification purposes. Facial recognition identifies and analyzes the characteristics of a human's facial images input with the help of a video camera. It measures various parameters of the face like the overall facial structure, distance between eyes, nose, mouth, and jaw edges. It has so far has not been very successful in large-population usage. Therefore it is currently used in verification-only systems with considerable success. The user is required to stand about two feet from the camera. The system will first locate the user's face and then perform matches against the claimed identity. The system usually comes to a decision in 3-5 seconds. Facial recognition, like other biometrics, has many advantages and drawbacks. These are discussed in detail below:

1.6.1 Advantages

1. The strongest point in favor of facial recognition is that it is non-intrusive.
2. It does not require any extensive co-operation from the user (except to stand fairly near and look in the general direction of the camera).
3. There are fairly large conventional databases of human faces (e.g.: DMV records, identity cards etc.) which can also be used for facial recognition.
4. It has fairly good user acceptance.
5. It can be considered to be a relatively 'strong' biometric provided a good quality image is obtained during enrollment.

6. It can easily be coupled with other biometrics to be a part of a multimodal biometric system.

1.6.2 Disadvantages

1. The facial recognition systems are easily affected due change in light, background and various other cosmetic changes to the face.
2. The human face is not time invariant unlike other biometrics like fingerprint and iris.
3. Facial recognition always needs extra hardware like lamps for lighting, uniform background etc.
4. Even though the hardware required for facial recognition is cheap, the software part can be expensive.
5. The non-intrusiveness is one of its drawbacks when it comes to the opinion of the public. People express concern over the use of facial recognition cameras to inconspicuously track people without their knowledge or consent.
6. Since a lot of privacy issues and human sentiments are related to the face, it may be susceptible to privacy rights concerns.
7. In the past it has been possible to spoof a facial recognition system using pictures, live video show with a laptop etc.

Chapter 2

Feature level fusion in biometrics

2.1 Introduction

Fusion at the feature level involves consolidating the information content of multiple feature sets pertaining to different biometric modalities into one single feature vector [1]. The resultant feature vector is then used by the matcher in order to determine the confidence score required to make the final decision. The flow of information in such a multimodal system is as shown in Figure 2.1. The information obtained from the multiple sources of a multimodal biometric system can be consolidated at three distinct levels [1] [2]: (i) feature extraction level; (ii) match score level; and (iii) decision level. While fusion at the match score and decision levels have been extensively studied in the literature, fusion at the feature level is a relatively understudied problem. In this thesis a novel technique to perform fusion at the feature level is used. Results indicate that the proposed technique can lead to substantial improvement in multimodal matching

performance especially when combining weak classifiers.

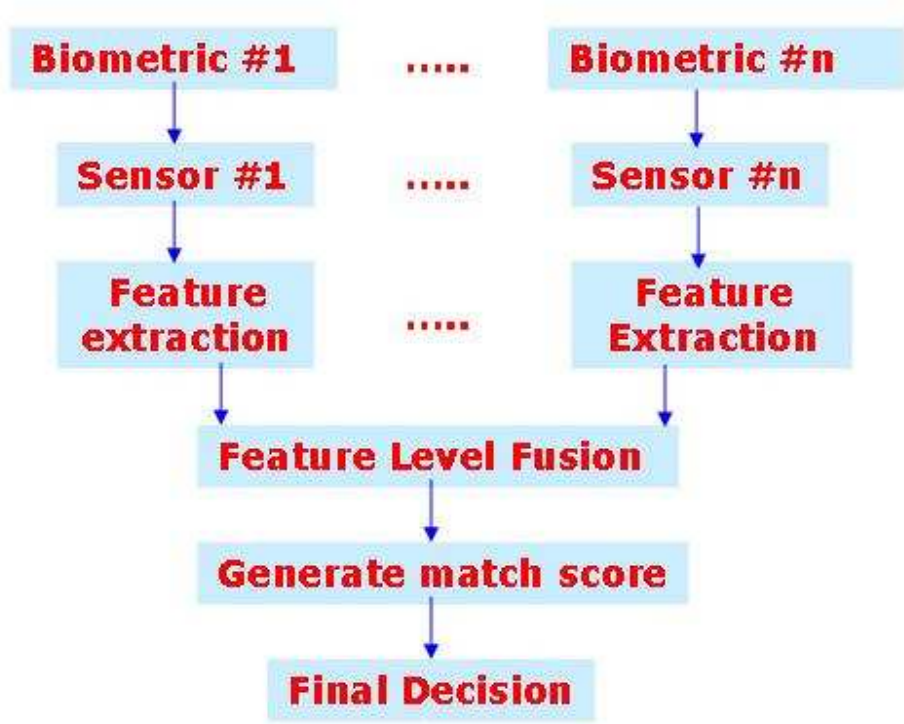


Figure 2.1: The flow of information in a feature level fused multimodal biometric system.

A brief description of the different hand and face data sets used in the experiments conducted in this thesis is given below.

1. Hand Geometry MSU-Database: This database comprises of the hand (right) images of 50 users, (5 samples per user) captured using a Pulnix TMC-7EX camera at Michigan State University [5] [1]. The feature set consists of 14 feature values comprising of the lengths of the fingers, widths of the fingers, and width of the palm at different locations of the hand [5].

2. Hand Geometry COTS Database: This database consists of hand (right) images corresponding to 50 users with 5 samples per user, obtained from a commercial off the shelf (COTS) hand geometry system installed at West Virginia University, Morgantown. The feature set consists of 9 features corresponding to different measurements of the hand image.
3. Face Database: Facial images corresponding to 50 users, 5 samples per user were obtained using a Panasonic CCD camera at Michigan State University [1]. The eigenface approach was used to extract 128 features from the images [6]. In our experiments only 25 of these were considered.

Each database corresponds to a different set of users collected separately. We have assumed the mutual independence between the hand and face modalities and, hence, have created a virtual multimodal biometric data set by augmenting the two unimodal data sets.

2.2 Advantages and disadvantages of feature level fusion

The feature set used to represent raw data is the richest source of biometric information. This may be attributed to the fact that there is a loss of information associated with every subsequent step in the hierarchy of a biometric system, i.e., in the match and decision levels, respectively. Therefore, in theory, feature level fusion is expected to perform better than fusion at the other levels. Unfortunately, this may not be true in practice as this technique is prone to several errors during its implementation. It can be seen in the results obtained in Figure 2.2, 2.3 that match

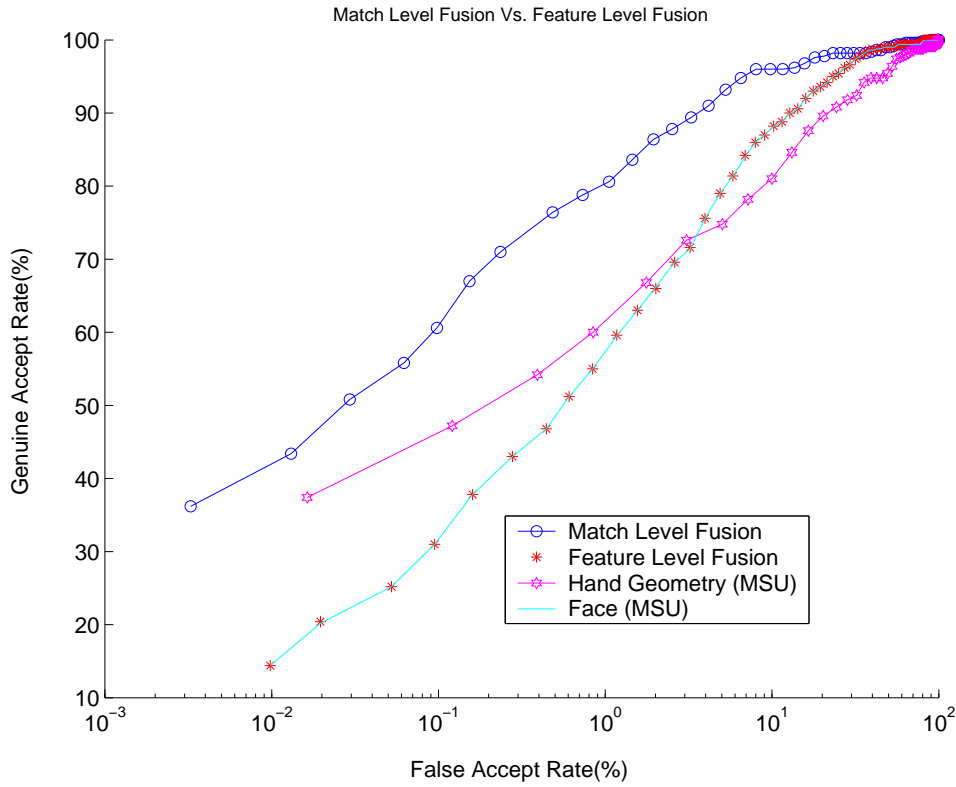


Figure 2.2: The performance of match level and feature level fusion using MSU hand and face data. The performance of feature level fusion is only as good as the weakest biometric.

level fusion performs much better than feature level fusion. Here, in both cases feature fusion has been accomplished by merely concatenating the component feature vectors. Feature fusion performs only as good as the weakest modality, contrary to our expectations. The problems listed below are typically the reasons for the observed deterioration in performance and, hence, feature level fusion has been avoided by most multimodal systems studied in the literature.

1. The feature vectors pertaining to the different modalities may exist in different domains and, therefore incompatible. For example, minutiae set of fingerprints and the eigen

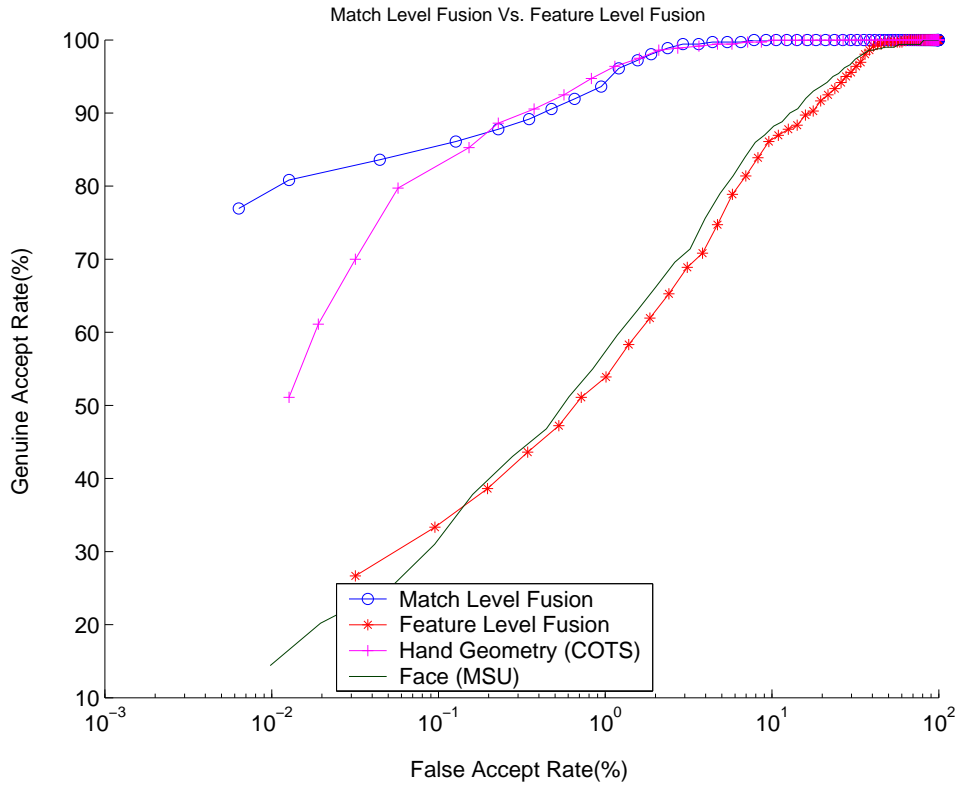
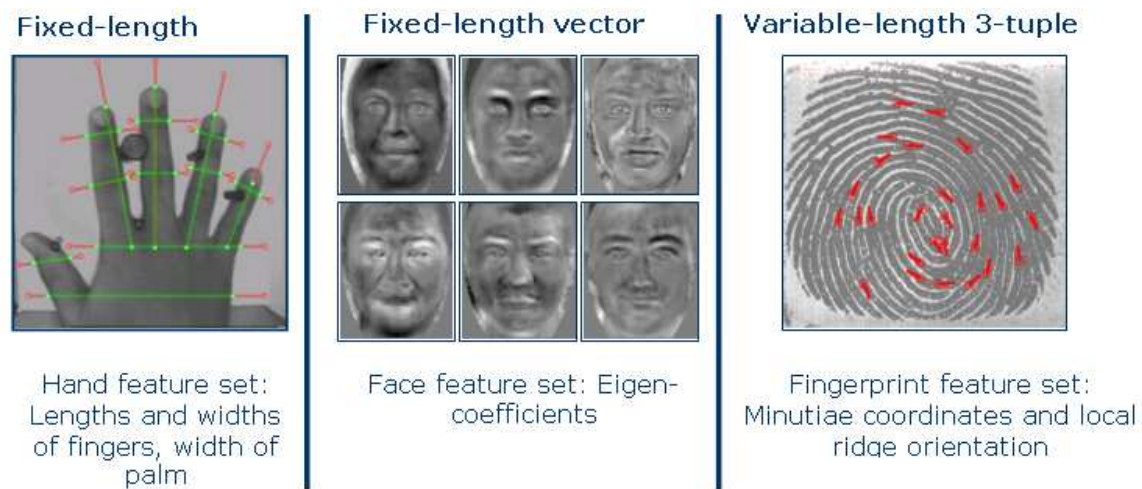


Figure 2.3: The performance of match level and feature level fusion schemes using COTS hand and MSU face data. The performance of feature level fusion is much lower than that of match level fusion.

coefficients of face as shown in Figure 2.4.

2. The relationship between the feature spaces of different modalities may not be known even after transformation is performed. For example, it can be observed that the hand and face vectors (Figure 2.4) exist in the same domain but in different numerical ranges.
3. When two or more feature vectors are concatenated, the dimensionality of the resulting feature vector becomes very large. Such high dimensional feature sets tend to be noisy

**Hand Feature Set (14 Features)**

67	60	67	58	68	55	53
50	261	335	253	286	242	122

The first 18 eigen coefficients of the face feature set

-315.91	-441.1	212.35	-90.78	-840.12	434.74	1077.58	-389.12	428.34
-95.56	382.71	416.84	105.61	-1162.25	174.63	113.68	-334.55	-846.01

Figure 2.4: The incompatibility problem in feature level fusion; the fingerprint template is incompatible with that of face and hand geometry.

requiring the need for feature reduction in order to separate the discriminatory features from the noisy ones.

4. Score generation is complex even in the case of a unimodal biometric system i.e. it is difficult to find a good classifier. Therefore, this task becomes even more arduous while working with the concatenated feature vectors.

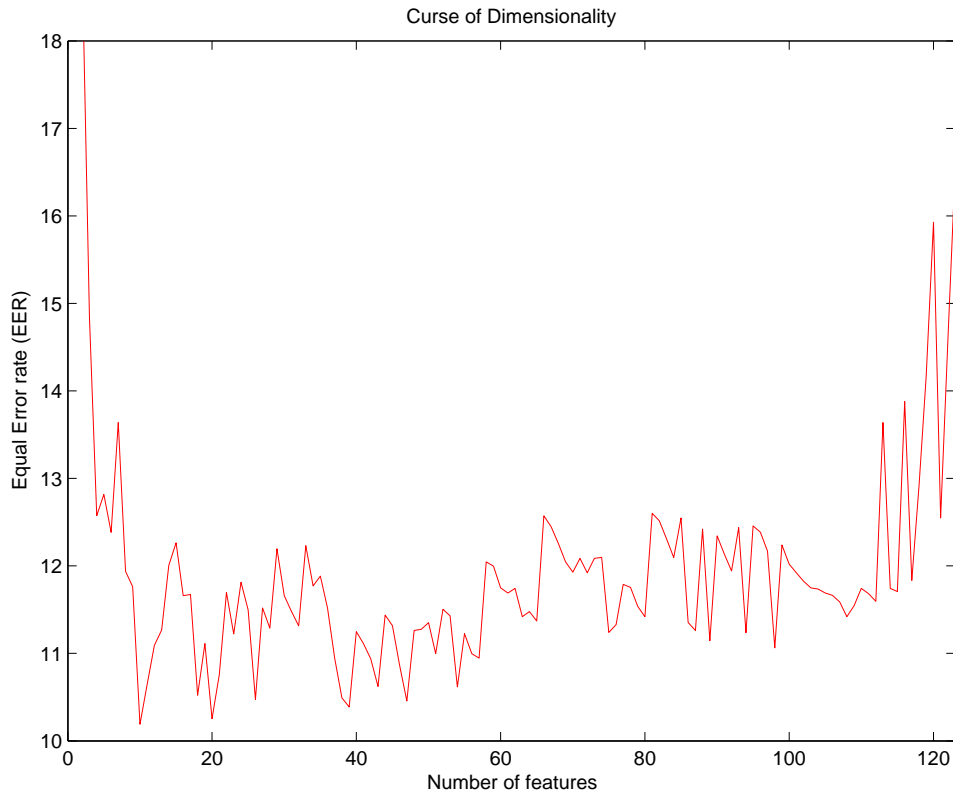


Figure 2.5: Performance of a face recognition system as a function of the number of features. The EER initially reduces with the number of features, reaches a minimum, and then starts increasing.

The next section helps identify the ways to overcome these disadvantages and make feature level fusion a viable technique.

2.3 Data preprocessing in feature level fusion

Data preprocessing is very critical in order to help overcome the above cited disadvantages and achieve optimal performance in a feature level fused biometric systems. This section explains

in detail, the techniques of dimensionality reduction and feature normalization as a means to overcome some of these problems.

2.3.1 Dimensionality Reduction:

The ‘curse of dimensionality’ along with the reduction of computational and measurement cost is the primary motivation behind dimensionality reduction [7]. This process needs to be performed in a very careful manner as an excessive reduction in the number of features may result in the loss of discrimination capability of the feature set and, hence, reduce the accuracy of the system. Watanabe’s ugly duckling theorem [8] also emphasizes the importance of selecting the right set of uncorrelated and discriminative features, as it is possible to incorrectly classify two different patterns as belonging to the same class if their feature sets have a sufficiently large number of redundant features. There are two different ways in which dimensionality reduction is achieved: feature extraction and feature selection.

2.3.1.1 Feature extraction:

Feature extraction is the process in which a new subspace of dimension m is identified from the original space of dimension ‘ n ’ in a linear or a non-linear fashion. It is done using methods like Principal Component Analysis (PCA), Linear Discriminant Analysis (LDA) and Multidimensional Scaling (MDS) that reduce the dimensions of the feature space from ‘ n ’ to ‘ m ’ where $m < n$ [9]. PCA works by considering the entire feature data together and transforming it to a subspace which has maximum variance along the component axis [6]. LDA performs

the same task but tries to maximize the ratio of the between-class variations to the within-class variations [39]. MDS finds the data points in lower dimensional space that best preserves the inter-point distance [40].

In the experiments conducted in this thesis, the face feature set was based on the PCA technique [6]. The hand geometry feature set was subjected to PCA, but did not result in any significant reduction in error rates. This might be because the hand feature set already exists in an optimal space and there is no other subspace where it has considerable more spread than the existing one.

2.3.1.2 Feature Selection:

The performance of a pattern recognition system is expected to increase with the number of features extracted. However, in reality, it reaches a maximum and then starts to degrade. This paradoxical behavior is called as the ‘peaking phenomenon’ or as the ‘curse of dimensionality’ [3]. This occurs when the number of training examples that are used to design the classifier is small relative to the number of features in consideration. In many commonly used parametric classifiers where the class conditional densities have to be determined, the unknown parameters are first estimated and then plugged in instead of the true ones. This leads to errors in classification if the model that is chosen is incorrect. Therefore for a fixed sample size, an increase in the number of features/parameters leads to a proportional increase in the number of unknown parameters to be estimated, resulting in the increased error. This problem may be partially solved by using large, representative training data sets which might help in making more

reliable estimations. The number of samples required to achieve generalization must be directly proportional to the dimensionality of the feature space. In the field of pattern recognition, it is generally accepted that there should be at least ten times as many training samples per class as the number of features. If the complexity of the classifier increases then this ratio should also change. The curse of dimensionality, along with the expenditure involved in measuring and including features, underscores the advantages of getting a minimal feature set that allows a classifier to discern pattern classes well. This minimal set of features containing maximum discriminatory information can be realized by the technique of feature selection. The purpose of performing feature selection on a data set is to reduce the search space (for attributes), by selecting only relevant features and eliminating the noisy ones. This would involve selecting 'm' features from the entire set of 'n' features such that $m \leq n$. Ideally, it should be $m \ll n$ [7] [9].

2.3.1.2.1 Feature selection techniques: The techniques for feature selection can be broadly classified into 3 different types. Some of the popular techniques used are as listed below:

1. Exhaustive search techniques:

- Simple exhaustive search [7]
- Branch and bound [41]
- Beam search [42]

2. Sequential search techniques:

- Sequential forward search (SFS) [4] [43]

- Sequential backward search (SBS) [4] [43]
- Plus-l-minus-r method [4] [43]
- Sequential forward floating selection (SFFS) [4] [43]
- Sequential backward floating selection (SBFS) [4] [43]

3. Stochastic techniques:

- Simulated annealing [45]
- Genetic Algorithm [44]

Every feature selection technique has its advantages and drawbacks, and is selected depending on the data set on which feature selection has to be performed. Techniques like SFS exhibit some serious drawbacks in the sense that, once the features have been selected then they cannot be discarded; analogously, in SBS, once the features are discarded, they cannot be re-selected. This results in a nesting effect, leading to a sub optimal solution, because this tends to find the local minima (with respect to error rates) instead of finding the global minima . The plus-l-minus-r technique is a complex sequential search technique introduced in-order to overcome the problems posed by SFS and SBS. The main limitation of this technique is that there is no well-defined criterion to select the values of 'l' and 'r'. SFFS and SBFS are also search techniques which were introduced to improve on the performance of SFS and SBS. They are superior than plus-l-minus-r because they dynamically change the number of features in each step and therefore allow the reconsideration of the features included or removed in the previous steps. They also do not require any parameters to be selected unlike the l-r technique. Genetic

algorithms (GA) perform well (even better than SFFS and SFBS) for medium size problems and for problems where classical methods fail or are not applicable. In virtue of the inherent randomization mechanism in searching, GA's can perform search in the near optimal region of space and can even be hybridized with the sequential methods to get the best of both techniques [4].

