Comparative Study of Normalization Techniques Used for the Fusion of Different Biometric Traits

A Thesis submitted in partial fulfillment of the
requirements for the award of degree of

Master of Engineering
in
Electronic Instrumentation and Control

Submitted by
SANTOSH KUMAR
(Roll No. 801051018)

Under the Guidance
Of
Dr. Sunil Kumar Singla
Assistant Professor

Department of Electrical and Instrumentation Engineering

Thapar University
(Established under the section 3 of UGC act, 1956)

Patiala, 147004, Punjab, India

July 2012

DECLARATION

I hereby certify that the work is presented in the thesis entitled **"Comparative Study of Normalization Techniques used for the Fusion of different Biometric Traits"** in partial fulfillment of the requirement for the award of degree of **Master of Engineering** in **Electronics Instrumentation and Control** submitted in Electrical and Instrumentation Engineering department, Thapar University, Patiala is an authentic record of my own work carried under the supervision of **Dr. Sunil Kumar Singla,** Assistant Professor, Department of Electrical and Instrumentation Engineering, Thapar University, Patiala, Punjab.

Date: 28/06/2012

(Santosh Kumar)

801051018

I certify that the above statement made by the student is correct to the best of my knowledge and belief.

28/6/2012

Date:

(Dr. Sunil Kumar Singla)
Assistant Professor,
Department of Electrical
and Instrumentation Engineering,
Thapar University, Patiala,
Punjab

S. Ghosh 3/7/12

Countersigned by

(Dr. Smarajit Ghosh)
Head of Department,
Department of Electrical and
Instrumentation Engineering,
Thapar University, Patiala,
Punjab

(Dr. Saroj Kumar Mohapatra)
Dean of Academic Affairs,
Thapar University, Patiala,
Punjab

II

ABSTRACT

These days biometric are one of the fundamental technologies that are being used for individual authentication in many industrial, confidential and domestic applications. When we consolidate the information from one biometric trait, is known as unimodal biometric. However unimodal systems are reliable, still the popularity of these systems is degrading due to the problems such as noisy sensor data, non-universality and spoof attacks. These limitations can be overcome if we fuse more than one trait to make a system called Multibiometric system. The research work demonstrated in this thesis describes fusion of the multiple biometric traits at score-level. The research work has been stressed around only identification mode i.e. fusion of face, left index finger and right index finger biometrics in the two recognition modes of verification and identification. The experimental approach in this study is also extended to the combination of transformed (normalized) score with fuzzy logic fusion. The results obtained after the experiment depict that, integrating the information at score level is more effectual than the use of single biometric trait. The thesis confronts an exhaustive description of the systematic investigation to establish facts undertaken for the purpose of authentication. This exhibits the consequences on the basis of experiment in terms of False Rejection Ratio and Genuine Acceptance Rate and provides a broad investigation on a moderate database.

In this thesis, the problem of score level fusion related to different range of data has been addressed. Due to the heterogeneous nature matching scores of the various biometric traits, score normalization is required to transform these scores into a common domain prior to fusion. The normalization schemes have been evaluated both in terms of their efficiency and robustness to the presence of outliers in the training data. We have developed an experimental environment based on transformation for the successful execution of the plan.

Further, a fuzzy logic based fusion system has also been developed to fuse three biometric traits. The advantage of using fuzzy logic is its ease of use and flexibility. With the help of fuzzy logic based system 91.3% genuine acceptance rate has been achieved.

ACKNOWLEDGEMENT

First and the foremost, I would like to thank my father Shri Ramesh Chandra and my mother Smt. Sarla Devi for all their approvals and blessings. Without their moral or psychological support and Encouragement at essential periods of my life, it would not have been possible for me to quest for post graduate studies and objective for greater affairs in my vocation. Their hard work and convinced posture is my main source of divine guidance. I am proud to dedicate this thesis and all the good things in my life to them.

Taking this opportunity I would like to express my gratitude to my very helpful supervisor Dr. Sunil Kumar Singla for his supervision, guidance and support. I am thankful for rendering me the chance to work in a stimulating and ambitious field of research. His invariable motivation, support and infectious exuberance have led me towards the productive completion of this dissertation. My regular interactions with him have been of immense assistance in determining my research aims and in distinguishing directions to accomplish them. His promoting and encouraging discussions have often forced me to put in my best potential efforts. I am hopeful that my M.E. experience with him would go forward as an unforgettable and productive for the further guidance in future.

I am also thankful and would like to acknowledge about my colleague and sister who played a major role throughout my research. She is the most valuable gift that God has blessed me. I am exceedingly fortunate to have her company. She is an honest friend and a very good judge. I will always remember the words, she used to say me "Do your work, don't think about result".

Place: Thapar University, Patiala

Date:

(Santosh Kumar)

801051018

IV

TABLE OF CONTENTS

LIST OF FIGURES

Figures **Page No.**

LIST OF TABLES

Table **Page No.**

CHAPTER 1

INTRODUCTION

The process of identity management leads to the creation, accumulation, maintenance and sometimes spoofing the identities of individuals in the target population. Conventionally, identity of any person refers to a set of characteristics (e.g., name, password, token, etc.) that are associated with that person. In order to increase the reliability along with improving the resistance against the epidemic growth in spoof attacks and to meet the increased security requirements in a variety of applications ranging from international border crossing to accessing personal information. Determining the identity of a person is known as individual's authentication which is a difficult task in any identity management system. Few ways to determine an individual are "something you know" (e.g., password, personal identification number), "something you carry" (e.g., physical key, ID card) and "something you are" (e.g., face, voice) [1]. This introduces numerous problems because sometimes it is very easy for application programmers to crack the password. Also risk of stolen identity and the risk of compromising the template are some of the most publicized issues and frequently cited in relation to the security of conventional identity management systems [2, 3].

Estimates taken from the report by the National Institute of Standards and Technology (NIST) reveals [4] that password generated by 7 bits/character (ASCII) provides only 18 bits of entropy, where as the security expectation is of 56 bits. Also, passwords and ID cards cannot provide critical recognition such as, non-repudiation and detecting multiple enrollments. True identity of an individual can be easily spoofed by presenting fake or duplicate verification documents. Therefore, it is important to develop such systems that are reliable and produce stronger authentication schemes based on "something you are", namely biometrics.

1.1 Biometric System

Biometric is one of hyped technology that set in motion for identifying a person or verifying the identity of a person based on a physiological or behavioral characteristic. The Biometric is a Greek word in which bio stands for life and metric for the measurement. Now days, a

wide variety of the biometric systems are available in the market which employ reliable and secure authentication methods to confirm the identity of person when he presents his/her identity to the system. Some examples of such system includes, insure admittance to buildings, control systems, mobile phones, laptops and many confidential areas. Hence, it is possible to setup an identity by considering "who you are" rather than by "what you have" [5] such as identification cards and passwords. Security is one of the most favoured applications of the biometrics. Some of the physiological and/or behavioral characteristics that are being used for the biometric recognition include face, retina, palm print, DNA, hand-geometry, ear, voice, finger print, gait, signature, key-stroke dynamics and iris [6].

1.2 History of the Biometric

In the ancient Egyptians times, the identification of any individual was done on the basis of measurement of the physiological characteristics such as height, eye color etc. Ancient China, Babylonia and Assyria, associated the person's identification through archaeological evidence of fingerprints. Later in the 19^{th} century, biometric came into existence for crime detection. Alphonse Bertillon, a French police clerk and anthropologist, developed a recording method where different body measurements, physical descriptions and photographs were used for identification purpose. During the 1890s, this identification method was adopted by many police authorities for crime detection, but soon it became obsolete since people shared the same physical measurements [7,8]. A British anthropologist, Sir Francis Galton, developed a physical identifier that was unique to every individual. He worked on the principle that fingerprints were permanent throughout life, and that no two people had identical fingerprints [9]. Galton calculated the odds of fingerprints from two people being identical to be 1 in 64 billion and also identified the characteristics which are known as minutiae. Minutiae are still used today for matching two impressions made by the same finger. The fingerprints were classified as whorl, arch and loop by Galton [7, 10].

In 1897, Sir Edward Henry and colleagues modified Galton's observations, where fingerprints were captured on paper using an ink pad to be classified, filed and referenced for comparison against thousands of others. By 1901, Henry's fingerprinting method was adopted by Scotland Yard in UK [11] and later, it was used worldwide as a standard method of identity detection and verification in criminal investigation. In 1904, United States at Leavenworth, Kansas and

the St. Louis, Missouri established fingerprint bureaus. In 1921, the "Identification Division of the FBI" was set up [12]. In 1936, Ophthalmologist Frank Burch introduced a new concept of using iris patterns as a method to recognize an individual [13]. In 1960, W. W. Bledsoe developed the first semi-automatic facial recognition system. In this system, the facial features such as eyes, ears, nose & mouth are located on the photographs and distances & ratios are calculated to a common reference point which was compared to the template data [14]. A system based on the analysis of X-rays of individuals describing the physiological components of acoustic speech production was introduced by A Swedish Professor, Gunnar Fant in 1960. Dr. Joseph Perkell, in 1970, extended this model by including the tongue and jaw and a more complex behavioral and biological component of speech was provided[15]. In 1974, the first hand geometry recognition system came into existence for applications such as in physical access control, time & attendance and personal identification. In 1977, a patent was awarded for the personal identification apparatus that was able to acquire dynamic pressure information [15]. In 1985, David Sidlauskas was awarded the patent for hand geometry for identification. In 1987, the face recognition problem was solved using the principle component analysis algorithm by Sirovich et al. [16]. This was a great achievement since it showed that less than one hundred values were required for approximating a suitably aligned and normalized face image. In 1994, Dr. John Daugman contributed a lot of research in the area of iris based biometric recognition and was awarded a patent for his iris recognition algorithms.

In 1998, a Combined DNA Index System (CODIS) was launched by the FBI to digitally store, search and retrieve DNA markers for forensic law enforcement purposes. In 2001, the first research paper on hand vein pattern biometric recognition system was published by Lm et al. [17]. In 2002, for supporting the standardization of generic biometric technologies, the International Standardization organization (ISO) established the ISO/IEC JTC1 Subcommittee 37 (JTC1/SC37) [16]. The Subcommittee developed the standards to promote interoperability and data interchange between applications and systems. In 2003, the European Biometric forum was established. In 2004, Connecticut, Rhode Island and California established statewide palm print databases that allow law enforcement agencies in each state to submit unidentified latent palm prints to be searched against each other's database of known offenders [18]. In 2005, NIST along with national security agency of USA sponsored a

number of biometric-related activities including the development of a common biometric exchange file format (CBEFF), NIST biometric interoperability, performance and assurance working group etc. [19]. In 2006, the department of passport USA (United States of America) started issuing the biometric passports to diplomats and other officials. These biometric passports were later issued to the public, in 2006 [20]. In 2009, National Authority for Unique Identity was set up by the Indian government to provide multipurpose national identity card to each of its 1.25 billion people, carrying the biometric information of the individuals [21].

1.3 Biometric Modalities for Identification

A Number of biometric traits have been used in the development of the biometric based authentication systems. Few of them are explained below.

1.3.1 Fingerprint Recognition: In fingerprint recognition system we required an image of the fingerprint either using scanner or ink as it is shown in the Figure 1.1. These images are then used to fetch the characteristics like loops, whorls, and arches patterns of ridges and minutiae. There are various encoding and decoding methods available for accumulating and processing these characteristics. When a person leaves his/her finger on the sensor, he/she can we identified or verified on basis of matching of previously saved templates. Fingerprint recognition system is very accurate and stable, and it can be used to enroll multiple fingers to increase the anti-spoofing property [22]. Some of the disadvantages of this method are that the sensor may get dirty and can give false result due to the presence of the residual of previous user. Database and template making may vary depending on the skin conditions of the different users [23].

Figure 1.1 Fingerprint images for recognition

1.3.2 Facial Recognition: It is the most natural means of biometric identification [24]. The facial recognition mainly works on the principle of distance measurement between the nose, mouth, eyes, and jaw edges, as it is depicted in Figure 1.2. These characteristic are then used to create the database/template. Hence for verification or identification of any person, an image of the person is taken using a camera and template is then compared to the characteristic of this image, which is already stored in the database.

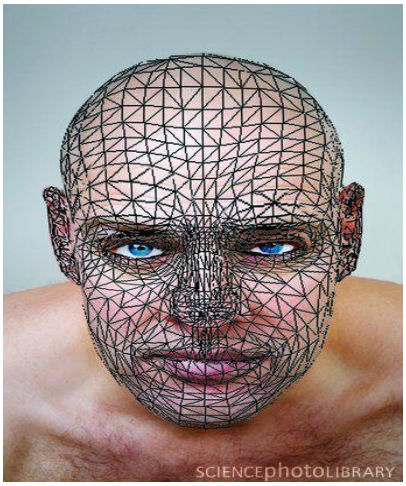


Figure 1.2 Facial image used as biometric trait

The advantage of facial recognition system is that it is non intrusive in nature. One of the major disadvantages of the facial recognition technique is that they are highly dependent on the quality of the image, which normally affected when low quality camera used or due to the environmental factors. System sometimes fails in verification process of identical twins [23].

1.3.3 Hand Geometry: The hand geometry recognition system uses a sensor, as shown in Figure 1.3, which has a metal surface in which some wooden pin are pushed or driven into the metal surface. When any user places his hand on the metal surface, this instrument reads about 90 characteristics of the hand, e.g. length of hand and fingers, thickness, surface area, width, of the finger and palm size [25]. These characteristics are used to create the database, and when a person places his hand on the device he can be verified on the basis of comparison with stored templates.

Figure 1.3 Hand geometry recognition used as biometric trait

This recognition system has a high user acceptance and is non intrusive. This method has a disadvantage as it occupies large area and the people suffering from arthritis, missing finger, or large hands might find it difficult to enroll.

1.3.4 Iris Recognition: Iris recognition system recognizes every individual on the basis of the characteristics that subsist in the colored tissues of the pupil. An iris image used for the biometric authentication is shown in the Figure 1.4. These tissues may lies in rings, groove and in the small brownish spot. In iris recognition system, the database is formed by taking the picture of the iris by some normal camera or video camera. While taking the image, the support of the user is required to get the clear and non-blurred image at the time of the verification the user is asked to put his eye in front of the light coming from the device and on the basis of template matching the user is declared as genuine or imposter. This is one of the most accurate biometric technologies that are available, because iris data never changes with age, and remain stable and identical for left and right eyes [26].

Figure 1.4 Iris image used as biometric trait

1.3.5 Signature Recognition: This recognition system works with behavioral characteristic of a person such as change in pressure, speed of signing, overall size of signature and various directions of movement during the flow of the signing[27,28]. The instrument consists of a stylus and a writing sheet in the form of the tablet which is connected to a computer as shown in the Figure 1.5. When user signs on the tablet using stylus the local computer connected to it accumulate the behavioral information and used to create the database. Device used here is a noninvasive tool, so it is not only widely accepted also difficult to mimic. It has certain limitation such that the signature should not be too long or too short. Problem with the long signature is that they have too many information which may lead to form a large database and the problem with the small signature is that they have only few information for unparalleled database creation.

Figure 1.5 Signature recognition used as biometric trait

1.3.6 Gait Recognition: Gait recognition technology is one of the most accurate and stable technology which uses idiosyncratic behavior of any individual to recognize him. Gait recognition technology works on dignified mode of walking of a person as illustrated in the Figure 1.6, and user can be taken under the observation without permission of the user. Gait parameters are very typical to Prevent from being seen and to make fool. Factors like hydroxyl compounds and drugs due to which a person may present unbalanced characteristics, pressure changes in pregnancy, accident, weight gain or weight loss, and the clothes worn by them may degrade the accuracy and stability of the system. Gait recognition process is done using close circuit cameras, so it is possible to perform these processes from

a distance. The only disadvantages of gait recognition process are that it can be easily fooled by foreground scenes, clothes and emotional status of the person.

Figure 1.6 Gait recognition used as biometric trait

1.3.7 Key Stroke Recognition: Keystroke Recognition is works on the principle that every individual types the computer keyboard in different manner, as illustrated in Figure 1.7. In key stroke recognition, a person is asked to type a certain set of word on a keypad that is connected to a computer. When a person is type these set of words, he should do this without any error or correction. If he is fail to do this is more attempts, he will be recognized as an imposter. Features that are taken in account are the way a person types, typing speed, propagation time between successive keys or words, time for each key is pressed down, different rate observation in capital and small letter [29]. These behavioral characteristics are used to make database for every individual. This technique has a unique advantage of not having too much hardware, hence only software required.

Figure 1.7 Keystroke recognition used as biometric trait

1.3.8 DNA (Deoxyribo Nucleic Acid): Since the discovery of the DNA, it has been used in many applications. The main sources of DNA are Blood, Semen, Tissues, Hair Roots, Saliva,

Urine, etc. DNA patterns are long helical string of the molecules of chemical building blocks known as “nucleotides” as shown in figure 1.8. DNA recognition technology is not only used by the forensic personals but also to find out blood relationships. In transplants process DNA are used to match the organs of donors and recipient [30]. So this technology can also be used to identify the authentication of a person. These features make this technique to achieve an extremely high degree of reliability and accuracy as compared to other biometrics. It has certain disadvantages such as DNA samples are having a tendency of combining with and contaminating by external sources.

Figure 1.8 DNA recognition used as biometric trait

1.3.9 Voice Recognition: Voice is a combination of physiological and behavioral biometric. The different features in an individual’s voice which are to be used for verification are based on the shape and size of the appendages such as, vocal tracts, mouth, nasal cavities & lips [23]. These physiological characteristics of human speech are invariant for an individual, but the behavioral part of the speech of a person changes over time due to age, medical conditions such as common cold, emotional state, etc [31].

The automatic recognition process of the human voice is often divided in speech recognition and speaker recognition [32]. These two areas use the same input signal (the voice), but have different purposes, where the speech recognition aims the translation of spoken words into text, while the speaker recognition wants to identify the person who is talking. This method captures the sound of the speaker's voice as well as the linguistic behaviors. The speaker-specific characteristics of speech are due to differences in physiological and behavioral aspects of the speech production system in humans [33]. These systems rely on very low-cost devices and are generally the least expensive systems to implement for large numbers of users. The acceptability level is very high in this type of biometric system. It allows a remote

verification using the phone such as phone banking but these systems have few disadvantages such as mimicry by imposter or recording the voice of the authorized person or emotional statement of the authorized person [23].

1.3.10 Palm Print: Palm print recognition deals with the inner surface of our palm which contains three flexion creases, secondary creases and ridges. The flexion creases are known as the principle lines whereas the secondary creases are called as the wrinkles. The flexion creases and the main creases are formed between the 3rd and 5th months after conception [34] and superficial lines appear after birth. These creases cannot be determined genetically. Even identical twins who share the same DNA sequences have different palm print [35].

This non-genetic determination and complex patterns have rich information for an individual's identification. The research area involves two types of palm print recognition, viz high resolution and low resolution as shown in Figure 1.9. High resolution approach is suitable for forensic applications such as criminal detection, while low resolution is more suitable for civil and commercial applications such as access control.

Figure 1.9 Palm print (a) High resolution image (b) Low resolution image

The advantage of using palm print is that they cannot be acquired without the knowledge of the person. Moreover, the uniqueness and permanence of palm print is also high while its universality is medium.

1.4 Sensor & Data Acquisition

The adroitness of a biometric system to adapt the raw data is the essential exercise. This ability of the biometric systems for the data acquisition and providing the high quality information at the very first stage of the sensors, determines the sensor incisiveness.

Acquisition Module interprets the biometric data into digital form. More precisely finger print biometric sensors are the integrated circuits with embedded principles and algorithms that are required for user authentication. When one places his/her finger on the chip they produce the electrical signal for the finger print images. Biometric sensors are semiconductors with embedded algorithms that are used in security systems or environments that require user authentication. They produce electrical signals from fingerprints or other physical characteristics in biometric access control systems. Biometric sensors consist of an array of tiny electrodes and an analog-to-digital converter (ADC) that digitizes information from the sensor array. In fingerprint access control systems, the user presses an index finger to a scanning device that includes a biometric sensor. The varying capacitive values across the sensor array are then converted into an image of the fingerprint. Other components of the biometric access control system then compare the image to a stored template.

Selection of biometric sensors needs an analysis of product specifications and features. Specifications include resolution, size, image area, operating current, standby current, voltage, frame rate, operating temperature, programmable gain, signal-to-noise ratio, interfaces and integrated circuit (IC) package type. Universal serial bus (USB), serial peripheral interface (SPI) and 8-bit multipoint control unit (MCU) are popular interfaces. IC packages use through-hole technology (THT) or surface mount technology (SMT) and include package types such as low quad flat package (LQFP). In terms of features, some biometric sensors are supplied with software development kits. Others have a waterproof or abrasion-resistant housing for outdoor applications. Products with a low-power sleep or standby mode send an interrupt signal only when a finger is detected. Shimon K. Modi (2008), presented a study to show that the components of the biometric access control system then compare the image to a stored template to achieve the genuine user authentication [36].

Construction of the data base for the face image is developed by acquiring information through the evidences obtained from face recognition sensors. 3-D laser scanner, which employs an optical triangulation method, is one of the most popular devices for acquiring the face images. The most meticulous 3-D face data can be obtained through this laser scanner. It analyzes the face of a person and collect data on its shape and possibly its appearance (i.e. color). The data which is collected from the face can then be used to construct, three dimensional digital models. However, the system is very expensive and acquisition time is

more [37]. Sometime using the stereo vision system for reconstruction of the 3-D image form the data which is obtained from the two images of same person is helpful. This technology requires only two cameras to reconstruct 3-D face data, but accuracy and reconstruction performance is hard to find [38].

The elementary step in the iris recognition is the Iris image acquisition, but capturing high-resolution iris images is very troublesome. In real time most of the system which has small capture volume requires user concentration with machines, which is the biggest barrier in iris image acquisition and recognition. Most of the products available in the market are non-contacting and acquire iris images at a distance. So to capture the unique feature of the iris, a high-quality (resolution) image of the eye in the near-infrared range (700-900nm) is required to be captured. The image consists of its own source of infrared illumination to the eye. The infrared illumination reveals patterns even for dark eyes. Hence for capturing the eye image at a distance, systems require users to conspire with the machine actively in good amount of visible light, e.g. as staring in camera. To overcome the disturbance due to movement of user, tilt-and-pan camera can be used. Because of the cost of tilt-and-pan cameras, most current applications involve manual alignment of the eye with the camera [39].

Accumulation point of a system i.e. acquisition subsystem is one of the main component, where the error rate can be minimized. If the sensor is not capable of acquiring the actual information at the origin point, it may deviate the performance of the system toward unsuccessfulness of the system and can result in increasing of error rates (Wayman, 1997). Bolle and Ratha (1998) also have given a report describing the problems of matching two fingerprints. Ultimately the information capturing subsystem plays main role for all of the variability. The problem of variability can be removed using distribution system., because distribution architecture provides the function of interoperability. A.K Jain and A.Ross (2004) observed that when the images for fingerprint are captured by two different sensors, the Equal Error Rates (EER) found to be 23.10%, whereas EER for two individual dataset were 6.14% and 10.39%. Ford and Sticha (1999) also submitted .to U.S. Department of Agriculture describing the use of biometric systems in reducing fraud in the food stamp program and other welfare programs. In 2001 eight states in the U.S.A. called for applicants for economic assistance in at-least some territorial division to submit to fingerprint recognition (Dean, Salstrom, & Wayman, 2001).

1.5 Market Trend & Share of Biometric Technologies

International Biometric group (IBG) has conducted a test program to evaluate the market trend and share of all existing biometric technologies [36]. This analysis presents the revenue of adoption of biometric technologies and applications from 2007-2012, which is illustrated in the Figure 1.10.

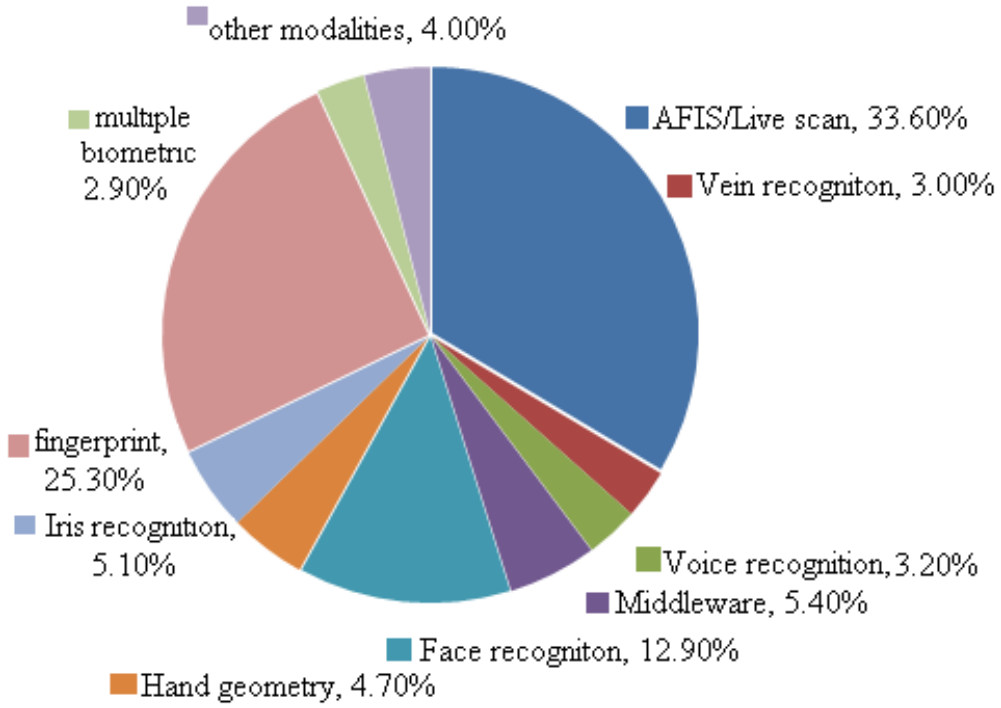


Figure1.10 Market size of the different biometric technology

Market size of the biometric technology is being incorporated by government and private organizations are growing inextricably. It is believed that till the end 0f 2012 the biometric market to grow from $3012 million USD in 2007 to $7407 million USD in 2012 (Figure 1.11) [36].

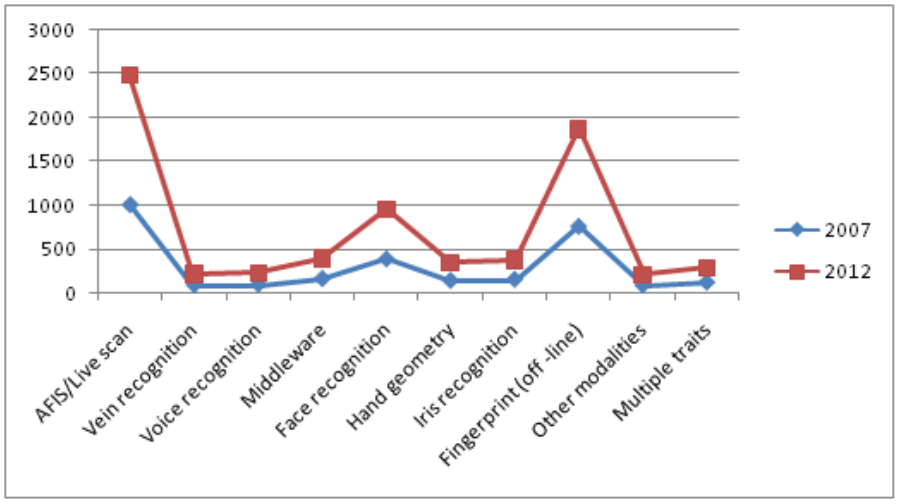


Figure 1.11 Annual Industry Revenue Projections 2007-2011[36]

1.6 Sensor Endorsement

Acceptance of the biometric technology is evaluated by usability and overall system performance. However cost, size, resolution and various error rates are the extraneous factor which plays a vital role while selecting a biometric sensor. In fact sensors for numerous biometric traits have recently dropped under the $10-$100. So at the enterprise level due to the competition, cost is no war in the selection of the system, but the accuracy. Figure 2 shows the usability of different type of fingerprint sensor on the basis of the error rates (FTA & FTE) [40, 41].

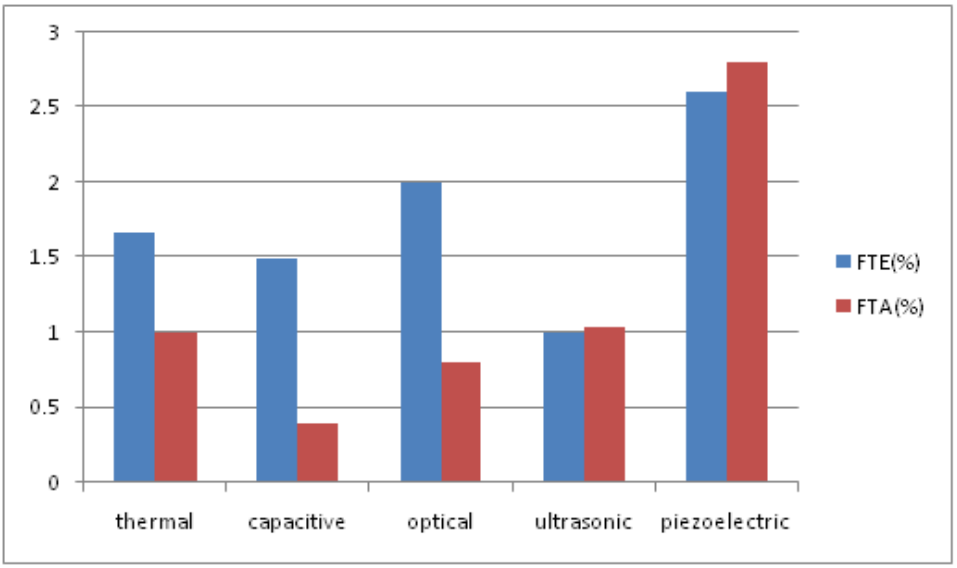


Figure 1.12 Usability of fingerprint sensors on the basis of FTA & FTE

1.7 Performance & Quality Parameters

The selection of the sensor to work efficiently under the influence of environmental as well as tradeoff factors such as temperature, humidity, power consumption, sensing area, resolution, image quality, scan time, cost etc.. Table 1.1 and Table 1.2 have been created using different fingerprint sensor from different manufacturers and the study shows that the accuracy and features of the sensors varies with the cost factor as well as with the manufacturers.