2.3.1.2.2 Criteria for feature selection: Feature selection is performed on a data set in order to maximize or minimize a particular criterion function. In the case of a biometric system, this becomes a very difficult task because the performance has to be measured across a range of FAR/GAR values. Therefore, the performance of the biometric systems is generally depicted as Receiver Operating Characteristic (ROC) curve or a Detection Error Trade-off (DET) curves. The only single value measure used is the Equal Error Rate (EER) [10]. EER is defined as the point in the ROC curve where the False Accept Rate (FAR) and the False Reject Rate (FRR) are the same. It is not a very efficient measure, as it typically tends to influence the performance only in the regions of lower thresholds while ignoring higher thresholds. This has been demonstrated in Figures 2.6, 2.7, 2.8, 2.9 which depict the results of feature selection experiments performed using EER as the criterion function. The features selected try to maximize the EER and hence only improve the performance at the lower thresholds. It can be observed that there is an obvious decrease in performance for both face and hand geometry data in the regions of higher thresholds. An alternative would be to perform feature selection on other criterions like the GAR and the FAR. But unfortunately this also results in maximizing the performance at select thresholds. In order to maximize the performance gain across a wide range of thresholds, we define the criterion

function to be the average of GAR at 4 different FAR's (0.05%,0.1%,1%,10%). The ROC curves in Figures 2.6, 2.7, 2.8, 2.9, 2.10 show the reliability of this criterion. Therefore, this new measure has been used as the criterion function for feature selection in this thesis.

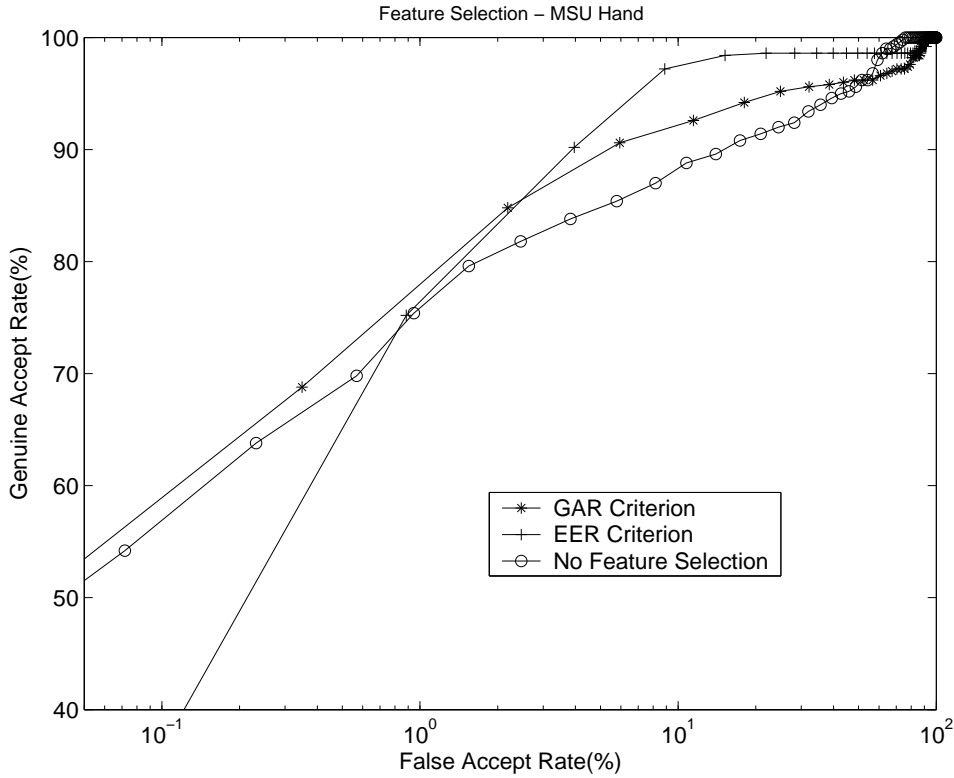


Figure 2.6: Forward selection on MSU Hand Geometry data.

It can be observed from Figures 2.9 and 2.10 that the feature level fusion without feature selection results in inferior performance. It is also demonstrated that feature level fusion helps in improving the performance between 20-40% depending on the threshold. Therefore, it may be implied that feature selection (dimensionality reduction) is mandatory in feature fusion schemes, especially in schemes that employ concatenation.

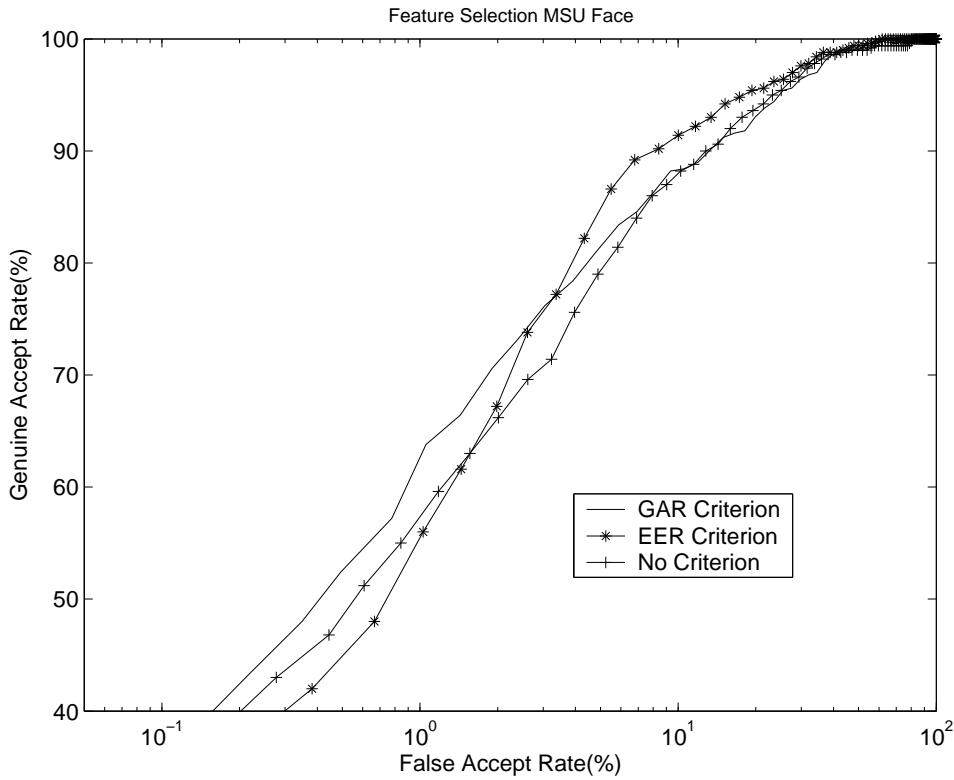


Figure 2.7: Forward selection on MSU Face data.

2.3.2 Feature Normalization:

Feature normalization is a technique utilized in feature fused multimodal biometric system in order to achieve two different goals. The primary motivation behind this technique is to ensure that the contribution of each feature value (pertaining to the individual biometric modalities represented in the joint feature vector) to the final match score is similar. It works by modifying the location and scale parameters of the features values in each of the component feature sets such that the contribution of each of the modalities to the final feature set is comparable. Jain, Karthik and Ross [2] have used different normalization techniques for integrating match scores.

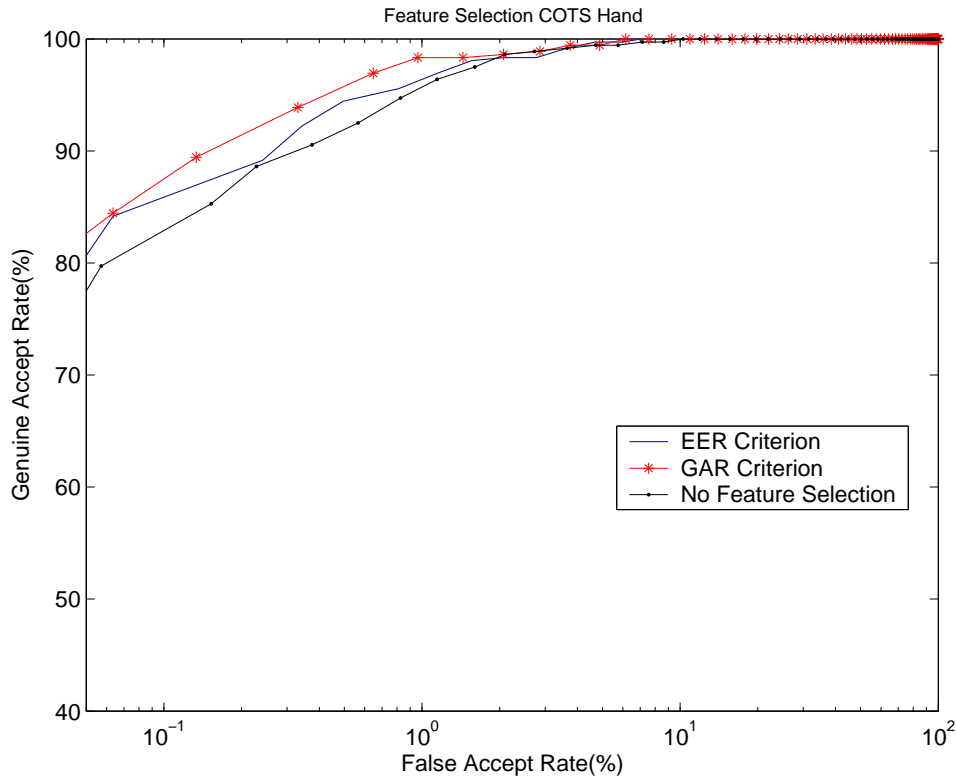


Figure 2.8: Forward selection on COTS Hand data.

They have used the ‘robustness’ and ‘efficiency’ measures to determine the suitability of each normalization scheme. There are a number of techniques to perform feature normalization. A few of the most suitable and popular techniques are enumerated below. While it is difficult to single out a particular technique to be superior compared to the other techniques, it is possible to identify a small subset of techniques as the ‘most suitable ones’ depending on the amount of *apriori* information available.

1. Min-max normalization:

The min-max normalization scheme is one of the simplest normalization schemes available.

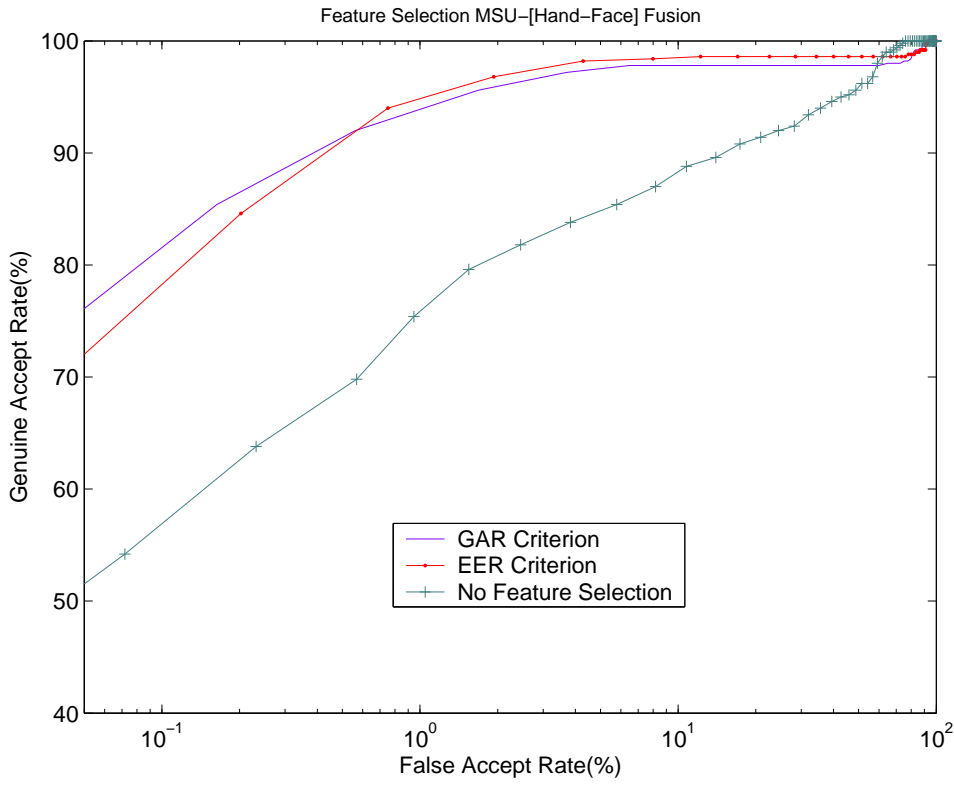


Figure 2.9: Forward selection on MSU Hand-Face feature level fused data.

This is effective when the minimum and the maximum values of the component feature values are known beforehand. In cases where such information is not available, an estimate of these parameters need to be obtained from the available sample training data. The estimate may be affected by the presence of outliers in the training data and hence makes minmax normalization sensitive to outliers . The results obtained for this technique indicate that it gives a marginal improvement for MSU hand geometry and no improvement for face and a decrease in performance for COTS hand data (Figure 2.11).

$$x'_{ij} = \frac{x_{ij} - \min_k(x_{ik})}{\max_k(x_{ik}) - \min_k(x_{ik})}$$

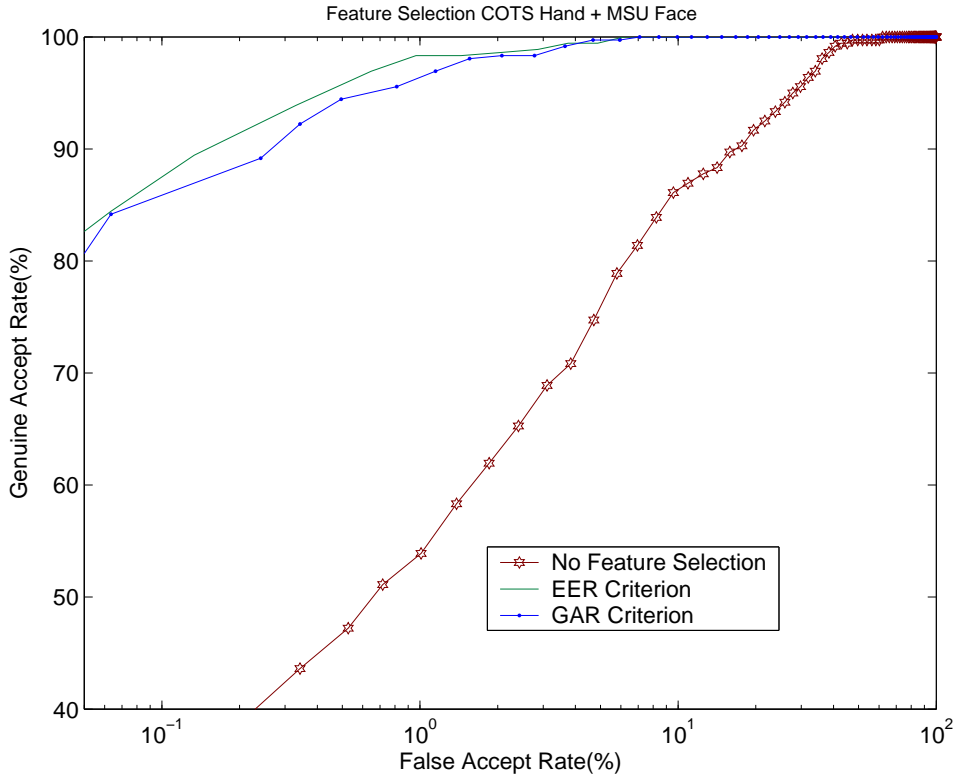


Figure 2.10: Forward selection on COTS Hand and MSU Face feature level fused data.

Here $\mathbf{X}_i = (x_{i1}, x_{i2}, \dots, x_{ij}, \dots, x_{in})$, x'_i is the normalized feature value obtained after applying min-max normalization on every feature x_{ij} over 'k' users. Here $\min_k(x_{ik})$ and $\max_k(x_{ik})$ refer to the known or the estimated min and max value that the feature in consideration can take. The hand geometry data should respond better to other techniques like MAD (described in the next subsection) as it has many outliers (missing values) in it.

2. Median Absolute Deviation (MAD) normalization:

The median and the Median Absolute Deviation (MAD) values are typically not influenced by the presence outliers in the training data. Hence the MAD normalization scheme is

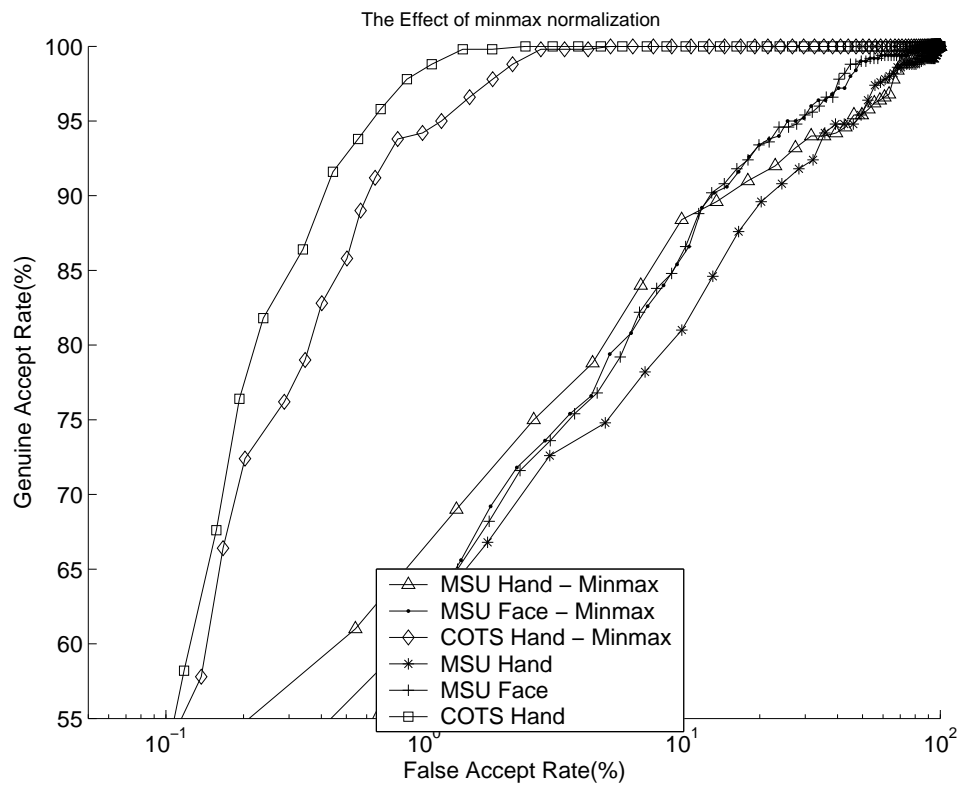


Figure 2.11: The effect of minmax normalization on MSU Hand, MSU Face and COTS Hand.

expected be more robust to outliers than the min-max scheme. The efficiency of this technique may be relatively lower, as the median is not a very good estimator of the location and scale parameters for a non-gaussian distribution. The results (Figure 2.12) obtained using this technique show that the performance of the MAD technique on MSU hand data was better than other techniques, while its effect on the face data was minimal. The improvement observed in the case of the MSU hand data, is an example of the MAD's robustness towards outliers. Here $\mathbf{X}_i = (x_{i1}, x_{i2}, \dots, x_{ij}, \dots, x_{in})$, x'_i is the normalized feature value obtained after applying MAD normalization on every feature x_{ij} over 'k' users. Then this technique can be represented as:

$$x'_{ij} = \frac{x_{ij} - \text{median}_k(x_{ik})}{MAD} \text{ where, } MAD = \text{median}(|x_{ij} - \text{median}_k(x_{ik})|)$$

3. Z-Score Normalization:

Z-score technique uses the known or estimated values of mean and standard deviation of the data to normalize it. However, since both mean and standard deviation are sensitive to outliers, it may be safe to assume that this technique will also lack the robustness to outliers, similar to the the min-max normalization scheme. Here $\mathbf{x}_i = (x_{i1}, x_{i2}, \dots, x_{ij}, \dots, x_{in})$, x'_i is the normalized feature value obtained after applying min-max normalization on every feature x_{ij} over 'k' users. Then this technique can be represented as:

$$x'_{ij} = \frac{x_{ij} - \text{mean}_k(x_{ik})}{\text{Standard Deviation}(x_{ik})}$$

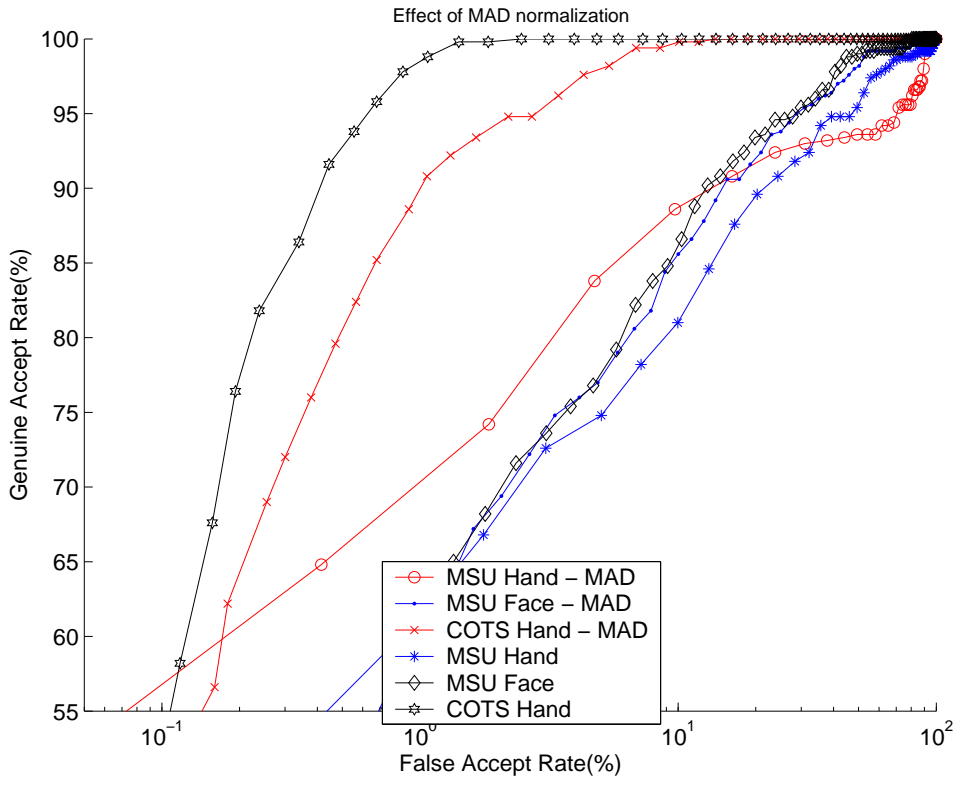


Figure 2.12: The effect of MAD normalization on MSU Hand, MSU Face and COTS Hand.