Table 1.1 Operation based performance parameters of the sensors [42, 43, & 44].

Sensors/Parameters	Cost	Temperature	Humidity	Power	Scan area
CMA S20	$10	20 to55°C	20-80%	3V	18mmx20mm
FPR-100	$15	25 to85°C	30-90%	12V	9.6mmx0.4mm
ZJ12	$35	-20 to+25°C	20-80%	3V	18mmx22mm
U.ARE.U4500	$66	0 to40°C	20-80%	5V	14.6mmx18.1mm
WG Reader208 Model	$80	-10 to+75°C	10-90%	12V	19mmX12.8mm
UPEK Eikon 500	$100	0 to40°C	5-93%	5V	12.8mm x 18mm
AET65	$115	0 to50°C	20-90%	5V	9.6mmx 0.2 mm
Marks 175 bio	$600	-10 to50°C	20-80%	5V	15mmX18.1mm
Rflogics FINGER006 Slave	$840	-10 to40°C	10-90%	12V	13mm x 15.2mm

Table 1.2 Quality based performance parameters of the sensors [42, 43, & 44].

Sensors/Parameters	Resolution	Scan time	FAR%	FRR%
CMA S20	500dpi	250ms	0.0001	<=1
FPR-100	508dpi	<100ms	<0.0001	<0.1
ZJ12	500dpi	250ms	0.001	0.01
U.ARE.U4500	512 dpi	140ms	0.001	1

WG Reader208 Model	450 dpi	< 200ms	< 0.0001	< 0.01
UPEK Eikon 500	508 dpi	500ms	0.001	1.00%
AET65	508dpi	<500ms	≤ 0.001	≤ 0.001
Marks 175 bio	500dpi	100ms	0.001	0.1
Rflogics FINGER006 Slave	500dpi	30ms	0.001	0.1

1.8 Hindrances of Unimodal Systems

The performance of all the biometric systems is depend upon the degree of freedom offered by the sensor module of it, so its reliability is completely based on quality of the information sensed by it sensor module. However, it is almost impossible to measure or sense the noiseless data every time. A brief description of these noises is discussed below.

1.8.1 Noisy Sensor Data: Noise in the acquired data from a biometric sensor occurred due defective acquisition conditions. For example, for face recognition, the captured images for biometric database might be noisy or distorted due to improperly maintained camera, illumination conditions, accumulation of dirt at the lens of camera and movement of user. Same is the case with the fingerprint data acquisition; if the residual of some other user remains on sensor, it may result in noisy fingerprint images. So the accuracy rate of recognizing personal is highly sensitive to attribute of sensed data and accumulation of noisy data can result in a definite less sensitive biometric system [45].

1.8.2 Non-Universality: Universality exists when each and every person is able to present a biometric clue for the authentication purpose. Although it is expected to get some biometric evidences in every single individual, but is almost impossible to obtain the biometric trait from approximately two percent (fingerprint) of the population [46]. Due to the non-universality, not only the individual suffers to give evidences for authentication, also it leads to create the problem of failure to enroll and failure to capture in biometrics [47].

1.8.3 Restricted Degrees of Freedom: It is believed, that every biometric trait has a significant variation in every individuals, but when the feature vectors are constructed out of it, similarities may exist in the feature set. Therefore, the degree of freedom provided by the

biometric evidences, are limited by the problem of homogeneity among the feature vector sets. Study shows that, the discrimination capability while using the fingerprints as biometric trait is approximately 10^4-10^5, it is also consider as keyspace. In addition to it, the keyspace for a randomly set password of 8-character is about $6.6x10^5$ [48]. The concept of discrimination is not only limited to the fingerprints, but to every biometric trait, hence every biometric trait has some upper bound in terms of its discrimination capability.

1.8.4 Lack of Individuality: The accuracy in biometric systems is affected, if the system is not able to discriminate between two biometric evidences of different persons. This problem occurs due to genital factor, for example, father and son or twin brothers can have the same facial expression. The problem of lack of individuality may help in increasing the false acceptance rate and low inter-class variations means that biometric evidences of different individuals may appear to be similar [40].

1.8.5 Lack of Homogeneous Imitation: This problem occurs when the biometric data acquired for the template generation is not similar to the data acquired for verification. This problem is also known as intra class variation, and is typically caused by a user who is improperly interacts with the sensor. The different face expression, improper placement of the finger on fingerprint sensor and other environment effect e.g. different light effects for facial images may create variation and affects the authentication process.

1.8.6 Spoof Attacks: Although Biometric systems are made to provide a barricade against the imposter attacks, however some time they are unable to block these spoof attacks. Therefore to alleviate the affects of the unimodal biometric systems, a consolidated multimodal system can be made by adjoining two or more sources of biometric traits [40]. Hence, a powerful database can be created by reducing FTE/FTC error rates and spoofing the multiple sources at a time is not as easy as it is for single source.

1.9 Why Biometrics, Multibiometric & Fusion?

Biometric technologies are becoming the foundation of an extensive array of highly secure identification and personal verification solutions [49]. As the level of security breaches and transaction fraud increases, the need for highly secure identification and personal verification technologies is becoming apparent. In recent years, biometric authentication has seen considerable improvements in reliability and accuracy, with some of the traits offering good

performances. However, even the best biometric traits till date are facing numerous problems; some of them are inherent to the technology itself. In particular, biometric authentication systems generally suffer from enrollment problems due to non-universality of biometric traits, susceptibility to biometric spoofing or insufficient accuracy caused by noisy data acquisition (sensor module) in certain environments [50].

Challenges of providing security to a genuine user and easy access to the information are achieved through identity management system. A typical identity management system is one that renders its services to a legitimate user and stops the imposter to access the security. Conventionally the security issues in the domestic and commercial organizations dealt with personal identities. Here, identity management achieved through hard-coded passwords and badge-based appliances (driver licenses, and passports) [51]. This introduces numerous problems because sometimes it is very easy for application programmer to crack the password. Also risk of stolen identity and the risk of compromising the template are some of the most publicized issues and frequently cited in relation to the security of conventional identity management systems. Biometrics offers a better and reliable approach to the identity management by recognizing individual based on their physiological and behavioral characteristics that are inherent to the person. An orthodox biometric system inherits four main modules namely sensor module, feature extraction module, matching module and decision module [52].

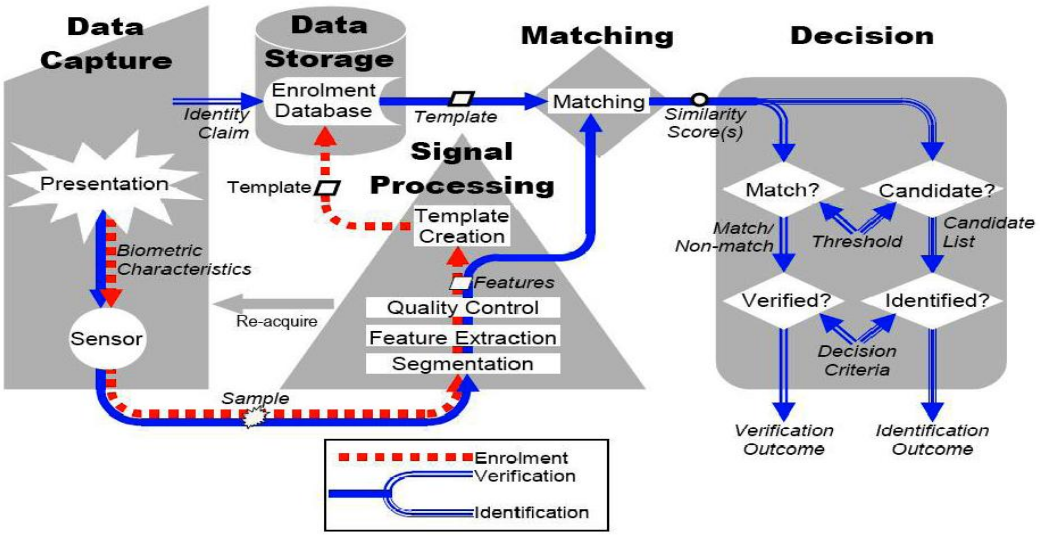


Figure 1.13 A general biometric system [52]

The sensor module is responsible for acquiring (collecting) the biometric information from the subject. Acquiring data at the very first stage of the biometric system is a very big-league because; it becomes extremely difficult to extract features from the fingerprint, iris, face images etc. if the quality & amount of information collected by the sensor is not accurate and efficient. Further, extracting the minutiae from the fingers of aged persons as well as manual worker are major problems in fingerprint based biometric system [53]. If the sensor is of good quality which can capture fine details then these problems can be minimized in fingerprint based system. Likewise, in face recognition system and Iris recognition system the choice of good sensor can eliminate or minimize the need of preprocessing for background area, coordination etc.. Therefore the choice of sensor is very critical for making the system more accurate and stable**.**

Along with the biometric sensors, the essential parameter in the implementation of a biometric system is its performance, acceptability, and circumvention. However these parameters in a unimodal biometric system are affected by several limitations such as noisy sensor data, non-universality, lack of individuality and lack of invariant representation etc [54]. Therefore, unimodal biometric systems suffer to fulfill the requirement in commercial and security levels, and hence they may not be able to achieve a high degree of accuracy. The limitation of the unimodal biometric system can be overcome with multimodal biometric systems [55]. In multimodal biometric systems the multiple evidences are combined together, so that an individual has to go through a number of evidence checks. Therefore, multimodal biometric system gives a higher degree of accuracy and its improved performance helps to design the more powerful and accurate security and personal identification systems.

1.10 Multimodal Biometric System

The Multimodal biometric systems are providing identification and human security over last few decades. Therefore, multimodal biometric systems are adapted to many fields of applications. In Multimodal biometric systems, more than one physiological or behavioral characteristic are used for enrollment, verification, or identification process. As we know that every biometric system is fundamentally a pattern recognition system. Multimodal biometric systems have some unique advantages over unimodal biometric in terms of accuracy, enrolment rates, and susceptibility to spoofing. This limitation occurs in several application

domains, example is face, fingerprint and iris recognition. Specifically the accuracy of face recognition is degraded by illumination and facial expressions. Unimodal biometric systems are also incapable of eliminating the spoof attacks. The NIST presented a report in which they recommended a system employing multiple biometrics traits in a cascade fashion. When more than one traits combines, it helps in improving the recognition rate, also multi biometrics helps in reducing the error rates such as, FAR, FRR, FTE, Susceptibility to environments or mimics.

Multi modal biometric systems are capable of receiving take biometric evidences from more than one sensor. In this approach the biometric data can be processed in a number of way e.g.

1.10.1 Multi Algorithmic Biometric Systems: In multi algorithmic biometric systems we obtain single biometric evidence from one sensor. However, data i.e. obtained from the sensor is processed through two or more algorithms.

1.10.2 Multi-Instance Biometric Systems: In this approach we use either one sensor or possibly more than one sensor to collect the random samples of a single biometric trait at different instances of time. Example is capturing images of face at different angle and in different illumination.

1.10.3 Multi-Sensorial Biometric Systems: In this approach we use multi sensors, and take the sample of a single biometric trait at the same time. Now, this collected data can be processed with the help of one or more algorithms. Example finger recognition application could use capacitive, thermal, piezoelectric, ultrasonic or optical sensor for information capturing.

The process of integrating the information from number of evidences to build-up a multi biometric system is called fusion. In multimodal biometric system the information can be integrated or fused at four levels, namely sensor level, feature extraction level, matching score level and decision level, and fusion can occur at any level [56]. However it is beneficial to fuse the information at that level only where maximum amount of information can be accessed with ease. Due to the presence of sufficient amount of information at matching score level, it is best suited for fusion purpose. In this report we have briefly explored the problem and better solution for choosing sensors and fusion methods, and present a case study describing its impact on biometric systems**.**

1.11 Problem Definition

Although, unimodal systems are reliable, still the popularity of these systems is degrading due to the problems such as noisy sensor data, non-universality and spoof attacks. These limitations can be overcome if we fuse more than one trait to make a system called multi-biometric system. The objectives of the thesis are.

(i) To study the different biometric traits.

(ii) To study different technologies/methods of multi-biometric system.

(iii) To compare the different normalization techniques for the fusion of left index finger, right index finger and face using unsupervised rules of fusion for standard database.

(iv) To develop a multi-biometric system using fuzzy logic.

1.12Thesis Contributions

In this thesis the performance of a multimodal biometric system is examined at matching score level fusion with various fusion rules and normalization methods. A follow-up of the aimed multimodal systems suggests that the major dispute in multimodal biometrics is the problem of selecting the correct methodology to combine the entropy obtained from multiple entities. The thesis has contributed with the implementation of the multiple traits with combination approach to score level integration and cover some of the consequences involved in calculating a single matching score from multiple matching score for individual traits. However, it is obvious for the different matchers and hence they are heterogeneous in nature. In order to convert these unlike matching score in a common domain we need to transform them using some normalization methods. In this thesis, we have studied various normalization techniques used on the matching scores before they combined together to obtain a single score.

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

This chapter reviews the extensive-range and multi disciplinary research on integration techniques in biometric field. An analysis of collective information of existing multimodal systems reveals that the principal challenge in multimodal biometrics is the issue of accepting the right approach for the fusion of the information obtained from more than one biometric cue. The Ideas or actions intended to enhance the performance of biometric authentication through fusion of multiple cues revolves around the output of multiple classifiers. The output of the classifier obtained in the form of matching score either can be combined using classification or combinational approach of integration. These matching score then combined in many ways to regenerate a final score or decision. Classifier output can be picked out in an alternative way to anticipate the accuracy of various classifiers. This chapter contributes to the information sharing for literature review of multimodal biometric fusion by improving the apprehension of fusion and by raising fusion performance using entropy specific to a user.

2.2 Overview of Data Fusion

Even the most advance unimodal biometric system endures from several difficulties. These offspring overcome by using a multi-modal biometric system which utilizes more than one biometric trait. The patterns of human face are more complex and random and hence it is difficult for an imposter to reproduce someone's behavior or looks. Fingerprint pattern are also typically different but can be spoofed by using gummy finger. By fusing them with other biometric attribute such as face, a more ensure multi-biometric security system can be formed for authentication. Rashmi Singhal et al. [57] reported a brief overview about problem of unimodal systems, information integration, levels of integration and classification of multi-biometric systems.

2.3 Functional Mode

Frame work of multimodal biometric organization be relevant to the serial arrangement which the multiple modalities are adopted and subjected to a special process or treatment of identification. A multimodal biometric system can function in three different ways:

2.3.1 Parallel Mode: In parallel mode of operation multiple numbers of biometric modalities can be combined together simultaneously. Parallel multimodal biometry figures out the above defined problems of unimodal system by combining the evidences using an appropriate fusion scheme.

2.3.2 Serial Mode: Serial mode of operation does not combine or fuse the multiple biometric modalities at once but one after the other. The main advantage of serial operation is that it allows the system to be free from multiple procedures at a single stage. This mode of operation helps in taking fast decision because verification can be done in between the processing depending upon the requirement and fusion algorithm.

2.3.3 Hierarchical Mode: In parallel mode of operation multiple numbers of biometric modalities can be combined together in a hierarchical fashion when large a number of classifiers are present, such as tree structure. There are, however, a couple of advantages of using a Hierarchical mode for fusion are that this function mode can also permit the user to make up his mind which modality he would introduce first. Furthermore, while identifying a user out of a large data base, it can use the consequence of every modality to successively reduce the database and it makes the search quicker and more effective.

Although, every fusion approach clears or reduces the problem of unimodal biometric the still almost every intended Multibiometric systems have a parallel functional mode of operation. But the ultimate choice of fusion scheme and its functional mode of operation rely upon the application.

2.4 Fusion Terminologies

The above mentioned limitations of unimodal Multimodal biometric systems are got over with some of biometric systems by uniting the manifest received from different origins [58]. The origins are explained below.

2.4.1 Single Biometry, Multiple Sensors: When same biometric evidence is adopted by multiple sensors and then integrated to accomplished and amend the authentication process (e.g. 2D and 3D images of the face). The use of multiple sensors can create the problem of high dimensionality while combining data from various sources and of noisy sensor data, but all other possible problems linked with unimodal biometric systems persist [58].

2.4.2 Single Biometry, Multiple Instances: When same biometric evidence is acquired several times by a same sensor and integrated to accomplish and amend the authentication process (e.g. multiple images of face of a person taken at different instance of time and under different pose/lighting conditions) [58].

2.4.3 Single Biometry, Multiple Units: Apart from above two approaches, here, different quantity acquired from a single biometric cue are and combined to accomplish and amend the recognition process (e.g. left and right index finger data) [58].

2.4.4 Single Biometry, Multiple Representations: if given input raw biometric data acquired by a single sensor and then it is used by different methodology of obtaining the feature and matching scores to fuse to accomplish and amend the recognition process comes under this category (e.g. LDA and ICA) [58].

2.4.5 Multiple Biometrics: In multimodal biometric more than one biometric modalities of the same person can be combined to accomplish and amend the authentication process (e.g. face, fingerprint and iris). Different application program demands different levels of data fusion. The only well-used structure of authentication is the multimodal biometric fusion scheme.

In spite of the fact that the unimodal biometric systems also improve the authentication process, they still lack in some of the particular environment and faced some of the problems explained above. Therefore, nowadays multimodal systems are the first choice for person recognition based on different modalities and seem to be more robust to noise, non-universality etc [58].

2.5 Levels of Integration

Fusion of the information not only makes the system robust, but also increases its performance by integrating different biometric information to make the system more consistent against the spoof attacks. A general biometric system model consists of four

modules, and the information from the different modalities can be fused at any level, depending upon the amount of data available at that level [59].

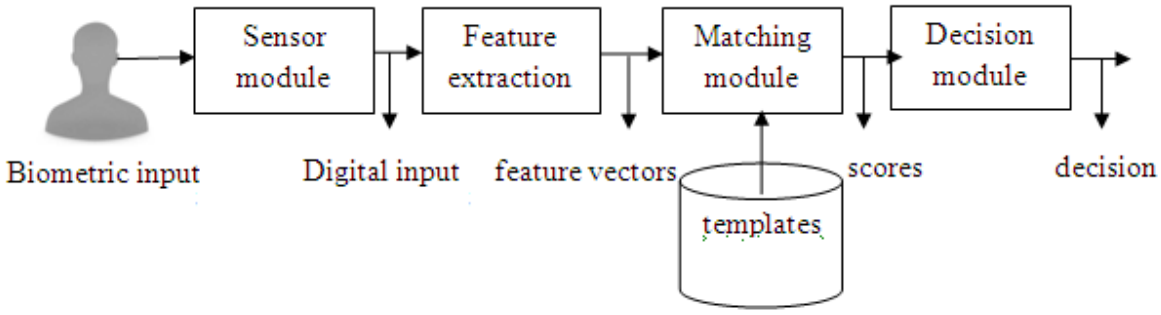


Figure 2.1 Modules of a general biometric system [60]

2.5.1 Fusion at Sensor Level: The information acquired by sensors, from the sources, remains available in raw form. This raw data can be combined or fused only if multiple evidences of same biometric trait, obtained by several sensors are compatible to each other or evidences of the same biometric trait taken at different instances by the same sensor [61]**.** Although, we have the sufficient amount of information at the sensor level, but due to the incompatibility among various evidences (face, iris and fingerprint), it is almost impossible to achieve the fusion at sensor level. However, the problem of incompatibility exists with same biometric trait too, e.g. the image taken by two different cameras may not have the same resolution or evidences of fingerprint may not be integrated, because these clues may have taken from different sensors (thermal, ultrasonic and/or capacitive).

Out of some of the work done at sensor level fusion Jain et al. [62] has given an algorithm for mosaicking the multiple fingerprint notions to develop a more perfect image. Here, they considered the problem of mosaicking the fingerprints as a 3-D surface enrollment problem that can be figured out using a modified ICP algorithm. For this multiple image of the fingerprint initially aligned by pressing out minutiae points from each individual fingerprint image, which then compared with two sets of minutiae points with the help of an elastic point matching algorithm. Initially the work done gives a better performance for the matching system, but scope for the future work reveals the short coming of the fusion at sensor level because it faces problem for non-linear deformation of the fingerprint.

In the majority of the literature on sensor level fusion Moon et al. [63] also developed an algorithm based on registration techniques for mosaicking the multiple images to generate a composite image. This technique was then analyzed to compare the unparalleled framework of the operating characteristics for fingerprint images of dissimilar sizes. For fingerprint template synthesis and fingerprint image mosaicking an alignment was explored for matching the comparable elements of the two templates or images. The optimal transformation for template alignment is achieved through Iterative Closet Point (ICP) algorithm, which is a well known methodology for the alignment of 3D geometric models. Hence the modified ICP algorithm for optimal transformation helped in improving the fingerprint authentication while merging the minutiae from two fingerprint images. Experiments reveal that image size plays an important role while confirming to be employed during fingerprint registration. The merging approaches a critical factor when deciding the particular merging approach to be used during fingerprint registration. One of the drawbacks of the approach is that even it is faster and more insensible by elastic distortion, but it is adapted for larger images only.

Raghavendra et al. [64] has demonstrated a novel approach of sensor level fusion for face and palmprint images applying Particle Swarm Optimization (PSO). This technique comprises of two main steps, i) Decomposition of the acquired face and palmprint images from different sensors with the help of wavelet transformation ii) now, to generate a new merged image of face and palmprint, PSO is used to pick out the most discriminative wavelet coefficients. In addition to this, a unique method Kernel Direct Discriminant Analysis (KDDA) has been implemented for feature extraction and then Nearest Neighbour Classifier (NNC) is used accomplish the process of identifying a person as a genuine or as an imposter.

Another novel method evidenced by Singh et al. [65] explains the concept of multispectral image integration of visible and infrared face images and the use of match score fusion to identify the genuineness of an individual. 2vn-granular SVM is used to combine the visible and farseeing wave infrared face images, by which local and global attributes of multispectral face images can be learnt involving more SVMs at different granularity degrees and resoluteness. The 2vn-GSVM executes precise classification which is later on used to dynamically calculate the weights of farseeing and infrared images for rendering a merged

face image. For the transformation of the fused face image 2D log polar Gabor transform is used and local binary pattern feature extraction algorithms is utilized to take out global and local features. Finally, theoretical framework developed by Dezert Smarandache based on plausible, is used to fuse the corresponding matching scores. The efficacy of the intended algorithm is corroborated utilizing the Notre Dame and Equinox information and is equated with subsisting statistical, learning, and evidence theory based fusion algorithms.

2.5.2 Fusion at Feature Extraction Level: The information acquired at the sensor level reaches to the feature extraction level in digital form, but only a salient piece of data is kept to make a new data type. In feature level fusion, this information is preprocessed, and feature vectors are fetched out separately. The extracted feature vector is then use to represent the distinctive characteristics of the biometric traits. Many algorithms have been developed for the effective feature extraction, which shows the importance of feature level fusion.

Xiao-na Xu1 et al. [66] demonstrates a new approach of feature-level integration based on kernel Fisher discriminant analysis (KFDA) and utilizes it to multimodal biometrics based on integration of ear and profile face biometrics. Here KFDA is used to calculate the fusion discriminant vectors of ear and profile face and helped in accomplishing a nonlinear feature integration projection. It is evidenced in study that when only one biometric trait i.e. ear and face, is used for the authentication purpose, only 91.77% and 93.46% persons are correctly recognized, respectively. But when fusion technique applied at feature level, the performance of the system increased to 96.84%, 96.41% and 96.20% respectively for the average, product and weighted sum rules.

The method proposed by Rattani et al. [67] presented a multimodal biometric system for the fusion of face and fingerprint images based upon a compatible feature extraction technique to receive corresponding features from the raw information. The algorithm is consist of three main steps, i) Feature set compatibility and normalization ii) decomposition or feature reduction and, iii) concatenation. The experimental consequences evidenced that fusion of the information from autonomous origins (face and fingerprint) at the feature level enhances the performance as compared to score level. It is evident that, while working with only fingerprint as the biometric trait, the FRR rate is 5.384% and FAR rate is 10.97 %. Fusion at feature level extensively helps to reduce the FRR rate to 1.98 % and FAR rate to 3.18% only.

The experimental framework developed by Zhang et al. [68] for the feature level fusion utilizes the Canonical Correlation Analysis (CCA) which is an ideal technique to formulate and assess the linear relationship between two data sets. In this paper, they present a multibiometric algorithm to combine the feature vectors of palm print and finger geometry with the help of Canonical Correlation Analysis. In order to obtain the palmprint feature vectors linear discriminant analysis (LDA) is used and then geometry feature of the middle finger is extracted. After generating the feature vectors for palmprint and finger geometry separately, they are fused by CCA to form a mixed feature which is implemented to announce the identity of a person either as a genuine or as an imposter. Additionally this approach helps to reduce the dimension of the obtained combined feature used for fusion. The proposed approach improved the average recognition rates by 0.18% & 3.85% and worst recognition rate by 0.30% & 7.21% for palmprint and fingerprint geometry respectively.

Several works earlier in time for feature fusion humanistic study has only stressed on the consequence of feature extraction and categorization. However, the decisive effect of analyzing the usefulness of extracted biometric feature vectors has been predominately pushed aside. Selection of the appropriate feature out of the cluster serves in brief study to identify and remove much irrelevant information. Kumar et al. [69] talks about the effect of feature subset choice and its potency in a distinctive bimodal biometric system. The extracted feature vectors of the hand image are compared and combined with Bayes transformation theory and sets are fused with learning rules & decision trees such as k-NN, SVM, and FFN.

The process of authenticating an individual on the basis of distance based video always remains a critical task for the fusion of multimodal biometrics. Zhou et al. [70] presented a Modern algorithm that uses and incorporates information from side face and gait at the feature level. Out of dozens features of face and gait, principle component analysis is used to decompose the main features from enhanced side face image (ESFI) and gait energy image (GEI), respectively. The separate feature vectors are then combined to get a complete and final feature vector. In the process of fetching the discriminating synthetic features from concatenated features of face and gait multiple discriminant analysis (MDA) is employed. This procedure allows the propagation of improved features and cuts down the curse of dimensionality. To check the performance of the suggestive study two relative data sets are used to demonstrate the outcome of altering clothes and face changing over time.

Furthermore, the comparative study of the proposed with another feature level fusion scheme demonstrate that the synthetic features, encrypting either side of the face and gait information, carry more demonstrating ability than the individual biometrics features, and this feature level fusion has a greater degree of accuracy than other.

Likewise the previous discussion Rattani et al. [71] suggests a refreshing person recognition algorithm in video, which mixes human face and gait modalities with the help of a dynamic multi-modal biometrics fusion strategy. The Fisherface method is followed to draw out face features, and to extract the gait features Locality Preserving Projection is considered to achieve low-dimensional manifold embedding of the temporal silhouette information inferred from logical order of images. After extracting the feature of gait and face images separately these feature vectors are fused with the help of a distance-driven fusion method. Method suggests that the careful selection of the system parameters can play a fundamental character with different fusion operations. An adaptive algorithm to pick out an improved quality parameter is being analyzed. Actually, there are various components which may shape the quality of single biometric feature like imaging region, viewing angle, and lightning condition etc. Productive structure of the reliable synthetic human features for better authentication depends upon the success rate of the determining and realizing the feature vectors.

Yan et al [72] demonstrated a novel class-dependence feature analysis algorithm grounded on Correlation Filter Bank (CFB) proficiency for efficient multimodal biometrics integration a for feature level fusion. In this approach, the unconstrained correlation filter shaped for a particular modality is contrived by optimizing the overall original correlation outturns. Consequently, the differences between modalities have been allowed and practicable entropy in several modalities is fully overworked. Preliminary observational consequences on the fusion of face and palmprint biometrics demonstrate the high quality of this method.

2.5.3 Fusion at Matching Score Level: The performance of several verification systems based on biometric can be increased when fusion rules applied at matching score-level. In score level fusion, the matching score is obtained from every individual system. In score level fusion, score normalization is a necessary task to do, because it converts the individual scores into a common meaning domain to achieve the compatibility. These normalized scores

are then combined to improve matching performance. Now, this single normalized score is compared with database, which stored previously and verifies whether the person is genuine or imposter based on degree of similarity and dissimilarity.

Jain et al. [73] introduced a system which was developed to integrate three biometric modalities face, fingerprint, and speaker verification to determine the identity of a person. This system capitalizes the potentialities of each and every biometrics modalities. This approach helped in removing some of the restrictions and problem faced by a single modality biometric system. Preliminary observational outcomes manifest that the identity laid down by such an integrated system is much more authentic than the identity installed by an individual face recognition system, fingerprint verification system, or speaker verification system.

In the process of recognition Kuncheva et al. [74] also gave decision templates based method for multiple classifier fusion, and compared it with Behavior knowledge space method, majority voting, Naïve Bayesian, average aggregation rule, product aggregation rule, maximum aggregation rule, minimum aggregation rule, probabilistic product, fuzzy integral, Linear discriminant classifier on the intercede end product space, Dempster-Shafer, Quadratic discriminant classifier, logistic classifier, Fisher linear classifier, decision templates with different models. The comparative study among these methods is given in this paper in detail.

For classifier fusion of fingerprint and face Toh et al. [75] developed a Hyperbolic function network with the help of forward neural network and SVM. They covered the state of difficulty by mixing decision outcomes of fingerprint and speech as classifier fusion problem. The matching scores obtained from every individual classifier are then used as the input of the neural networks, and the output matching scores of the neural network are the concluding matching scores. They used the different neural networks to improve the recognition performance of the fusion process; the detailed study is given in the paper.

In another study reported by Jain et al. [76] for the fusion of three modalities such as face, fingerprint and hand geometry at the matching score level is researched. The research explains that user autonomous Weighted Linear combination of similarity matching scores can be intensified by utilizing either user dependent weights or user dependent decision doorways. Weights and doorways are calculated by in-depth exploration on the exploitation

data. The deep analysis reveals that use of doorways enhances the performance by about 2%, whilst the use of weights enhances it by about 3%.

Verikas et al. [77] compared eleven classifier fusion terminologies in his study. The comparability admitted amalgamation by fuzzy integral, Bayesian compounding theory, weighted averaging rule, averaging rule, majority rule, Borda count, amalgamation by fuzzy inherent with data-dependent densities, admixture by weighted averaging with data-dependent weights, combination by the BADD defuzzification strategy, admixture by Zimmermann's counterbalance manipulator and optimizing the fuzzy assess.

Toh et al. [78] aimed to make a multivariate polynomial model which helped in reducing the complexity for the fusion approach at classifier. This technology defeats the defects being connected logically, causally or by shared characteristics complexity of schematic multivariate polynomial simulation for high-dimensional jobs. The authors enforced the raw model to merge fingerprint and voice data for individual recognition. Preliminary experimental results are made on the basis of comparative study of second-order (RM2) and third-order (RM3) multivariate polynomial models. The recognition functioning can be made more desirable or valuable greatly by the fusion methods for low acceptance rate instances.

Some other consideration by Frischholz et al. [79] looks at two different fusion terminologies of fusing the matching scores or decisions for speech, face, and lip motion. The terminologies considered for fusing the matching scores obtained from the different classifier are the Sum rule and Majority voting. Majority voting mainly used at decision level and requires the understanding of two traits out of the three so that there should not be a tie, even though, for a high security system all three decision can be made in favor of algreement. It has been encountered that the mixed system could render more defenses against the spoof attacks than each of the single systems alone.

A multimodal biometric user-identification tool based is offered on the fusion of face and gait for a single camera case by Kale et al. [80]. For practical implementation of fusion, there are two different scripts are used in order to integrate the matching scores for face and gait. The very first scheme includes a classifier to generate the matching scores for gate and works as a filter to clear a limited number of users. On the other hand second scheme used to combine the matching scores of both the modalities to achieve the fusion. Likewise some

previous work done this terminology also employ fusion rules such as Sum rule, Minimum rule and Product rule. They analyzed that even though first scheme which worked for gate modality has depicted a desirable improvement in the system performance, but the second scheme is favored it fulfilled the demand of fusion in terms of accuracy, computational speed. Based on the above consideration, it can be resolved that fusion proficiencies established on fixed rules have more or less Benefits.

In addition to the previous approach, Shakhnarovich et al. [81] also proposes a study on matching score fusion of face and gait cues for recognition and in they chooses matching score and decision level to implement the fusion strategy. Along with the implementation of the approach they empirically equated four different score-level fusion methods and one decision level fusion methods in this study. The method used for matching score level are the Product rule, Sum rule, Maximum rule, Minimum rule and for decision level is the Majority voting rule. In preliminary result of the comparison Product rule has depicted the best execution out of all the fusion methods conceived. Due to the presence of maximum number of outlier in the matching scores Minimum and Maximum rules manifest poor performance. Because this both the methods has considered less robust than Sum and Product rules.

There have been some experimental studies on integration of three modalities for matching score level. One of these technologies a system is proposed by Ribaric et al. [82] which is established by combining the matching scores for hand geometry, palm and fingerprint. Fusion method used in this paper was the Weighted Sum rule which is a widely used for fusion purpose. Results of this experiment designate that the Weighted Sum rule furnishes comparatively better execution than even the best individual modality.

Hazen et al. in [83], tried to explore the fusion for face and speaker biometric modalities for the identification purpose. These modalities are then examined on data gathered in ungoverned environments using budget sound and image capture malware. Their research brushed aside the facts that the system functioning can be underestimated under these considerations, it has been depicted that using a combination of biometric modalities can enhance the robustness and accuracy of the person recognition task. Another method used in the paper is Simple Brute Force Search which is a novel approach of the fusion. According to

the result obtained for this approach the fusion strategy gives the better performance than individual modalities involved.

Another method discussed by Czyz et al. [84] for multimodal biometric authentication system which is having a base of operations on the integration of the matching scores for face image and text independent speech data of a person. The two method used in the research for the integration purpose are Multi-Layered Perceptron and Weighted Average. It has been noticed in the research that text autonomous speaker confirmation algorithm is more accurate and robust compared to the face verification algorithm. Furthermore, integration of these two cues has contributed to an appreciable improvement.

Luettin et al. [85] also gave their contribution in the development of two different speaker verification method which after considered as an accurate and robust person authentication technique. The basis of the discussion of the study in the paper is the implementation of the fusion strategy for scores of speech and facial images. These are a text sovereign method employing a second order statistical measurement and a text dependent method based on hidden Markov modeling. The unimodal identification system, text dependent has expressed the best result compared to face and text independent modules. In this research paper the fusion at matching score level is achieved with the help of Support Vector Machine for the different identification modules and it has been encountered that the integration of different modalities outdoes even the best individual modality necessitated. The Consequences obtained from the analyses depicts that the integration of the two biometric cues with the minimum performance outperforms the best single modality results.

In another study suggested by Sanderson et al. [86] which evokes an adaptive multimodal person authentication system based on speech and face images as biometric cues has observed that the system accommodates to noise present in the speech signal by altering the arguments of the integration method. A set of arguments can be calculated theoretically all the way through the exploitation phase for different Peak Signal to Noise Ratio of the speech signal. In addition to this, during the trial stage, the approximation of the Peak Signal to Noise Ratio of the given speech signal occurs and arguments most intimately corresponding to that Peak Signal to Noise Ratio are practiced by Linear and SVM fusion terminology. The

outcomes of the practical work have manifested that the adaptive system importantly gives a greater degree of accuracy and robustness.

2.5.4 Decision Level Fusion: Biometric fusion at decision level lined up at a very low frequency and very less number of research paper published in this field. Decision-level fusion can be thought as a pattern categorization problem such as biometrics verification and target identification. At this level user claims an identity either explicitly or implicitly, depending upon whether the screening is 1:1 or 1:N respectively. If the screening is 1:1, then the process is called verification and claim of identity either will be rejected or accepted. In case, if the screening is 1: N, then the process is called identification and the implicit claim made by the user will be checked to determine whether the user is already enrolled in the system or not.

At decision level, each classifier avails a decision. In decision level approach scores normalization is not required as it was mandatory in matching score level. Use of the decision level for fusion is beneficial only if the numbers of classifier are more than two, because the problem that may occur with decision level fusion is the possibility of ties. Decision at this level can be combined in serial and parallel form, through AND and OR fusion rules respectively and rule helps to reduce FAR and OR rule helps to reduce the FRR. M. William et al. [87] has shown that if two system, each having an FAR & FRR of 1%, on combination of AND and OR rules yields to FAR = 0.0882% and FRR = 0.0002%.

Some of the common methods used for the decision level fusion are discussed below.

1. Fix Rule based: AND/OR and PROD/SUM rules Majority voting
2. Classifier based: Quadratic Discriminant Analysis, Fisher Linear Discriminant, k-NN based classifiers, linear classifier, and decision trees.
3. Machine learning and neural network : FFNN, Support Vector Machine, Multi-Layer Perceptron, Expert learning, fuzzy set , particle swarm
4. Clustering for decision level fusion: fuzzy vector quantization, Fuzzy k-means, and median radial basis function.
5. Statistical decision theory: Maximum a posterior, maximum likelihood, Min-Max, Bayesian decision theory.

Prabhakar et al. [88] used an optimal Neyman-Pearson rule to aggregate more than one fingerprint matching techniques at the decision-level to avail a conclusion. Preliminary observation of the approach when upheld on a prominent fingerprint database proved that the ordinary matching performance upraised approximately 3%. In the more advanced stages of the experiment they demonstrated that a combination of multiple notions and multiple fingers amended the recognition performance by more than 4% and 5%, respectively.

Recently, one multimodal biometrics fusion techniques which has attracted much attention for decision level fusion is SVM. Fierrez et al. [89] used the auxiliary information of SVM to fuse three biometric modalities fingerprint, Face and signature. The research work in this approach, considered the fusion of these modalities as a pattern recognition problem, which later was applied through SVM. It is carried out in this study is that the classification problem modified into a quadratic problem to make the approach easier and analytical. Next, the score which was obtained from the output of the SVM network is the concluding fused score. Accuracy of the system is checked while comparing the testing data set with previously stored template/database.

Verlinde et al. [90] also considered the decision level fusion as a classifier problem. The final result in the decision level fusion is accomplished when more than half of the classifiers declare the same decision. In this paper they focus their efforts mainly on fusing the obtained decisions from a variety of independent classifiers such as k-NN, decision trees, and logistic regression in a multi-modal identification problem. Along with this Zhang et al [91] also developed adaptive model person identification by fusing the speech and image data at decision level. Both the method was compared to carry out the performance of the fusion with face recognition model and speck recognition model. The average recognition rate of the first integration technique is approximately 91.6% while the recognition rates for the second technique working with voice and face biometric are approximately 85% and 79.29%, respectively.

Naguib et al. [92] presents a thorough experimental investigation, based on three types of biometrics face, voice, and signature into the effectiveness of various fusion approaches in multimodal biometrics. They used Multi-Layer Perceptron to accomplish fusion employing face, voice, and signature at decision level. The matching score obtained from the different

classier for face, voice and signature are used as the input for the MLP neural network and the outputs of the MLP are the fused decision scores. In approach like this two kind of data set are created, one for the training and other for the testing. Therefore, the MLP network is trained by some training data sets before testing. It is observed in the final results that the recognition rate improved to is 100% with fusion which was 89%, 99.5%, and 93% for face, voice and signature respectively, without fusion.

Based on the Israel et al. [93] studies, it can be resolved that fusion proficiencies have some advantages over unimodal biometric identification systems. They include the conception that the fusion of face and ECG in this paper show better performance when compared to single modalities for person identification. Mono-modal biometric recognition systems demonstrate such a performance that may not be enough for many security diligences. There have been some researches which demonstrate the functionality of the electrocardiogram as a refreshing biometric cue. This paper dug into the integration of a conventional face recognition method with ECG.

A brief introduction about previously developed methods and tools are given in Table 2.1.

Table 2.1 Fusion for different biometric traits

Biometric Traits	**Author & Year**	**Features**	**Terminology**	**Architecture Mode**	**Level of Fusion**
Face & Finger	Marcialis et al.2007[94]	Eigenfaces and finger minute	PCA and string	Parallel	Score level
Iris & Face	Zhang et al. 2010 [95]	Pixel probes of face and iris	CCA(canonical correlation analysis)	Parallel	Score level
Fingerprint & Iris	Lumini et al. 2007[96]	Eye's Polar coordinates & fingerprint's ridge feature	Support vector machine	Parallel	Decision level
Hand	Ong et al.	Tip and root	Sum rule ,	Parallel	Decision

Geometry & Palmprint	2003 [97]	point of finger and fisher palm	weighted sum and SVM		level
Gait & Face	Kale et al. [98]	Velocity and weight motion vector and the identity variable	SUM or PRODUCT rule	Holistic Fusion	Decision level
Fingerprint & Gait	Derawi et al. [99]	Minutia and g-force feature vector	User weight and weighted sum	Parallel	Score level
Ear & Fingerprint	Kiskul et al. [100]	Shift feature vectors	Adaptive Weighting using Doddington's Approach	Parallel	Feature level

2.6 Summary

In this chapter we have summarized the main work related to the fusion of various biometric traits. We have started by describing the general problems of the unimodal biometric systems such as Noisy sensor data, Non-universality, Lack of individuality, Lack of homogeneous, Limitation, Spoof attacks etc. Then we have focused on architectural approach of various modes of operation on fusion (e.g. parallel mode, serial mode and hierarchical mode). Within all adapted study on fusion we have selected few of them which have motivated us to focus to implement the research at matching score level.

CHAPTER 3

METHODOLOGY

3.1 Introduction

Although the problem of biometric fusion has been studied in a widespread way, it is however, not an entirely solved problem. This dissertation begins to deal with an information fusion approach followed to deal some of the restrictions of existing fingerprint and face matching systems. A hybrid fingerprint and face system that utilizes the matching scores of face, left index finger and right index finger are obtained from a freely available database (i.e. NIST BSSR1) has been developed. Fusion of these matching scores is depicted to execute significantly better results than any other conventional and preexisting score fusion schemes. A new mathematical transformation (i.e. normalization) technique has been used to normalize the data in a common domain. Normalization is also used to mitigate the effect of non-linear distribution of matching score due to different matching technique for face and fingerprint. The model is developed by fusing the normalized score with unsupervised fusion rules SUM, PRODUCT, MIN and, MAX rule. Furthermore, to present a comparative study a fuzzy rule base is also created to fuse the matching scores obtained for face and fingerprints. As earlier discussed, a unimodal biometric system recognizes an individual based on a single source of biometric cue and are suffered in many ways like non-universality, noisy sensor data and lack of indistinctive data of the preferred biometric modality. Some of these problems can be facilitated by using multimodal biometric systems that unite evidence from multiple biometric origins. Selective information fusion system, which is discussed in this dissertation, is anticipated to be more authentic and robust than systems that depend on a single origin of information.

3.2 Objectives of the Chapter

a) To study the nomenclature of different kind of fusion models.

b) To study the various levels of information fusion.

c) To transform the information in a common domain with help of various normalization techniques.

d) Evaluation criterion of verification and identification on the basis of various error rates.

e) To develop a fusion model on the basis of unsupervised fusion rules.

3.3 Common Nomenclatures for Information Fusion

In agreement with to Ross et al. [101] and Jain et al. [102], the entropy origins adopted for integration can be place into to a category of following types.

3.3.1 Multi Sensor Systems: These systems include the acquisition of biometric information from single biometric evidence from different types of sensors. It is believed that multi sensor systems a variety of raw information can be attained from several sensors. For instance, if consider two finger sensor i.e. optical and the CMOS sensors to capture the fingerprint image they can probably help to distinguish an instance of change of signal and interference sources in the captured image. A comparative overview of these two sensors is given below.

Table 3.1 Functional detail of the multisensory system

Preliminary Information	**Data**	**Feature**	**Decision**
Bandwidth	Possibly very large	medium	very small
Information Loss	no loss	some	possibly significant
Significant Performance	no loss	some	possibly significant
Operational complexity	High	medium	low

3.3.2 Multi-Instance Systems: In this approach, a single biometric sample is acquired from user but at different instances of time. As an example, fingerprints images of index and

middle fingers of a user can be utilized in an integration system to prevail a higher degree of security. In addition to this, we can also consider the right and left eye image to use iris or retina as biometric clue as multi instances.

3.3.3 Multi Sample Systems: In multi sample terminologies multiple numbers of same biometric is used to develop a recognition system. In order to dominate an outcome for overall identification a single methodology is used to process each of the samples and then every individual consequence are fused. One of the main advantages of using multiple samples for identification over multi algorithm method is that it may help to overcome poor execution of the system due to one sample that has unflavored attributes. Adopting multiple samples demands either multiple replicates of the sensor or the user handiness for a longer period of time. Examined and noted the similarities or differences with multi algorithm, multi sample appears to necessitate either higher amounts paid for goods and services for sensors, greater cooperation from the user, or a combination of both. Chang et al. has discussed a multi-sample approach in [103] in which they considered 2D face images as a baseline in contact with which to compare the outcome of multi sample 2D + 3D face.

3.3.4 Multi Algorithm Systems: Unlike multi sample, multi algorithm terminology uses a single biometric sample adopted from single sensor. In this approaches two or less like terminologies are used for the post processing on previously acquired sample. In order to dominate overall identification result of the system every individual result is fused. This approach is having ability to arouse interest, mainly in application and research areas because the use of single sensor may help in cutting down data acquisition cost. According to a study presented by Phillips et al. [104] in which a Face Recognition Vendor Test has demonstrated the modified performance in 2D identification by fusing the consequences of different commercial identification systems.

3.3.5 Multimodal Systems: A multi-modal biometric system conceives more than one biometric modality in the process of identification. In one of the research work develop by Ko [105] proposes that multi-modal fusion welfares the most when the biometric cues are extraneous. These biometric evidences can be considered extraneous to each other when the match performance of one cue does not anticipate the other's operation. It is supposed that ideally all of the biometric evidences would be extraneous to each other, at the same instant

captured with the same sensor, and at superiority. However, it is beneficial to have few algorithm of categorizing multi-biometric systems, and realizing the rewards and hinders linked with each approach is essential to effective system invention.

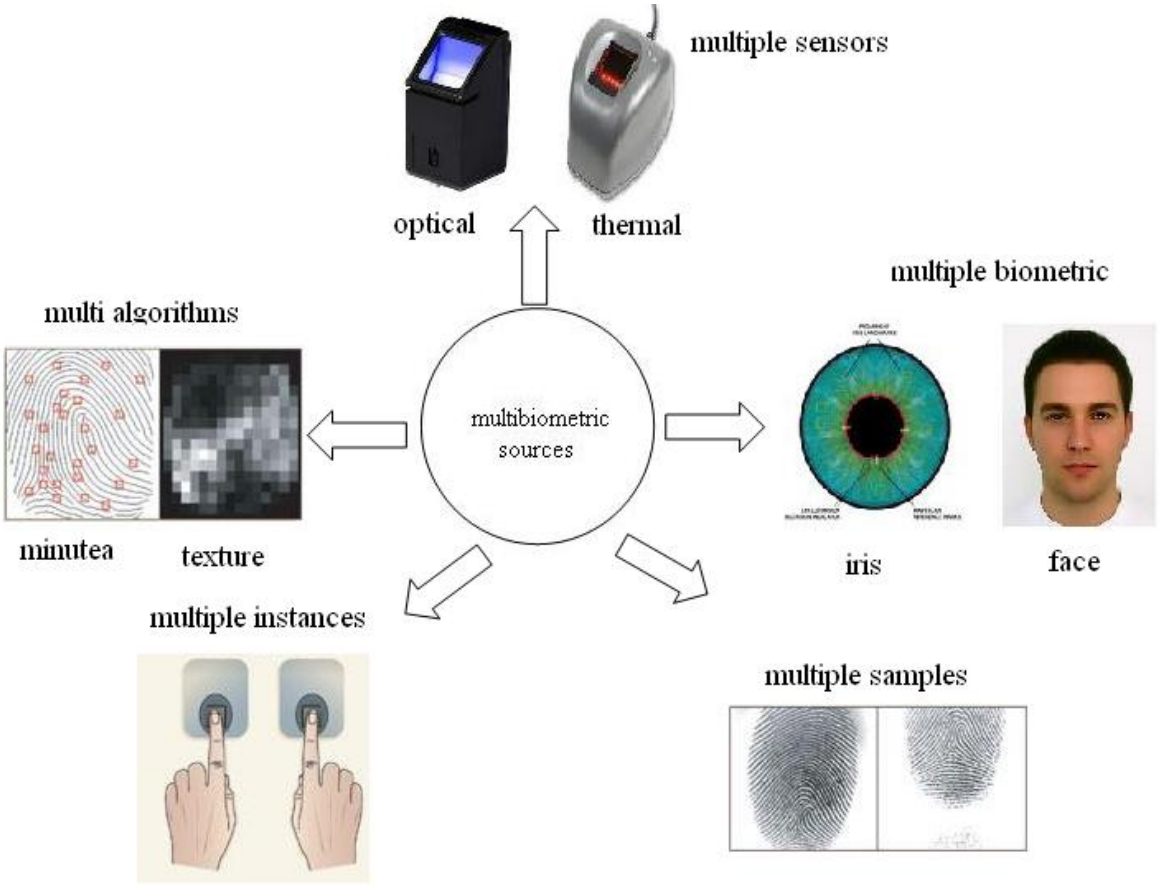


Figure 3.1 Different module representations of fusion systems

3.4 Levels of Fusion

According to the selective information acquired, the methods for fusion can be categories in to fusion of information before matching and fusion of information after matching score level [106].

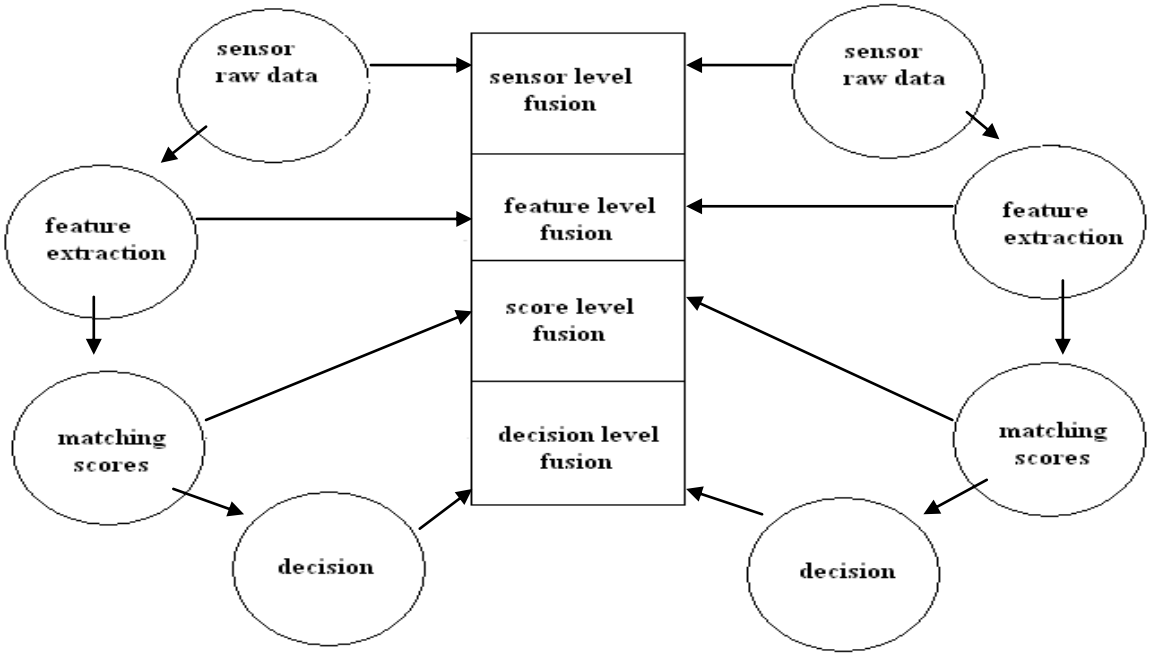


Figure 3.2 Various level of fusion

Figure 3.2 depict various levels of fusion with an illustration before and after matching score level. As it is clear from the figure, raw information acquired from different sensors are combined together before matching includes that raw information. Before the raw information processed to the matchers, features of the data are extracted in the form of feature vectors. These fusions are respectively called sensor-level fusion and feature-level fusion. These feature vectors are then used to generate the matching score when they are compared with previously saved templates. For information acquired in fusion after matching, the matching results at score and decision levels can be employed. The following sections provide a brief account of highest level of development over recent epoch.

3.4.1 Sensor Level Fusion: Sensor level is the most aboveboard level for the fusion because the information in the form of raw images can be fused here. However, the problem of incompatibility between the images or raw data (e.g. face and fingerprint) of different biometric modality, in raw form, it is very strange and impractical to concatenate the adopted data at this level. However, the problem of incompatibility exists with same biometric trait

too, e.g. the image taken by two different cameras may not have the same resolution or evidences of fingerprint may not be integrated, because these clues may have taken from different sensors (thermal, ultrasonic and/or capacitive).

3.4.2 Feature-Level Fusion: The information acquired at the sensor level reaches to the feature extraction level in digital form, but only a salient piece of data is kept to make a new data type. In feature level fusion, this information is preprocessed, and feature vectors are fetched out separately. The extracted feature vector is then use to represent the distinctive characteristics of the biometric traits. Many algorithms have been developed for the effective feature extraction, which shows the importance of feature level fusion. Fusion at feature level made up out of geometrical conjunction, coding means, and series/parallel schemes. According to Toh et al. [107] in fingerprint identification dealing with small sensor area a geometrical transformation was utilized to adjust the extracted minutia features prior to fuse them to figure out a large minutia template for later matching process.

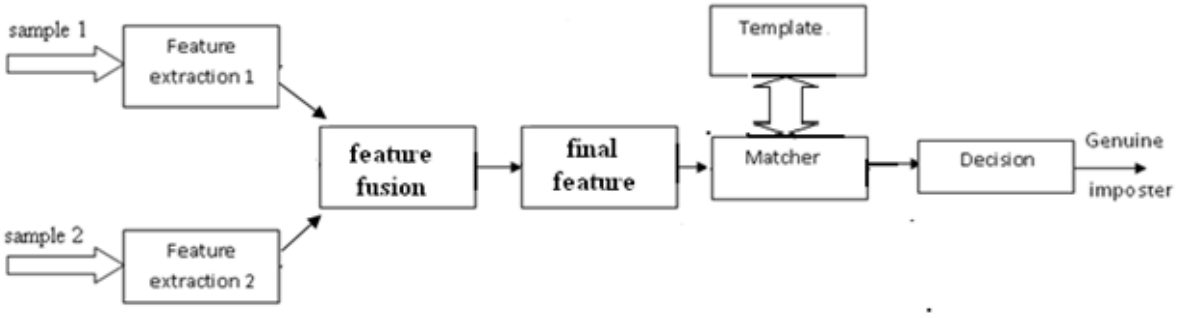


Figure 3.3 Feature level fusions

3.4.3 Decision Level Fusion: At this level user claims an identity either explicitly or implicitly, depending upon whether the screening is 1:1 or 1:N respectively. If the screening is 1:1, then the process is called verification and claim of identity either will be rejected or accepted. In case, if the screening is 1:N, then the process is called identification and the implicit claim made by the user will be checked to determine whether the user is already enrolled in the system or not.

At decision level, each classifier avails a decision. In decision level approach scores normalization is not required as it was mandatory in matching score level. Use of the decision level for fusion is beneficial only if the numbers of classifier are more than two,

because the problem that may occur with decision level fusion is the possibility of ties. Decision at this level can be combined in serial and parallel form, through AND and OR fusion rules respectively and rule helps to reduce FAR and OR rule helps to reduce the FRR. M. William et al. [[108] has shown that if two system, each having an FAR & FRR of 1%, on combination of AND and OR rules yields to FAR = 0.0882% and FRR = 0.0002%.

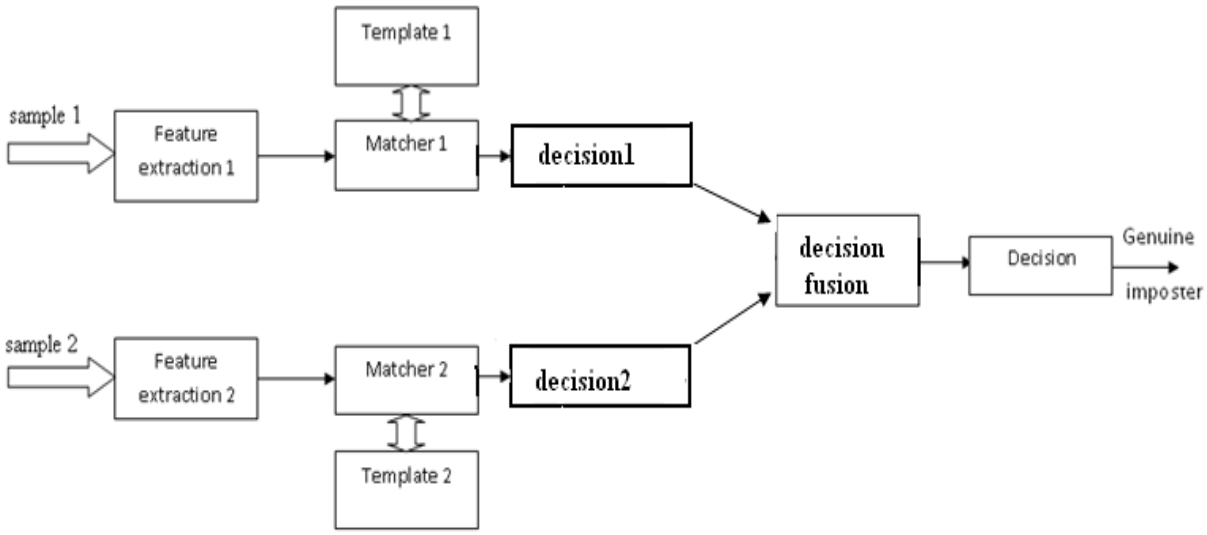


Figure 3.4 Decision level fusions

3.4.4 Score Level Fusion: It is obvious for every biometric system that they possess the information at sensors level in raw form only. Due to the incompatibility among the samples of different trait, in raw form, it is very unusual and impractical to fuse the acquired information at sensor level. However, at feature extraction level, if we look for and gather a salient piece of information, we can create the feature vectors out of raw data. Although, feature vectors contain a sufficient amount of information, achieving fusion is a bit complicated due to incompatibility in feature sets [109,110]. At decision level, user claims an identity to be verified or identified; depending upon the screening is either 1:1 or 1:N. In addition to this, the possibility of ties among the classifier results, make it impractical for fusion and the use of more number of classifier makes the system complex. When various feature vectors are compared with matchers, matching scores are generated. The main advantage of matching score level fusion is that either the problem of incompatibility of

scores is eliminated or the system can be trained. There are several methodologies have been developed for score level fusion which shows the importance of this level, such as:

- Transformation-based score level fusion
- Classifier-based score level fusion
- Density-based score level fusion

In our thesis we have worked on transformation based fusion, the matching score are needed to be normalized or transform to convert them in common domain.