2.4 Distance measures

The experiments conducted in this thesis utilize ‘Euclidean distance’ as the distance measure in order to perform template matching. Let X_i and Y_i be two feature vectors of length ‘n’ that need to be matched against each other. Then the Euclidean distance D_e is given by $D_e = \sum_{i=0}^n \sqrt{x_i^2 - y_i^2}$. Whenever a ‘distance’ score is used to measure the dissimilarity between two templates, a smaller match score would indicate a better match and vice versa. A match score is typically transformed into a decision with the help of a decision threshold ‘t’, i.e., if $D_e < t$, then genuine; else imposter.

Euclidean distance is generally a good distance measure and can perform well when the templates are of good quality. However, on the downside it is sensitive to noise in the templates (missing features, gaussian noise etc) and, hence, deteriorates rapidly with the increase in noise (Figures 2.13, 2.14, 2.15, 2.16). For example, it is observed that performance of Euclidean distance for MSU hand geometry data (Figure 2.13) is poor without normalization. This can be attributed to the zero values (missing features) present in this data set. However, when the outliers are neutralized using a normalization technique (MAD, min-max, etc.) the performance is seen to increase. Similar observations can be made in the case of MSU hand-face FLF data set also (Figure 2.15). Feature selection techniques can also be used to increase the performance of the Euclidean measure, as they help to eliminate the ‘noisy’ or redundant features from the original feature set. It is noticed from the Figure 2.16 that the maximum performance is achieved only when both feature selection and normalization is performed on the data.

Due to the sensitivity of the Euclidean distance to noise, an effort was made to come up with a distance measure which would be more robust to the real world data. This motivation led to the finding of a new distance measure called as the ‘Thresholded Absolute Distance’ (TAD). TAD can be used as a distance measure by itself or can be used in conjunction with the Euclidean distance. As mentioned previously, while using a distance measure, a smaller distance score would imply a better match and vice versa. Hence all genuine comparisons are expected to result in a small distance score. Unfortunately, in the real world, a genuine comparison can sometimes result in large scores and a imposter comparisons result in small one. Such scores contribute to the overlap of genuine and imposter score distribution as shown in Figure 3.4. The scores in the

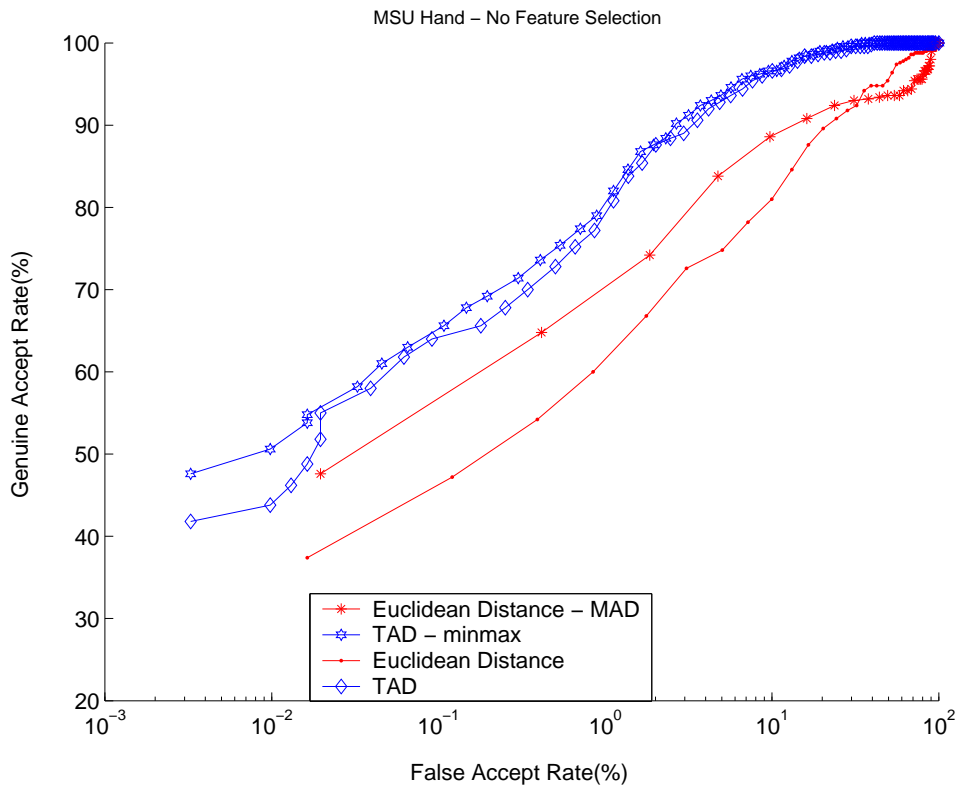


Figure 2.13: The comparison of the performance of MSU hand geometry data without feature selection using Euclidean distance and TAD.

regions of overlap (identified as the ‘critical region’ in Figure 3.4) contribute towards the errors (FAR and FRR) in a biometric system. High genuine scores may be associated with incorrect presentation of the biometric trait, bad enrollment or some temporal ‘cosmetic’ change in the biometric. For example, in the case of hand geometry if a person was enrolled without a ring and then tries to verify with a ring it would result in a poor genuine score. Such scores may also be a result of improper hand placement, bandages on the fingers, etc (Figure 2.18). This kind of problem is expected to be more evident in the case of face, as it has a high probability

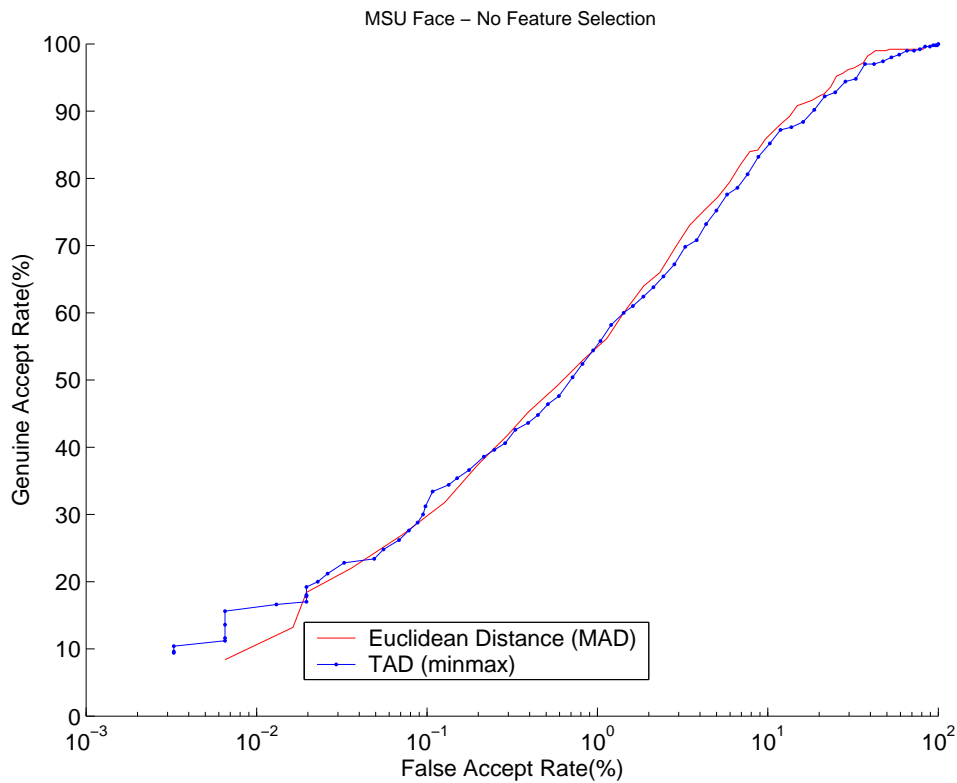


Figure 2.14: The comparison of the performance of MSU face geometry data without feature selection using Euclidean distance and TAD.

to have cosmetic changes. For example, wearing eye glasses, growing a beard or changing the hair style might lead to errors in a face recognition system. An careful analysis of the templates involved in a genuine match, but yielding ‘bad’ scores (scores that lie in the critical region) reveal some interesting observations. It is noticed that only a small minority of features in the feature set get considerably distorted (Figure 3.4) due the reasons discussed above. These features contribute majorally to the observed ‘bad’ score resulting from the genuine comparison. On the other hand, bad imposter scores are obtained due to the inherent similarities between the feature

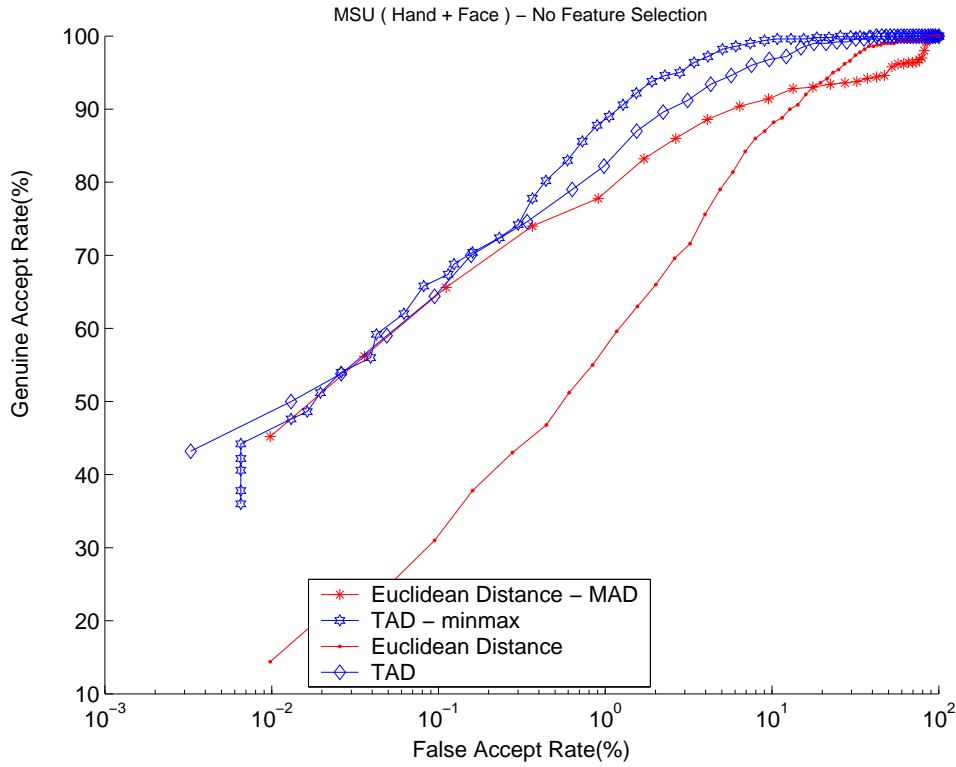


Figure 2.15: The comparison of the performance of MSU hand + MSU face FLF geometry data without feature selection using Euclidean distance and TAD.

sets being compared. Therefore, such a score would be due to the combined effect of a majority of the features, in the feature set. The proposed algorithm exploits this observation, and helps in enhancing the existing discrimination capability (Euclidean distance).

The purpose of the TAD is to help reduce the error by resolving the scores in the critical region as ‘imposter’ or ‘genuine’. The number of match scores present in the critical region is more, when using ‘weak’ classifiers like MSU hand geometry or MSU face data. Therefore, the performance improvement caused by TAD would be considerably higher on a weak classifier as opposed to a strong classifier. It is observed that in some cases (Figure 2.19), there is a

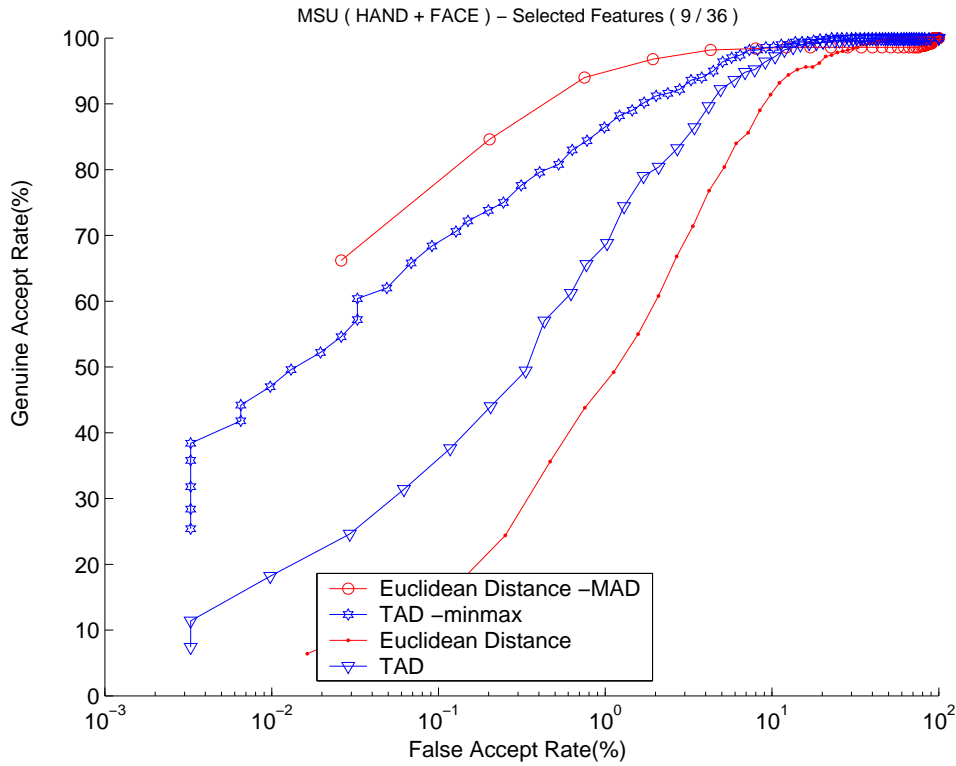


Figure 2.16: The comparison of the performance of MSU hand + MSU face FLF geometry data with feature selection using Euclidean distance and TAD.

reasonable similarity between the biometric templates of two different users in the MSU hand data. In such cases, it can clearly be seen that the majority of the features differ by a small degree from their counterparts and therefore contribute equally towards the match score, unlike the case of a genuine match. In order to observe this property and utilize it during the matching process we perform the following steps.

1. Let $\mathbf{X}_i = \{x_{i,1}, x_{i,2}, \dots, x_{i,n}\}$ and $\mathbf{Y}_i = \{y_{i,1}, y_{i,2}, \dots, y_{i,n}\}$ represent the two feature sets to be compared. Here 'n' is the length of the feature vectors.

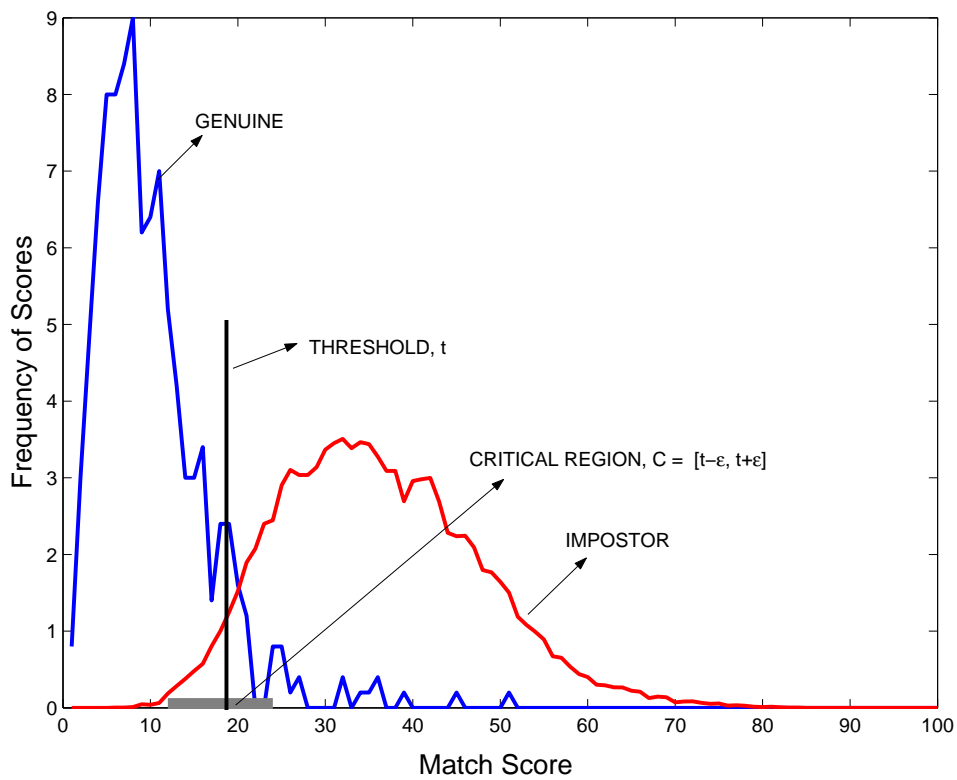


Figure 2.17: The genuine and imposter score distribution in a hand geometry system.



Figure 2.18: The reasons for error in a hand geometry system.

An imposter match falling in the critical region:

67	60	67	58	68	55	53	50	261	335	253	286	242	122
72	54	63	54	72	50	45	49	259	330	252	284	241	127

A genuine match falling in the critical region:

67	60	67	58	68	55	53	50	261	335	253	286	242	126
68	59	67	59	67	55	53	50	261	335	253	286	243	160

Figure 2.19: The reason for a bad genuine score is due to a small subset of features (highlighted) while an imposter score is due to the overall effect of all features.

2. Compute the set $D = \{d_i : d_i = x_i - y_i\}$. Here 'D' is a vector of length 'n', consisting of the absolute distances of each of the feature values in the first feature set X_i to their counterparts in Y_i .
3. Determine the number of elements, n_{t1} , in D that are greater than a threshold t_1 . A score which lies within the defined threshold is classified as 'good' and vice versa.
4. $n_{t1} > t_2$ indicates an impostor. The count of the 'good' or the 'bad' features would help us classify the comparison as 'genuine' or as an 'imposter' one. This information can be used by itself or to augment the Euclidean distance metric in order to get the final decision.

The robustness of the TAD towards noise can be observed in Figures 2.13, 2.14, 2.15, 2.16. It can be seen that the performance of the TAD does not drop drastically even when the outliers are present in the data. For example, the performance of TAD on un-normalized MSU hand

data (contains missing features) is much better than Euclidean distance as shown in Figure 2.13. Similar observations are also made for MSU hand face feature fused data (shown in Figure 2.15). The performance is robust even when the noisy features (data without feature selection) are presented to the matcher. On the downside, this technique has an upper bound on its discrimination capabilities i.e., it does not perform as well as the Euclidean distance when the features are good and have less noise. In the case of hand geometry or face where the set of features is limited and their discrimination capability is restricted, TAD proves to be a good distance measure. On the other hand, Euclidean distance proves to be the better measure, when a sufficient number of strong features are available and the data does not contain outliers in it. For example, the MSU face-hand FLF data is subject to normalization and feature selection in order to eliminate the noisy features from them. It also contains a good discrimination capability as the good features of hand and face have been consolidated together. In such a case Euclidean distance is observed to perform better than TAD. In this thesis, the TAD measure is used on the ‘need to use’ basis depending on the quality of the data set. For example, it is used when matching a MSU hand-face FLF data set and not in the case of a COTS hand - MSU Face FLF data. This is because the feature sets of the COTS hand system are less error prone and, hence, do not contain any outliers.

2.5 Feature level fusion

The previous sections of this chapter stress the importance of data preprocessing in feature level fusion. In this chapter we examine the performance of a feature level fused system (by feature set concatenation) against a match level fused system.

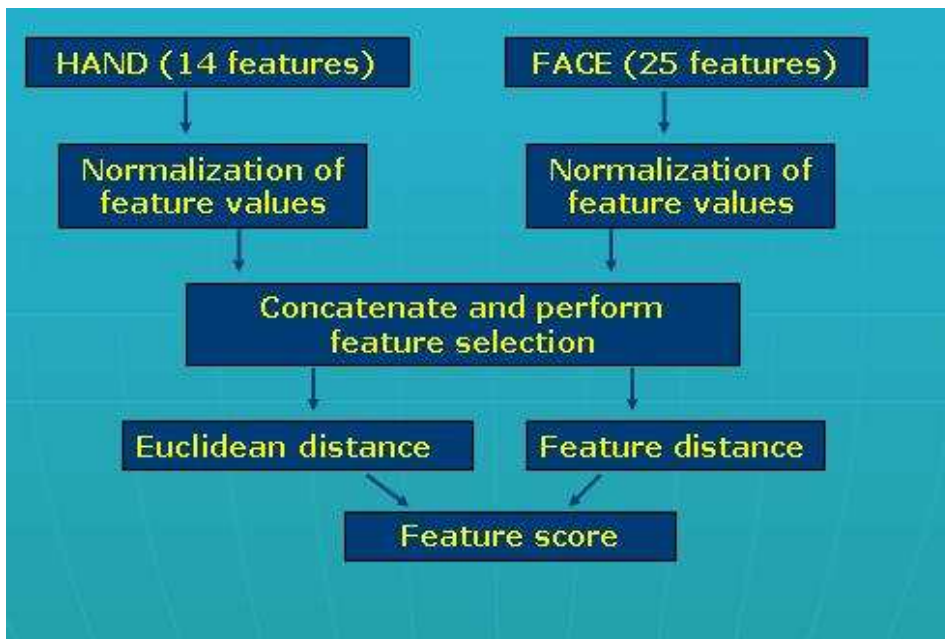


Figure 2.20: Feature level fusion in multimodal biometric systems.