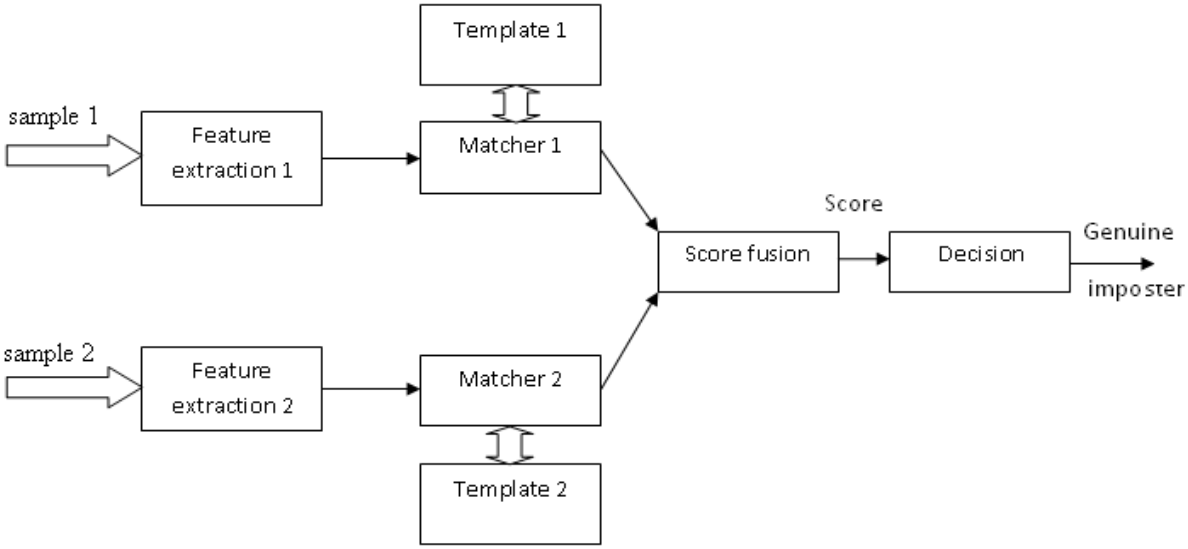


Figure 3.5 Score level fusions

3.5 Normalization

Normalization is a method to convert the matching scores obtained from the different matchers in a common domain [111]. In other words, normalization is used to unionize the database and to eliminate the inconsistency in the data. An effective transformation scheme not only estimates the location but also the scale parameters of the database. The matching scores obtained after normalization must be robust and efficient over the entire distribution. Robustness is necessary in case if outliers are present in the distribution and efficiency is required as to check the proximity of the estimated distribution [112]. But, the main issue is to select a technique which is robust and efficient in nature. Many normalization techniques have been discussed in the literature for the transformation of the data such as, Min-Max normalization, Z-Score normalization, Tanh-estimators normalization, Reduction of high-

scores effect (RHE) normalization, Decimal scaling etc. In this paper, Min-Max normalization technique, Z-score normalization technique and a new mathematical normalization technique [113] have been used to evaluate the performance of a biometric system.

3.5.1 Min-Max Normalization: This is one of the bare normalization methods, which uses upper and lower destined of the distribution. However, the whole distribution is confined in a range of 0 and 1. In case if minimum and maximum values are not known, they can be estimated by taking a finite range of the distribution, by following mathematical form [111]:

$$S'_k = \frac{S_k - min}{max - min}$$

Where, for a given set of matching scores S_k , S'_k are their normalized scores (k =1, 2, 3…, n).

3.5.2 Z-Score Normalization: z-score normalization technique estimates mean and standard deviation of matching scores to normalize the entire distribution. If μ and σ are the mean and standard deviation of the given database then normalized scores are given as [111]:

$$S'_k = \frac{S_k - \mu}{\sigma}$$

3.5.3 Tanh-Estimator: The tanh-estimator is one of the most commonly used normalization techniques and, is robust and highly efficient. This technique estimates the mean and standard deviation of the genuine and imposter score distribution. The normalized scores are given by [111]:

$$s'_k = \frac{1}{2}\left\{\tanh\left(0.01\left(\frac{s_k - \text{mean}}{\text{standard deviatio}}\right)\right) + 1\right\}$$

However, at the time of estimation, scores distributed at the end points are reduced. Therefore, this method is insensitive, efficient and robust. Karthik Nandakumar, developed a quality based fusion technique, in which biometric evidences of iris and fingerprint are integrated at matching score level. In this approach, the performance of the fusion is compared to the single biometric modality (iris) on the basis of genuine acceptance rate (GAR).

3.5.4 Median and Median Absolute Deviation: The median and median absolute deviation (MAD), are used for one of those normalization technique, which employ a moderate ratio of estimation on matching score. However, due to moderate assumption of estimation, the score may deviate from Gaussian assumption and, hence transformation lies far from optimal range of the score. The normalized scores are given by [111]:

$$s'_k = \frac{s_k - \text{median}}{|s_k - \text{median}|}$$

Median and MAD gives a normalization scheme which is robust in nature.

3.5.5 Decimal Scaling: when the matching scores for different modalities of different matchers are in logarithmic range decimal scaling normalization technique favoured above others. For example, if one matcher has scores in the range [0, 1] and the other has scores in the range [0, 1000], the following normalization could be applied. If $n = \log 10 \max(s_k)$ then,

$$S'_k = \frac{S_k}{10^n}$$

Due to the lack of robustness and the anticipation about matching scores to be for varied by a logarithmic range this approach is not widely used for normalization[111].

3.5.6 Mathematical Functional Normalization: A novel approach which employ a mathematical function which has two different forms; one is used for dissimilarity matching scores and other for the similarity matching scores. After normalization, the whole distribution spreads in the range of 0 and 1, i.e. the minimum values approaches toward 0 and maximum toward 1.this method is both efficient and robust in nature because it does not estimate the distribution and reduces the effect of outliers too. If s_k is the original matching score then normalized scores s'_k are given by [113].

$$S'_k = \frac{1}{2}\left(1 - \frac{S_k}{\sqrt{S_k^2 + \alpha}}\right)$$

And

$$S'_k = \frac{S_k}{\sqrt{s_k^2 + \alpha}}$$

Equation (1) and (2) give the transformation of dissimilarity and similarity scores respectively in the range of [0, 1]. Where, α is a constant which is known as smoothing parameter, i.e. it removes the irregularities from the distribution when assigned the higher value (e.g. α =50, 100…).

A general summary of the above discussed normalization techniques are given below.

Table3.2 Robustness and efficiency analysis of normalization technologies

Normalization techniques	Robustness	Efficiency
Min-Max	No	N/A
Decimal scaling	No	N/A
Z-Score	No	High (optimal for Gaussian data)
Median and MAD	Yes	Moderate
Tanh-Estimators	Yes	High
Mathematical Function	Yes	High

3.6 Evaluation Criterion for Identity Authentication

Any general biometric system works in two modes, first is verification and the other one is identification. In order to make a system to work in verification mode, the identity claimed by the user is compared with his template only i.e. in verification the screening is 1:1 always. In case of identification the test data is compared only against the templates of as many persons enrolled in the system. Since, in identification, the test data is compared with the template of every enrollee so here the screening is 1:N. The consequences of these matching are used to declare an individual as a genuine or as an imposter. In the process of verification or identification, there are some factors which help in deciding the accuracy and reliability of the system. The factors are given here in the form of different error rates.

- Genuine Acceptance Rate (GAR)
- False Acceptance Rate (FAR)
- False Rejection Rate (FRR)

3.7 Fusion Terminologies

The fusion methods can be divided in the following two categories.

3.7.1 Unsupervised Methods: in unsupervised methods of fusion there is no training process exist because learning rules are best suited for physical applications which works for pre-decided target marks. One of the most widely used unsupervised fusion method is SUM rule which inherently selects a balanced Gaussian distribution form the matching score of multiple biometrics used in fusion. Some other commonly followed unsupervised methods are as PRODUCT, MIN and MAX rules and weighted- SUM rule [114]. Most of the time these unsupervised methods are used in conjunction with normalization techniques to fuse the information of common type.

For the fusion at matching scores level, the approach developed by kittler et al. [114], is one of the favorite choice. As per the kittler theory, the posterior probabilities (which are obtained from matching scores of genuine or imposter) can be fused using sum, product, min and max rules. For this, if $\vec{x}_i$ be the feature vectors of the input pattern X, then the output is the posterior probability i.e. $P(w_j | \vec{x}_i)$, where w_j is class given the feature vector $\vec{x}_i$. These rules for R number of matchers are given below.

3.7.1.1 Sum Rule: This is one of the producive rule because it eliminates the problem of equivocalness during classification. In sum rule, transformed scores of every class are added together to get the final score. Here, input pattern is delegated to the class c such that[115]:

$$c = \text{argmax}_j \sum_{i=1}^{R} P\ \ w_j \mid \vec{x}_i$$

3.7.1.2 Product Rule: The product rule provides a less intended results than sum rule because it is based on the statistical independence of the feature vectores. The input pattern delegated to the class c is given by [115]:

$$c = \text{argmax}_j \prod_{i=1}^{R} P\ w_j \mid \vec{x}_i$$

3.7.1.3 Min Rule: In this rule a mimnum posterior probability is collected out of all classes. Hence, the input pattern delegated to the class c such that[115]:

$$c = \text{argmax}_j \min_i P\ w_j \mid \vec{x}_i$$

3.7.1.4 Max Rule: In max rule, the posterior probability is approximated by the maximum value of the input pattern.The input pattern delegated to the class c is given by [115]:

$$c = \text{argmax}_j \max_i P\ w_j \mid \vec{x}_i$$

3.7.2 Supervised Methods: The supervised methods of fusion make up a major factor in integration and decision making. Especially, a healthy number of studies in the field of pattern classification can be followed freely without any ambiguity for fusion and decision. The basis of the fusion work in this thesis is unsupervised methods so we limit our discussion to unsupervised methods of fusion only.

3.8 Database

To evaluate the performance of the above said three normalization techniques with the various fusion rules discussed in section 2.2 the NIST- *Biometric Scores Set - Release 1 (*BSSR1), biometric database has been used. This database has a large amount of matching scores of face, left index finger and right index finger, specially derived for the fusion process. BSSR1 biometric database consists of three different directories. The first directory contains 3000 face-face files, the second directory contains 6000 finger-finger files and the third directory contains 517 finger-face files. The third directory has a true multimodal database in which all three biometric evidences of a same person are accumulated. Hence for 517 subjects the third directory contains 517 genuine and 517 × 516 imposter scores for all three biometric modalities.

3.9 Summary

For the procedural examination of fusion approach, various set of matching scores are selected. Every time these data sets are normalized for the distribution of different scores in a common domain. These data sets are normalized using above discussed normalization techniques. This is to mention here while transforming the data in a common domain the removal of the outliers in from the matching score is not considered. Since the presence of outliers affect the ultimate result of the normalization so a comparative study is taken in to account to check the robustness and efficiency of every method. A novel approach which utilizes a mathematical function also used in the model development and has shown an appreciable performance over other methods. The evaluation of the unsupervised rule (sum, product, min and max) based score level fusion, is demonstrated in the form of FAR, FRR and GAR. In order to calculate FAR, FRR and GAR, from the matching scores we require setting up a minimum value after the fusion in the form of threshold to identify a person as an imposter or as genuine. The FAR and FRR value are the percentage of falsely accepted impostor scores divided by the total number of impostor scores and falsely rejected genuine scores divided by total number of rejection, respectively. The GAR value is the percentage of the number of genuinely given an entry divided by the total number of genuine scores. Hence, performance evaluation of unsupervised rules based score level fusion is dependent on FAR, FAR and GAR values obtained for different data set.

The purpose of analytical study is to investigate how multiple biometric modalities can be fuse for the creation of an effective authentication system. In this paper, the fusion of different biometric traits using transformation schemes and fusion rules is examined, and it is evaluated that every rule has its different advantages and drawbacks. The significant distinction between these methods has been made on the basis of recognition rates. It is clear from the performance tables that on an appropriate database, a good percentage of GARs over FARs & FRRs can be achieved with ease.

CHAPTER 4

RESULTS

4.1 Introduction

This chapter deals with the experimental studies that are pertained with the integration of face, left index finger and right index finger biometrics. The normalization techniques to convert the matching scores in common domain and unsupervised fusion approaches have been used to evaluate the model performance. As discussed earlier in chapter three, 2 preexisting normalization and a new normalization technique have been used to evaluate the system performance along with four unsupervised fusion rule. The investigations with each normalization and fusion method give different results. In these iterations, the matching scores of three biometric modalities subjected to one normalization and one fusion rule at a time and then a compassion table is formed to evaluate the comparative study of the experiment. The experiment results have been carried out on the database of 10 and 100 users.

4.2 Matching Scores from NIST BSSR- Relies 1

4.2.1 Origin of the Database: The matching score for all three biometric have been collected from NIST BSSR- Relies 1. Matching scores for fingerprints and faces have come from a freely available multi recognition system. The matching scores for these traits have been created when this system was examined with commercial arrangements in the FpVTE test. These tests were specially conducted for fingerprints. On the other side, the face scores were bringing into existence by two commercial face recognition systems.

4.2.2 Genuine Vs Impostor: In order to obtain the experiment results we have placed the matching scores in excel sheets. The genuine scores are separated from the impostor scores in a way that they arranged in the diagonals of the matrix.

4.2.3 Matching Scores for the Face, Left Index Finger and Right Index Finger: In Tables 4.1, Table 4.2 and Table 4.3 the matching scores that are settled at diagonal are the genuine scores, because they are generated after the matching of two images same person. Rest of the

matching score located in other places is the impostor scores, since they are produced after the comparing two images that belong to different persons.

Table 4.1 Matching score for faces of 10 users

Users	1	2	3	4	5	6	7	8	9	10
1	**0.575**	0.537	0.528	0.555	0.541	0.544	0.550	0.558	0.581	0.527
2	0.566	**0.785**	0.519	0.511	0.519	0.528	0.513	0.548	0.567	0.522
3	0.459	0.524	**0.814**	0.494	0.519	0.547	0.537	0.507	0.549	0.587
4	0.511	0.532	0.494	**0.829**	0.476	0.512	0.532	0.511	0.517	0.529
5	0.509	0.550	0.543	0.509	**0.590**	0.545	0.549	0.527	0.522	0.512
6	0.455	0.492	0.522	0.521	0.490	**0.675**	0.528	0.478	0.514	0.521
7	0.532	0.574	0.526	0.536	0.494	0.506	**0.671**	0.525	0.552	0.521
8	0.548	0.540	0.486	0.535	0.572	0.499	0.524	**0.778**	0.499	0.519
9	0.529	0.537	0.521	0.531	0.546	0.506	0.520	0.501	**0.699**	0.523
10	0.507	0.525	0.508	0.559	0.579	0.528	0.524	0.609	0.548	**0.589**

Table 4.2 Matching score for Left index finger of 10 users

Users	1	2	3	4	5	6	7	8	9	10
1	**29**	4	6	4	4	7	5	6	6	5
2		**6**	12	4	11	9	4	9	6	10
3	8	5	**63**	6	7	5	9	6	7	6
4	8	5	10	**73**	9	8	12	6	16	10
5	11	5	12	6	**175**	6	9	8	8	11
6	8	4	6	3	4	**10**	6	5	6	6
7	9	3	6	5	5	5	**11**	5	4	5
8	8	4	10	5	9	10	8	**38**	8	19
9	6	6	5	7	11	4	11	6	**142**	3
10	8	5	8	4	14	6	6	10	6	**34**

Table 4.3 Matching score for right index finger of 10 users

Users	1	2	3	4	5	6	7	8	9	10
1	**84**	5	5	4	8	6	10	7	5	4
2	7	**57**	4	8	11	10	7	7	5	5
3	7	7	**81**	4	6	9	5	4	9	9
4	5	6	5	**65**	6	8	4	4	13	5
5	5	10	7	5	**158**	14	3	5	5	13
6	8	6	5	4	5	**25**	7	6	4	4
7	14	7	5	8	8	6	**17**	10	9	9
8	8	5	4	3	6	7	5	**130**	5	5
9	6	5	7	12	6	7	5	6	**94**	7
10	6	11	9	5	10	11	5	8	5	**66**

4.3 Normalized Scores

Here we have calculated the normalized scores for these given matching scores. For this reason we use the formula for mathematical normalization, min–max normalization and Z-score normalization which are explained in third chapter.

4.3.1 Mathematical Function: In Table 4.4, Table 4.5 and Table 4.6 we have calculated the normalized scores for the for faces, left index finger and right index finger of 10 users through mathematical normalization respectively.

Table 4.4 Normalized scores for face of 10 users through Mathematical Normalization

Users	1	2	3	4	5	6	7	8	9	10
1	0.0287	0.0269	0.0264	0.0277	0.027	0.0272	0.0275	0.0279	0.029	0.0263
2	0.0283	0.0391	0.0259	0.0255	0.0259	0.0264	0.0256	0.0274	0.0284	0.0261
3	0.023	0.0262	0.0406	0.0247	0.0259	0.0273	0.0268	0.0254	0.0274	0.0293
4	0.0255	0.0266	0.0247	0.0413	0.0238	0.0256	0.0266	0.0256	0.0258	0.0264
5	0.0255	0.0275	0.0272	0.0255	0.0295	0.0273	0.0274	0.0264	0.0261	0.0256
6	0.0228	0.0246	0.0261	0.026	0.0245	0.0337	0.0264	0.0239	0.0257	0.026
7	0.0266	0.0287	0.0263	0.0268	0.0247	0.0253	0.0335	0.0262	0.0276	0.0261
8	0.0274	0.027	0.0243	0.0267	0.0286	0.025	0.0262	0.0388	0.0249	0.0259
9	0.0264	0.0268	0.026	0.0265	0.0273	0.0253	0.026	0.025	0.0349	0.0261
10	0.0254	0.0263	0.0254	0.0279	0.0289	0.0264	0.0262	0.0304	0.0274	0.0294

Table 4.5 Normalized scores for left index finger of 10 users through Mathematical Normalization

Users	1	2	3	4	5	6	7	8	9	10
1	0.473	0.186	0.257	0.186	0.186	0.287	0.224	0.257	0.257	0.224
2	0.431	0.257	0.384	0.186	0.37	0.334	0.186	0.334	0.257	0.354
3	0.312	0.224	0.494	0.257	0.287	0.224	0.334	0.257	0.287	0.257
4	0.312	0.224	0.354	0.495	0.334	0.312	0.384	0.257	0.424	0.354
5	0.37	0.224	0.384	0.257	0.499	0.257	0.334	0.312	0.312	0.37
6	0.312	0.186	0.257	0.144	0.186	0.354	0.257	0.224	0.257	0.257
7	0.334	0.144	0.257	0.224	0.224	0.224	0.37	0.224	0.186	0.224
8	0.312	0.186	0.354	0.224	0.334	0.354	0.312	0.484	0.312	0.442
9	0.257	0.257	0.224	0.287	0.37	0.186	0.37	0.257	0.499	0.144
10	0.312	0.224	0.312	0.186	0.407	0.257	0.257	0.354	0.257	0.48

Table 4.6 Normalized scores for right index finger of 10 users through Mathematical Normalization

Users	1	2	3	4	5	6	7	8	9	10
1	0.496	0.224	0.224	0.186	0.312	0.257	0.354	0.287	0.224	0.186
2	0.287	0.492	0.186	0.312	0.37	0.354	0.287	0.287	0.224	0.224
3	0.287	0.287	0.496	0.186	0.257	0.334	0.224	0.186	0.334	0.334
4	0.224	0.257	0.224	0.494	0.257	0.312	0.186	0.186	0.396	0.224
5	0.224	0.354	0.287	0.224	0.499	0.407	0.144	0.224	0.224	0.396
6	0.312	0.257	0.224	0.186	0.224	0.464	0.287	0.257	0.186	0.186
7	0.407	0.287	0.224	0.312	0.312	0.257	0.431	0.354	0.334	0.334
8	0.312	0.224	0.186	0.144	0.257	0.287	0.224	0.499	0.224	0.224
9	0.257	0.224	0.287	0.384	0.257	0.287	0.224	0.257	0.497	0.287
10	0.257	0.37	0.334	0.224	0.354	0.37	0.224	0.312	0.224	0.494

4.3.2 Min-Max Normalization Function: In Table 4.7, Table 4.8 and Table 4.9 we have calculated the normalized scores for the for faces, left index finger and right index finger of 10 users through min-max normalization respectively.

Table 4.7 Normalized scores for face of 10 users through Min-Max normalization

Users	1	2	3	4	5	6	7	8	9	10
1	1.0000	0.1554	0.1277	0.1821	0.5660	0.2544	0.2377	0.2687	0.4102	0.1876
2	0.9234	1.0000	0.0991	0.0493	0.3756	0.1623	0.0000	0.2337	0.3418	0.1214
3	0.0317	0.1079	1.0000	0.0000	0.3742	0.2701	0.1519	0.0988	0.2499	0.9632
4	0.4626	0.1376	0.0240	1.0000	0.0000	0.0735	0.1244	0.1127	0.0886	0.2111
5	0.4507	0.1980	0.1749	0.0446	1.0000	0.2607	0.2277	0.1654	0.1137	0.0000
6	0.0000	0.0000	0.1100	0.0794	0.1226	1.0000	0.0975	0.0000	0.0739	0.1060
7	0.6431	0.2792	0.1203	0.1259	0.1513	0.0362	1.0000	0.1567	0.2628	0.1187
8	0.7766	0.1647	0.0000	0.1202	0.8429	0.0000	0.0728	1.0000	0.0000	0.0842
9	0.6138	0.1521	0.1050	0.1102	0.6142	0.0350	0.0464	0.0766	1.0000	0.1329
10	0.4334	0.1144	0.0668	0.1936	0.9025	0.1636	0.0688	0.4364	0.2447	1.0000

Table 4.8 Normalized scores for left index finger of 10 users through Min-Max normalization

Users	1	2	3	4	5	6	7	8	9	10
1	1.0000	0.3333	0.0172	0.0143	0.0000	0.5000	0.1250	0.0303	0.0145	0.0645
2	0.4783	1.0000	0.1207	0.0143	0.0409	0.8333	0.0000	0.1212	0.0145	0.2258
3	0.0870	0.6667	1.0000	0.0429	0.0175	0.1667	0.6250	0.0303	0.0217	0.0968
4	0.0870	0.6667	0.0862	1.0000	0.0292	0.6667	1.0000	0.0303	0.0870	0.2258
5	0.2174	0.6667	0.1207	0.0429	1.0000	0.3333	0.6250	0.0909	0.0290	0.2581
6	0.0870	0.3333	0.0172	0.0000	0.0000	1.0000	0.2500	0.0000	0.0145	0.0968
7	0.1304	0.0000	0.0172	0.0286	0.0058	0.1667	0.8750	0.0000	0.0000	0.0645
8	0.0870	0.3333	0.0862	0.0286	0.0292	1.0000	0.5000	1.0000	0.0290	0.5161
9	0.0000	1.0000	0.0000	0.0571	0.0409	0.0000	0.8750	0.0303	1.0000	0.0000
10	0.0870	0.6667	0.0517	0.0143	0.0585	0.3333	0.2500	0.1515	0.0145	1.0000

Table 4.9 Normalized scores for right index finger of 10 users through Min-Max normalization

Users	1	2	3	4	5	6	7	8	9	10
1	2.6129	0.0645	0.0645	0.0323	0.1613	0.0968	0.2258	0.1290	0.0645	0.0323
2	0.1290	1.7419	0.0323	0.1613	0.2581	0.2258	0.1290	0.1290	0.0645	0.0645
3	0.1290	0.1290	2.5161	0.0323	0.0968	0.1935	0.0645	0.0323	0.1935	0.1935
4	0.0645	0.0968	0.0645	2.0000	0.0968	0.1613	0.0323	0.0323	0.3226	0.0645
5	0.0645	0.2258	0.1290	0.0645	5.0000	0.3548	0.0000	0.0645	0.0645	0.3226
6	0.1613	0.0968	0.0645	0.0323	0.0645	0.7097	0.1290	0.0968	0.0323	0.0323
7	0.3548	0.1290	0.0645	0.1613	0.1613	0.0968	0.4516	0.2258	0.1935	0.1935
8	0.1613	0.0645	0.0323	0.0000	0.0968	0.1290	0.0645	4.0968	0.0645	0.0645
9	0.0968	0.0645	0.1290	0.2903	0.0968	0.1290	0.0645	0.0968	2.9355	0.1290
10	0.0968	0.2581	0.1935	0.0645	0.2258	0.2581	0.0645	0.1613	0.0645	2.0323

4.3.3 Z-Score Normalization Function: In Table 4.10, Table 4.11 and Table 4.12 we have calculated the normalized scores for the for faces, left index finger and right index finger of 10 users through Z-score normalization respectively.

Table 4.10 Normalized scores for face of 10 users through Z-Score normalization

users	1	2	3	4	5	6	7	8	9	10
1	1.3956	-0.2705	-0.1888	-0.0291	0.2039	0.0994	0.1206	0.0480	0.4631	-0.2853
2	1.1663	2.7539	-0.2871	-0.4858	-0.3426	-0.2181	-0.6987	-0.0734	0.2225	-0.4653
3	-1.5014	-0.4405	2.8025	-0.6553	-0.3467	0.1534	-0.1751	-0.5416	-0.1009	1.8240
4	-0.2121	-0.3342	-0.5445	2.7841	-1.4208	-0.5240	-0.2698	-0.4934	-0.6687	-0.2214
5	-0.2478	-0.1180	-0.0270	-0.5017	1.4499	0.1211	0.0861	-0.3106	-0.5800	-0.7956
6	-1.5962	-0.8269	-0.2495	-0.3822	-1.0689	2.6688	-0.3626	-0.8843	-0.7201	-0.5073
7	0.3277	0.1727	-0.2143	-0.2224	-0.9864	-0.6527	2.7479	-0.3407	-0.0554	-0.4727
8	0.7273	-0.2370	-0.6268	-0.2418	0.9991	-0.7775	-0.4477	2.5850	-0.9803	-0.5666
9	0.2402	-0.2821	-0.2666	-0.2764	0.3425	-0.6568	-0.5390	-0.6186	2.5388	-0.4342
10	-0.2996	-0.4172	-0.3979	0.0106	1.1700	-0.2136	-0.4617	0.6296	-0.1191	1.9243

Table 4.11 Normalized scores for left index finger of 10 users through Z-Score normalization

Users	1	2	3	4	5	6	7	8	9	10
1	2.5645	-0.7379	-0.4463	-0.3569	-0.3955	0.0000	-1.1204	-0.3894	-0.3492	-0.6334
2	0.8356	1.3703	-0.1030	-0.3569	-0.2630	0.9258	-1.4818	-0.0899	-0.3492	-0.0966
3	-0.4610	0.3162	2.8148	-0.2642	-0.3387	-0.9258	0.3253	-0.3894	-0.3257	-0.5260
4	-0.4610	0.3162	-0.2174	2.8417	-0.3009	0.4629	1.4095	-0.3894	-0.1148	-0.0966
5	-0.0288	0.3162	-0.1030	-0.2642	2.8405	-0.4629	0.3253	-0.1897	-0.3023	0.0107
6	-0.4610	-0.7379	-0.4463	-0.4033	-0.3955	1.3887	-0.7590	-0.4892	-0.3492	-0.5260
7	-0.3170	-1.7920	-0.4463	-0.3106	-0.3766	-0.9258	1.0481	-0.4892	-0.3960	-0.6334
8	-0.4610	-0.7379	-0.2174	-0.3106	-0.3009	1.3887	-0.0361	2.8055	-0.3023	0.8696
9	-0.7492	1.3703	-0.5035	-0.2179	-0.2630	-1.3887	1.0481	-0.3894	2.8379	-0.8481
10	-0.4610	0.3162	-0.3318	-0.3569	-0.2063	-0.4629	-0.7590	0.0100	-0.3492	2.4799

Table 4.12 Normalized scores for right index finger of 10 users through Z-Score normalization

Users	1	2	3	4	5	6	7	8	9	10
1	7.8477	-0.6334	-0.6334	-0.7408	-0.3113	-0.5260	-0.0966	-0.4187	-0.6334	-0.7408
2	-0.4187	4.9491	-0.7408	-0.3113	0.0107	-0.0966	-0.4187	-0.4187	-0.6334	-0.6334
3	-0.4187	-0.4187	7.5256	-0.7408	-0.5260	-0.2040	-0.6334	-0.7408	-0.2040	-0.2040
4	-0.6334	-0.5260	-0.6334	5.8079	-0.5260	-0.3113	-0.7408	-0.7408	0.2254	-0.6334

5	-0.6334	-0.0966	-0.4187	-0.6334	15.7920	0.3328	-0.8481	-0.6334	-0.6334	0.2254
6	-0.3113	-0.5260	-0.6334	-0.7408	-0.6334	1.5137	-0.4187	-0.5260	-0.7408	-0.7408
7	0.3328	-0.4187	-0.6334	-0.3113	-0.3113	-0.5260	0.6549	-0.0966	-0.2040	-0.2040
8	-0.3113	-0.6334	-0.7408	-0.8481	-0.5260	-0.4187	-0.6334	12.7860	-0.6334	-0.6334
9	-0.5260	-0.6334	-0.4187	0.1181	-0.5260	-0.4187	-0.6334	-0.5260	8.9212	-0.4187
10	-0.5260	0.0107	-0.2040	-0.6334	-0.0966	0.0107	-0.6334	-0.3113	-0.6334	5.9153

4.4 Fused Scores

As discussed earlier, the fusion the data for three biometric traits has been evaluated with various fusion strategies. The data are not derived through any training process because those processes are best suited for physical applications which work for pre-decided target marks. These unsupervised fusion methods inherently selects a balanced Gaussian distribution form the matching score of multiple biometrics used in fusion. These unsupervised methods are used in conjunction with normalization techniques to fuse the information of common type.

4.4.1 Fused Data for Face, Left Index Finger and Right Index Finger: (Mathematics Normalization: Sum Rule Fusion) : The fusion scores in table 4.13 have been calculated by the simple sum of element of three biometrics traits with each other on the normalized data which is already evaluated through mathematical normalization. In Tables 4.13, the scores that are placed at diagonal are the fused genuine scores, afterward they are the outcome of combining three images that belong to the same user. The scores placed at other positions are the fused impostor scores and are obtained by combining three images that belong to different users.