Match score level fusion and feature level fusion can be tested under two different scenarios.

They would be as follows:

1. CASE 1: Fusing two weak classifiers (MSU HAND + MSU FACE).
2. CASE 2: Fusing a strong classifier with a weak classifier (COTS HAND + MSU FACE).

CASE I: This case involves the comparison of the two fusion techniques while consolidating two weak modalities. MSU hand and MSU face are used for this experiment as both are relatively weak classifiers (Figures 2.2, 2.3), compared to the commercial systems available in the market. In Figure 2.21, it can be observed that feature level fusion has nearly 10% performance gain over the match level fusion. It is also observed that the preprocessing techniques described in the previous chapter help in increasing the performance of feature level fusion by nearly 25%. In case

of weak classifiers it becomes mandatory to identify the weak features and eliminate them as they would contribute a lot to the error rates in the feature level fused template. In this case (fusion of weak classifiers) it is ‘expected’ that the performance of feature level fusion be superior to that of match level fusion. This might be because the probability of obtaining a good match score is more in a feature fused template (contains more information) than in merging two comparatively bad scores (scores based on less information).

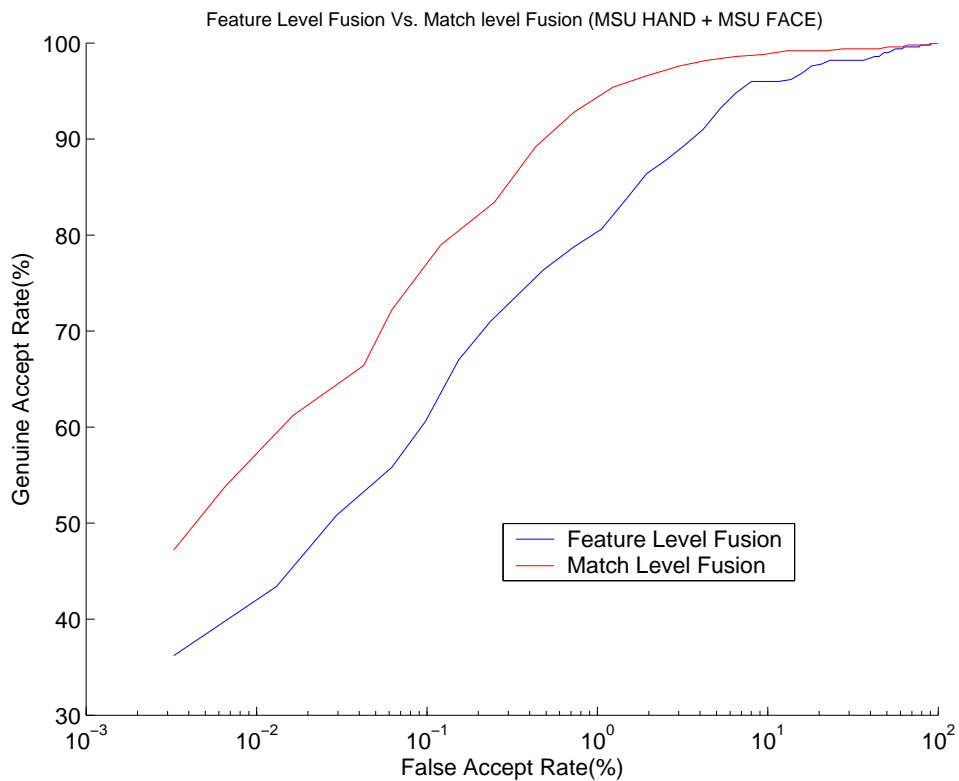


Figure 2.21: Case I : Comparison of match level fusion and feature level fusion when consolidating information pertaining to weak classifiers.

CASE II: In Figure 2.22, it can be observed that feature level fusion performs marginally

better (1-5%) than match level fusion. In this case of fusing strong classifiers with weak ones, the resulting performance is equal to or lower than that of the stronger classifier, irrespective of the type of fusion performed. This may be due to fact that the the weak classifier's performance affects that of the stronger one. This can be observed in Figure 2.3. This problem can be alleviated by performing feature level fusion after feature selection. The feature selection process on the feature fused vector ensures that only the features helping to increase the performance are selected, while all others are eliminated. Therefore, this ensures that the resulting performance is equal to, or higher than that of the highest classifier. The feature selection process typically will not be as effective in the case of match level fusion as it has to be performed on individual feature sets. It might help in increasing their individual performances but would still result in the weaker modality affecting the overall performance. Therefore the result of such a fusion will result in performances which are equal to or below that of the stronger classifier.

It is imperative to test a system's robustness towards noise in-order to effectively test a system, as noise plays a major role during deployment in the real world. Therefore, it becomes mandatory to study and compare the robustness of match level fusion and feature level fusion towards noise before commenting on the superiority of one technique over the other. The Figure 2.23 shows the effect of adding a gaussian noise of mean 0 and variance 5 to the COTS hand and MSU face data. The effect of noise does not affect both the techniques and only causes them to deteriorate marginally (1-2%).

Feature level fusion is a computationally more expensive and relatively difficult to implement as compared to match level fusion. The question is whether a gain of 5-10% is a reason significant

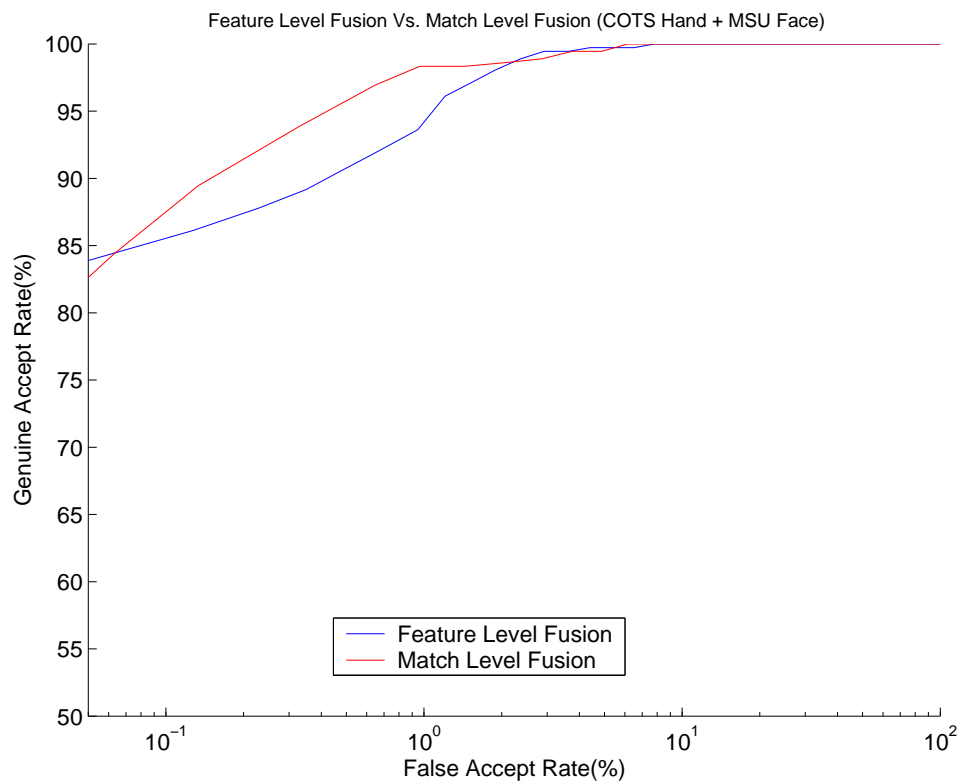


Figure 2.22: Comparison of match level fusion as opposed to feature level fusion while consolidating information from a strong classifier and a weak classifier.

enough to justify the adoption of this method over match level fusion. The answer to this question may be specific to the application it is used and the environment on which it is deployed.

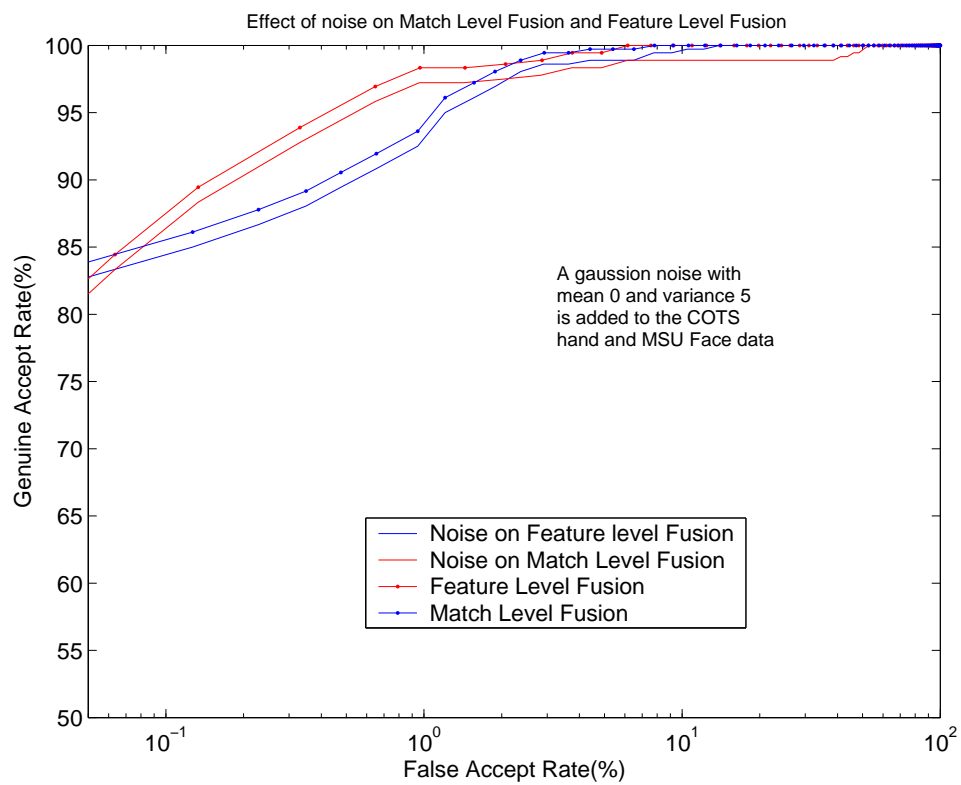


Figure 2.23: The effect of noise on feature level fusion and match level fusion.

Chapter 3

Synthesizing information across fusion levels

3.1 Introduction

As discussed in the previous chapters the fusion of the component modalities can happen at three different levels namely the decision level, the match score level and the feature level. Even though one technique might be better than the other by a small margin, as demonstrated in the previous chapter, no single fusion technique has provided significant performance gains over the others under all conditions. Also each one of its three techniques of fusion has its own upper bound on their performance capabilities as well. Therefore, a solution to this would be to keep increasing the number of modalities until the required performance is obtained. This may not be practically implementable due to the time, computational complexity, cost, the deployment constraints on the

system, and the well known ‘curse of dimensionality’ problem. This thesis proposes a technique which works by consolidating the information available at these various fusion levels in order to obtain a better performance with the same information by merging match score fusion with feature level fusion.

This ‘fusion’ of fusion levels can be performed in two different ways. This classification is based on how the information is consolidated between the match score level and the feature level and are discussed in detail in the following subsections.

3.1.1 The selective feedback scheme

The selective feedback scheme of merging fusion levels works by supplying information from the feature fusion level to augment the information present in the match score fusion level only when a concrete decision regarding the authenticity of the subject cannot be reached with the available information. Figure 3.4 shows the distribution of genuine and imposter scores in a face-hand MLF multimodal biometric system. The error in this system would be mainly due to the scores present in the region identified as the ‘critical region’ which is formed due to the overlap of genuine and imposter scores. Hence a final decision cannot be reached with a 100% certainty unless some extra information is available about those feature sets which were used to generate the match score in consideration. To achieve the same, a feedback is given which helps to augment the existing confidence value with the confidence obtained using a different fusion technique. This may enable the final result to be more reliable than the result that might have been obtained with just one method of fusion. The fusion method that is used for giving the feedback

might be called as the ‘secondary’ technique and the main scheme used for authentication be called as the ‘primary’ one.

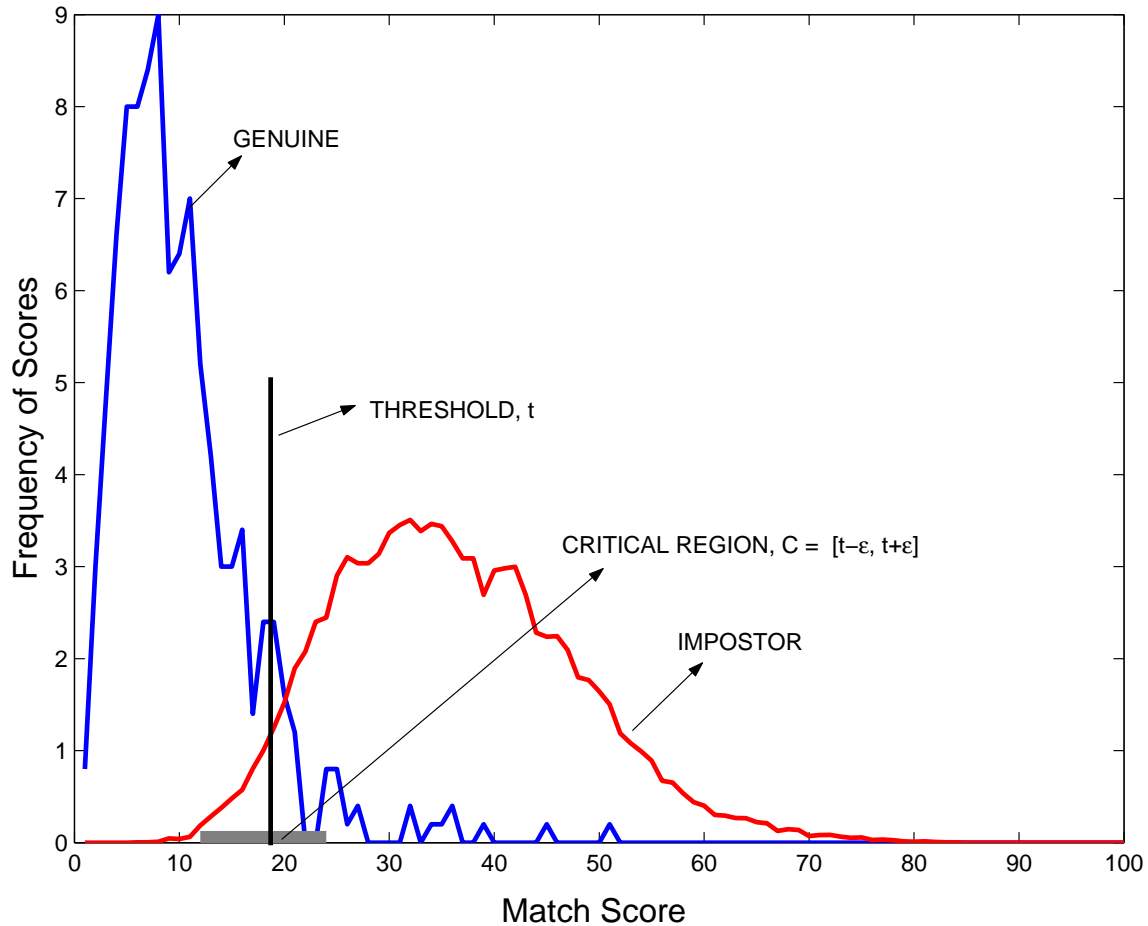


Figure 3.1: The motivation for the selective feedback technique is the existence of the ‘critical’ region where a decision cannot be made with 100% certainty without the availability of some extra information.

The primary and the secondary technique can be interchangeable if their performance levels are reasonably comparable. In cases where there is a significant difference in the performance of one technique over the other, the one with the higher performance might be used as the main

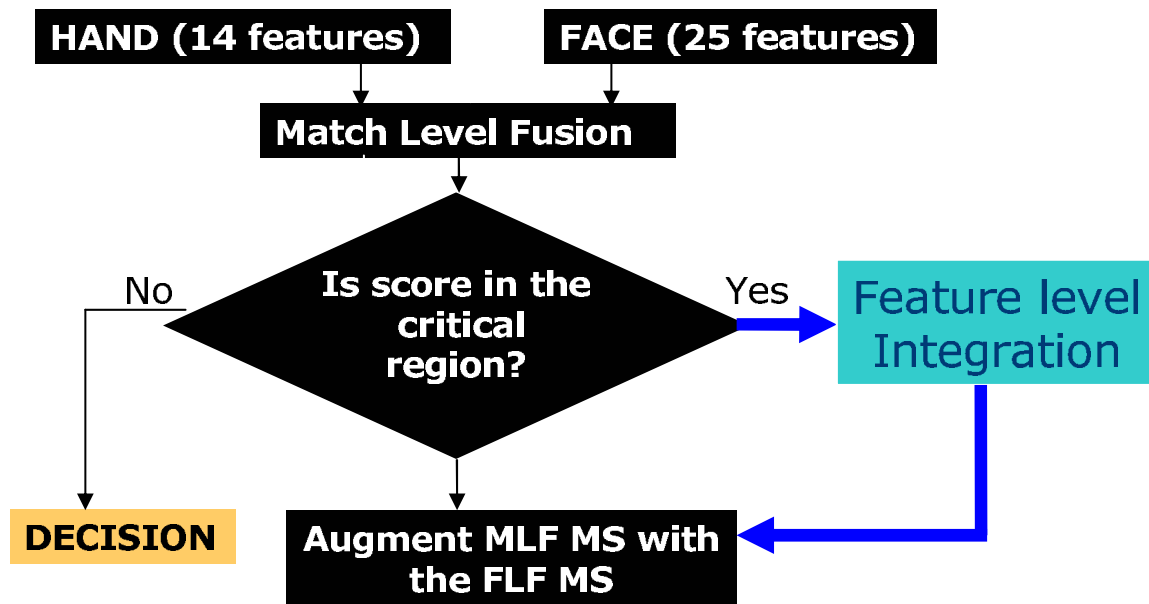


Figure 3.2: This feedback technique works by employing match level fusion as the primary scheme and obtaining feedback from the feature fusion level when the score falls in the critical region.

method and the other used selectively to provide feedback. Another factor to be considered while deciding on the primary and the secondary technique is the computational complexity of the schemes in consideration. e.g. The feature level fusion scheme has a 5% performance advantage over the match level scheme for the face-hand multimodal biometric system used in this thesis. This does not necessarily qualify it to be the primary scheme as it requires a lot more computational resources than the match level fusion. This decision can therefore be specific to the priorities in the domain on which this system is to be deployed. In the experiments conducted in this thesis, the match score level fusion was considered as the primary technique as it was computationally simpler and also its performance was only marginally lower than that of the

feature level fusion.

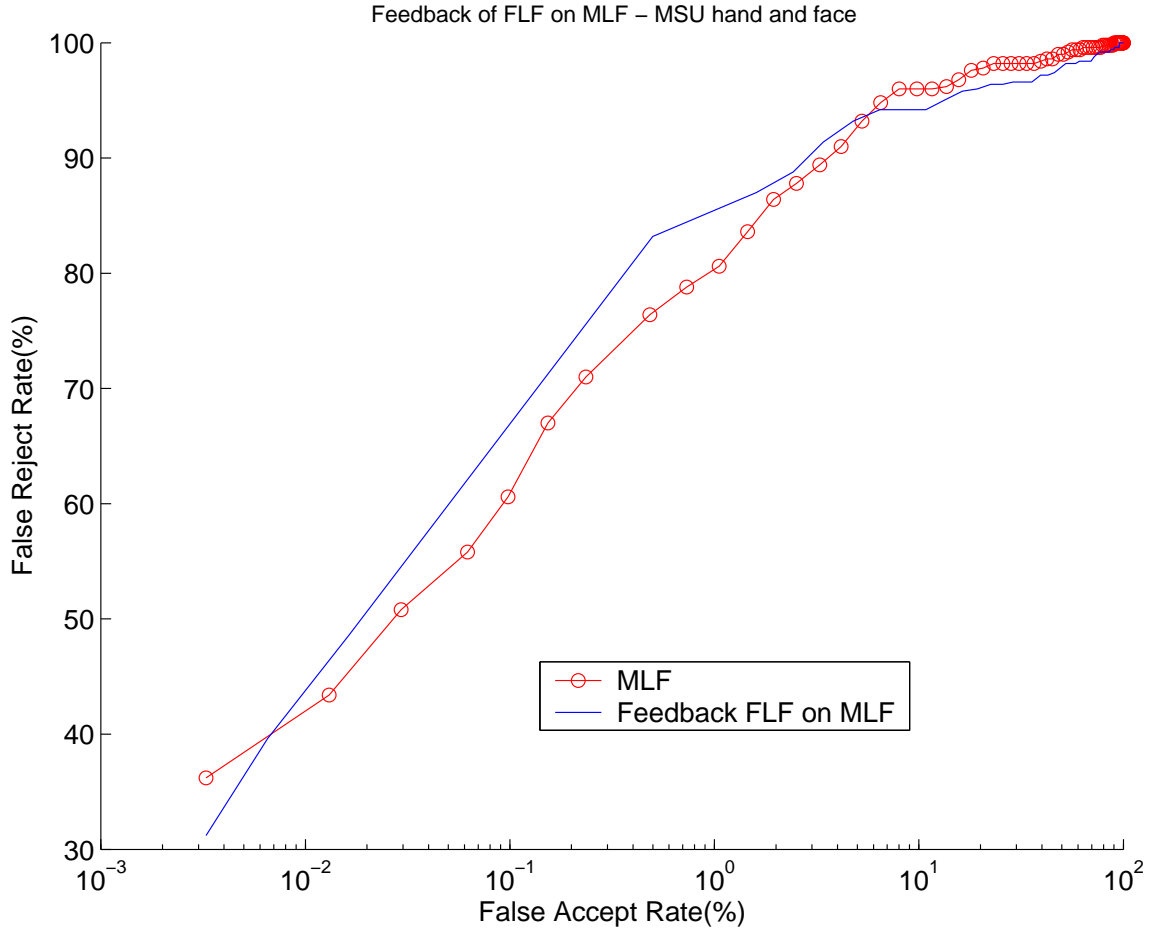


Figure 3.3: The feedback technique results in approximately 5% improvement in the performance of the system across all thresholds.

3.1.2 The exhaustive fusion schemes

This technique unlike the previous one is an exhaustive merging scheme which consolidates the match scores resulting from the match level fusion and the match scores from the feature fusion

```
graph TD; I1[Input 1: Palm] --> FE1[Feature Extraction Module]; I2[Input 2: Face] --> FE2[Feature Extraction Module]; FE1 --> FU1((FU)); FE2 --> FU2((FU)); FE1 --> MM1[Matching Module]; FE2 --> MM2[Matching Module]; FU1 --> MM3[MM]; FU2 --> MM3; MM3 --> DM1[DM]; MM1 --> DM1; MM2 --> DM1; DM1 --> AR[Accept/Reject]
```

DM Decision-making module

MM Matching module

The results demonstrated with the help of Figure 5.5 shows that there is a 10-15% performance advantage using this new system against the conventional match level fused systems. This is a substantial gain in the performance given that no extra biometric modalities or classifiers are used. But as emphasized before, the performance gain comes at a price as the computational needs of this system is more than that of the feedback technique.

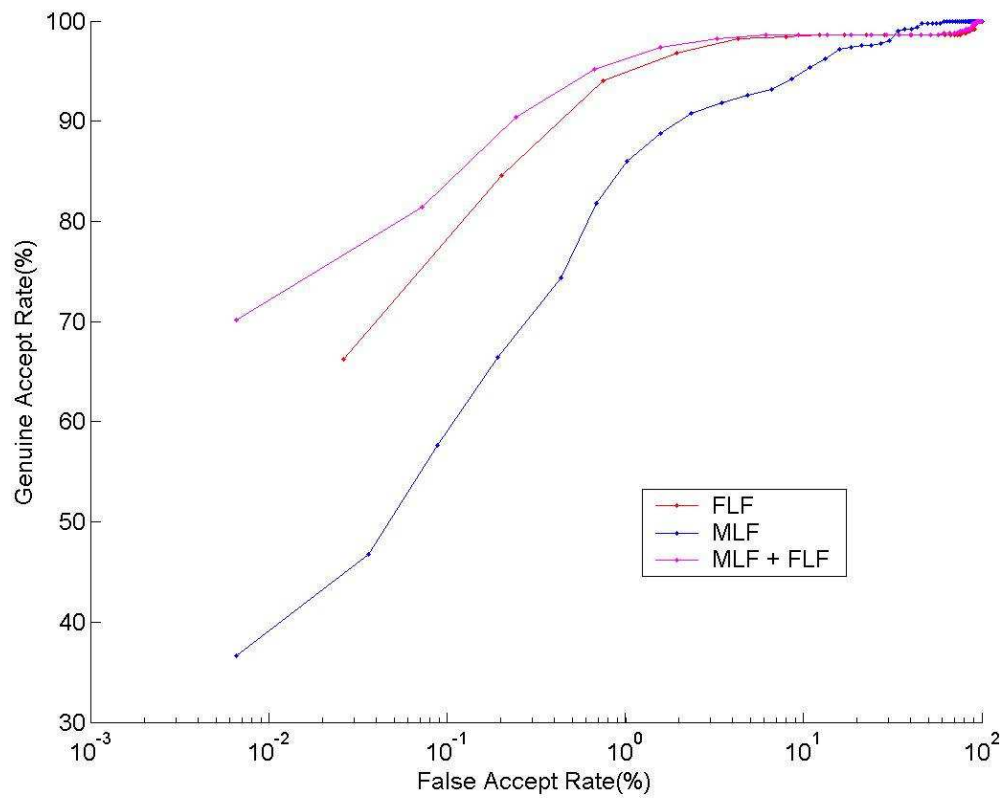


Figure 3.5: The exhaustive fusion technique results in up to approximately 10% improvement in the performance of the system across all thresholds.

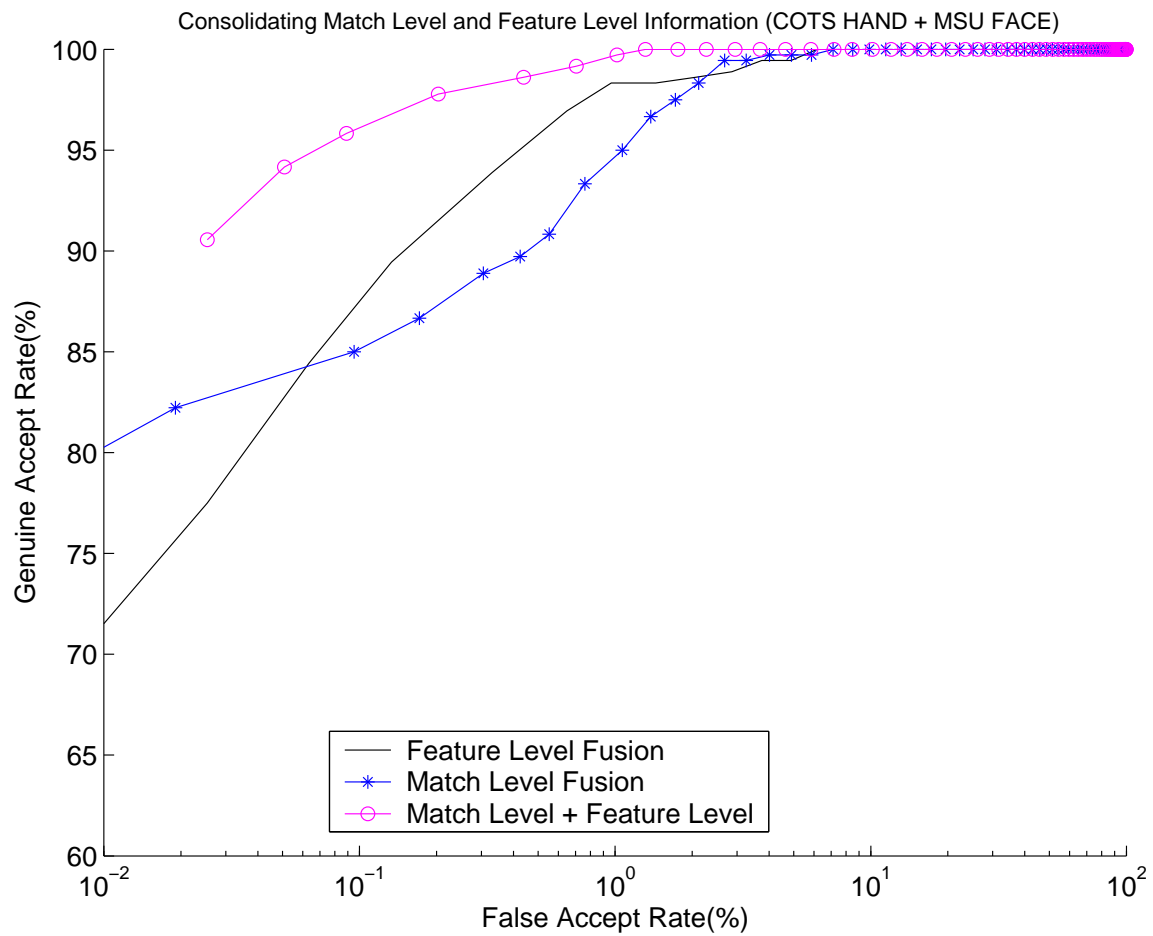


Figure 3.6: The exhaustive fusion technique results in up to approximately 10-15% improvement in the performance of the system across all thresholds.

Chapter 4

Biometrics with group consensus

4.1 Introduction

In this chapter we present a novel idea called Biometric authentication with group consensus, which improves the performance of biometric systems in applications, where there is a requirement to authenticate multiple users simultaneously. Currently applications employing biometrics typically involve, authenticating a single individual, in order to grant him/her access to a secure resource. We foresee a requirement for higher security in some special applications which operate in scenarios where mutual trust among co-users cannot be assumed, and hence necessitating the need to authenticate more than one individual simultaneously. For example, the launch of a missile might require the consent of multiple individuals and would, therefore, require validating the identity of multiple subjects at the same time. Similarly, a bank vault containing valuable goods might be accessed by authorizing the identity of both the bank manager and

the customer. This kind of security measures are also common when accessing highly secure computer systems and in places where repudiation claims are frequently filed. This can be achieved by fusing the biometric traits of multiple individuals (pertaining to a single modality) at different functional levels (decision level, match level, feature set level) to obtain a consolidated decision. In this thesis we study the fusion of multi user information in the match score level and the feature level and discuss the advantages and disadvantages of each of these techniques. The experimental are conducted to determine the suitability of a different fusion techniques to the multi-user scenario. Preliminary results indicate the suitability of feature level fusion in MUB systems.

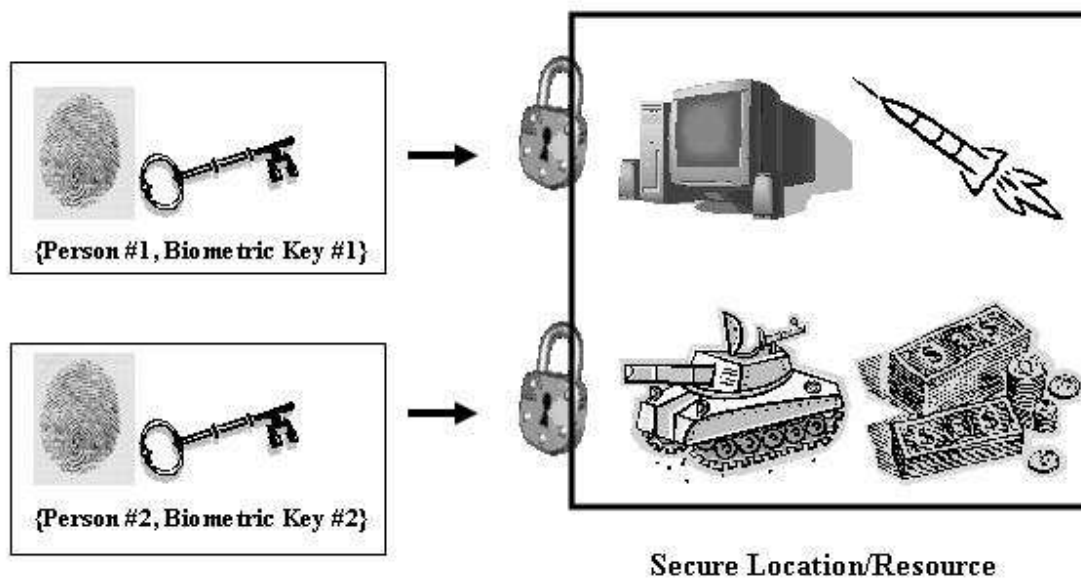


Figure 4.1: Usage of multiple keys to access a secure resource.

The Multi-user technique has been demonstrated to have considerable performance gain over the conventional method of authenticating each user in an independent manner and then consolidating those distinct results to obtain a joint decision, i.e., fusing the biometric of

users at the decision level. With the advent match level fusion (better performing and more flexible than decision level fusion) in multimodal biometrics it becomes logical to utilize match level fusion for such applications. The new scheme proposed in this thesis would involve consolidating the biometrics templates of multiple users into a single multi-user biometric template for authentication. This process requires the same amount of time and hardware as the previously described methods but is shown to have better error rates and performance across different operating thresholds. The resulting template is also much more secure than the regular biometric template and would not be susceptible to biometric reconstruction techniques (used to obtain the original biometric data of a user from the templates) [32] [33]. This concept is also extended to fuse multiple biometric traits of multiple users to further reduce the error rates. Further, a consolidation of information across the different fusion levels can help us increase the performance beyond the upper bounds of both match level and feature level fusion.

$$\text{New Biometric} = \text{func}(\text{Biometric (user \# 1)}, \dots, \text{Biometric (user \# n)})$$

In this chapter we first describe the concepts and fusion techniques involved in designing a Multiuser Biometric System (MUB) system. We then present results obtained using a MUB system for each of the fusion techniques. The results are demonstrated using two biometric modalities viz. hand and face. Finally, we discuss the results and comment on the future work that can be done to further enhance this concept.

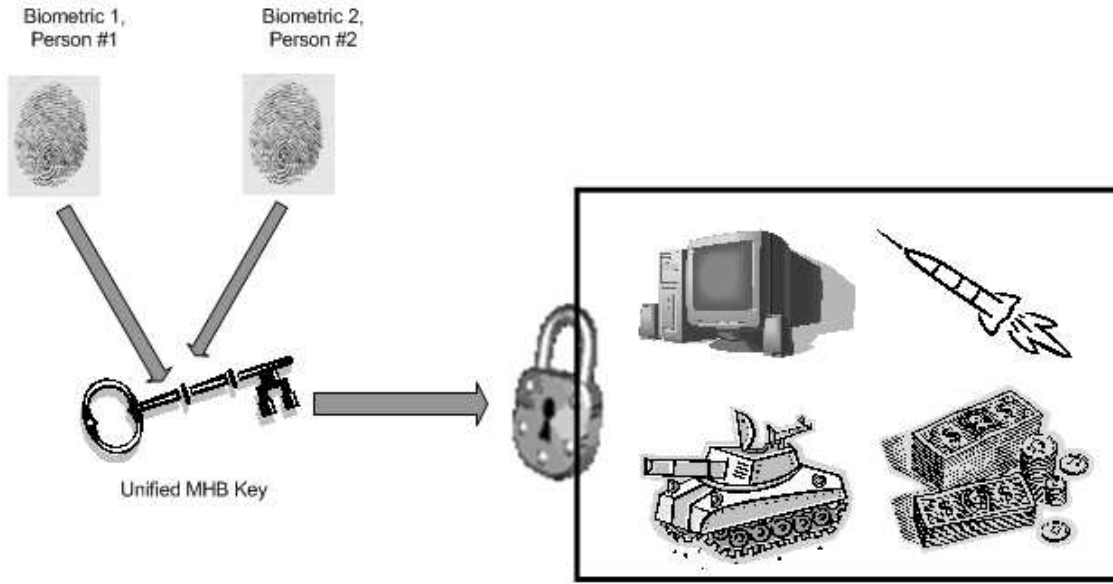


Figure 4.2: A multi-user biometric system is more secure than a conventional biometric system.

4.2 Biometrics with group consensus

The techniques used in MUB follows to a certain degree the same concept as the fusion techniques used in multimodal biometrics (MB). Instead of fusing two different biometrics of the same individual, a single biometric of the same modality but of multiple individuals are used in authentication. Let $\mathbf{H}_i = \{h_{i,1}, h_{i,2}, \dots, h_{i,m}\}$ and $\mathbf{H}_j = \{h_{j,1}, h_{j,2}, \dots, h_{j,m}\}$ represent the hand feature vector (geometric features) of two users, respectively. The fused feature vector $\mathbf{X}_i = \{x_{i,1}, x_{i,2}, \dots, x_{i,d}\}$ can be obtained by augmenting the feature vectors \mathbf{H}_i and \mathbf{H}_j , and performing feature selection on the concatenated vector. This feature vector \mathbf{X}_i would be compared to a similar multi-user feature vector \mathbf{X}_{iE} registered during the enrollment phase of the system and thus result in a distance score S_i which is used to make the final decision. Therefore,

this technique suffers from the same set of drawbacks as feature level fusion (FLF) in MB except that the feature set compatibility problem is eliminated. Feature set compatibility pertains to the problems involved during the ‘complex’ process of mapping feature sets, existing in different domains, to a similar domain before concatenation (fusion) is performed (e.g. minutiae sets of fingerprints and eigen co-efficients of face). Eliminating the need for this process implies that, FLF in a MUB system is now much simpler and more reliable than FLF in a MB system. Match level fusion in a multiuser system would involve consolidating the match scores of individual users in order to obtain the final decision. Let S_{H_i} and S_{H_j} be the normalized match (distance) scores generated by comparing the feature sets H_i and H_j of users 1 and 2, with their enrollment templates (H_{iE}, H_{jE}). Therefore, $S_{HM-fus} = (S_{H1} + S_{H2})/2$ will be the fused match score, when using the simple sum rule.

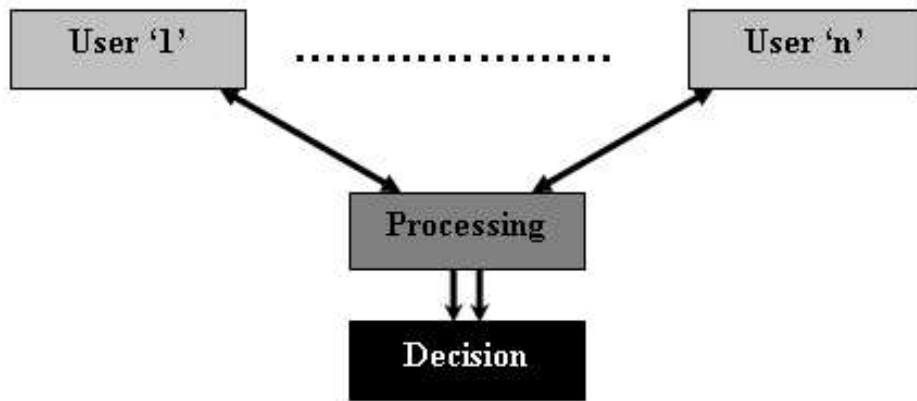


Figure 4.3: A multi-user approach which combines the biometric of two or more persons.

Ross and Jain [1] describe the advantages and disadvantages of combining multiple biometric

modalities at various fusion levels viz., the feature level, match score level and decision level in a MB system. They also discuss the techniques involved in combining multiple classifiers for a single biometric and describe the resulting performance gains. Feature fusion even in MB systems has been an relatively under studied problem, due to hindrances arising from combining heterogeneous feature vectors, the curse of dimensionality, etc. But in general as per the results viewed in the previous chapter (related to the performance of FLF in MB systems), it is expected that the performance of FLF in MUB systems should also surpass the performance of MLF MUB systems.

4.3 The different levels of fusion in a Multi-user biometric system

4.3.1 Feature level fusion

This approach involves the consolidation of information at the feature level (template level). Let the template set of n individuals be denoted as $T_i, i = 1, 2, \dots, n$. Then, for the ' i^{th} ' individual would be $T_i = X_{i1}, X_{i2} \dots, X_{im}$. The fused template that is formed by MUB would involve consolidating the information from the ' n ' templates inorder to form a new one $T_{MUB} = F(T_1, T_2, \dots, T_n)$.

The MUB template being constructed will be a function of the ' n ' individual templates and, in most cases, it is a direct concatenation of all the individual templates. In this chapter we also

experiment with new techniques like using the mean of the individual templates to obtain the final MUB templates.

$$\begin{aligned}
 MUB\ Template &= [X_{11}, X_{21}, X_{31} \cdots X_{1m}, X_{2m}, X_{3m}, \cdots, X_{nm}] \longrightarrow \text{Concatenation} \\
 MUB\ Template &= \left[\frac{(X_{11}+X_{12}+\cdots+X_{1m})}{m}, \frac{(X_{21}+X_{22}+\cdots+X_{2m})}{m}, \dots, \frac{(X_{n1}+X_{n2}+\cdots+X_{nm})}{m} \right] \longrightarrow \\
 &\hspace{15em} \text{Average}
 \end{aligned}$$

A system of ‘x’ modality, fusing ‘t’ people to make a successful authentication will be termed as a ‘MUB - t X’ system. For example, a ‘MUB-2 hand system’ uses the hand geometry of 2 individuals to make a successful authentication. In real-time applications using the MUB system it is possible to assign different weights to the match score or the templates of various individuals. Apart from a higher performance relative to other fusion techniques, feature level fusion also ensures that the resulting template is highly secure and cannot be used to reconstruct the original biometric image. This is because only partial information from each user is employed to construct the final MUB template. Also this method reduces the space requirements for template storage, as we store only one template (size is comparable to the template of a single user) rather than storing two templates individually.

The number of people to be fused together may be limited due to the well studied ‘curse of dimensionality’ problem. Trunk [3] has demonstrated that the error rate in a pattern recognition system increases when the size of the feature set increases beyond a certain limit. The size of the feature-set in a MUB-t system is obviously related to the size of a single feature set (template) for the biometric in consideration. For example, if hand geometry contains only 9 features per person while face systems record 128 features per person and then, the MUB template of face

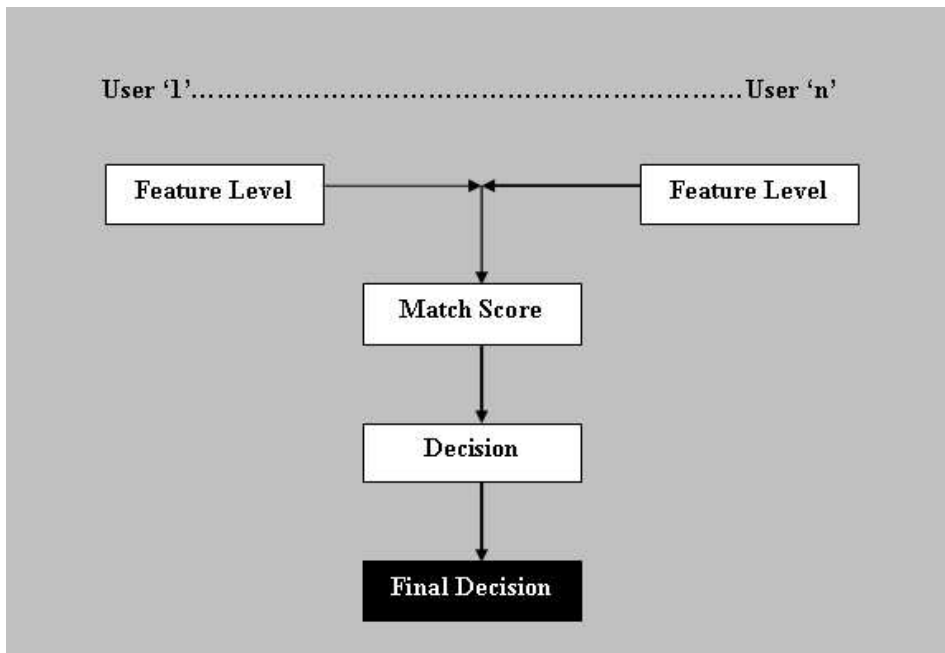


Figure 4.4: Feature level fusion in MUB systems.

would be larger than that of the hand. Also a MUB face system and a MUB hand system would encounter the ‘peaking phenomenon’ or the ‘curse of dimensionality’ at a different people counts. Another reason for the performance degradation may be because of the similarity of feature sets obtained as the number of people being combined increases in a fixed user population. If ‘n’ users need to be provided access to a room using a MUB approach and the MUB needs ‘t’ people for a positive authentication then there are ${}_nC_t$ possible multi-users who can gain access to the room. As the value of $t \rightarrow n$, the similarity between feature sets keep increasing. Initially the performance increases as ‘t’ increases and after the value of ‘t’ crosses a threshold ‘ t_0 ’ the performance starts degrading gradually [3].