Table 4.13 Fusion scores of mathematically normalized data using Sum rule

Users	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
1	0.9979	0.4362	0.5072	0.3991	0.5251	0.5712	0.6047	0.5719	0.5099	0.4356
2	0.7460	0.7889	0.5957	0.5236	0.7659	0.7144	0.4981	0.6486	0.5092	0.6032
3	0.6220	0.5365	1.0306	0.4677	0.5699	0.5854	0.5849	0.4683	0.6486	0.6210
4	0.5615	0.5075	0.6019	1.0309	0.6155	0.6503	0.5964	0.4685	0.8461	0.6036
5	0.6190	0.6046	0.6980	0.5063	1.0277	0.6914	0.5056	0.5623	0.5620	0.7919
6	0.6475	0.4675	0.5070	0.3554	0.4338	0.8515	0.5704	0.5047	0.4686	0.4690
7	0.7680	0.4591	0.5071	0.5628	0.5606	0.5061	0.8344	0.6034	0.5477	0.5842
8	0.6521	0.4363	0.5636	0.3940	0.6203	0.6653	0.5622	1.0209	0.5609	0.6920
9	0.5409	0.5077	0.5364	0.6974	0.6545	0.4977	0.6196	0.5395	1.0309	0.4565
10	0.5950	0.6198	0.6722	0.4372	0.7893	0.6536	0.5070	0.6963	0.5082	1.0035

4.4.2 Fused Data for Face, Left Index Finger and Right Index Finger: (Mathematics Normalization: Product Rule Fusion): The fusion scores in table 4.14 have been calculated by the simple product of elements of three biometrics traits with each other on the normalized data which is already evaluated through mathematical normalization. In Tables 4.14, the scores that are placed at diagonal are the fused genuine scores, afterward they are the outcome of combining three images that belong to the same user. The scores placed at other positions are the fused impostor scores and are obtained by combining three images that belong to different users.

Table 4.14 Fusion scores of mathematically normalized data using product rule

Users	1	2	3	4	5	6	7	8	9	10
1	0.0067	0.0011	0.0015	0.0010	0.0016	0.0020	0.0022	0.0021	0.0017	0.0011
2	0.0035	0.0050	0.0018	0.0015	0.0036	0.0031	0.0014	0.0026	0.0016	0.0021
3	0.0021	0.0017	0.0099	0.0012	0.0019	0.0020	0.0020	0.0012	0.0026	0.0025
4	0.0018	0.0015	0.0020	0.0101	0.0020	0.0025	0.0019	0.0012	0.0043	0.0021
5	0.0021	0.0022	0.0030	0.0015	0.0073	0.0029	0.0013	0.0018	0.0018	0.0038
6	0.0022	0.0012	0.0015	0.0007	0.0010	0.0055	0.0019	0.0014	0.0012	0.0012
7	0.0036	0.0012	0.0015	0.0019	0.0017	0.0015	0.0053	0.0021	0.0017	0.0019
8	0.0027	0.0011	0.0016	0.0009	0.0025	0.0025	0.0018	0.0094	0.0017	0.0026
9	0.0017	0.0015	0.0017	0.0029	0.0026	0.0013	0.0022	0.0017	0.0087	0.0011
10	0.0020	0.0022	0.0027	0.0012	0.0042	0.0025	0.0015	0.0034	0.0016	0.0070

4.4.3 Fused Data for Face, Left Index Finger and Right Index Finger: (Mathematics Normalization: Min Rule Fusion): The fusion scores in table 4.15 have been calculated by the taking the minimum of elements of three biometrics traits with from the normalized data which is already evaluated through mathematical normalization. In Tables 4.15, the scores that are placed at diagonal are the fused genuine scores, afterward they are the outcome of combining three images that belong to the same user. The scores placed at other positions are the fused impostor scores and are obtained by combining three images that belong to different users.

Table 4.15 Fusion scores of mathematically normalized data using min rule

Users	1	2	3	4	5	6	7	8	9	10
1	0.0287	0.0269	0.0264	0.0277	0.0270	0.0272	0.0275	0.0279	0.0290	0.0263
2	0.0283	0.0391	0.0259	0.0255	0.0259	0.0264	0.0256	0.0274	0.0284	0.0261
3	0.0230	0.0262	0.0406	0.0247	0.0259	0.0273	0.0268	0.0254	0.0274	0.0293
4	0.0255	0.0266	0.0247	0.0413	0.0238	0.0256	0.0266	0.0256	0.0258	0.0264
5	0.0255	0.0275	0.0272	0.0255	0.0295	0.0273	0.0274	0.0264	0.0261	0.0256
6	0.0228	0.0246	0.0261	0.0260	0.0245	0.0337	0.0264	0.0239	0.0257	0.0260
7	0.0266	0.0287	0.0263	0.0268	0.0247	0.0253	0.0335	0.0262	0.0276	0.0261
8	0.0274	0.0270	0.0243	0.0267	0.0286	0.0250	0.0262	0.0388	0.0249	0.0259
9	0.0264	0.0268	0.0260	0.0265	0.0273	0.0253	0.0260	0.0250	0.0349	0.0261
10	0.0254	0.0263	0.0254	0.0279	0.0289	0.0264	0.0262	0.0304	0.0274	0.0294

4.4.4 Fused Data for Face, Left Index Finger and Right Index Finger: (Mathematics Normalization: Max Rule Fusion): The fusion scores in table 4.16 have been calculated by the taking the maximum of elements of three biometrics traits with from the normalized data which is already evaluated through mathematical normalization. In Tables 4.16, the scores that are placed at diagonal are the fused genuine scores, afterward they are the outcome of combining three images that belong to the same user. The scores placed at other positions are the fused impostor scores and are obtained by combining three images that belong to different users.

Table 4.16 Fusion scores of mathematically normalized data using max rule

Users	1	2	3	4	5	6	7	8	9	10
1	0.496	0.224	0.257	0.186	0.312	0.287	0.354	0.287	0.257	0.224
2	0.431	0.492	0.384	0.312	0.37	0.354	0.287	0.334	0.257	0.354
3	0.312	0.287	0.496	0.257	0.287	0.334	0.334	0.257	0.334	0.334
4	0.312	0.257	0.354	0.495	0.334	0.312	0.384	0.257	0.424	0.354
5	0.37	0.354	0.384	0.257	0.499	0.407	0.334	0.312	0.312	0.396
6	0.312	0.257	0.257	0.186	0.224	0.464	0.287	0.257	0.257	0.257
7	0.407	0.287	0.257	0.312	0.312	0.257	0.431	0.354	0.334	0.334
8	0.312	0.224	0.354	0.224	0.334	0.354	0.312	0.499	0.312	0.442
9	0.257	0.257	0.287	0.384	0.37	0.287	0.37	0.257	0.499	0.287
10	0.312	0.37	0.334	0.224	0.407	0.37	0.257	0.354	0.257	0.494

4.4.5 Fused Data for Face, Left Index Finger and Right Index Finger (Min-Max Normalization: Sum Rule Fusion): The fusion scores in table 4.17 have been calculated by the simple sum of element of three biometrics traits with each other on the normalized data which is already evaluated through Min-Max normalization. In Tables 4.17, the scores that are placed at diagonal are the fused genuine scores, afterward they are the outcome of combining three images that belong to the same user. The scores placed at other positions are the fused impostor scores and are obtained by combining three images that belong to different users.

Table 4.17 Fusion scores of normalized (Min-Max) data using sum rule

Users	1	2	3	4	5	6	7	8	9	10
1	4.6129	0.5532	0.2095	0.2286	0.7272	0.8512	0.5885	0.4281	0.4892	0.2844
2	1.5307	3.7419	0.2520	0.2248	0.6746	1.2214	0.1290	0.4840	0.4208	0.4118
3	0.2477	0.9036	4.5161	0.0751	0.4885	0.6303	0.8414	0.1613	0.4652	1.2535
4	0.6141	0.9010	0.1747	4.0000	0.1260	0.9015	1.1567	0.1752	0.4981	0.5014
5	0.7326	1.0904	0.4246	0.1520	7.0000	0.9489	0.8527	0.3208	0.2072	0.5806
6	0.2482	0.4301	0.1918	0.1117	0.1871	2.7097	0.4766	0.0968	0.1207	0.2350
7	1.1283	0.4082	0.2021	0.3157	0.3185	0.2996	2.3266	0.3825	0.4564	0.3768
8	1.0249	0.5626	0.1185	0.1488	0.9690	1.1290	0.6373	6.0968	0.0935	0.6649
9	0.7106	1.2166	0.2341	0.4576	0.7519	0.1640	0.9859	0.2037	4.9355	0.2619
10	0.6171	1.0392	0.3120	0.2724	1.1868	0.7550	0.3833	0.7492	0.3237	4.0323

4.4.6 Fused Data for Face, Left Index Finger and Right Index Finger (Min-Max Normalization: Product Rule Fusion): The fusion scores in table 4.18 have been calculated by the simple sum of element of three biometrics traits with each other on the normalized data which is already evaluated through Min-Max normalization. In Tables 4.18, the scores that are placed at diagonal are the fused genuine scores, afterward they are the outcome of combining three images that belong to the same user. The scores placed at other positions are the fused impostor scores and are obtained by combining three images that belong to different users.

Table 4.18 Fusion scores of normalized (Min-Max) data using product rule.

Users	1	2	3	4	5	6	7	8	9	10
1	2.6129	0.0033	0.0001	0.0001	0.0000	0.0123	0.0067	0.0011	0.0004	0.0004
2	0.0570	1.7419	0.0004	0.0001	0.0040	0.0305	0.0000	0.0037	0.0003	0.0018
3	0.0004	0.0093	2.5161	0.0000	0.0006	0.0087	0.0061	0.0001	0.0011	0.0180
4	0.0026	0.0089	0.0001	2.0000	0.0000	0.0079	0.0040	0.0001	0.0025	0.0031
5	0.0063	0.0298	0.0027	0.0001	5.0000	0.0308	0.0000	0.0010	0.0002	0.0000
6	0.0000	0.0000	0.0001	0.0000	0.0000	0.7097	0.0031	0.0000	0.0000	0.0003
7	0.0298	0.0000	0.0001	0.0006	0.0001	0.0006	0.3952	0.0000	0.0000	0.0015
8	0.0109	0.0035	0.0000	0.0000	0.0024	0.0000	0.0023	4.0968	0.0000	0.0028
9	0.0000	0.0098	0.0000	0.0018	0.0024	0.0000	0.0026	0.0002	2.9355	0.0000
10	0.0036	0.0197	0.0007	0.0002	0.0119	0.0141	0.0011	0.0107	0.0002	2.0323

4.4.7 Fused Data for Face, Left Index Finger and Right Index Finger (Min-Max Normalization: Min Rule Fusion): The fusion scores in table 4.19 have been calculated by the taking the minimum of elements of three biometrics traits with from the normalized data which is already evaluated through mathematical normalization. In Tables 4.19, the scores that are placed at diagonal are the fused genuine scores, afterward they are the outcome of combining three images that belong to the same user. The scores placed at other positions are the fused impostor scores and are obtained by combining three images that belong to different users.

Table 4.19 Fusion scores of normalized (Min-Max) data using min rule

Users	1	2	3	4	5	6	7	8	9	10
1	1.0000	0.0645	0.0172	0.0143	0.0000	0.0968	0.1250	0.0303	0.0145	0.0323
2	0.1290	1.0000	0.0323	0.0143	0.0409	0.1623	0.0000	0.1212	0.0145	0.0645
3	0.0317	0.1079	1.0000	0.0000	0.0175	0.1667	0.0645	0.0303	0.0217	0.0968
4	0.0645	0.0968	0.0240	1.0000	0.0000	0.0735	0.0323	0.0303	0.0870	0.0645
5	0.0645	0.1980	0.1207	0.0429	1.0000	0.2607	0.0000	0.0645	0.0290	0.0000
6	0.0000	0.0000	0.0172	0.0000	0.0000	0.7097	0.0975	0.0000	0.0145	0.0323
7	0.1304	0.0000	0.0172	0.0286	0.0058	0.0362	0.4516	0.0000	0.0000	0.0645
8	0.0870	0.0645	0.0000	0.0000	0.0292	0.0000	0.0645	1.0000	0.0000	0.0645
9	0.0000	0.0645	0.0000	0.0571	0.0409	0.0000	0.0464	0.0303	1.0000	0.0000
10	0.0870	0.1144	0.0517	0.0143	0.0585	0.1636	0.0645	0.1515	0.0145	1.0000

4.4.8 Fused Data for Face, Left Index Finger and Right Index Finger (Min-Max Normalization: Max Rule Fusion): The fusion scores in table 4.20 have been calculated by the taking the minimum of elements of three biometrics traits with from the normalized data which is already evaluated through mathematical normalization. In Tables 4.20, the scores that are placed at diagonal are the fused genuine scores, afterward they are the outcome of combining three images that belong to the same user. The scores placed at other positions are the fused impostor scores and are obtained by combining three images that belong to different users.

Table 4.20 Fusion scores of normalized (Min-Max) data using max rule

Users	1	2	3	4	5	6	7	8	9	10
1	2.6129	0.3333	0.1277	0.1821	0.5660	0.5000	0.2377	0.2687	0.4102	0.1876
2	0.9234	1.7419	0.1207	0.1613	0.3756	0.8333	0.1290	0.2337	0.3418	0.2258
3	0.1290	0.6667	2.5161	0.0429	0.3742	0.2701	0.6250	0.0988	0.2499	0.9632
4	0.4626	0.6667	0.0862	2.0000	0.0968	0.6667	1.0000	0.1127	0.3226	0.2258
5	0.4507	0.6667	0.1749	0.0645	5.0000	0.3548	0.6250	0.1654	0.1137	0.3226
6	0.1613	0.3333	0.1100	0.0794	0.1226	1.0000	0.2500	0.0968	0.0739	0.1060
7	0.6431	0.2792	0.1203	0.1613	0.1613	0.1667	1.0000	0.2258	0.2628	0.1935
8	0.7766	0.3333	0.0862	0.1202	0.8429	1.0000	0.5000	4.0968	0.0645	0.5161
9	0.6138	1.0000	0.1290	0.2903	0.6142	0.1290	0.8750	0.0968	2.9355	0.1329
10	0.4334	0.6667	0.1935	0.1936	0.9025	0.3333	0.2500	0.4364	0.2447	2.0323

4.4.9 Fused Data for Face, Left Index Finger and Right Index Finger (Z-Score Normalization: Sum Rule Fusion): The fusion scores in table 4.21 have been calculated by the simple sum of element of three biometrics traits with each other on the normalized data which is already evaluated through Min-Max normalization. In Tables 4.21, the scores that are placed at diagonal are the fused genuine scores, afterward they are the outcome of combining three images that belong to the same user. The scores placed at other positions are the fused impostor scores and are obtained by combining three images that belong to different users.

Table 4.21 Fusion scores of normalized (Z-Score) data using sum rule.

Users	1	2	3	4	5	6	7	8	9	10
1	11.8077	-1.6418	-1.2685	-1.1268	-0.5029	-0.4267	-1.0964	-0.7601	-0.5195	-1.6594
2	1.5832	9.0733	-1.1309	-1.1541	-0.5949	0.6111	-2.5992	-0.5820	-0.7600	-1.1953
3	-2.3811	-0.5430	13.1430	-1.6603	-1.2115	-0.9764	-0.4832	-1.6717	-0.6306	1.0940
4	-1.3065	-0.5441	-1.3953	11.4337	-2.2477	-0.3724	0.3989	-1.6235	-0.5580	-0.9514
5	-0.9100	0.1016	-0.5487	-1.3994	20.0824	-0.0090	-0.4367	-1.1337	-1.5157	-0.5594
6	-2.3685	-2.0908	-1.3292	-1.5262	-2.0978	5.5712	-1.5403	-1.8995	-1.8100	-1.7741
7	0.3436	-2.0380	-1.2939	-0.8443	-1.6743	-2.1046	4.4508	-0.9265	-0.6554	-1.3101
8	-0.0451	-1.6083	-1.5850	-1.4005	0.1721	0.1926	-1.1173	18.1765	-1.9160	-0.3304
9	-1.0350	0.4548	-1.1888	-0.3762	-0.4466	-2.4642	-0.1242	-1.5340	14.2979	-1.7010
10	-1.2866	-0.0902	-0.9337	-0.9798	0.8671	-0.6658	-1.8541	0.3283	-1.1017	10.3194

4.4.10 Fused Data for Face, Left Index Finger and Right Index Finger (Z-Score Normalization: Product Rule Fusion): The fusion scores in table 4.22 have been calculated by the simple sum of element of three biometrics traits with each other on the normalized data which is already evaluated through Min-Max normalization. In Tables 4.22, the scores that are placed at diagonal are the fused genuine scores, afterward they are the outcome of combining three images that belong to the same user. The scores placed at other positions are the fused impostor scores and are obtained by combining three images that belong to different users.

Table 4.22 Fusion scores of normalized (Z-Score) data using product rule.

Users	1	2	3	4	5	6	7	8	9	10
1	28.0857	-0.1264	-0.0534	-0.0077	0.0251	0.0000	0.0131	0.0078	0.1024	-0.1339
2	-0.4080	18.6762	-0.0219	-0.0540	0.0010	0.0195	-0.4335	-0.0028	0.0492	-0.0285
3	-0.2898	0.0583	59.3670	-0.1283	-0.0618	0.0290	0.0361	-0.1562	-0.0067	0.1957
4	-0.0619	0.0556	-0.0750	45.9500	-0.2249	0.0755	0.2817	-0.1423	0.0173	-0.0136
5	-0.0045	0.0036	-0.0012	-0.0840	65.0407	-0.0187	-0.0238	-0.0373	-0.1111	-0.0019
6	-0.2291	-0.3210	-0.0705	-0.1142	-0.2678	5.6101	-0.1152	-0.2276	-0.1862	-0.1977
7	-0.0346	0.1296	-0.0606	-0.0215	-0.1156	-0.3179	1.8861	-0.0161	-0.0045	-0.0611
8	0.1044	-0.1108	-0.1009	-0.0637	0.1581	0.4520	-0.0102	92.7252	-0.1877	0.3121
9	0.0947	0.2449	-0.0562	0.0071	0.0474	-0.3819	0.3578	-0.1267	64.2757	-0.1542
10	-0.0727	-0.0014	-0.0269	0.0024	0.0233	0.0011	-0.2220	-0.0020	-0.0263	28.2276

4.4.11 Fused Data for Face, Left Index Finger and Right Index Finger (Z-Score Normalization: Min Rule Fusion): The fusion scores in table 4.23 have been calculated by the taking the minimum of elements of three biometrics traits with from the normalized data which is already evaluated through mathematical normalization. In Tables 4.23, the scores that are placed at diagonal are the fused genuine scores, afterward they are the outcome of combining three images that belong to the same user. The scores placed at other positions are the fused impostor scores and are obtained by combining three images that belong to different users.

Table 4.23 Fusion scores of normalized (z-score) data using min rule

Users	1	2	3	4	5	6	7	8	9	10
1	1.3956	-0.7379	-0.6334	-0.7408	-0.3955	-0.5260	-1.1204	-0.4187	-0.6334	-0.7408
2	-0.4187	1.3703	-0.7408	-0.4858	-0.3426	-0.2181	-1.4818	-0.4187	-0.6334	-0.6334
3	-1.5014	-0.4405	2.8025	-0.7408	-0.5260	-0.9258	-0.6334	-0.7408	-0.3257	-0.5260
4	-0.6334	-0.5260	-0.6334	2.7841	-1.4208	-0.5240	-0.7408	-0.7408	-0.6687	-0.6334
5	-0.6334	-0.1180	-0.4187	-0.6334	1.4499	-0.4629	-0.8481	-0.6334	-0.6334	-0.7956
6	-1.5962	-0.8269	-0.6334	-0.7408	-1.0689	1.3887	-0.7590	-0.8843	-0.7408	-0.7408
7	-0.3170	-1.7920	-0.6334	-0.3113	-0.9864	-0.9258	0.6549	-0.4892	-0.3960	-0.6334
8	-0.4610	-0.7379	-0.7408	-0.8481	-0.5260	-0.7775	-0.6334	2.5850	-0.9803	-0.6334
9	-0.7492	-0.6334	-0.5035	-0.2764	-0.5260	-1.3887	-0.6334	-0.6186	2.5388	-0.8481
10	-0.5260	-0.4172	-0.3979	-0.6334	-0.2063	-0.4629	-0.7590	-0.3113	-0.6334	1.9243

4.4.12 Fused Data for Face, Left Index Finger and Right Index Finger (Z-Score Normalization: Max Rule Fusion): The fusion scores in table 4.24 have been calculated by the taking the maximum of elements of three biometrics traits with from the normalized data which is already evaluated through mathematical normalization. In Tables 4.24, the scores that are placed at diagonal are the fused genuine scores, afterward they are the outcome of combining three images that belong to the same user. The scores placed at other positions are the fused impostor scores and are obtained by combining three images that belong to different users.

Table 4.24 Fusion scores of normalized (z-score) data using max rule

Users	1	2	3	4	5	6	7	8	9	10
1	7.8477	-0.2705	-0.1888	-0.0291	0.2039	0.0994	0.1206	0.0480	0.4631	-0.2853
2	1.1663	4.9491	-0.1030	-0.3113	0.0107	0.9258	-0.4187	-0.0734	0.2225	-0.0966
3	-0.4187	0.3162	7.5256	-0.2642	-0.3387	0.1534	0.3253	-0.3894	-0.1009	1.8240
4	-0.2121	0.3162	-0.2174	5.8079	-0.3009	0.4629	1.4095	-0.3894	0.2254	-0.0966
5	-0.0288	0.3162	-0.0270	-0.2642	15.7920	0.3328	0.3253	-0.1897	-0.3023	0.2254
6	-0.3113	-0.5260	-0.2495	-0.3822	-0.3955	2.6688	-0.3626	-0.4892	-0.3492	-0.5073
7	0.3328	0.1727	-0.2143	-0.2224	-0.3113	-0.5260	2.7479	-0.0966	-0.0554	-0.2040
8	0.7273	-0.2370	-0.2174	-0.2418	0.9991	1.3887	-0.0361	12.7860	-0.3023	0.8696
9	0.2402	1.3703	-0.2666	0.1181	0.3425	-0.4187	1.0481	-0.3894	8.9212	-0.4187
10	-0.2996	0.3162	-0.2040	0.0106	1.1700	0.0107	-0.4617	0.6296	-0.1191	5.9153

4.5 Performance Analysis on The Basis of Genuine Acceptance Rate (GAR) and False Acceptance Rate (FAR)

The operational consequences of unsupervised rules based fusion strategy have been evaluated in terms of Genuine Acceptance Rate (GAR) and False Acceptance Rate (FAR) for various thresholds. The GARs and FARs for all normalizations and fusion rules are computed as follows.

4.5.1 GAR and FRR Calculation for Mathematical Normalization: The Genuine Acceptance Rate and False Acceptance Rate for mathematical normalization with various fusion strategies have been evaluated and are shown in table 4.25.

Table 4.25 GAR and FRR for mathematical normalization with four fusion rules

	Sum			Product			Min			Max		
	Thres hold	GAR	FRR	Thres hold	GAR	FRR	Thres hold	GAR	FRR	Thres hold	GAR	FRR
Math. Norm.	0.7888	97	3	0.0049	100	0	0.0287	96	4	0.4310	98	2
	0.8344	99	1	0.0053	100	0	0.0294	99	1	0.4642	100	0
	0.8515		0	0.0055	100	0	0.0295	99	1	0.4925	100	0
	0.9979	100	0	0.0067	100	0	0.0335	100	0	0.4944	100	0
	1.0034	100	0	0.0069	100	0	0.0337	100	0	0.4954	100	0
	1.0208	100	0	0.0073	100	0	0.0349	100	0	0.4962	100	0
	1.0276	100	0	0.0086	100	0	0.0388	100	0	0.4965	100	0
	1.0306	100	0	0.0093	100	0	0.0391	100	0	0.4985	100	0
	1.0308	100	0	0.0099	100	0	0.0406	100	0	0.4988	100	0
	1.0309	100	0	0.0101	100	0	0.0413	100	0	0.4992	100	0

4.5.2 GAR and FRR Calculation for Min-Max Normalization: The Genuine Acceptance Rate and False Acceptance Rate for Min-Max normalization with various fusion strategies have been evaluated and are shown in table 4.26.

Table 4.26 GAR and FRR for Min-Max normalization with four fusion rules

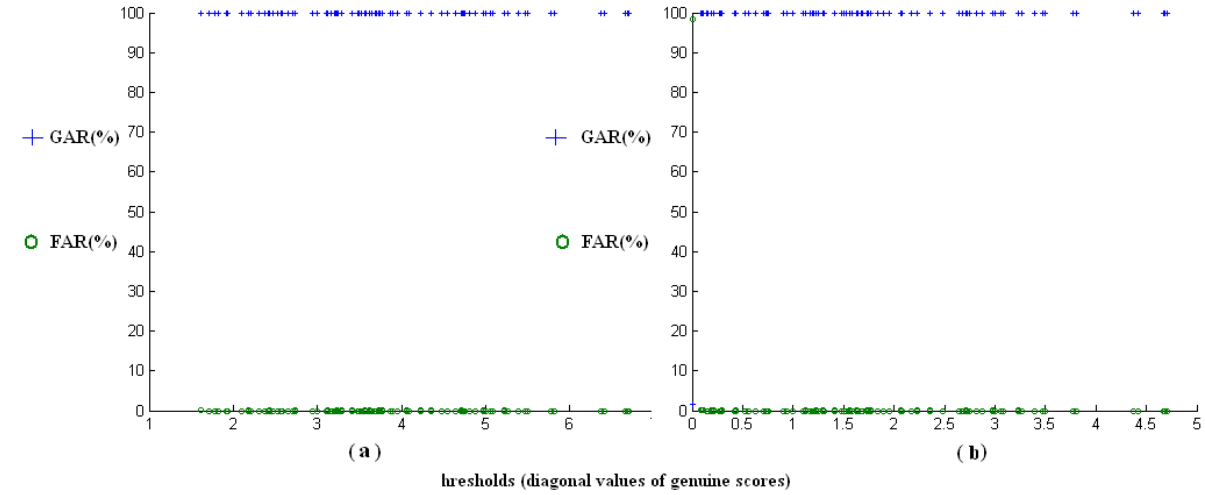
	Sum			**Product**			**Min**			**Max**		
	Thres hold	**GAR**	**FRR**	**Thres hold**	**GAR**	**FRR**	**Thres hold**	**GAR**	**FRR**	**Thres hold**	**GAR**	**FRR**
Min Max Norm	2.3266	100	0	0.3952	100	0	0.4516	93	7	1.0000	97	3
	2.7097	100	0	0.7097	100	0	0.7097	94	6	1.0000	96	4
	3.7419	100	0	1.7419	100	0	1.0000	95	5	1.7419	100	0
	4.0000	100	0	2.0000	100	0	1.0000	96	4	2.0000	100	0
	4.0323	100	0	2.0323	100	0	1.0000	97	3	2.0323	100	0
	4.5161	100	0	2.5161	100	0	1.0000	98	2	2.5161	100	0
	4.6129	100	0	2.6129	100	0	1.0000	99	1	2.6129	100	0
	4.9355	100	0	2.9355	100	0	1.0000	100	0	2.9355	100	0
	7.0000	100	0	4.0968	100	0	1.0000	100	0	4.0968	100	0
	2.3266	100	0	5.0000	100	0	1.0000	100	0	5.0000	100	0

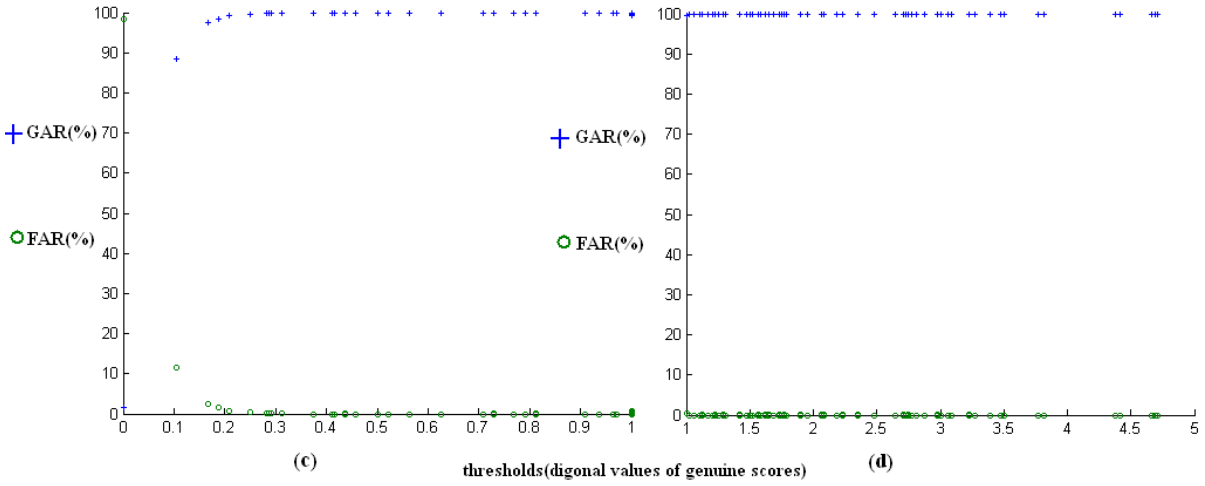
4.5.3 GAR and FRR Calculation for Z-Score Normalization: The Genuine Acceptance Rate and False Acceptance Rate for Z-score normalization with various fusion strategies have been evaluated and are shown in table 4.27.