The entire MUB feature fusion process of authentication can be clearly described in the following steps:

1. Data is obtained from all the ‘t’ users in either a serial or parallel fashion from all the involved users.
2. The feature vectors are computed for each user from their biometric data.
3. The feature vectors are combined to generate a new feature vector.
4. The matcher generates a match score by comparing the generated feature vector with the enrolled template.
5. The match score is used by the decision level to either accept or reject the claim.

The empirical results pertaining to the performance of this technique are present in the results subsection of this chapter.

4.3.2 Match score level fusion

In this approach, the information of multiple users is fused at the match score level. This implies that each user’s biometric is compared to his/her enrollment template and a match score generated independent of the other user. A new combined match score is then generated as a function of the independent match scores m_1, m_2, \dots, m_n .

$$M = f(m_1, m_2, m_3, \dots, m_n)$$

Kittler et al. [22] have developed a framework for consolidating the evidence of different matchers using techniques like the sum rule, product rule, max rule, median rule and majority voting. Ross and Jain [1] use decision trees and linear discriminant classifiers for combining multiple match scores. This kind of fusion between match scores can take place between similar or dissimilar biometric modalities. There is a lot of flexibility in this level of fusion, as it is oblivious to the source of the match score. User-specific weights can be assigned in the fusion process, to further improve performance. They suggest this technique in the context of multimodal biometrics. The entire MUB match score fusion authentication process might involve the following steps:

1. The data for the MUB system is collected either in the serial or the parallel mode. (In the experiments conducted for this paper the data is assumed to be collected in the serial mode).
2. The match scores ' m_1 ', ' m_2 ', are calculated independently for each user's biometric.
3. The match scores are fused together in-order to obtain a new match score.

$$e.g., S_{fus} = \frac{m_1 + m_2}{2}$$

4.3.3 Decision level fusion

The MUB approach at the decision level is similar to the decision level fusion in multimodal biometrics. This is the most simplistic and intuitive way of authenticating multiple individual.

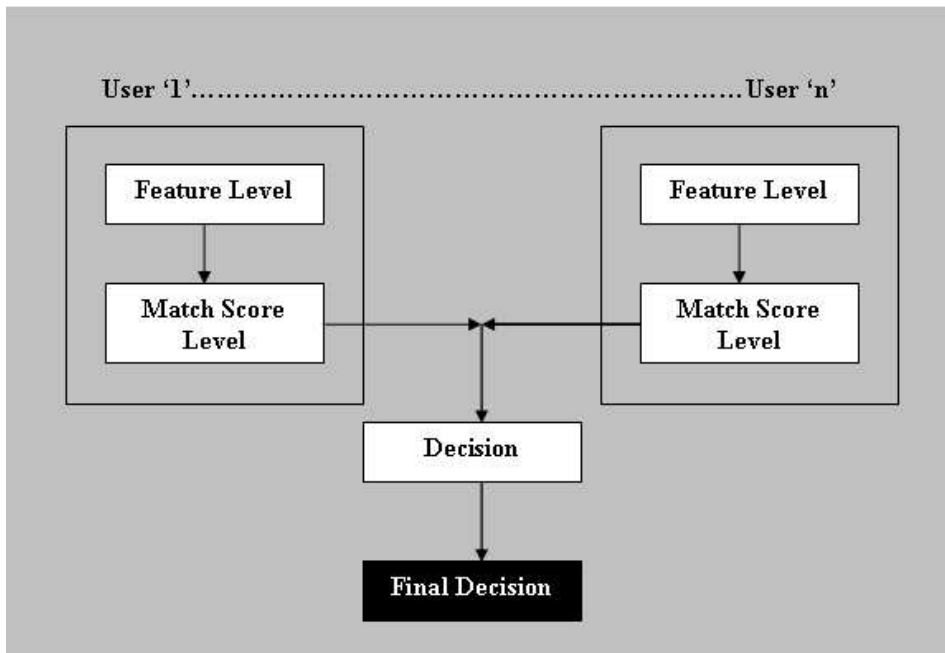


Figure 4.5: Match score level fusion in MUB systems.

A number of fusion methods like majority voting [28], behavior knowledge space [29], and weighted voting based on Dempster-Shafer theory of evidence [30] are used in order to converge to a final decision. This is very similar to what would be done in a conventional biometric system where the biometric traits of different individuals are separately extracted, compared and a consolidated decision taken based on these independent comparisons.

4.4 Modes of operation in a MUB system

This MHB approach can be realized in two fashions namely serial mode and parallel mode.

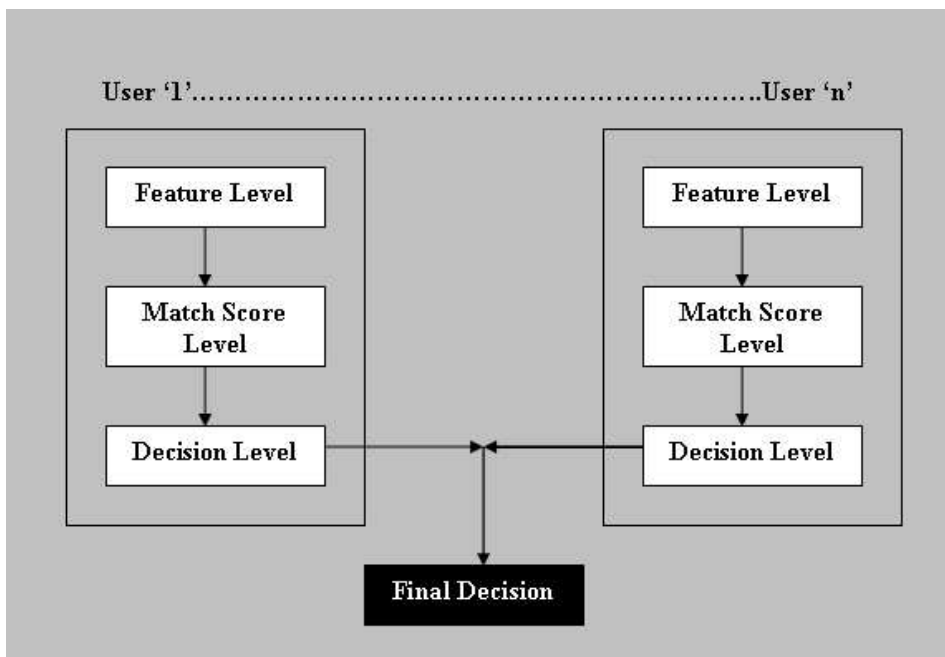


Figure 4.6: Decision level fusion in MUB systems.

4.4.1 Serial operation mode

In this mode of operation, only one biometric device exists and hence the biometrics of the different individuals needs to be collected in a serial manner. Therefore, this procedure is fairly time consuming. If the time required to collect data from one person is ' T ' and if the MUB requires ' t ' individuals for a positive id then the time interval needs to be ' $Tt + C$ ' where ' C ' is the comfort factor. The decision is taken after the data from all the involved people is obtained. The time taken in this mode is equal to that taken by a normal biometric system to authenticate ' n ' persons individually in a serial fashion.

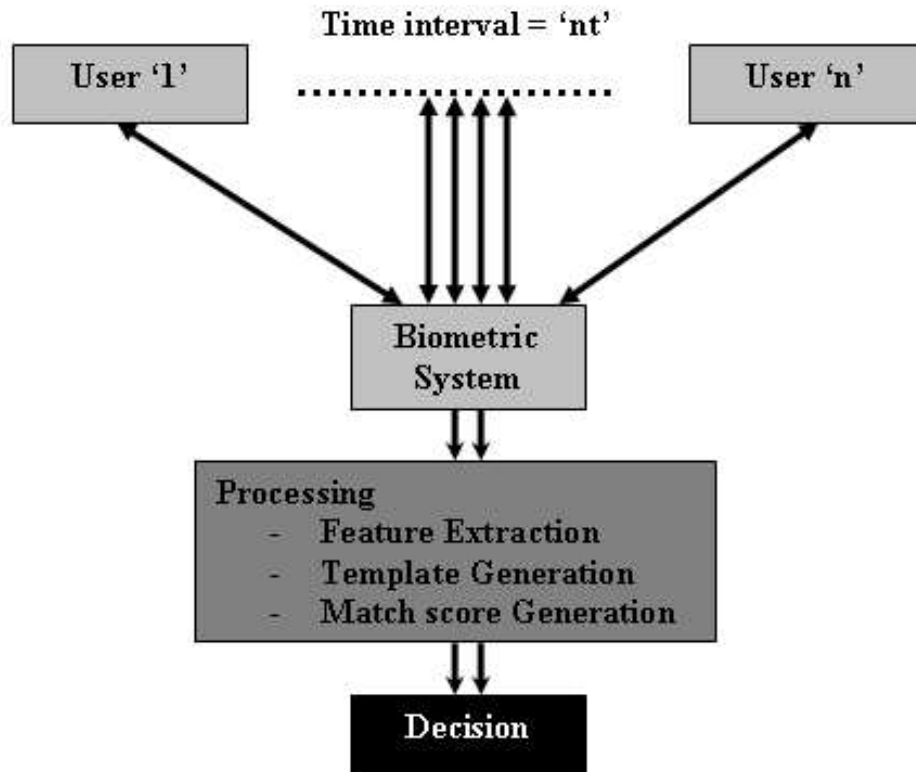


Figure 4.7: Serial mode of operation in a MUB systems.

4.4.2 Parallel operation mode

In this mode the data is collected in parallel from two or more users. This mode requires more resources in terms of hardware, software and space but requires less time to procure and process data. Here, every individual requires a separate scanner. If the average time required to collect data from one user is 'T' seconds then the total time required is also 'T + C' where 'C' is the comfort factor.

The data used in the experiments conducted for this paper were collected in the serial mode. This was because of the insufficient number devices and other space constraints.

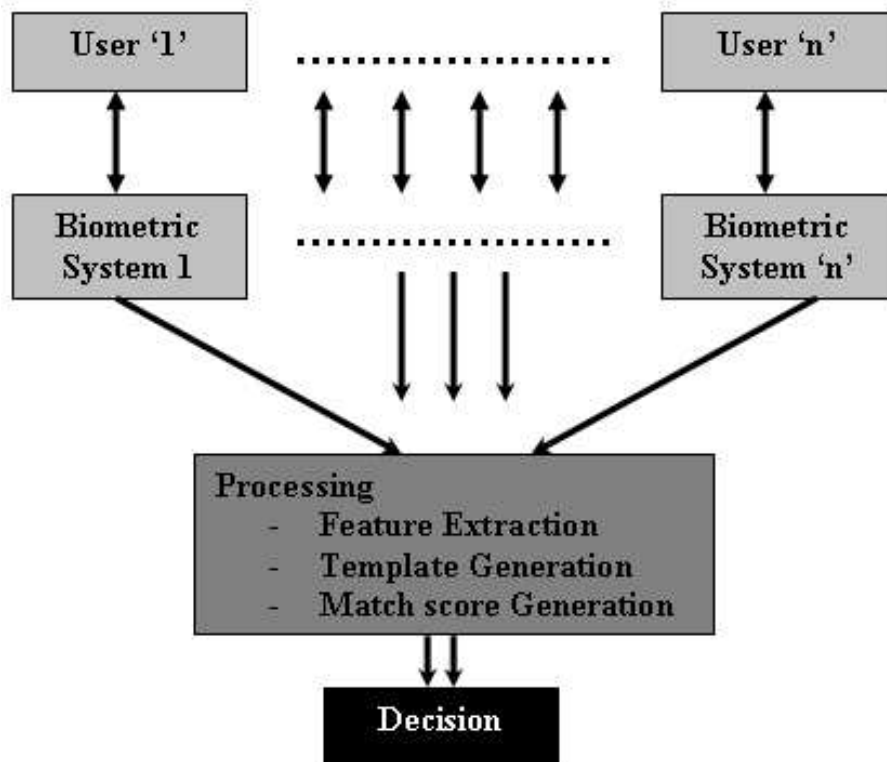


Figure 4.8: Parallel mode of operation in a MUB systems.

Biometrics	# of Subjects	# of Features	# of collections/subject	Type of feature sets
Hand	50	14	5	MSU Data Collection [5]
Face	50	25	5	PCA

Figure 4.9: Final Data Collection Count

4.5 Experiments

The purpose of this section is to discuss the results of certain preliminary experiments in order to demonstrate the superiority of the MUB system fused at the feature level over the conventional way of biometrically authenticating individuals (decision level or match level). The False Accept Rate (FAR) of the MUB are plotted against their Genuine Accept Rate (GAR) for a range of threshold values, in-order to demonstrate the overall performance.

4.5.1 Data preprocessing

The Feature level fusion performed in this section is based on the techniques described in chapter 2. Therefore, the data of individual modalities are subjected to normalization before their concatenation into one single joint feature vector. Also the joint vector is subjected to feature selection based on the average GAR criterion as discussed before.

4.5.2 Distance Measure

Distance measures are used to measure the distance or the dissimilarity between two templates. If the distance is more than a specified threshold then the two templates are declared to belong to different people and vice-versa. The distance measure used in these experiments is the Euclidean distance. The Euclidean distance ' D_E ' between two feature sets of length 'm' is given by

$$D_E = \sqrt{\sum_{i=1}^m (x_i - y_i)^2}$$

Here 'd' is the Euclidean distance to be calculated. The Figure [5] shows the performance of a hand geometry system over a range of thresholds.

4.5.3 Preliminary Experiments

There are two ways in which multi-users can be formed in a MUB system. They are as given below:

1. **DISJOINT MULTI-USERS:** A multibiometric template may be formed in such a manner that the individual constituent users of each template do not overlap with any other multibiometric template formed by that system i.e. they are disjoint. For example, let user 'u1' and 'u2' are used to form a MUB user 'U1' and let user 'u3' and 'u4' form a MUB user 'U2'. Then it is not possible for a MUB user to be formed by combining 'u1' with 'u3' as the MUB users need to be disjoint. Therefore, if 'n' individuals are required to access a resource and if the MUB system uses 't' users to perform an successful authentication, then the total number of multi-users which can be generated is n/t . For the experiments conducted in this thesis, the number of MUB-2 users generated by this technique was 25 as the total number of individual users were 50.
2. **OVERLAPPING MULTI-USERS:** In this type of MUB template formation, only the combination of individuals that constitute an MUB are unique. Unlike the previous case, here a user can be a constituent of multiple MUB users. For example, let user 'u1' and 'u2' are used to form a MUB user 'U1' and let user 'u3' and 'u4' form a MUB user 'U2'. Then it is possible for a MUB user to be formed by combining 'u1' with 'u3'. In this case,if

'n' individuals are required to access a resource and if the MUB system uses 't' users to perform an successful authentication, then the total number of multi-users which can be generated is ${}_nC_t$. Therefore, the number of MUB-2 users generated by this technique was 25 as the total number of individual users were 1225.

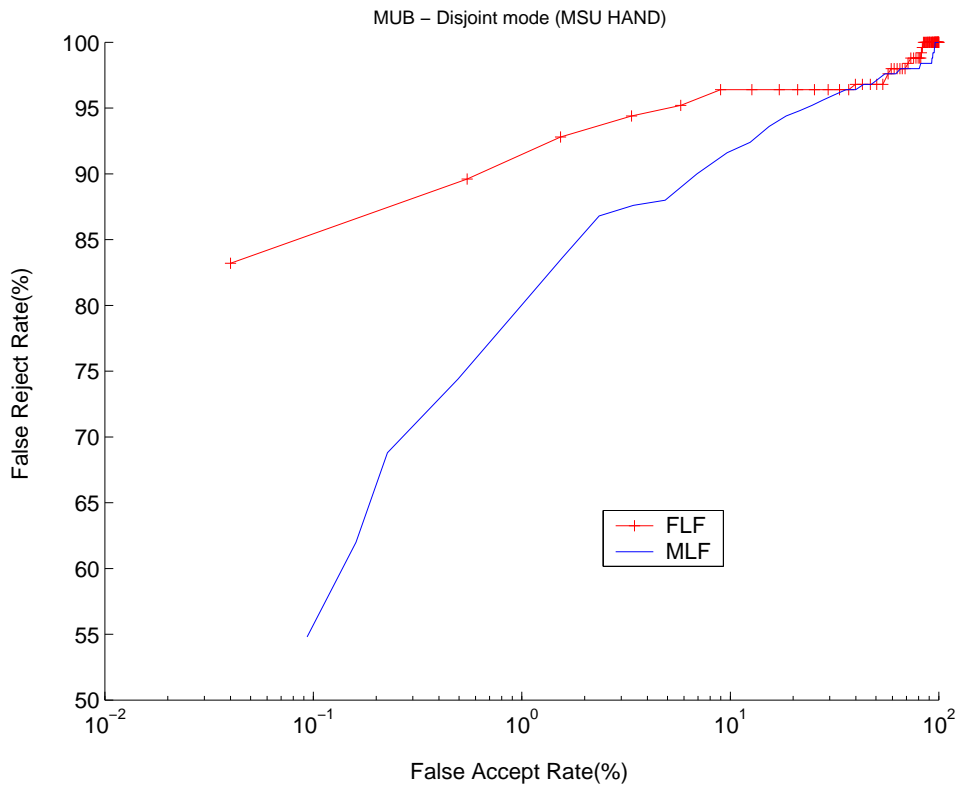


Figure 4.10: The feature level fusion outperforms match level fusion in MUB-2 hand systems constructed in the DISJOINT mode.

The preliminary results of MUB face, hand systems constructed in both overlap and disjoint modes are shown in Figures 4.10 4.11 4.12 4.13. It is observed that feature level fusion (performed as described in chapter 2) performs 10-15% better than match level fusion (simple sum rule) in all

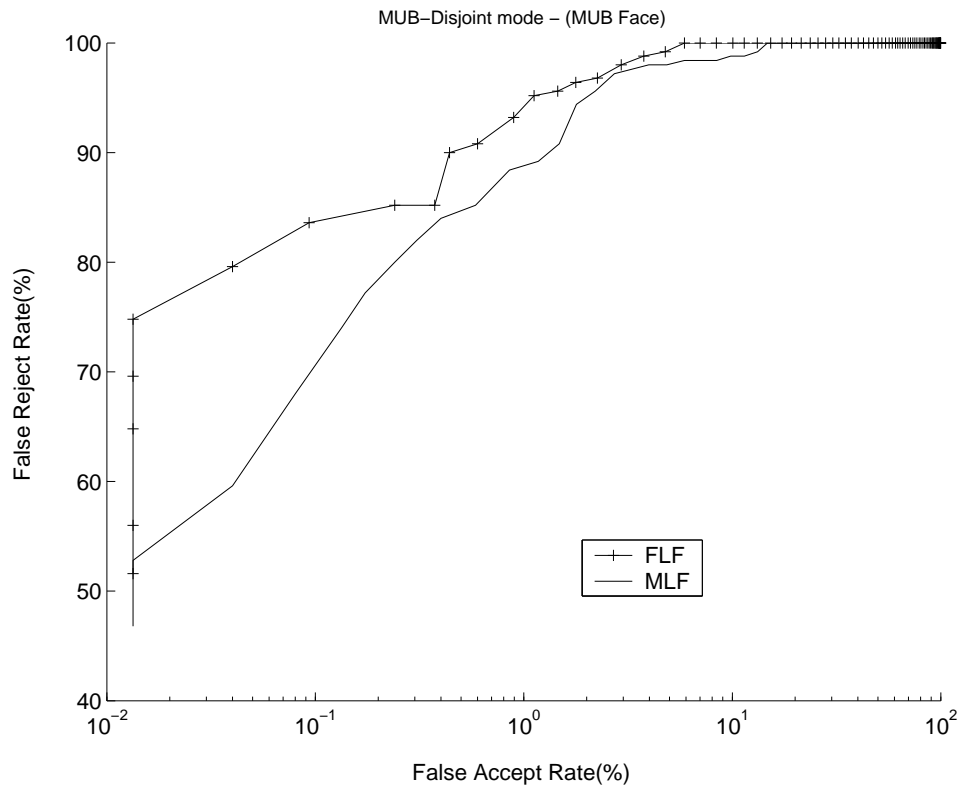


Figure 4.11: The feature level fusion outperforms match level fusion in MUB-2 face systems constructed in the DISJOINT mode.

the four cases. An MUB system can be made of more than 2 users. Typically the performance of a MUB system is expected to increase with the number of component users. But unfortunately it might not stand true because of the ‘curse of dimensionality’ problem, resulting from the increased size of the feature set. This phenomenon has been demonstrated in Figure 4.14 where the performance increases with the increase in users, reaches a maximum and then starts to deteriorate.

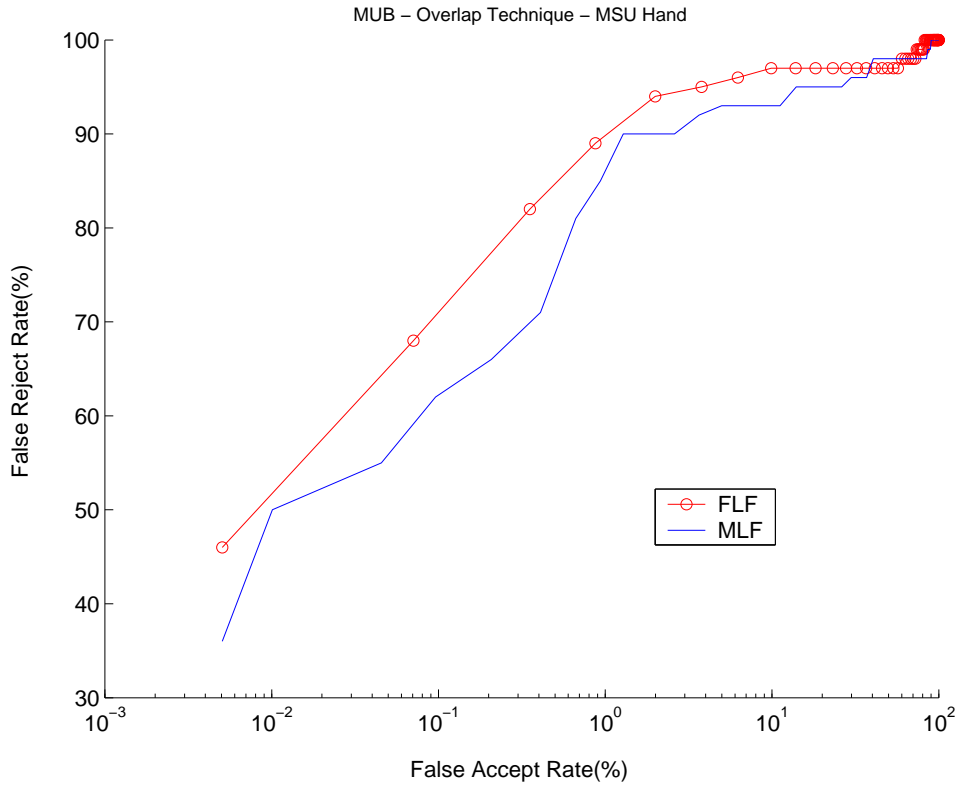


Figure 4.12: The feature level fusion outperforms match level fusion in MUB-2 hand systems constructed in the OVERLAP mode.

4.6 Multi-user multimodal biometrics

Multi-user multimodal biometrics can be defined as the fusion of multiple modalities of multiple individual. This can be used in multimodal biometric systems where more than one individual needs to be verified for a successful authentication. In this system a variety of levels of inter-biometric and intra-biometric fusion is possible. Such systems may require a lot of hardware and processing power especially when operating in the parallel mode.

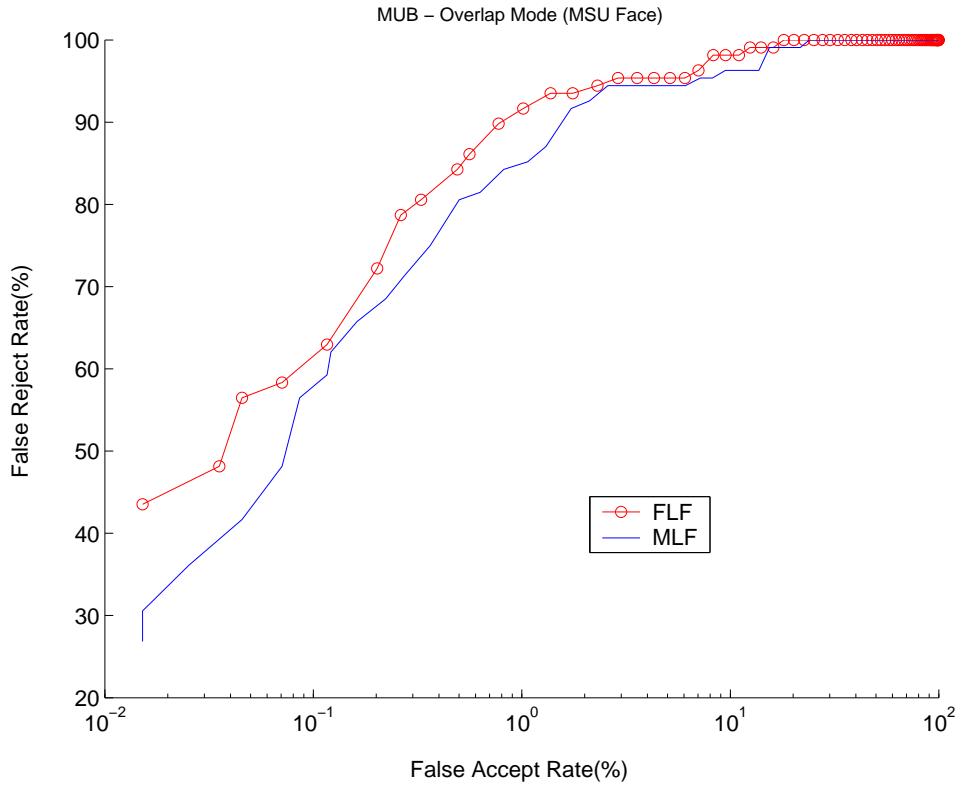


Figure 4.13: The performance of feature level fusion is better than that of match level fusion in MUB-2 face systems constructed in the OVERLAP mode.

4.7 Conclusion & Future Work

The MUB systems outperform the conventional systems by a considerable margin for both the modalities, viz., Face and hand considered in this thesis. The application of this system is limited to places requiring very high security and where there is a need for authenticating more than one individual simultaneously.

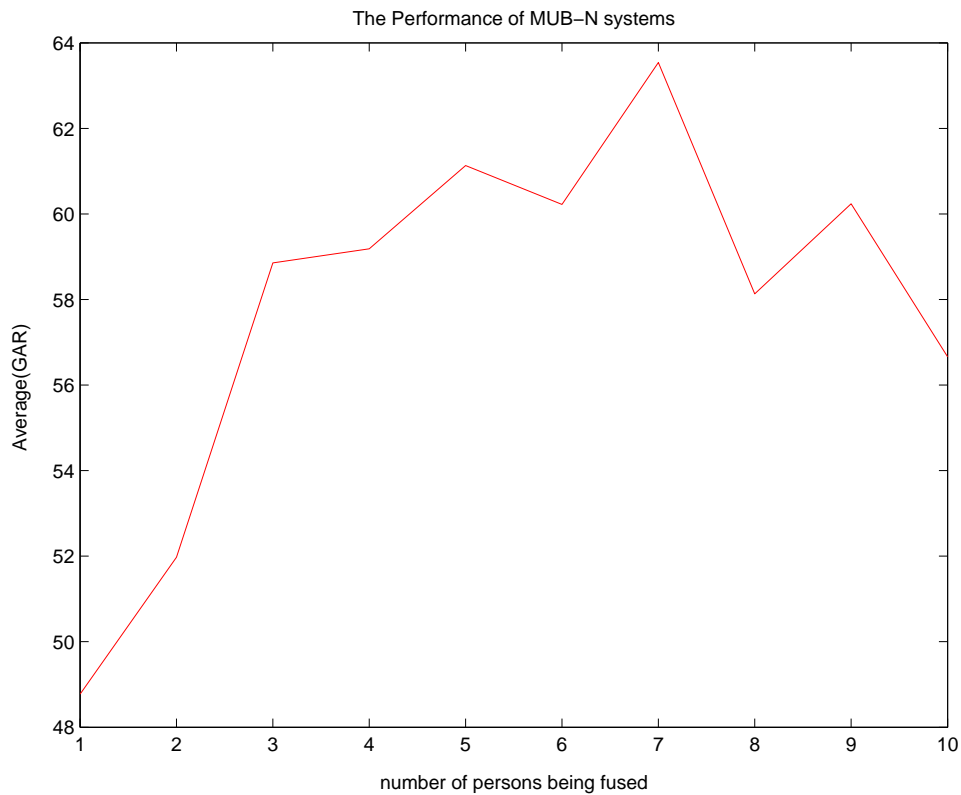


Figure 4.14: The performance of the MUB system increases as the number of people being fused increases, reaches a maximum and then starts to deteriorate.

4.8 Future work

Future work would include:

1. The experiments will be done using a larger data set (500 subjects).
2. Different matching schemes can be used to boost performance. This will increase the performance of both the MUB system and also that of the conventional biometric systems.
3. Feature reduction in the feature level fused MHB systems might improve performance.

4. Multi-human multimodal biometrics can be used to obtain higher performance. This involves the fusion of more than one biometric modality of a person with more than one biometric modality of other individuals.

Chapter 5

Multimodal biometric Databases

5.1 Introduction

Biometrics is a rapidly growing field offering plenty of opportunities for research especially in the areas of information assurance and access control. Data collection is central to all aspects of biometrics research and thereby essential to advancement of the state of art. Unfortunately biometric researchers face numerous hurdles due to the lack of reliable, accurate and adequate biometric data for their research. This was also true while procuring data for this thesis and also for other research projects being conducted at WVU. An appreciable amount of time is lost in data collection, which in most cases is unorganized, non-centralized and informal. This results in lack of data integrity and consistency, inferior data retrieval times, limited reusability of data and large amount of redundancy.

For example, in this thesis, it was difficult to obtain a database containing multimodal

information pertaining to hand and face. The few biometric databases that do exist are mostly unimodal, limited by age groups or race, non-centralized and are generally not made public. Therefore, we associated the hand and face data obtained from two independent databases under the assumption that the hand and face biometric traits of a person are independent.

This is the primary motivation behind the multimodal data collection effort initiated here in WVU i.e. to design a database system which would help researchers overcome the above mentioned hurdles and help facilitate research here and at the other participant universities. This chapter briefly outlines and discusses the key characteristics that make this centralized multimodal biometric data collection effort unique.

The establishment of a multimodal testbed database presents very important research questions in and of itself. These research questions primarily center around the data to be collected and the database design given the interplay of this design with the data requirements of researchers, the IP constraints of vendors, and the privacy needs for the subjects. With government agencies looking to multimodal biometric systems to address their authentication and identification needs, there is a critical need for understanding the issues and best practices associated with their database generation. The system to be developed here at WVU is a web enabled, centralized, multi-modal, unbiased and formal data store that is expected to alleviate some of the problems faced by researchers on a day-to-day basis.

5.2 Multimodal biometric databases

This section enumerates and briefly describes the different multimodal databases that currently exist.

5.2.0.1 M2VTS Multimodal Face and Voice Database [47]

The primary object of this project is to enhance the security of network-based services by enabling by automatic verification schemes combining multimodal biometric strategy (speaker recognition and face recognition). The database is made up from 37 different faces with five shots per individual taken at a week's intervals. During the data collection, the subject has been asked to count from '0' to '9' in their native language , rotate the head from 0 to -90 degrees, again to 0, then to +90 and back to 0 degrees (with/without glasses). From this whole sequence, 3 parts have been extracted : the voice sequence, the motion sequence and the glasses off motion sequence (if any). These are used for speech verification, 2-D/3-D face verification, speech/lips correlation analysis. A Hi8 video camera (576x720, 50Hz-interlaced, 4:2:2) was used for the image capture with D1 digital recorder. During the voice acquisition, the sound track is digitally recorded using a 48kHz sampling frequency and 16 bit linear encoding.

5.2.0.2 XM2VTS Multimodal Face and Voice Database [47]

The XM2VTSDB is an extension of the M2VTS project and is a large multi-modal database containing high quality digital video. The XM2VTSDB contains four recordings of 295 subjects taken over a period of four months. Each recording contains a speaking head shot and a rotating

head shot. Sets of data taken from this database include high quality color images, 32 KHz 16-bit sound files, video sequences and a 3D Model.

5.2.0.3 BioID Face, Voice and Lip movement [48]

The BioID multimodal database has been created in order to provide researchers with a benchmark to compare the quality of their face detection algorithms with those of their competitors. During data acquisition an effort was made to simulate real world conditions. Therefore, the data contains a variety of illumination, background and face sizes. This database comprises of 1521 gray level images pertaining to 23 users and having a resolution of 384x286 pixel. Each image contains the frontal view of a face. For comparison reasons manually set eye positions are also provided with each image in the database.

5.2.0.4 Notre Dame multimodal database [49]

The Computer Vision Research Laboratory at the University of Notre Dame has multimodal data sets containing facial images (multiple poses), hand geometry and ear images. The images were collected at the University of Notre Dame in two phases conducted approximately six weeks apart. The first was used to collect the gallery images and the second was to collect the probe images. The image acquisition was done using a Minolta Vivid 900 range scanner. A total of 275 different subjects participated in this study.

5.2.0.5 BANCA multimodal database [50]

The BANCA multi-modal database is intended for training and testing of multi-modal biometric systems. It contains two biometric modalities (face and voice). The data capture was done with both high and low quality acquisition devices (microphones and cameras). The collection were performed in three different environment namely controlled, degraded and adverse, over a time period of three months and contains a total of 208 subjects. The database would be available on the web for the research community.

5.2.1 Limitation of these existing multimodal biometric databases

The existing biometric databases have the one or all of the following disadvantages:

1. They may be restricted to a certain age group, community, race or gender.
2. They may not be freely available to the public.
3. They may not be web-enabled.

5.3 System Description

The database web server to be developed and deployed will be on a Linux based platform with Oracle 9i database management system as its back end ensuring that the data is safely stored and properly stored. The user-friendly web interface will be developed using PSP (PL/SQL server pages) and Java. It will operate on 3Ghz Intel xeon machine with 2GB RAM in order to aid memory and processor intensive data searches.

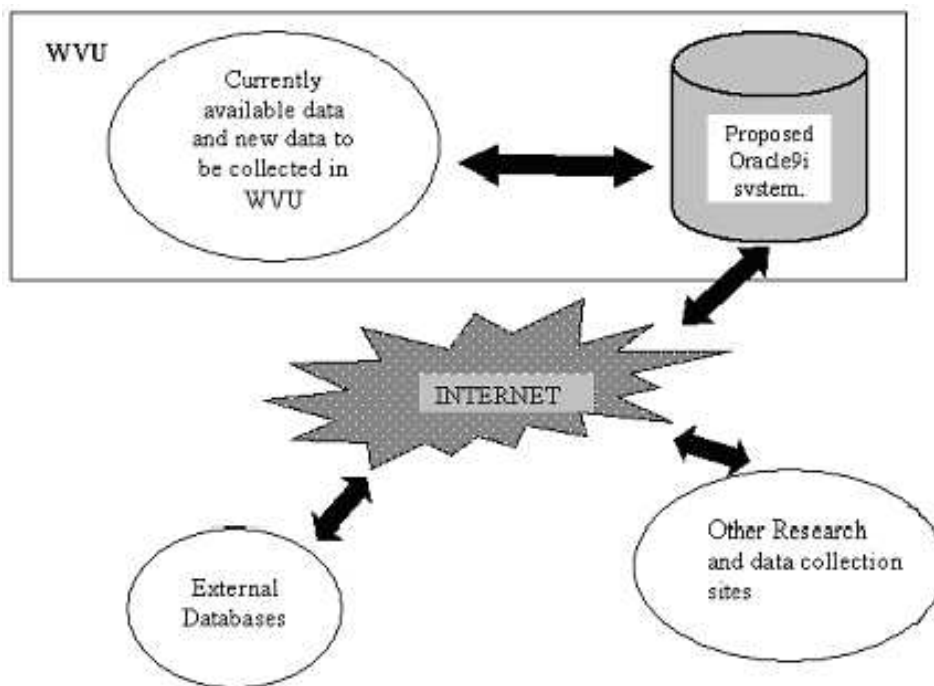


Figure 5.1: An overall view of the dataflow to and from the database to be developed.

5.3.1 System Features

The system being specially designed to meet the needs of personnel in the field of biometric research and testing has the following attributes making it very unique. These attributes are listed below and discussed in detail.

5.3.1.1 Centralized data store

Research in biometrics is an inter-disciplinary activity involving personnel from varied fields ranging from statistics to computer science to law enforcement agencies. Currently, there is no centralized system available to store the information in a secure, reliable and organized

fashion. This leads to an increased amount of time to locate relevant information, low sharing of information between researchers, data loss due to inefficient and unreliable storage, and lack of data consistency and integrity. There is a continuous transfer of raw data and other related information (e.g. ID card, collection date etc.) from one location to the other using conventional data transfer media (e.g. compact disks and floppy disks) that cannot be used when the data to be transferred is large. Current systems entail data replication at each research site leading to a loss in data consistency and integrity. There is also considerable cost involved in this periodic transfer of data. The proposed system will be web enabled and act as a central data repository to all involved researchers. It will make the data available to the researches in real time, and address the problem of periodic data transfer, data replication and loss of data integrity.

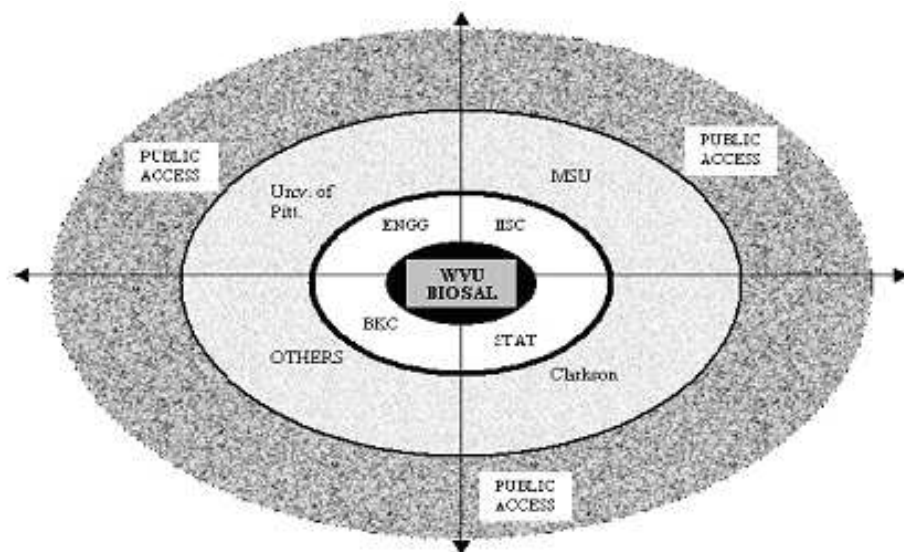


Figure 5.2: Data collected at different places are stored in one central repository, located in WVU.

5.3.1.2 Reliable and accurate

The process of data collection is the first step in most biometric research projects. It is usually done in an ‘informal’ fashion, without being guided by any protocol or rules. This results in a lot of variation in the data due to changes in environmental conditions, changes in biometric acquisition devices, etc., which in turn leads to erroneous results and produce incorrect conclusions. These problems can be overcome by carefully monitoring the data that is stored in the system. Any biometric data being stored will be labelled with information pertaining to the conditions under which they were obtained, the acquisition devices which were used, detailed information about the devices, the protocol adopted to capture the data and information about the data itself like resolution, file type, compression type, etc. This results in a reliable and accurate data source based on which concrete conclusions can be made.

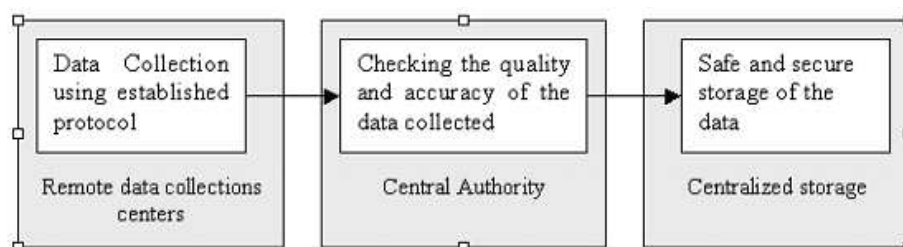


Figure 5.3: The data acquisition and storage process.

5.3.1.3 Multimodal

It is generally accepted that a single biometric in most cases is not sufficiently accurate to recognize a person. This has resulted in multimodal biometric systems that use more than one

physiological or behavioral characteristic to recognize an individual. A good database for multimodal data is very hard to find. This database will be designed to store the multimodal biometric data of a person over a period of time and, hence, act as a common data source for both multi and unimodal research.

5.3.1.4 Web-enabled

A joint research project conducted at two or more remote locations may need to share data and information in real-time. In such cases copying or transferring data using off line techniques creates redundancy, and lead to loss of data consistency and integrity. Being web-enabled this database will provide the functionality to share and access the data in real time, thus alleviating this problem. The web interface also provides other information and resources like abstract statistical information about the database, forms needed to request access to the database and other information that may be granted public access.

5.3.1.5 Time series biometric data

Liveness detection forms a very important part of current biometric research activities. The term ‘Liveness’ solves the problem of distinguishing between a living person and an artificial representation of person in a biometric system. The inability of a biometric system to detect liveness leads to spoofing. ‘Spoofing’ is the process of defeating a biometric system through fake biometric samples. There are new algorithms being developed in this field, most of which require biometric samples from live, cadaver and spoof subjects acquired small units of time (5s - 20s) in-order to analyze the temporal changes to the biometric to detect the liveness in them.

This database will have the ability to store multi-modal biometric. It will also store other related information such as the time of each capture and the time interval between captures.