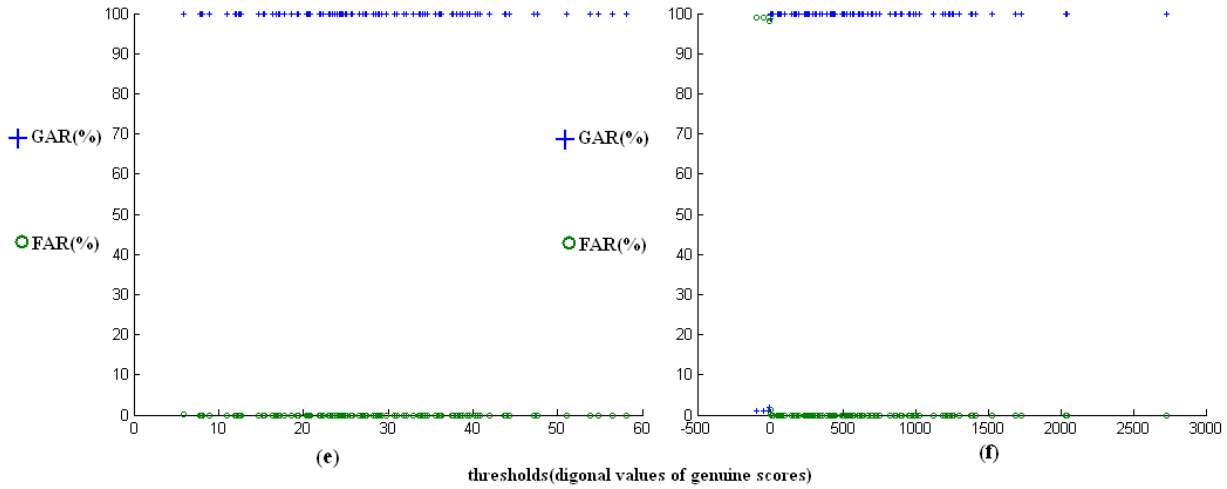
Table 4.27 GAR and FRR for Z-Score normalization with four fusion rules

	Sum			**Product**			**Min**			**Max**		
	Thres hold	**GAR**	**FAR**	**Thres hold**	**GAR**	**FAR**	**Thres hold**	**GAR**	**FAR**	**Thres hold**	**GAR**	**FAR**
Z-Score Norm	4.4508	100	0	1.8861	100	0	0.6549	100	0	2.6688	100	0
	5.5712	100	0	5.6101	100	0	1.3703	100	0	2.7479	100	0
	9.0733	100	0	18.676	100	0	1.3887	100	0	4.9491	100	0
	10.319	100	0	28.086	100	0	1.3956	100	0	5.8079	100	0
	11.434	100	0	28.228	100	0	1.4499	100	0	5.9153	100	0
	11.808	100	0	45.950	100	0	1.9243	100	0	7.5256	100	0
	13.143	100	0	59.367	100	0	2.5388	100	0	7.8477	100	0
	14.298	100	0	64.276	100	0	2.5850	100	0	8.9212	100	0
	18.177	100	0	65.041	100	0	2.7841	100	0	12.786	100	0
	20.082	100	0	92.725	100	0	2.8025	100	0	15.792	100	0

The results shown above are derived for 10 user data. We have also conducted the same procedure for the database of 100 users, and have shown the results in following graphs.


GAR(%)
FAR(%)
(a)
(b)
lresholds (diagonal values of genuine scores)


GAR(%)
FAR(%)
(c)
(d)
thresholds(digonal values of genuine scores)


GAR(%)
FAR(%)
(e)
(f)
thresholds(digonal values of genuine scores)

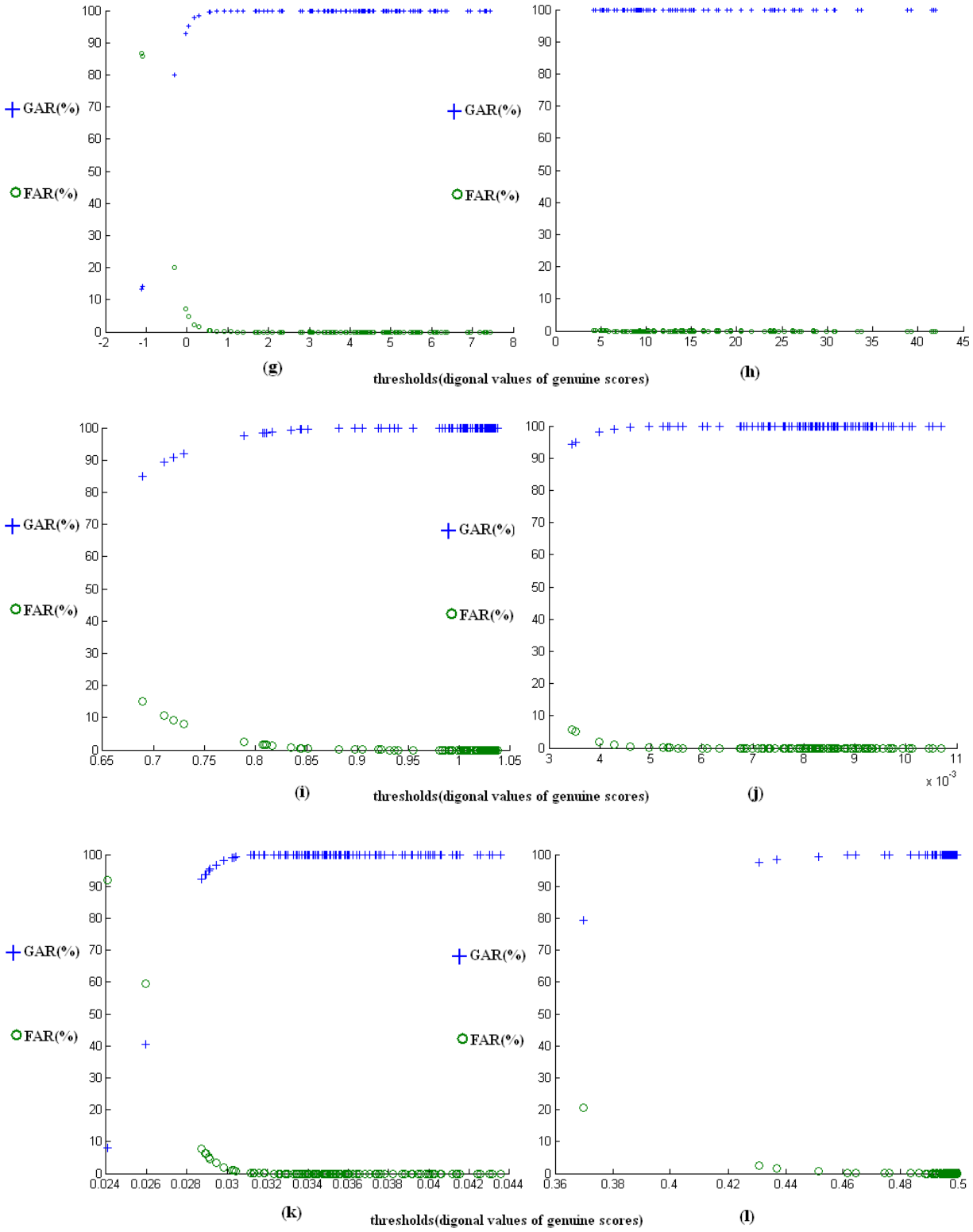


Figure 4.1 GARs and FARs for 100 users using for three normalization and four fusion rules.

Results obtained here are derived on the basis of various threshold values (genuine matching score obtained after the fusion) when compared with all other imposter values. Figure 4.1 (a), (b), (c) and (d) depicts the GARs and FARs for sum rule, product rule, min rule and max rule fusion respectively through min-max normalization. Figure 4.1 (e), (f), (g) and (h) depicts the GARs and FARs for sum rule, product rule, min rule and max rule fusion respectively through z-score normalization. Figure 4.1 (i), (j), (k) and (l) depicts the GARs and FARs for sum rule, product rule, min rule and max rule fusion respectively through mathematical normalization.

4.6 Summary

The operational performance of unsupervised rule-based integration on multimodal systems based on fingerprint and face have been judged. Our observational consequences suggest that a multimodal biometric system which aggregate more than one biometric entropies can accomplish statistically improve functioning compared to a single biometric arrangement. The performance of unsupervised rule-based fusion devolves on the alternative of standardization technique. Here in our experiment a novel normalization technique has been acquainted, which is called mathematical normalization. The output on all databases studied in this research disclose that mathematical normalization technique has improved performance when used for converting data in common domain and then used to implement fusion process. A comparative study has been carried out to check the performance of the mathematical normalization when compared with Min-Max and Z-Score normalization.

CHAPTER 5

Fuzzy Logic Implementation of Fusion

5.1 Introduction

This chapter provides a comprehensive overview of fuzzy logic in information fusion applications. Fuzzy logic offers an alternative mode to correspond verbal and subjective properties of the practical world in computing. Most of the time, fuzzy logic is able to be practised on control systems, but its utility is also appreciable in other applications due to its easiness of amending the efficiency and simplicity of the design process. It is a multi-valued system that permits intermediate values to be set between traditional evaluations like yes/no, high/low, true/false and 0/1. Opinions like instead tall or very fast can be developed mathematically and processed by computers, in order to achieve a more human-like behavior in programming of computers.

5.2 Why One Should Prefer Fuzzy Logic?

There are number of reasons based on the general observation that reveals the unmatched utility of the fuzzy logic, some of them are explained below.

- Fuzzy logic is user friendly and can be combined with conventional control proficiencies. The fact with the fuzzy logic system is that they don't inevitably substitute conventional control algorithms but most of the time it increase the efficiency of them and modify their execution.
- It is in wellness of the fuzzy system that it does not require prices data all the time i.e. Fuzzy logic is liberal of inaccurate information. In general every data that is available in raw form is almost imprecise or mixed with noise, but fuzzy logic system make the decision on the data instantly so as to avoid the misunderstanding and while waiting for the final result.
- Fuzzy logic is an expert tool which can model higher order functions of impulsive complexity.
- In a conceptual manner Fuzzy logic is effortless to realize and manipulate. The approach of mathematician implementation of fuzzy logic controller is very simple. This approach is so natural that every developed system has the quality of being intricate and compounded.

- Generally **f**uzzy logic is elastic in nature. One of the main advantages of the fuzzy system is that any number of input and out layer can be added to the system without affecting the previous functioning.
- In fuzzy logic a highly effective neural network can be implemented which works on training data and generate fuzzy results and a very dense model. Fuzzy logic lets you depend on the accumulation of knowledge or skill that result from direct participation in events or activities of someone who has prior knowledge of your system [116].

5.3 Why One Should Not Use Fuzzy Logic?

As we already know that a fuzzy logic is a preferential means to connect an input modality to an output modality. Fuzzy logic is based on the decision we made with commonsense i.e. fuzzy logic is an act of arranging in a systematic order of common sense we are likely build the correct decision. However, there are number of controllers, which perform a better job in absence of fuzzy logic. Furthermore, if we give proper time to get familiar with fuzzy logic, we can develop a very powerful system for that can perform well with imprecision and nonlinearity and can give. Some of the issue that give rise to not to use the fuzzy logic are mentioned below [116].

- Some time it is difficult to formulate a model with fuzzy logic due to complexity and more number of inputs/outputs.
- The input and out are fuzzy in nature for a fuzzy logic system i.e. they are not crisp in nature, so demand of a fine tuning to a greater extent during simulation is almost impossible.
- Fuzzy log is not discrete in nature
- Fuzzy logic system does not always give the definitive answers.
- In addition, it requires lot of data and expertise to develop a fuzzy system so it is difficult for an engineer to develop a system for a doctor.

5.4 Fuzzy Logic Toolbox

Fuzzy logic is one strongest part or the function of MATLAB i.e. a numeric computing tool for the engineering and scientific research work. The flexibility and usability of the fuzzy logic system with MATLAB explain its wide range of approach we can make and edit fuzzy inference systems within MATLAB; we can simulate the problem in the simulink of the MATLAB. Apart from this we can even make an independent program in the editors like

turboC, which then can be called in conjunction with MATLAB. Fuzzy logic works with both graphical user interface (GUI) tools and command line in MATLAB command window.

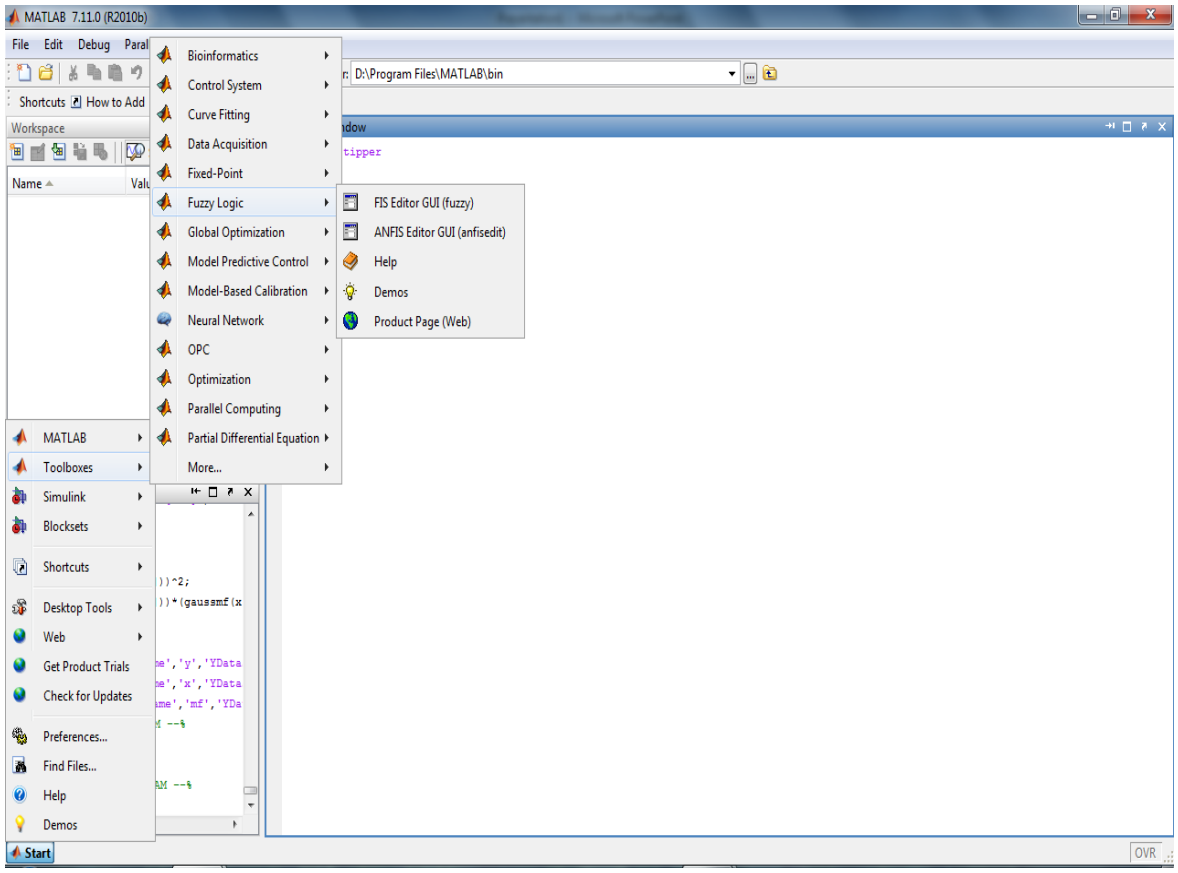


Figure 5.1 MATLAB: Fuzzy Logic Toolbox

The fuzzy logic toolbox consists of three classes of tools[116]:

- **Command Line Functions:** command line functions of the developed fuzz system can be called in the command prompt of the MATLAB or they can written as series of the commands in the M-file of system we developed. The ease of using the M-file for developing the system is that the system can be modified easily within the few change in the M-file.
- **Graphical Interactive Tools:** Working directly with the interactive tool of the fuzzy system is made possible by working with the GUI setup of the fuzzy system. In GUI based tool design, analysis, and implementation of the fuzzy inference system becomes easy and interactive.

➢ **Simulink Blocks and Examples:** fuzzy logic model can also be build up in Simulink simulation software with the using set of blocks. Simulink helps in developing a high speed fuzzy logic inference in the Simulink surroundings.

The basic structure of a fuzzy toolbox is consisting of various functions shown in the figure 5.2.

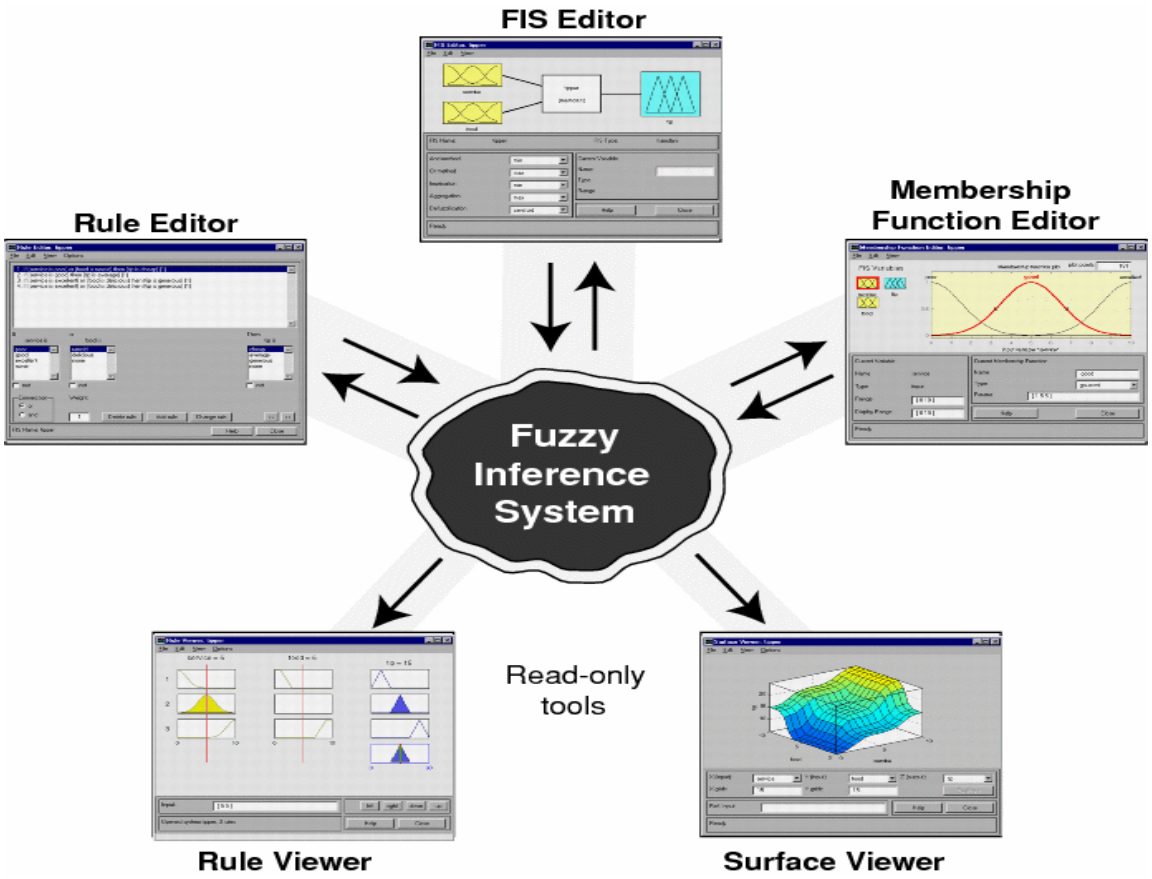


Figure 5.2 Fuzzy logic toolbox functions

5.5 Fusion Approach of Multiple Traits through Fuzzy Logic

Fuzzy logic is a powerful tool which has shown its ultimate utility in applications such as modeling, designing, and controlling of complex and non-linear systems. In our research work we have also demonstrated some of the ability of fuzzy logic through a fusion example of multiple biometric traits. For the analytical reasoning of the fusion process, fuzzy logic

comprises input from various matching score of different modality to control the spoof attacks and verifying genuine persons.

5.5.1 Fuzzy Inference System (FIS) Editor: The very first component of the fuzzy logic toolbox is FIS editor which covers the upper-level consequences for the system of rules. It is the FIS editor which deals in determining the number of input and out modalities and specifies them with a certain name. The number of input and the output of the model depend upon the kind of application and system memory, fuzzy logic toolbox never limits them. Although, it is very high speed environment, but, if there are multiple inputs with high valued membership functions, then it is difficult for the FIS system to implement or examine the model using the other GUI tools.

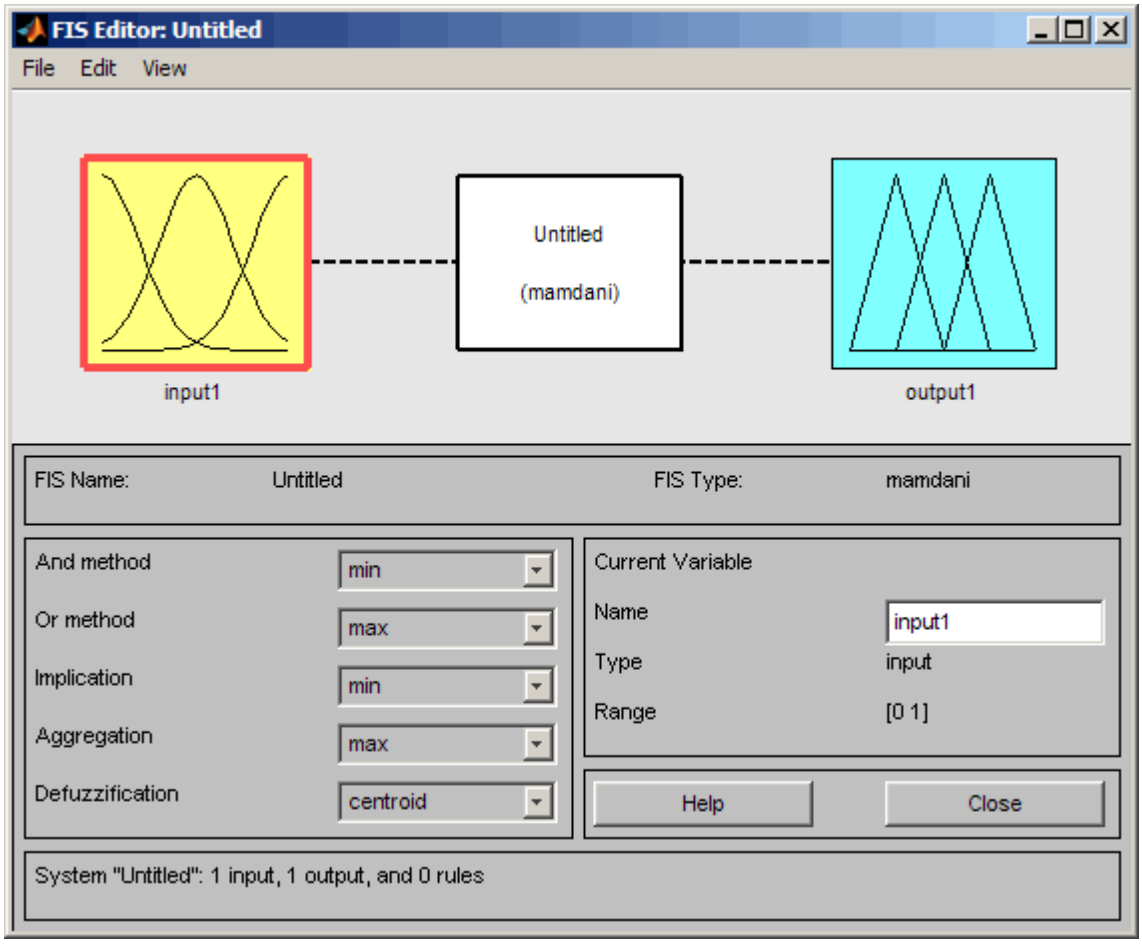


Figure 5.3 FIS editor of fuzzy logic toolbox

5.5.2 Adding & Defining Input/Output: When we work with fuzzy toolbox we need to define the input and output variable according to the system requirement. In order to define

the variables, when we type <fuzzy> on the command window of the MATLAB following window will open as shown in the figure 5.4. This window is basically the Fuzzy Inference System editor. For every fuzzy logic we have one input and one output by default and we use the Mamdani inference and collection method. The FIS editor of the fuzzy toolbox consists of three component of a fuzzy system;

1) Fuzzification

2) Fuzzy inference

3) Defuzzification

Practically any number of input/out variables can be added to a fuzzy inference system. The process of adding the new variable is depicted in the Figure 5.4

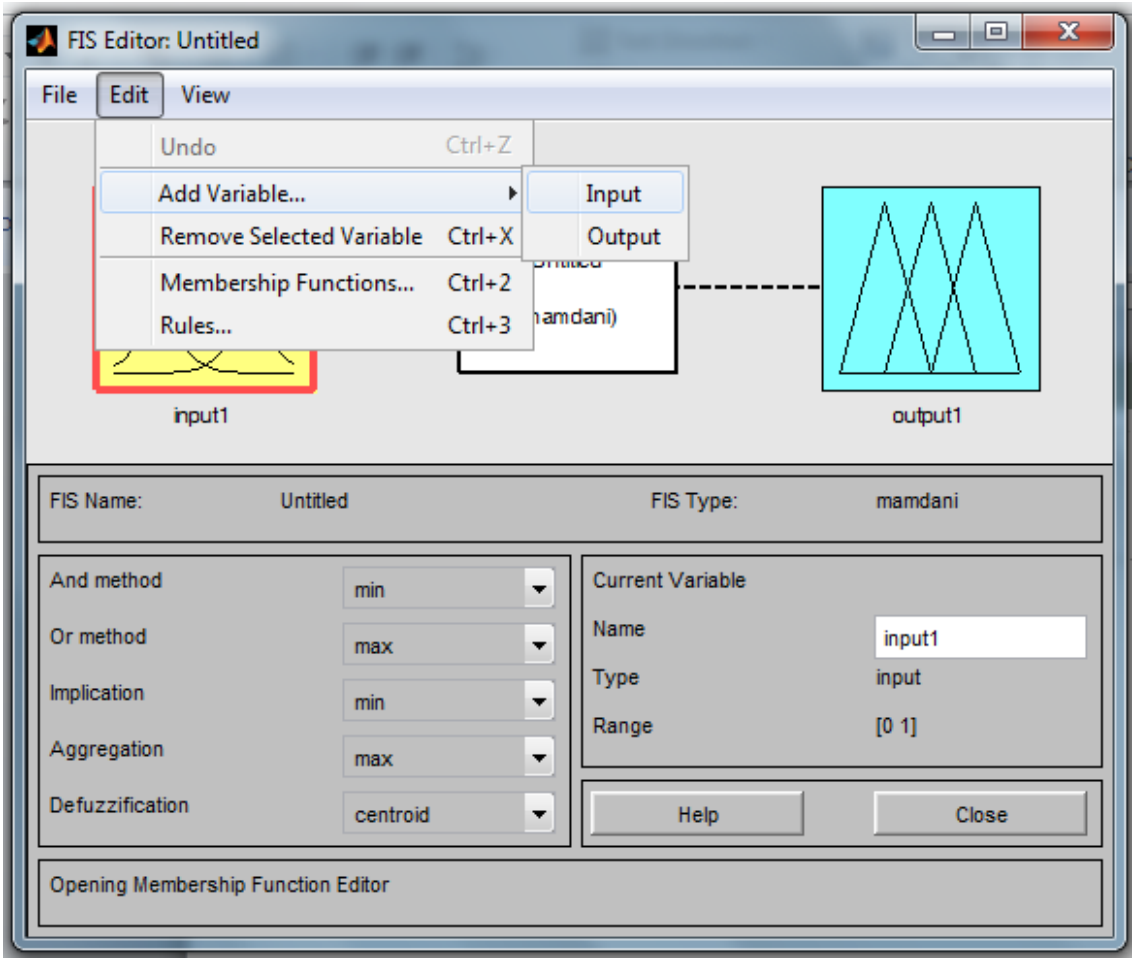


Figure 5.4 FIS Editor: Adding Input / Output

In figure 5.5, we have defined the three input variables as face_data, lf_data and rf_data and an output variable as final_decision. In this editor,

- when we double click on an input/output variable a membership function editor opens. Here, we can define the multiple number of membership functions for every input and output variable according to the need of the application and fuzziness of the system.
- Double clicking on system diagram which is named as fusion_bio opens a rule editor window.
- The pop-up menus are used to set up the fuzzy inference system such as defuzzification method.

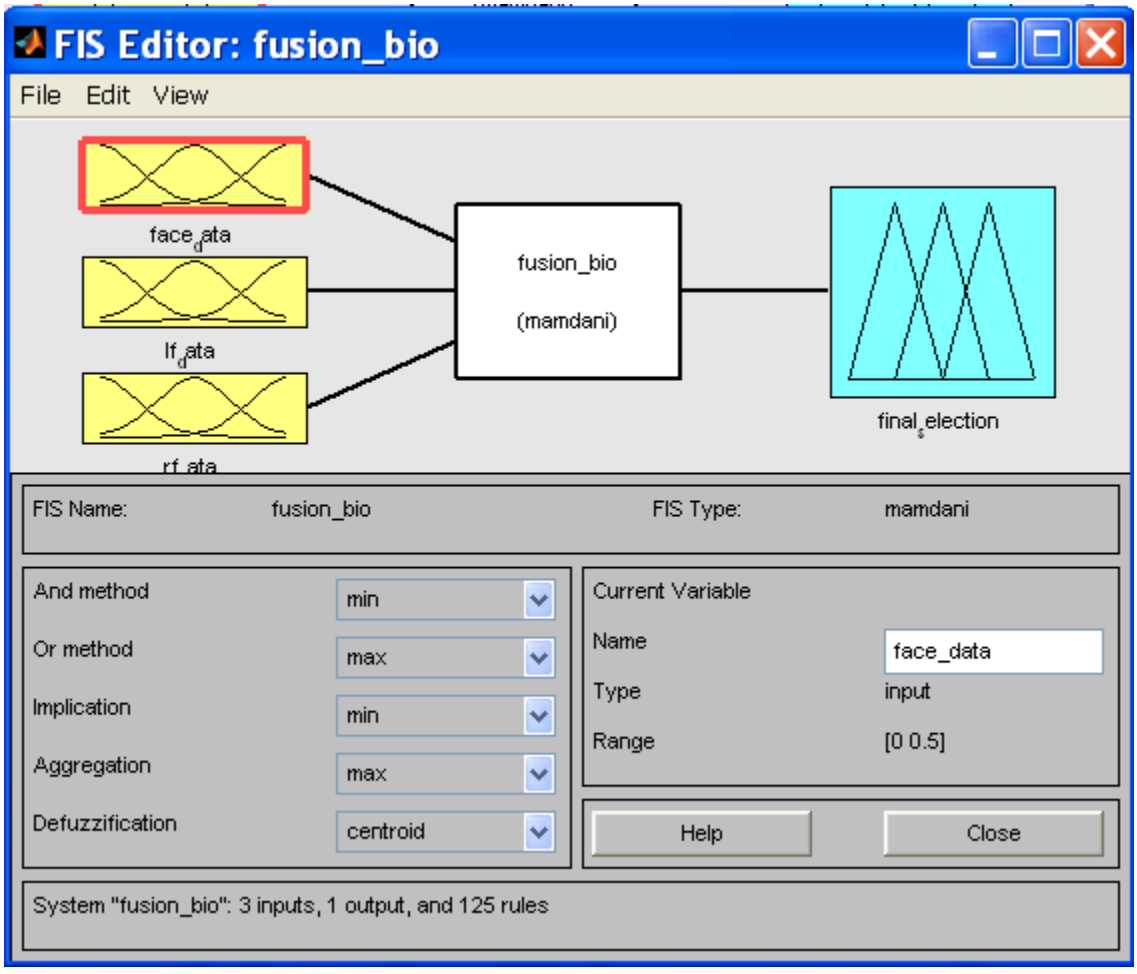


Figure 5.5 Fusion problem: defining input and output

5.5.3 Membership Functions: Although the Membership Function Editor is different from the FIS editor still it contributes some characteristics with the FIS Editor. If we consider the fact then almost every basic GUI of the fuzzy toolbox shares some of the parts or characteristics with each other such as menu alternatives, position lines, and Help and Close option. With the help of the Membership Function Editor we can edit and exhibit all of the membership functions linked with all of the input and output variables of the given fuzzy inference system.