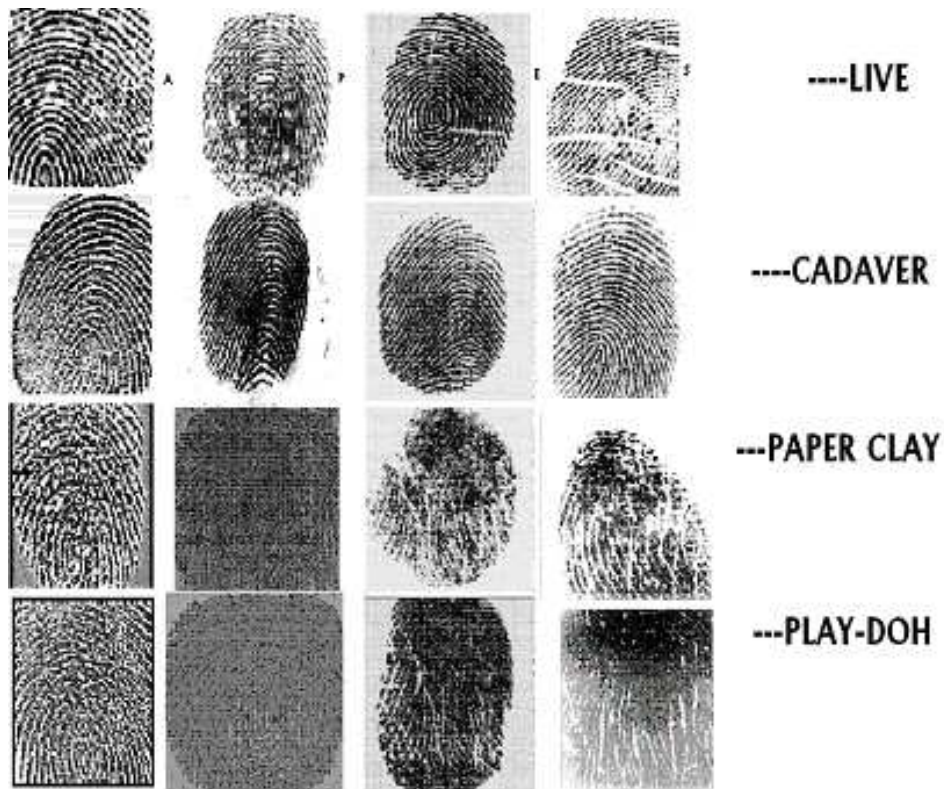


Figure 5.4: The fingerprint liveness data that will be stored in the system.

5.3.1.6 Template aging or biometric aging

Template aging refers to the changes that occur to a biometric data/time years due to environment conditions, natural aging of the human body, or wear and tear of body parts. Research in this field is greatly hampered due to lack of adequate biometric data acquired over a considerable period of time. This proposed system would help overcome this problem by acquiring and storing the

biometric information of an individual repeatedly over a number of years. It will also record the date of each data capture and the changes in the work or living environment of the individual (if any) from the time of last capture.

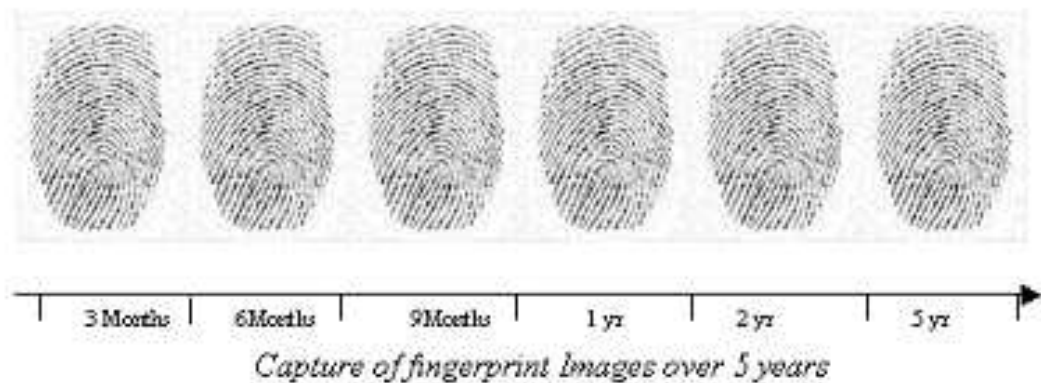


Figure 5.5: Research on template aging is being greatly hampered due to the non-availability of sufficient data. This problem will be addressed in this data collection effort.

5.3.1.7 Biographic data

There is a lot of information that can be associated with the biometric capture of person like gender, age, eye color, hair color, race, dialect and other details unique to each biometric modality. The details help to establish relationships and track associated variations in the biometrics, if any. The database will store this information along with the raw data. It will also store information like the date, time and place of capture, the information on the personnel who assisted during the capture, and the time taken to perform the capture.

5.3.1.8 Processed data and reusability

Processed data refers to the data that is obtained after certain operations are performed on the raw data in-order to improve their quality or to convert them into more usable form. For example preprocessing operations are necessary on fingerprint images to account for moisture, dry skin and dirt during the capture. There are many research projects, which operate on processed data rather than raw data. Storing and sharing processed data will save time and computational resources.

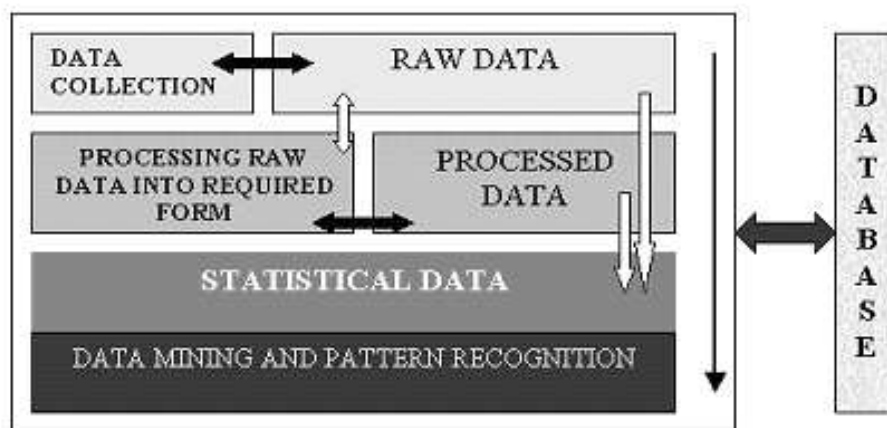


Figure 5.6: Data reuse is also a major advantage of this system. The data output of one research project can be used as input in another project.

5.3.1.9 Interface with existing databases

The database will be made to interface and exchange data with any good databases that are currently available. The decision to import data will be taken only after careful analysis of the data is done to check for its accuracy and reliability.

5.3.1.10 High Security

The web-enabled database will have high security, as the biometric data of a person is very sensitive information. For security reasons, user accounts will be created with password authentication, and different level of access to the data access will be provided through roles and privileges. Depending on the level of access granted, users will be able to view and modify the database information through a layer of database objects (views, procedures, functions etc.), and will not be access the tables directly. The computers that can access the database server will be restricted by IP addresses. The subjects providing the biometric information will be assigned unique ID number as id's and all their personal information will be stored in a encrypted form to prevent it from being associated with their biometric information. The data will be backed up on tape on regular basis and the database will record all changes to data.

5.4 Limitations

The proposed system is being designed in order to meet the current needs of the biometric research society comprehensively. But due to economic constraints, non-availability of data or equipment, or just to keep the system within a feasible scope in the first phase, certain constraints or limitations have been imposed on the system.

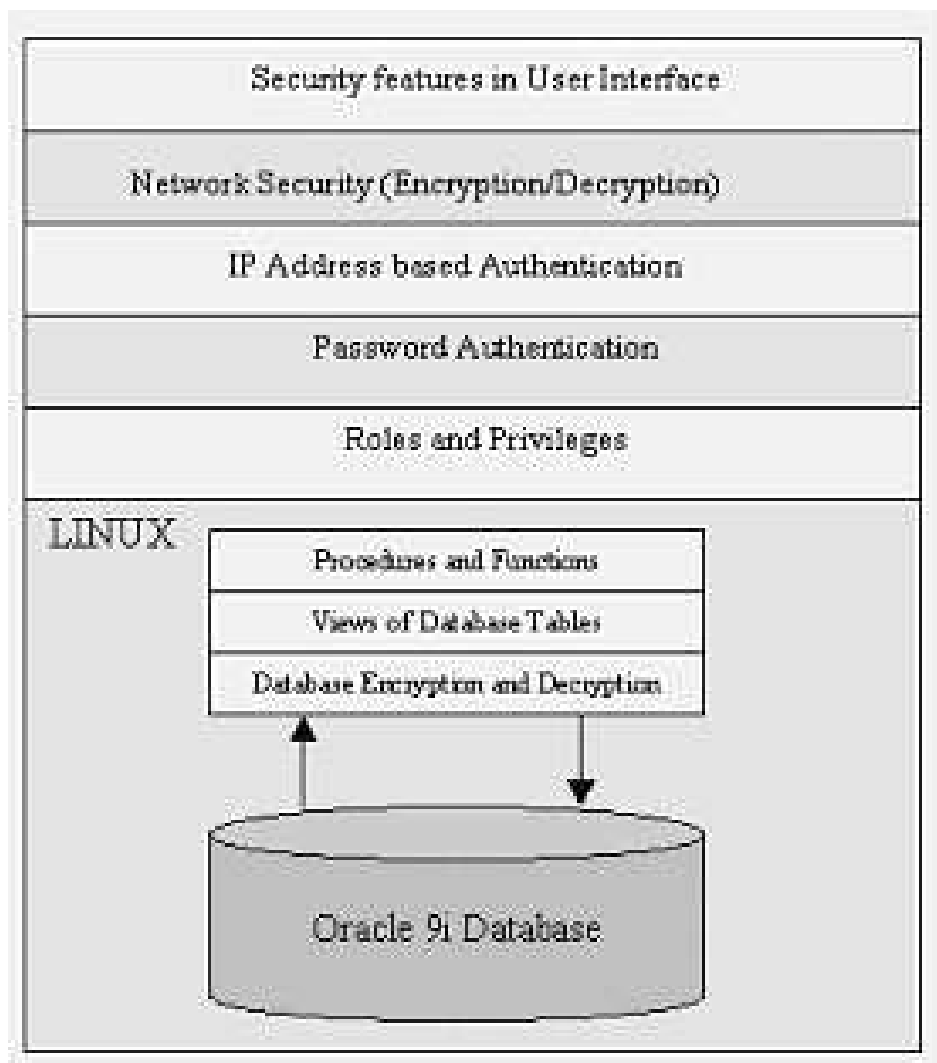


Figure 5.7: An elaborate security mechanism will be developed to safeguard the sensitive biometric data.

5.4.1 Data restricted to 2D information

The image data in all biometric modalities is restricted to two-dimensional information in the first phase of this project. This is due to the high procurement cost, limited availability of the equipment needed to procure three-dimensional biometric data. The technology is still immature

and the research being done using this kind of data is in very small scale. Therefore the inclusion of three-dimensional data will be addressed only in the phase II of the project.

5.4.2 Data Acquisition is driven by research requirements

The data collection needed to store data in the database is going to be done from remote locations. Data collection from each source is going to be biased based on the ongoing research at that location and their predictable future requirements. Therefore the data collected and stored may not comprehensively suit the requirements of all research projects.

A more detailed discussion with the technical details concerning the design and the architecture of the database, the problems and constrain faced during data collection etc. would be made available as the project progresses and a prototype system is brought into operation.

Chapter 6

Summary and future work

The Research community is investing a lot of effort in the field of multimodal biometrics. Match level fusion and decision level fusion have been extensively studied in the literature while feature level fusion is a relatively understudied problem. The following are the contributions of this thesis towards feature level fusion:

1. **Feature level fusion:** It has been shown that the fusion of multiple modalities at the feature level can result in lower error rates as opposed to fusion at the match score level or decision level. The resulting template is also much more secure than the regular biometric template and would not be susceptible to biometric reconstruction techniques. Data preprocessing techniques like feature selection and normalization have been shown to help make feature fusion a viable technique.
2. **Criterion function:** The need for a good criterion function to perform feature selection is demonstrated. The effect of EER, GAR and FAR as criterion functions is discussed and

their weaknesses are identified. The average of GAR at four different values of FAR is shown to be a relatively robust criterion for feature selection.

3. **Thresholded Absolute Distance:** A reliable distance measure called Thresholded Absolute Distance (TAD) has been introduced in this thesis. The performance of TAD is compared to the performance of the Euclidean distance measure in order to demonstrate its relatively superior robustness towards noise in data. It is shown that TAD and Euclidean distance compliment each other's disadvantages and hence work well together.
4. **Information fusion across fusion levels:** The merging of information across match and feature fusion levels has helped to further improve the performance of a multimodal biometric system. They can be used to determine an approximate upper bound in multimodal biometric matching performance. Two methods (feedback & comprehensive) were discussed as ways to merge information across fusion levels.
5. **Usage of weak modalities:** Weak classifiers (MSU Hand and MSU Face) have been used together to obtain a relatively high performance. Fusion of strong biometrics will further improve performance.
6. **Multi-user Biometrics:** A novel application called multiuser biometrics has been proposed for effective biometric authentication with group consensus. It has shown to increase the performance substantially relative to conventional means of authenticating multiple users.

7. **Multimodal biometric databases:** The main features that go into the development of a multimodal research database have been enumerated and briefly discussed.

I would like to conclude this thesis with a short list of future work that might help to further enhance the system. They are as follows:

1. It is required to address issues related to incompatible feature sets and high-dimensional feature sets.
2. The experiments must be performed using larger data sets (500 subjects)
3. Different matchers should be tried in order to establish the inadequacies of matchers of single modalities for a feature fused template

Bibliography

- [1] A. Ross, A. K. Jain, and Jian Zhong Qian, “Information Fusion in Biometrics,” *Proc. 3rd International Conference on Audio- and Video-Based Person Authentication (AVBPA)*, pp. 354-359, 2001.
- [2] A.Ross, K.Nandakumar, and A.Jain, “Score Normalization in Multimodal biometric systems,” To appear in pattern recognition journal.
- [3] G.V. Trunk, “A Problem of Dimensionality: A Simple Example,” *IEEE Trans. Pattern Analysis and Machine Intelligence*, Vol. 1, No. 3, pp. 306–307, 1979.
- [4] Ferri et al., “Comparative study of techniques for large-scale feature selection,” *Pattern Recognition in Practice IV* (Gelsema and Kanal, eds.), Elsevier, pp. 403–413, 1994.
- [5] A. K. Jain, A. Ross, and S. Pankanti, “A prototype hand geometry-based verification system,” in *Second International Conference on Audio and Video-based Biometric Person Authentication*, pp. 166–171, 1999.
- [6] M. Turk and A. Pentland, “Eigenfaces for recognition,” *Journal of Cognitive Neuroscience*, Vol. 3, No. 1, pp. 71–86, 1991.

- [7] A. K. Jain, R. P. W. Duin, and J. Mao, "Statistical Pattern Recognition: A Review," *IEEE Trans. on Pattern Analysis and Machine Intelligence*, Vol. 22, No. 1, pp. 4–37, 2000.
- [8] S. Watanabe, "Pattern Recognition: Human and Mechanical," New York: Wiley, 1985.
- [9] Duda, Hart and Stork, "Pattern Classification," 2nd edition, Wiley-Interscience, 2000.
- [10] A.J Mansfield and J.L.Wayman, "Best Practices in testing and reporting performance of Biometric Devices," *National Physical Laboratory*, 2002.
- [11] A.K. Jain, R. Bolle and S. Pankanti (Eds.), "BIOMETRICS: Personal Identification in Networked society," 1st edition, Kluwer Academic Publishers, 1999.
- [12] Biometric consortium "An introduction to biometrics," available at:
(<http://www.biometrics.org/html/introduction.html>).
- [13] A. K. Jain, A. Ross and S. Prabhakar, "An Introduction to Biometric Recognition," *IEEE Trans. on Circuits and Systems for Video Technology*, Special Issue on Image and Video Based Biometrics, Vol. 14, No. 1, pp. 4–20, 2004.
- [14] A. K. Jain and A. Ross, "Multibiometric Systems," *Communications of the ACM*, Special Issue on Multimodal Interfaces , Vol. 47, No. 1, pp. 34–40, 2004.
- [15] Y. Wang, T. Tan, and A. K. Jain, "Combining face and iris biometrics for identity verification," *4th Audio and Video based Person Authentication*, 2003.

- [16] K. Chang, K. Bowyer, V. Barnabas, and S. Sarkar, "Comparison and combination of ear and face images in appearancebased biometrics," *IEEE Trans. on Pattern Analysis and Machine Intelligence*, Vol. 25, pp. 1160-1165, 2003.
- [17] G. Shakhnarovich and T. Darrell, "On Probabilistic Combination of Face and Gait Cues for Identification," *Intl Conf. on Automatic Face and Gesture Recognition*, pp. 169-174, 2002.
- [18] R. Frischholz and U. Dieckmann, "BioID: A multimodal biometric identification system," *IEEE Computer*, Vol. 33, No. 2, pp. 64-68, 2000.
- [19] S. Ben-Yacoub, "Multi-modal data fusion for person authentication using SVM," *Audio and Video based Person Authentication*, pp. 25-30, 1999.
- [20] L. Hong and A. Jain, "Integrating faces and fingerprints for personal identification," *IEEE Trans. on Pattern Analysis and Machine Intelligence*, Vol. 20, No. 12, pp. 1295-1307, 1998.
- [21] E. Bigun, J. Bigun, B. Duc, and S. Fischer, "Expert conciliation for multi modal person authentication systems by bayesian statistics," *Audio and Video based Person Authentication*, pp. 311-318, 1997.
- [22] J. Kittler, G. Matas, K. Jonsson, and M. Sanchez, "Combining evidence in personal identity verification systems," *Pattern Recognition Letters*, No. 9, pp. 845-852, 1997.
- [23] R. Brunelli and D. Falavigna, "Person identification using multiple cues," *IEEE Trans. on Pattern Analysis and Machine Intelligence*, Vol.17, No.10, 1995.

- [24] A. Kumar, D. C. M. Wong, H. Shen, and A. K. Jain, "Personal verification using palmprint and hand geometry biometric," *Proc. Audio and Video based Person Authentication*, pp. 668–675, 2003.
- [25] A. Kumar, D. Zhang, "Integrating palmprint with face for user authentication," *Proc. Multi Modal User Authentication*, pp. 107–112, Dec 2003.
- [26] K. Chang, K. Bowyer and P. Flynn, "Face recognition using 2D and 3D Faces," *Proc. Multi Modal User Authentication*, pp. 25–32, 2003.
- [27] L. Hong, A. Jain and S. Pankanti, "Can Multibiometrics Improve performance?," *Proceedings AutoID'99*, pp. 59–64, 1999.
- [28] L. Lam, C. Y. Suen, "Application of Majority Voting to Pattern Recognition: An Analysis of Its Behavior and Performance," *IEEE Transactions on Systems, Man, and Cybernetics*, Part A: Systems and Humans 27 (5), 553-568, 1997.
- [29] L. Lam, C. Y. Suen, "Optimal Combination of Pattern Classifiers," *Pattern Recognition Letters* 16, pp. 945-954, 1995.
- [30] L. Xu, A. Krzyzak, C. Y. Suen, "Methods for Combining Multiple Classifiers and their Applications to Handwriting Recognition," *IEEE Trans. on Systems, Man, and Cybernetics* Vol. 22, No.3, pp. 418-435, 1992.
- [31] J. Daugman, "Combining Multiple Biometrics,"
available at: (<http://www.cl.cam.ac.uk/users/jgd1000/combine/combine.html>).

- [32] Hill, C.J., "Risk of Masquerade Attack from the storage of Biometrics," B.S. Thesis, Australian National University, 2001.
- [33] Adler A., "Sample images can be independently restored from face recognition templates," University of Ottawa, 2003.
- [34] Martin, A. F. Phillips, P. J. Przybocki, M. A. Wilson, "Introduction to Evaluating Biometric Systems," *IEEE Computing in Science and Engineering*, 2000.
- [35] Huayan Amy Wang, Diana Melick, Rick Vollkommer, Bruce Willins, "Lessons learned from iris trial," *Biometric Consortium Conference*, 2002.
- [36] S. A. C. Schuckers, L. Hornak, R. Derakshani, S. Parthasaradhi, "Making Biometrics Spoof-Proof," *Proc of Biometrics*, 2002.
- [37] Recognition Systems Inc., available at (http://www.handreader.com/products/acs/op_handreader_enclosures). Last accessed on 'June 24 2003'.
- [38] Crihalmeanu, Musat C. (2003), "Adding Liveness Detection To The Hand Geometry Scanner," Master's Thesis, West Virginia University.
- [39] R. A. Fisher, "The use of Multiple Measurements in Taxonomic Problems," *Ann. Eugenics.*, vol. 7, pp. 179–186, 1936.
- [40] Kruskal, J. B., and Wish, M. "Multidimensional Scaling," Beverly Hills, California: Sage, 1978.

- [41] A. Djouadi and E. Bouktache, "A Fast Algorithm for the Nearest- Neighbor Classifier," *IEEE Trans. Pattern Analysis and Machine Intelligence*, Vol. 19, No. 3, pp. 277–282, 1997.
- [42] W. Siedlecki and J. Skalsky, "On automatic feature selection," *International Journal of Pattern Recognition and Artificial Intelligence*, 197–220, 1988.
- [43] P. Pudil, J. Novovicova, and J. Kittler, "Floating Search Methods in Feature Selection," *Pattern Recognition Letters*, Vol. 15, No. 11, pp. 1119–1125, 1994.
- [44] S.K. Mishra and V.V. Raghavan, "An Empirical Study of the Performance of Heuristic Methods for Clustering," *Pattern Recognition in Practice*. E.S. Gelsema and L.N. Kanal, eds., pp. 425–436, 1994.
- [45] K. Rose, "Deterministic Annealing for Clustering, Compression, Classification, Regression and Related Optimization Problems," *Proc. of IEEE*, Vol. 86, pp. 2,210–2,239, 1998.
- [46] Center for Identification Technology and Research, available at: (www.csee.wvu.edu/citer).
- [47] Extended Multi Modal Verification for Teleservices and Security applications, available at: (<http://www.ee.surrey.ac.uk/Research/VSSP/xm2vtsdb/>).
- [48] HumanScan Inc - BioID Database, available at: (<http://www.humanscan.de/support/downloads/index.php>).
- [49] The multi-modal biometric data collection at the university of Notre Dame, available at: (<http://www.nd.edu/%7Ecvtl/UNDBiometricsDatabase.html>).
- [50] Enrique Bailly-Bailliere, Samy Bengio, Frederic Bimbot, Miroslav Hamouz, Josef Kittler, Johnny Mariethoz, Jiri Matas, Kieron Messer, Vlad Popovici, Fabienne Poree, Belen Ruiz,

and Jean-Philippe Thiran, “The BANCA Database and Evaluation Protocol”, available at:
(<http://www.ee.surrey.ac.uk/Research/VSSP/banca>).