In order to assemble our own membership functions linked with the input and output variable for the Fuzzy Inference System, select an FIS variable in this region from the edit menu. From here, we can choose option of adding the membership functions of input or output type.

Furthermore, after the selection of the membership function we can change the name, type (e.g. triangular and trapezoidal), and parameters.

The procedure of assigning the input membership functions for this three input fusion problem is as follows:

- Select variable of input type, name it as face_data. Now adjust both the Range and the Display Range to the vector [0 1] in the GUI.
- Add five membership functions from the Edit menu.
- Classify all the membership functions as triangular and trapezoidal accordingly.
- This adds three triangular curves and 2 trapezoidal curves to the input variable face_data.
- Here we can give the appropriate name to all five membership functions such as Very low, Low, medium, High and Very high respectively.
- To adjust the shape of the membership function we can give desired parameter change to the membership functions.
- Likewise we will select the other input variables, lf_data and rf_data, to set the Range and
- the Display Range to the vector [0 1] in the GUI.
- The only output variable will also be set up accordingly, here in output variable we will take three membership functions named as reject, reenter and accepted on the basis of decision made by the rules formed.

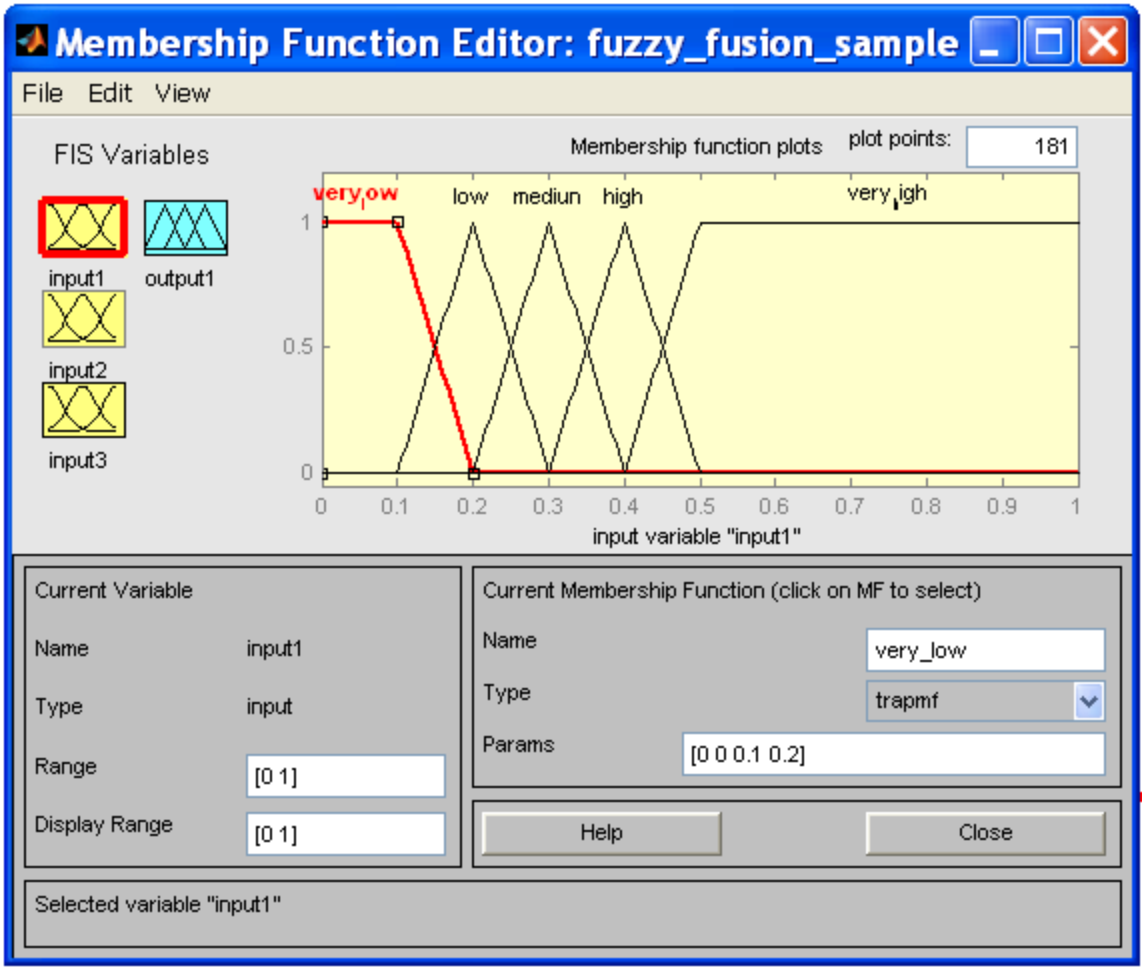


Figure 5.6 Input variable for the face matching scores

Table 5.1 Range for the membership functions of face (input1)

Membership function	Function Type	Range
Very_Low	trapezoidal	[0 0 0.1 0.2]
Low	tringular	[0.1 0.2 0.3]
Medium	tringular	[0.2 0.3 0.4]
High	tringular	[0.3 0.4 0.5]
Very_High	trapezoidal	[0.4 0.5 1 1]

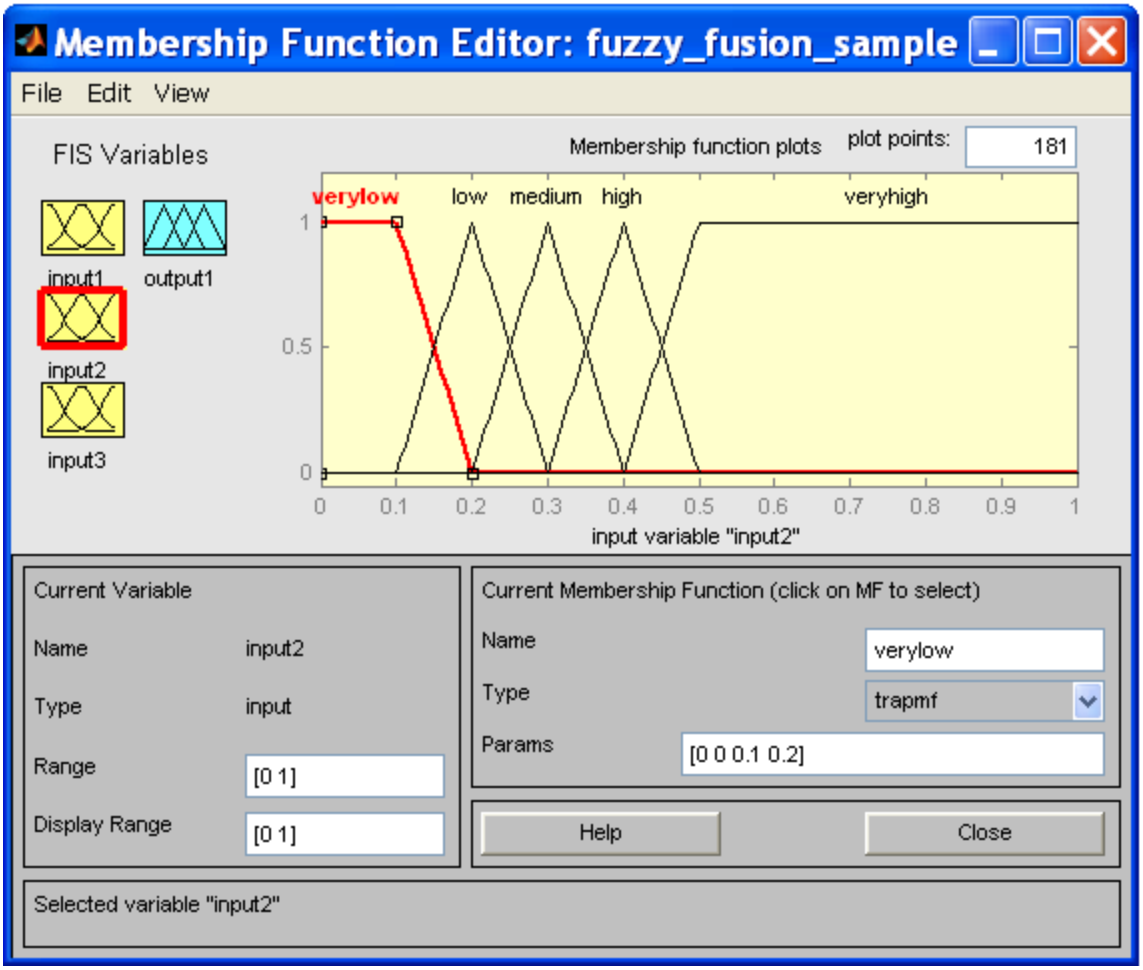


Figure 5.7 Input variable for the lf_data (left index finger) matching scores

Table 5.2 Range for the membership functions of left index finger (input2)

Membership Functions	Function Type	Range
Very_Low	trapezoidal	[0 0 0.1 0.2]
Low	triangular	[0.1 0.2 0.3]
Medium	triangular	[0.2 0.3 0.4]
High	triangular	[0.3 0.4 0.5]
Very_High	trapezoidal	[0.4 0.5 1 1]

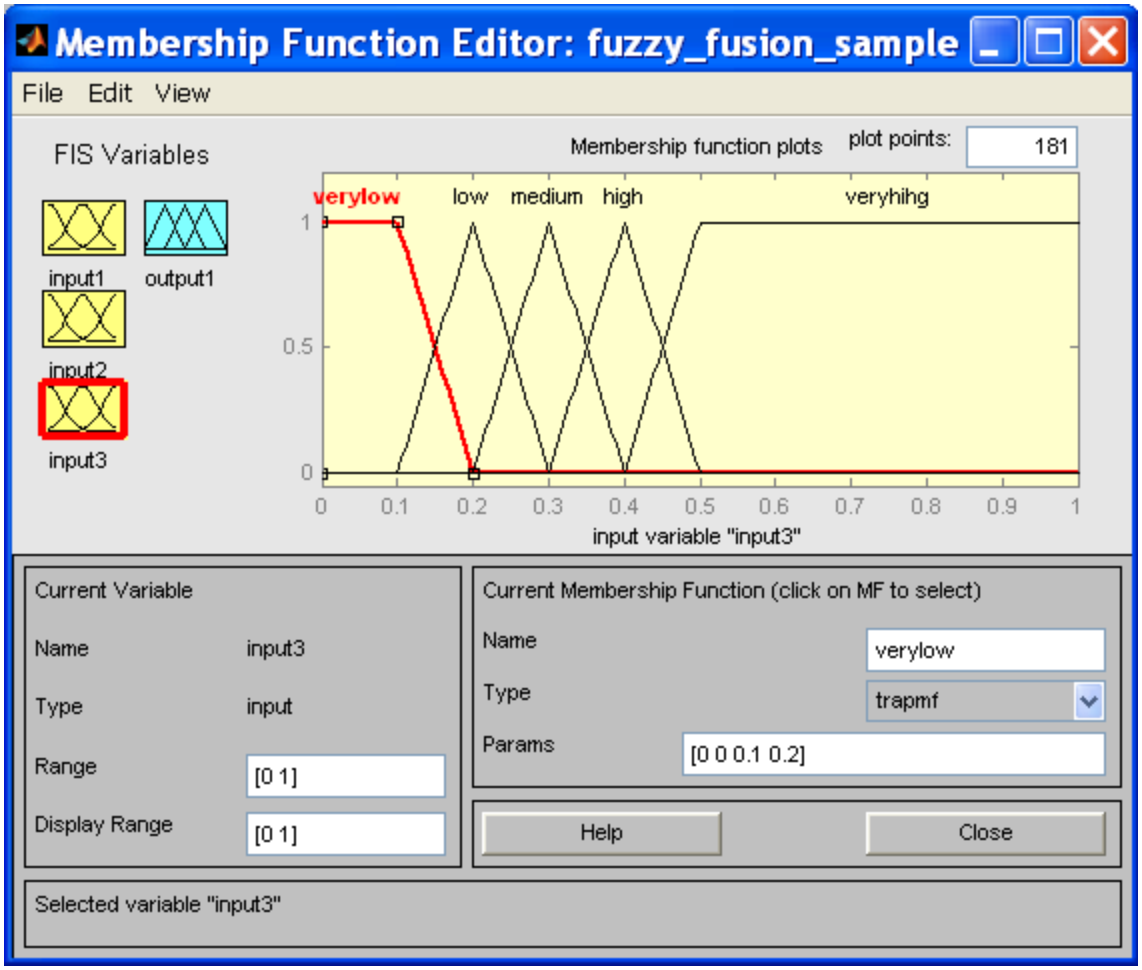


Figure 5.8 Input variable for the rf_data(right index finger) matching scores

Table 5.3 Range for the membership functions of right index finger (input2):

Membership Functions	Function Type	Range
Very_Low	Trapezoidal	[0 0 0.1 0.2]
Low	Triangular	[0.1 0.2 0.3]
Medium	Triangular	[0.2 0.3 0.4]
High	Triangular	[0.3 0.4 0.5]
Very_High	Trapezoidal	[0.4 0.5 1 1]

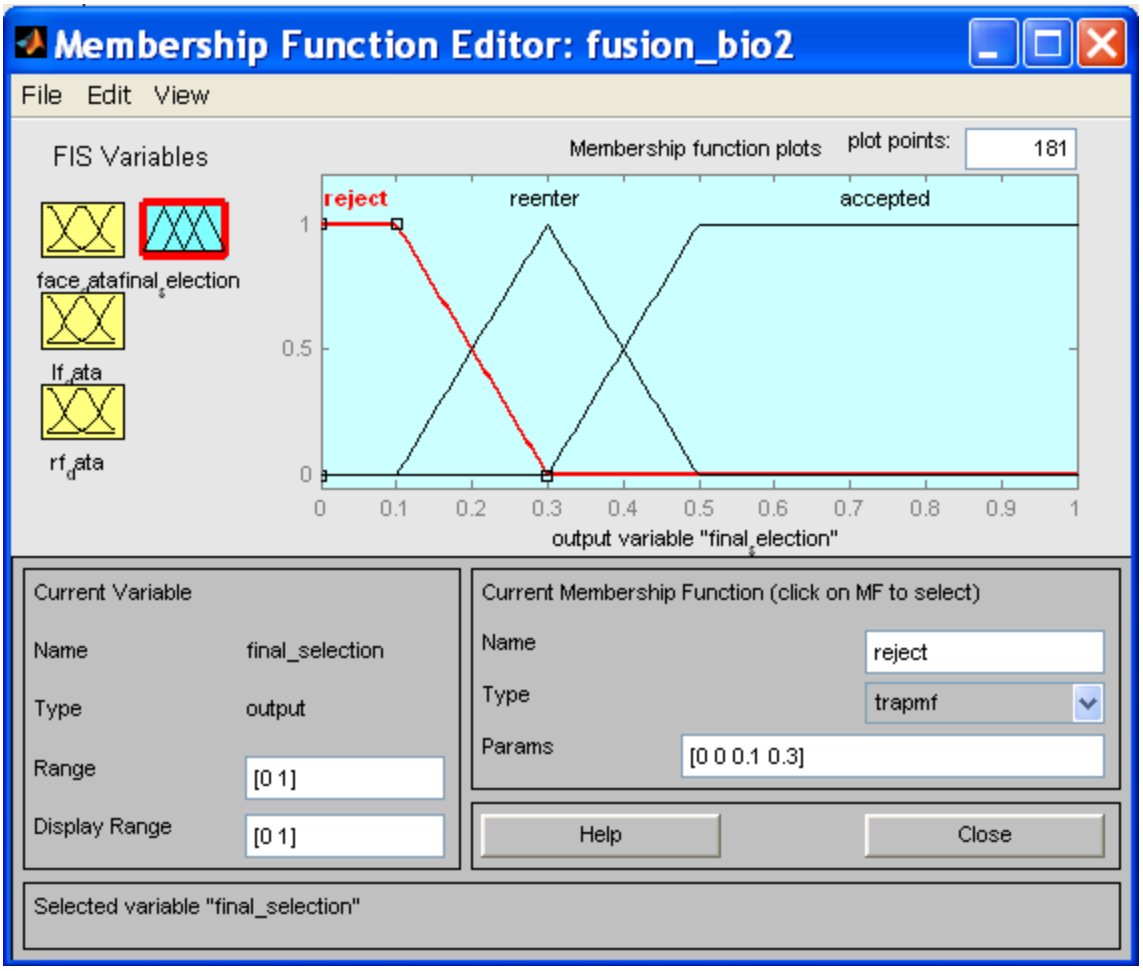


Figure 5.9 Output variable for the final decision of the fusion

Table 5.4 Output of the comparison study

Membership Functions	Function Type	Range
Reject	trapezoidal	[0 0 0.1 0.3]
Reenter	triangular	[0.1 0.3 0.5]
accepted	trapezoidal	[0.3 0.5 1 1]

5.5.4 Fuzzy Set of Rules

The construction of the rules can be achieved either using graphical Rule Editor Interface or using M-file. The structure of the fuzzy rules is based on the statements of the input and

output variables set to achieve a higher degree of accurate and precise decision with FIS Editor. In our research work we have developed the rule base for the fusion system in M-file only. The use of M-file for the construction of the rule base gives a higher degree of freedom and fastens the process.

The resulting rules are:

1. If (face_data is very low) and (lf_data is very low) and (rf_data is very low) then (final_selection is reject) (1)
2. If (face_data is very low) and (lf_data is very low) and (rf_data is low) then (final_selection is reject) (1)
3. If (face_data is very low) and (lf_data is very low) and (rf_data is medium) then (final_selection is reenter) (1)
4. If (face_data is very low) and (lf_data is very low) and (rf_data is high) then (final_selection is reenter) (1)
5. If (face_data is very low) and (lf_data is very low) and (rf_data is very high) then (final_selection is accepted) (1)
6. If (face_data is very low) and (lf_data is low) and (rf_data is very low) then (final_selection is reenter) (1)
7. If (face_data is very low) and (lf_data is low) and (rf_data is low) then (final_selection is reject) (1)
8. If (face_data is very low) and (lf_data is low) and (rf_data is medium) then (final_selection is reenter) (1)
9. If (face_data is very low) and (lf_data is low) and (rf_data is high) then (final_selection is reenter) (1)
10. If (face_data is very low) and (lf_data is low) and (rf_data is very high) then (final_selection is accepted) (1)
11. If (face_data is very low) and (lf_data is medium) and (rf_data is very low) then (final_selection is accepted) (1)

12. If (face_data is very low) and (lf_data is medium) and (rf_data is low) then (final_selection is reenter) (1)

13. If (face_data is very low) and (lf_data is medium) and (rf_data is medium) then (final_selection is reject) (1)

14. If (face_data is very low) and (lf_data is medium) and (rf_data is high) then (final_selection is reenter) (1)

15. If (face_data is very low) and (lf_data is medium) and (rf_data is very high) then (final_selection is accepted) (1)

16. If (face_data is very low) and (lf_data is high) and (rf_data is very low) then (final_selection is reenter) (1)

17. If (face_data is very low) and (lf_data is high) and (rf_data is low) then (final_selection is accepted) (1)

18. If (face_data is very low) and (lf_data is high) and (rf_data is medium) then (final_selection is reenter) (1)

19. If (face_data is very low) and (lf_data is high) and (rf_data is high) then (final_selection is reenter) (1)

20. If (face_data is very low) and (lf_data is high) and (rf_data is very high) then (final_selection is reenter) (1)

21. If (face_data is very low) and (lf_data is very high) and (rf_data is very low) then (final_selection is accepted) (1)

22. If (face_data is very low) and (lf_data is very high) and (rf_data is low) then (final_selection is accepted) (1)

23. If (face_data is very low) and (lf_data is very high) and (rf_data is medium) then (final_selection is accepted) (1)

24. If (face_data is very low) and (lf_data is very high) and (rf_data is high) then (final_selection is accepted) (1)

25. If (face_data is very low) and (lf_data is very high) and (rf_data is very high) then (final_selection is reenter) (1)

26. If (face_data is low) and (lf_data is very low) and (rf_data is very low) then (final_selection is reenter) (1)

27. If (face_data is low) and (lf_data is very low) and (rf_data is low) then (final_selection is accepted) (1)

28. If (face_data is low) and (lf_data is very low) and (rf_data is medium) then (final_selection is reenter) (1)

29. If (face_data is low) and (lf_data is very low) and (rf_data is high) then (final_selection is reenter) (1)

30. If (face_data is low) and (lf_data is very low) and (rf_data is very high) then (final_selection is reenter) (1)

31. If (face_data is low) and (lf_data is low) and (rf_data is very low) then (final_selection is accepted) (1)

32. If (face_data is low) and (lf_data is low) and (rf_data is low) then (final_selection is accepted) (1)

33. If (face_data is low) and (lf_data is low) and (rf_data is medium) then (final_selection is accepted) (1)

34. If (face_data is low) and (lf_data is low) and (rf_data is high) then (final_selection is accepted) (1)

35. If (face_data is low) and (lf_data is low) and (rf_data is very high) then (final_selection is accepted) (1)

36. If (face_data is low) and (lf_data is medium) and (rf_data is very low) then (final_selection is reenter) (1)

37. If (face_data is low) and (lf_data is medium) and (rf_data is low) then (final_selection is reenter) (1)

38. If (face_data is low) and (lf_data is medium) and (rf_data is medium) then (final_selection is reenter) (1)

39. If (face_data is low) and (lf_data is medium) and (rf_data is high) then (final_selection is reenter) (1)

40. If (face_data is low) and (lf_data is medium) and (rf_data is very high) then (final_selection is reenter) (1)

41. If (face_data is low) and (lf_data is high) and (rf_data is very low) then (final_selection is reenter) (1)

42. If (face_data is low) and (lf_data is high) and (rf_data is low) then (final_selection is reenter) (1)

43. If (face_data is low) and (lf_data is high) and (rf_data is medium) then (final_selection is reenter) (1)

44. If (face_data is low) and (lf_data is high) and (rf_data is high) then (final_selection is reenter) (1)

45. If (face_data is low) and (lf_data is high) and (rf_data is very high) then (final_selection is reenter) (1)

46. If (face_data is low) and (lf_data is very high) and (rf_data is very low) then (final_selection is reenter) (1)

47. If (face_data is low) and (lf_data is very high) and (rf_data is low) then (final_selection is reenter) (1)

48. If (face_data is low) and (lf_data is very high) and (rf_data is medium) then (final_selection is reenter) (1)

49. If (face_data is low) and (lf_data is very high) and (rf_data is high) then (final_selection is reenter) (1)

50. If (face_data is low) and (lf_data is very high) and (rf_data is very high) then (final_selection is reenter) (1)

51. If (face_data is medium) and (lf_data is very low) and (rf_data is very low) then (final_selection is reenter) (1)

52. If (face_data is medium) and (lf_data is very low) and (rf_data is low) then (final_selection is reenter) (1)

53. If (face_data is medium) and (lf_data is very low) and (rf_data is medium) then (final_selection is reenter) (1)

54. If (face_data is medium) and (lf_data is very low) and (rf_data is high) then (final_selection is reenter) (1)

55. If (face_data is medium) and (lf_data is very low) and (rf_data is very high) then (final_selection is reenter) (1)

56. If (face_data is medium) and (lf_data is low) and (rf_data is very low) then (final_selection is reenter) (1)

57. If (face_data is medium) and (lf_data is low) and (rf_data is low) then (final_selection is reenter) (1)

58. If (face_data is medium) and (lf_data is low) and (rf_data is medium) then (final_selection is reenter) (1)

59. If (face_data is medium) and (lf_data is low) and (rf_data is high) then (final_selection is accepted) (1)

60. If (face_data is medium) and (lf_data is low) and (rf_data is very high) then (final_selection is reenter) (1)

61. If (face_data is medium) and (lf_data is medium) and (rf_data is very low) then (final_selection is reenter) (1)

62. If (face_data is medium) and (lf_data is medium) and (rf_data is low) then (final_selection is reenter) (1)

63. If (face_data is medium) and (lf_data is medium) and (rf_data is medium) then (final_selection is accepted) (1)

64. If (face_data is medium) and (lf_data is medium) and (rf_data is high) then (final_selection is accepted) (1)

65. If (face_data is medium) and (lf_data is medium) and (rf_data is very high) then (final_selection is accepted) (1)

66. If (face_data is medium) and (lf_data is high) and (rf_data is very low) then (final_selection is accepted) (1)

67. If (face_data is medium) and (lf_data is high) and (rf_data is low) then (final_selection is accepted) (1)

68. If (face_data is medium) and (lf_data is high) and (rf_data is medium) then (final_selection is accepted) (1)

69. If (face_data is medium) and (lf_data is high) and (rf_data is high) then (final_selection is accepted) (1)

70. If (face_data is medium) and (lf_data is high) and (rf_data is very high) then (final_selection is accepted) (1)

71. If (face_data is medium) and (lf_data is very high) and (rf_data is very low) then (final_selection is accepted) (1)

72. If (face_data is medium) and (lf_data is very high) and (rf_data is low) then (final_selection is accepted) (1)

73. If (face_data is medium) and (lf_data is very high) and (rf_data is medium) then (final_selection is accepted) (1)

74. If (face_data is medium) and (lf_data is very high) and (rf_data is high) then (final_selection is accepted) (1)

75. If (face_data is medium) and (lf_data is very high) and (rf_data is very high) then (final_selection is accepted) (1)

76. If (face_data is high) and (lf_data is very low) and (rf_data is very low) then (final_selection is reenter) (1)

77. If (face_data is high) and (lf_data is very low) and (rf_data is low) then (final_selection is reenter) (1)

78. If (face_data is high) and (lf_data is very low) and (rf_data is medium) then (final_selection is reenter) (1)

79. If (face_data is high) and (lf_data is very low) and (rf_data is high) then (final_selection is reenter) (1)

80. If (face_data is high) and (lf_data is very low) and (rf_data is very high) then (final_selection is accepted) (1)

81. If (face_data is high) and (lf_data is low) and (rf_data is very low) then (final_selection is reenter) (1)

82. If (face_data is high) and (lf_data is low) and (rf_data is low) then (final_selection is accepted) (1)

83. If (face_data is high) and (lf_data is low) and (rf_data is medium) then (final_selection is accepted) (1)

84. If (face_data is high) and (lf_data is low) and (rf_data is high) then (final_selection is accepted) (1)

85. If (face_data is high) and (lf_data is low) and (rf_data is very high) then (final_selection is accepted) (1)

86. If (face_data is high) and (lf_data is medium) and (rf_data is very low) then (final_selection is reenter) (1)

87. If (face_data is high) and (lf_data is medium) and (rf_data is low) then (final_selection is accepted) (1)

88. If (face_data is high) and (lf_data is medium) and (rf_data is medium) then (final_selection is accepted) (1)

89. If (face_data is high) and (lf_data is medium) and (rf_data is high) then (final_selection is accepted) (1)

90. If (face_data is high) and (lf_data is medium) and (rf_data is very high) then (final_selection is accepted) (1)

91. If (face_data is high) and (lf_data is high) and (rf_data is very low) then (final_selection is accepted) (1)

92. If (face_data is high) and (lf_data is high) and (rf_data is low) then (final_selection is accepted) (1)

93. If (face_data is high) and (lf_data is high) and (rf_data is medium) then (final_selection is accepted) (1)

94. If (face_data is high) and (lf_data is high) and (rf_data is high) then (final_selection is accepted) (1)

95. If (face_data is high) and (lf_data is high) and (rf_data is very high) then (final_selection is accepted) (1)

96. If (face_data is high) and (lf_data is very high) and (rf_data is very low) then (final_selection is accepted) (1)

97. If (face_data is high) and (lf_data is very high) and (rf_data is low) then (final_selection is accepted) (1)

98. If (face_data is high) and (lf_data is very high) and (rf_data is medium) then (final_selection is accepted) (1)

99. If (face_data is high) and (lf_data is very high) and (rf_data is high) then (final_selection is accepted) (1)

100. If (face_data is high) and (lf_data is very high) and (rf_data is very high) then (final_selection is accepted) (1)

101. If (face_data is very high) and (lf_data is very low) and (rf_data is very low) then (final_selection is accepted) (1)

102. If (face_data is very high) and (lf_data is very low) and (rf_data is low) then (final_selection is accepted) (1)

103. If (face_data is very high) and (lf_data is very low) and (rf_data is medium) then (final_selection is accepted) (1)

104. If (face_data is very high) and (lf_data is very low) and (rf_data is high) then (final_selection is accepted) (1)

105. If (face_data is very high) and (lf_data is very low) and (rf_data is very high) then (final_selection is accepted) (1)

106. If (face_data is very high) and (lf_data is low) and (rf_data is very low) then (final_selection is accepted) (1)

107. If (face_data is very high) and (lf_data is low) and (rf_data is low) then (final_selection is accepted) (1)

108. If (face_data is very high) and (lf_data is low) and (rf_data is medium) then (final_selection is accepted) (1)

109. If (face_data is very high) and (lf_data is low) and (rf_data is high) then (final_selection is accepted) (1)

110. If (face_data is very high) and (lf_data is low) and (rf_data is very high) then (final_selection is accepted) (1)

111. If (face_data is very high) and (lf_data is medium) and (rf_data is very low) then (final_selection is accepted) (1)

112. If (face_data is very high) and (lf_data is medium) and (rf_data is low) then (final_selection is accepted) (1)

113. If (face_data is very high) and (lf_data is medium) and (rf_data is medium) then (final_selection is accepted) (1)

114. If (face_data is very high) and (lf_data is medium) and (rf_data is high) then (final_selection is accepted) (1)

115. If (face_data is very high) and (lf_data is medium) and (rf_data is very high) then (final_selection is accepted) (1)

116. If (face_data is very high) and (lf_data is high) and (rf_data is very low) then (final_selection is accepted) (1)

117. If (face_data is very high) and (lf_data is high) and (rf_data is low) then (final_selection is accepted) (1)

118. If (face_data is very high) and (lf_data is high) and (rf_data is medium) then (final_selection is accepted) (1)

119. If (face_data is very high) and (lf_data is high) and (rf_data is high) then (final_selection is accepted) (1)

120. If (face_data is very high) and (lf_data is high) and (rf_data is very high) then (final_selection is accepted) (1)

121. If (face_data is very high) and (lf_data is very high) and (rf_data is very low) then (final_selection is accepted) (1)

122. If (face_data is very high) and (lf_data is very high) and (rf_data is low) then (final_selection is accepted) (1)

123. If (face_data is very high) and (lf_data is very high) and (rf_data is medium) then (final_selection is accepted) (1)

124. If (face_data is very high) and (lf_data is very high) and (rf_data is high) then (final_selection is accepted) (1)

125. If (face_data is very high) and (lf_data is very high) and (rf_data is very high) then (final_selection is accepted) (1)

5.5.5 Results

On the basis of above rule base we have derived the following table. The table consists of various numerical data in the range of 0 to 1. The numerical values have been distributed to identify the decision out of reject, reenter and accepted.

It is clear from table 4.4 that the range for the to be rejected is in between 0 to 0.3, the range for person to be reenter is in between 0.1 to 0.5 and finally range for the person to be accepted is in between 0.3 to 1. These ranges are selected in a fuzzy way so that final

consequences are made on the basis of fuzzy rule base. But, in the result we have got the crisp values in order to clearly distinguish the category of person to be rejected, reenter and accepted. The table 5.5 has been derived from the result obtained after getting the crisp values of the output centroids. Most of the values are approaching range in between 0.3 to 0.659 and above which are naturally depicting the accuracy of the system. This range of the final result very much near to take a decision that the person who is approaching to go through the security is a genuine person. For the above discussed criteria of rulebase, values approaching near about 0.3 are representing the decision of reentering and values less than 0.3 belong to the category of rejection.

Table 5.5 Result obtained from fuzzy logic rule base in crisp form.

Result obtained for the 1000 rules (10x10x10 inputs)									
1-100	101-200	201-300	301-400	401-500	501-600	601-700	701-800	801-900	901-1000
rejected	rejected	rejected	accepted	accepted	accepted	accepted	accepted	accepted	accepted
accepted	accepted	accepted	accepted	accepted	accepted	accepted	accepted	accepted	accepted
accepted	accepted	accepted	accepted	accepted	accepted	accepted	accepted	accepted	accepted
accepted	accepted	accepted	accepted	accepted	accepted	accepted	accepted	accepted	accepted
accepted	accepted	accepted	accepted	accepted	accepted	accepted	accepted	accepted	accepted
accepted	accepted	accepted	accepted	accepted	accepted	accepted	accepted	accepted	accepted
accepted	accepted	accepted	accepted	accepted	accepted	accepted	accepted	accepted	accepted
accepted	accepted	accepted	accepted	accepted	accepted	accepted	accepted	accepted	accepted
accepted	accepted	accepted	accepted	accepted	accepted	accepted	accepted	accepted	accepted
accepted	accepted	accepted	accepted	accepted	accepted	accepted	accepted	accepted	accepted
accepted	accepted	accepted	accepted	accepted	accepted	accepted	accepted	accepted	accepted
accepted	accepted	accepted	accepted	accepted	accepted	accepted	accepted	accepted	accepted
accepted	accepted	accepted	accepted	accepted	accepted	accepted	accepted	accepted	accepted
accepted	accepted	accepted	accepted	accepted	accepted	accepted	accepted	accepted	accepted
accepted	accepted	accepted	accepted	accepted	accepted	accepted	accepted	accepted	accepted
accepted	accepted	accepted	accepted	accepted	accepted	accepted	accepted	accepted	accepted
reentered	reentered	reentered	accepted	accepted	accepted	accepted	accepted	accepted	accepted
reentered	reentered	reentered	accepted	accepted	accepted	accepted	accepted	accepted	accepted
reentered	reentered	reentered	accepted	accepted	accepted	accepted	accepted	accepted	accepted
accepted	accepted	accepted	accepted	accepted	accepted	accepted	accepted	accepted	accepted
accepted	accepted	accepted	accepted	accepted	accepted	accepted	accepted	accepted	accepted
accepted	accepted	accepted	accepted	accepted	accepted	accepted	accepted	accepted	accepted
accepted	accepted	accepted	accepted	accepted	accepted	accepted	accepted	accepted	accepted
accepted	accepted	accepted	accepted	accepted	accepted	accepted	accepted	accepted	accepted
accepted	accepted	accepted	accepted	accepted	accepted	accepted	accepted	accepted	accepted

accepted	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**
reentered	**reentered**	**reentered**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**
reentered	**reentered**	**reentered**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**
reentered	**reentered**	**reentered**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**
accepted	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**
accepted	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**
accepted	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**
accepted	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**
accepted	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**
accepted	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**
accepted	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**
reentered	**reentered**	**reentered**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**
reentered	**reentered**	**reentered**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**
reentered	**reentered**	**reentered**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**
accepted	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**
accepted	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**
accepted	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**
accepted	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**
accepted	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**
accepted	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**
accepted	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**
accepted	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**
reentered	**reentered**	**reentered**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**
reentered	**reentered**	**reentered**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**
accepted	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**
accepted	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**
accepted	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**
accepted	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**
accepted	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**
accepted	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**
accepted	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**
reentered	**reentered**	**reentered**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**
reentered	**reentered**	**reentered**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**
reentered	**reentered**	**reentered**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**
accepted	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**
accepted	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**
accepted	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**
accepted	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**
accepted	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**
accepted	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**
accepted	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**

reentered	**reentered**	**reentered**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**
reentered	**reentered**	**reentered**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**
reentered	**reentered**	**reentered**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**
accepted	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**
accepted	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**
accepted	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**
accepted	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**
accepted	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**
accepted	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**
accepted	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**
reentered	**reentered**	**reentered**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**
reentered	**reentered**	**reentered**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**
reentered	**reentered**	**reentered**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**
accepted	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**
accepted	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**
accepted	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**
accepted	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**
accepted	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**
accepted	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**
accepted	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**
reentered	**reentered**	**reentered**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**
reentered	**reentered**	**reentered**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**
reentered	**reentered**	**reentered**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**
accepted	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**
accepted	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**
accepted	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**
accepted	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**
accepted	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**
accepted	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**
accepted	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**
reentered	**reentered**	**reentered**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**
reentered	**reentered**	**reentered**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**
reentered	**reentered**	**reentered**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**
accepted	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**	**accepted**

Calculation of false rejection rate and genuine acceptance rate on the basis of above discussed fuzzy fusion system is shown in Table 5.6.

Table 5.6 GAR and FRR calculated from fuzzy based fusion system

GAR (%)	FRR (%)	Reenter (%)
91.3	0.3	8.4

5.5.6 Surface Rule Viewer

Surface Viewer is the graphical representation of the output of fuzzy based fusion system which is demonstrated with a three dimensional curve that constitutes the mapping of fusion of three biometric traits. Since, the Surface Viewer is provided with pop-up menus that tends us to choose three inputs and one output for plotting. In the GUI, below the pop-up menus there are two text input fields for the x-axis and y-axis grid lines inclusion.

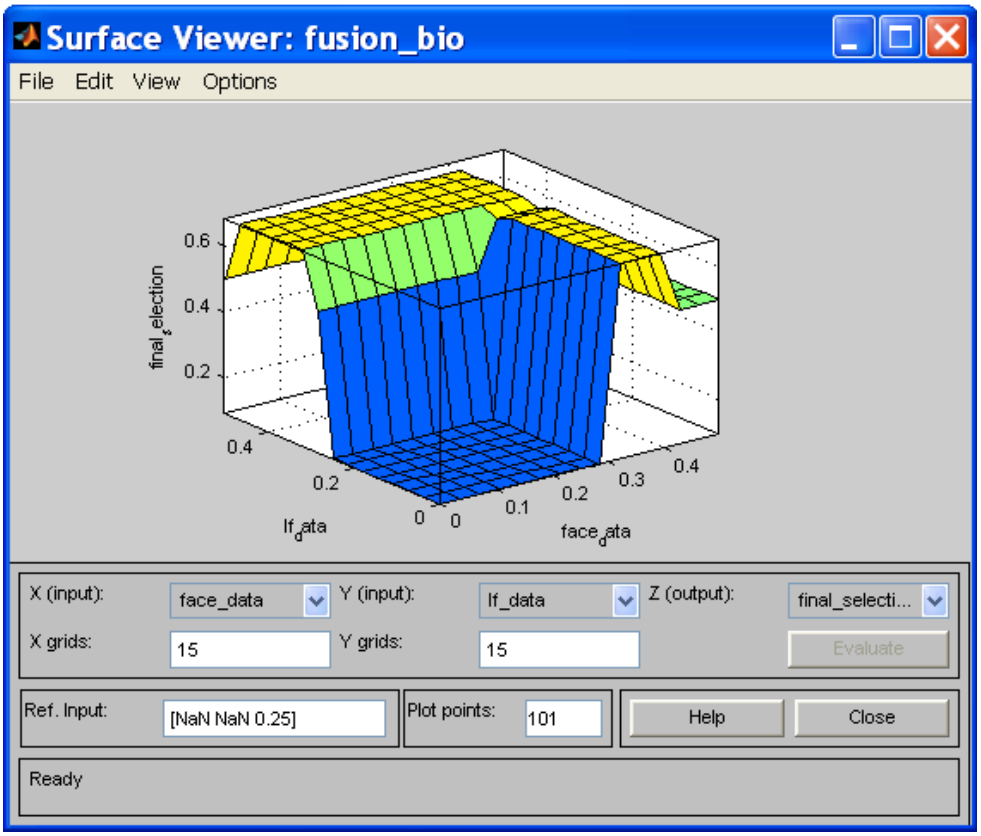


Figure 5.10 Surface viewer

5.7 Summary

This computational analysis summarizes the quick explanation of each of the main GUI tools of the fuzzy toolbox used in the fuzzy based fusion process. The fusion analysis demonstrates that the output obtained from the process corresponds to our original estimation of conventional or any other novel approach. Furthermore, with the increasing interest of solving the complex problem an integral category of alike decision-making problems, fuzzy logic may furnish a particular methodology for the resolution, applied its easiness with which a system can be rapidly altered.

CHAPTER 6

Conclusions and Future Work

6.1 Conclusions

Biometric is one of the fundamental technologies that are being used for individual authentication in many industrial, confidential and domestic applications. Unimodal systems are reliable, still the popularity of these systems is degrading due to the problems such as noisy sensor data, non-universality and spoof attacks etc. Few of these limitations have been either eliminated or reduced to a less extent by multi biometric system. In this thesis the performance of a multimodal biometric system has been examined at matching score level fusion with various fusion rules and normalization methods. The purpose of analytical study is to investigate how multiple biometric modalities can together be made a more useful to create an effective authentication system. We have examined the, with three normalization method (Min-Max, Z-Score and Mathematical normalizations) and four fusion rules(Sum, Product, Min and Max), every rule has its different advantages and drawbacks. In this thesis, NIST BSSR release1 database has been used. The significant distinction between these methods has made on the basis of recognition rates (FRR and FAR). We have seen that even after min–max and z-score normalization are sensitive to outliers but they have given a reasonable performance, and they have provided superior GARs than FRRs.

6.2 Future Work

The experimental probes, in this thesis, involve open-set identification recognition mode, in clean, fused-quality and conventional data conditions. The outcomes show that the carrying out of biometric systems can be welfare from score level fusion, but that this depends highly on the types of integration methods as well as the transformation method used. Therefore, improvement in existing work can be achieved by focusing on these two factors which play a vital role in the effectiveness of multimodal biometric systems.

Some normalization techniques give a better performance when they work with a proper distribution of matching scores for example, z-score normalization is most desirable possible under a restriction that if the scores of all the modalities follow a Gaussian distribution.

Hence, it is required to develop the techniques such that they permit a user to prefer a normalization technique after examining the genuine and impostor score statistical distribution of the individual matchers. Due to the extensive statistical rigorness in the score level fusion method they are quite ad-hoc in nature. If we consider the fusion problem as a statistical issue then likelihood ratios based on the estimation of genuine and impostor score would be a better choice. In order to increase the tolerance limit of the estimation of distribution an automatic bandwidth selection techniques can be utilized to find the width of the kernels to be applied in non-parametric compactness approximation. The problem with Bayesian framework is that it is not able to deal with time varying parameters of the biometric traits. We will enquire technologies and algorithms which can remove the above discussed artifacts such that an unparallel biometric authentication system can be developed.

References

[1] IBM Corporation. The Consideration of Data Security in a Computer Environment. Technical Report G520-2169, IBM, White Plains, USA, 1970.

[2] Mitnick, K. D., Simon, W. L. and Wozniak, S. The Art of Deception: Controlling the Human Element of Security. Wiley, 2002.

[3] Klien, D. V. Foiling the Cracker; A Survey of, and Improvements to Unix Password Security. In Proceedings of the Second USENIX Workshop on Security, pages 5–14, August 1990.

[4] Burr, W.E., Dodson, D.F., and Polk, W.T. Information Security: Electronic Authentication Guideline. Technical Report Special Report 800-63, NIST, April 2006.

[5] Jain, A.K., Bolle, R. and Pankanti, S. editors. Biometrics: Personal Identification in Networked Society. Kluwer Academic Publishers, 1999.

[6] Jain, A.K., Ross, A., Prabhakar, S.: An introduction to biometric recognition. IEEE Trans. On Circuits and Systems for Video Technology 14 (2004) 4–20

[7]http://www.globalsecurity.org/security/systems/biometrics-history.htm

[8] http://www.questbiometrics.com/biometric-history.html

[9] http://terrorism.about.com/od/issuestrends/tp/History-of-Biometrics.htm

[10]http://www.biometricgroup.com/Henry%20Fingerprint%20Classification.pdf

[11] http://www.reachoutmichigan.org/funexperiments/agesubject/lessons/prints_ext.html

[12] http:// www.globalsecurity.org/security/systems/fingerprint.htm

[13] http://ctl.ncsc.dni.us/biomet%20web/BMIris.html

[14] http://userweb.cs.utexas.edu/users/boyer/bledsoe-memorial-resolution.pdf

[15] Woodward, J. D., N. Orlans, M. and Higgins, P. T. "Identity Assurance in the Information Age- Biometrics", McGr aw Hill, New York, 2003.

[16] Sirovich, L. and Kirby, M.. 1987. "Low-Dimensional Procedure for the Characterization of Human Faces", Journal of the Optical Society of America, A: Optics, Image

Science and Vision, 4, 519-524.

[17] Im, S. K., Park, H.M., Kim, Y.W., Han, S.C., Kim, S.W. and Kang, C.H. 2001. "An Biometric Identification System by Extracting Hand Vein Patterns", Journal of the Korean Physical Society, 38, 268-272.

[18] http://cogt.client.shareholder.com/ReleaseDetail.cfm?ReleaseID=145765

[19] http://www.globalsecurity.org/security/systems/biometrics.htm

[20] http://en.wikipedia.org/wiki/United_States_passport

[21] http://en.wikipedia.org/wiki/Biometrics

[22] Upendra, K., Singh, S., Kumar, V. and Verma, H. K. 2007. "Online Fingerprint Verification", Journal of Medical Engineering and Technology, 31, 36-45.

[23] Reid, P. "Biometric for Network Security", First Indian Reprint, Pearson Education, 2004.

[24] Dabbah, M. A., Woo, W. L. and Dlay, S. S. "Secure Authentication for Face Recognition," In Proc. of IEEE Symposium on Computational Intelligence in Image and Signal Processing, Apr. 2007. USA, pp. 121 - 126.

[25] Jain, A. K., Ross, A. and S. Pankanti, "A Proto type Hand Gemetry- based Verification System", 2nd International conference on Audio and Video based Biometric Personal Authentication, Washington, USA, pp. 166-171, 1999.

[26] Mason, J. S. and Brand, J. D. "The Role of Dynamics in Visual Speech Biometric". Proceedings of IEEE International Conference on Acoustics, Speech and Signal Processing, Orlando, Florida, pp. 142-147, 2002.

[27] http://www.biometricnewsportal.com/signature_biometrics.asp

[28] Guest, R. "Age Dependency in Handwritten Dynamic Signature Verification Systems", Pattern Recognition Letters, vol. 27, no. 10, pp. 1098-1104, 2006.

[29] Saevanee, H. and Bhattarakosol, P. "Authenticating User using Keystroke Dynamics and Finger Pressur e", Proceedings of 6th IEEE Conference on Consumer Communications and Networking, Las Vegas, pp. 1-2, 2009.

[30] Leonard, D. C., Pons, A. P. and Asfour, S. S. “Realization of a Universal Patient Identifier for Electronic Medical Records through Biometric Technology”, IEEE Transactions on Information Technology in Biomedicine, vol. 13, no. 4, pp. 494-500, 2009.

[31] Soutar, C. "Implementation of Biometric System-Security and Privacy Considerations", Information security Technical report, vol.7, no.4, Dec 2002.

[32] Mason, J. S. and Brand, J. D. "The Role of Dynamics in Visual Speech Biometric", proceedings of IEEE International Conference on Acoustics, Speech and Signal Processing, Orlando, Florida, pp.142-147, 2002

[33] Jain, A. K., Ross A. and Pankanti, S. " A proto- type Hand Geometry- based Verification System", 2nd International Conference on Audio and Video based Biometric Personal Authentication, Washington, USA, PP. 166-171, 199.

[34] Cannon, M., Byrne, M., Cotter, D., Sham, P., Larkin, C. and O'Callaghan, E. "Further Evidence for Anomalies in the hand-prints of patients and Schizophrenia: A study of Secondary Creases", Schizophrenia Research, vol.13,pp. 179-184, 1994.

[35] Kong, A., Zhang, D. and Lu, G. "A study of Identical twins palm print for Personal Verification", Pattern Recognition, vol.39, no.11, pp. 2149-2156, 2006.

[36] Modi, S, K. ANALYSIS OF FINGERPRINT SENSOR INTEROPERABILITY ON SYSTEM PERFORMANCE, Purdue University West Lafayette, Indiana August 2008.

[37] Cyberware Inc., http://www.cyberware.com/. Model 15 scanner, 2001

[38] Ohta, Y. and Kanade, T. "Stereo by intra and inter scan line search using dynamic programming,"IEEE Transaction on Pattern Analysis and Machine Intelligence, vol. 7, no.2, pp.139-154, 1985.

[39] Nanavati, S, Thieme, M. and Nanavati, R. Biometrics: Identity Verification in a Networked World. Wiley Computer Publishing: New York. 2002. 79.

[40] Wechsler, H. et al (Eds.) “Face Recognition From Theory to Applications”, NATO ASI series. SERS. F, Springer-Verlag, Berlin/Heidelberg, 1998.

[41] Biometric Product Final Report, CESG contract X92A/4009309, Centre for Mathematics and Scientific Computing, National Physical Laboratory, 19 March 2001

[42]http://fingerchip.pagespersoorange.fr/biometrics/types/fingerprint_sensors_productsi.htm

[43] http://www.globalsources.com/manufacturers/Finger-Print-Sensor.html

[44] Ruttenbur, B.W. and Jones, A. L.: "Industry Overview for the investment community", Morgan keegan company & Inc., October 23, 2006.

[45] Chen, Y., Das, S.C. and Jain, A.K. Fingerprint quality indices for predicting authentication performance.In preceding to the fifth international conference on Audio and Video-Based Biometric Person Authentication (AVBPA) (To appear), New York, U.S.A., July 2005.

[46] NIST report to the united State of Congress. Summary of the NIST Standard for Biometric Accuracy, Temper Resistance, and Interoperability. Available at ftp://sequoyah.nist.gov/pub/nist_internal_report/NISTAPP_Nov 2.pdf, November 2002.

[47] Kukula, E.P., Sutton, M.J. and Elliott, S. J. The Human–Biometric-Sensor Interaction Evaluation Method: Biometric Performance and Usability Measurements. (59), 784 – 791, 01 March 2010.

[48] O'Gorman, L. "Seven issues with human authentication technologies," in Proc. Of Workshop on Automatic Identification Advanced Technologies (AutoID), (Tarrytown, New York), pp. 185–186, Mar 2002.

[49] Zhan, X., Meng X., Yin, Y. and Yang, G.: A Method Combined on Multi-Level Factors for Fingerprint Image Quality Estimation 10.1109/FSKD.2008.582

[50] Yagiz Sutcu, Shantanu Rane, Jonathan S.Yedidia, Stark C.Draper and Anthony Vetro, Transformation of Biometric Templates for Secure Biometric Systems based on Error Correcting Codes, Polytechnic University, Brooklyn, NY 11201,

[51] Lawrence O'Gorman, "Comparing Passwords, Tokens, and Biometrics for User Authentication," in Proc. IEEE, vol. 91, No. 12, December, 2003

[52]. Ross, A. and Jain, A.K. Appeared in Proc. of International ECCV Workshop on Biometric Authentication (BioAW), (Prague, Czech-Republic), LNCS Vol. 3087, pp. 134-145, Springer Publishers, May 2004.

[53] NIST report to the United State Congress. Summary of the NIST standard for the Biometric accuracy, Temper Resistance and Interoperability. Available at:
ftp://sequoyah.nist.gov/pub/nist_internal_report/NISTAPP_Nov 2.pdf, November 2002.

[54] Nanavati, S., Thieme, M. and Nanavati, R. Biometrics: Identity in a networked world, Ed. John Wiley 20M

[55] Hong, L., Jain, A. K. and Pankanti, S. Can Multibiometric improves performance? "In Proceedings Auto ID'99, (Summit (NJ), USA), pp. 59{64, Oct 1999.

[56] A. Ross and A. K. Jain. Multimodal biometrics: An overview. In Proceeding of the Twelfth European Signal Processing Conference, pages 1221–1224, 2004.

[57] Miller, B. "Vital Signs of Identity," IEEE Spectrum, pp. 22-30, Feb1994.

[58] Ross, A. and Jain, A.K. MULTIMODAL BIOMETRICS: AN OVERVIEW Appeared in Proc. of 12th European Signal Processing Conference (EUSIPCO), (Vienna, Austria), pp. 1221-1224, September 2004.

[59] Deriche, M. "Trends and Challenges in Mono and Multi Biometrics", IEEE 2008.

[60] Maltoni, D., Maio, D., Jain, A.K. and Prabhakr, S. Hand Book of Pattern Recognition. Spring 2003, 1, 3, 34, 61, 101, 102.

[61] Iyengar, S.S., Prasad, L. and Min, H. Advances in Distributed Sensor Technology. Printice Hall, 1995.

[62] Jain, A.K. and Ross, A. 2002. FINGERPRINT MOSAICKING. Proceedings of IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP), Orlando, Florida, May 13 - 17, 2002.

[63] Moon, Y.S., Yeung, H.W., Chan, K.C., Chan, S.O. TEMPLATE SYNTHESIS AND IMAGE MOSAICKING FOR FINGERPRINTREGISTRATION: AN EXPERIMENTAL STUDY. International journal of ICASSP. 4, 409-412.

[64] Raghavendra, R., Rao, A. and Kumar, G.H. (2010). Multisensor biometric evidence fusion of face and palmprint for person authentication using Particle Swarm Optimization (PSO). International Journal of Biometrics (IJBM), Vol. 2, No. 1.

[65] Singh, R., Vatsa, M. and Noore, A. (2008). Integrated Multilevel Image Fusion and Match Score Fusion of Visible and Infrared Face Images for Robust Face Recognition. Pattern Recognition - Special Issue on Multimodal Biometrics, Vol. 41, No. 3, pp. 880-893.

[67] Wu, Q., Wang, L., Geng, X., Li, M. and He, X. 'Dynamic Biometrics Fusion at Feature Level for Video-Based Human Recognition', Proceedings of Image and Vision Computing New Zealand 2007, pp. 152–157, Hamilton, New Zealand, December 2007.

[68] Zhang, Y. and Yan, Y. 2008. Multimodal Biometrics Fusion Using Correlation Filter Banḳinternational journal of IEEE, 8, 1-4.

[69] Kumar A. and Zhang, D. Biometric Recognition using Feature Selection and Combination. Internation journal of ICIP, 4, 1-10.

[70] Zhou, X. and Bhanu, B. 2007. Feature fusion of side face and gait for video-based human identification. Center for Research in Intelligent Systems, University of California, Riverside,, USA,41, 778-795.

[71] Rattani, A. Kisku, D. R. and Bicego, M. 2007. Feature Level Fusion of Face and Fingerprint Biometrics. International jouran of IEEE. 30, 1-16.

[72] Yan, Y. and Zhang Y. 2008. Multimodal Biometrics Fusion Using Correlation Filter Banḳinternational journal of IEEE, 8, 1-4.

[73] Jain, A.K., Hong, L. and Kulkarni, Y. "A multimodal biometric system using fingerprint, face, and speech, "in Second International Conference on AVBPA, Washington, DC, USA, pp. 182-187, 1999.

[74] Kuncheva, L. I., Bezdek, J. C. and Duin, R. P. W. "Decision templates for multiple classifier fusion: an experimental comparison," Pattern Recognition, vol. 34, pp. 299-314, 2001.

[75] Toh, K. and Yau, W. "Combination of hyperbolic functions for multimodal biometrics data fusion," IEEE Trans. Systems, Man, and Cybernetics – Part B. Cybernetics, vol. 34, no. 2, pp. 1196-1209, April 2004.

[76] Jain, A. K. and Ross, A. "Learning User-specific Parameters in a Multibiometric System, "Proceedings of the IEEE International Conference on Image Processing (ICIP), vol. 1, pp. 57-60, 2002.

[77] Verikas, A. Lipnickas, A., Malmqvist, K., Bacauskiene, M. and Gelzinis, A. “Soft combination of neural classifiers,” Pattern Recognition Letters, vol. 20, pp. 429-444, 1999.

[78] Toh K. and Yan, W. “Multi-modal biometrics fusion: beyond optimal weighting,” 7th International Conference on Control, Automation, Robotics, and Vision (ICACV’02), pp. 788-792, Singapore, Dec. 2002.

[79] Frischholz, R. and Dieckmann, U. "BioID: A Multimodal Biometric Identification System," IEEE, vol. 33, pp. 64-68, 2000.

[80] Kale, A., Chowdhury A. R, and Chellappa, R. "Fusion of gait and face for human identification," International Conference on Acoustics, Speech and Signal Processing, 2004.

[81] Shakhnarovich, G. and Darrell, T. "On probabilistic combination of face and gait cues for identification," Proceedings of the 5th IEEE International Conference on Automatic Face and Gesture Recognition, 2002.

[82] Ribaric, S., Ribaric, D. and Pavesic, N. "A Multimodal Biometric Useridentification System for Network-based Applications," IEE Proceedings on Vision, Image and Signal Processing, vol. 150, pp. 409-416, 2003.

[83] Hazen, T., Weinstein, E. and Park, A. "Towards robust person recognition on handheld devices using face and speaker identification technologies, "Proceedings of the International Conference on Multimodal Interfaces, pp. 289- 292, 2003.

[84] Czyz, J., Bengio, S., Marcel, C. Vandendorpe, and L. "Scalability analysis of audio-visual person identity verification," Audio- and Video-based Biometric Person Authentication, pp. 752–760, 2003.

[85] Luettin, J. and Ben-Yacoub, S. "Robust Person Verification based on Speech and Facial Images," Proceedings of the European Conference on Speech Communication and Technology, pp. 991-994, 1999.

[86] Sanderson, C. and Paliwal, K. K. "Adaptive Multi-Modal Person Verification System", Proceedings of the First IEEE Pacific-Rim Conference on Multimedia, 2000.

[87] Willem, M. and Fmet, P. December 1997, Layped Biometric Verification, White paper, Keywm Technologies, December 1997.

[88] Prabhakar, S. and Jain, A. K. "Decision-level fusion in fingerprint verification", Pattern Recognition, vol. 35, pp. 861-874, 2002.

[89] J. Fierrez-Aguilar, J. Ortega-Garcia, D. Garcia-Romero, and J. Gonzalez-Rodriguez, "A comparative evaluation of fusion strategies for multimodal biometric verification", AVBPA 2003, LNCS 2688, pp. 830-837, 2003.

[90] Verlinde, P. and Cholet, G. "Comparing decision fusion paradigrams using k-NN based classifiers, decision trees, and logistic regression in a multi-modal identity verification application," in Second International Conference on AVBPA, Washington, DC, USA, pp. 188-193.

[91] Zhang, D., Ghobakhlou A. and Kasabov, N. "An adaptive model of person identification combining speech and image formation," http://www.aut.ac.nz/research_showcase/research_activity_areas/kedri/downloads/pdf/Da

vidICARCV.pdf, accessed Mar. 2005.

[92] Naguib, A. M. et al. "A multi-modal distributed biometric authentication system BioSecure," in Proc. 46th IEEE Midwest Symposium On Circuits and Systems, Egypt, 2003.

[93] Israel, S. A., Todd Scruggs, W. T., Worek, W. J. and Irvine, J. M. "Fusing face and ECG for personal identification," Proceedings of the 32nd Applied Imagery Pattern Recognition Workshop AIPR'03, 2003.

[94] Gian Luca Marcialis and Fabio Roli. Score-level fusion of fingerprint and face matchers for personal verification under "stress" conditions. 14th International Conference on Image Analysis and Processing USA september 10-14 2007, 1.1, 259-264.

[95] Zhang, X., Sun, Z. and Tan, T. 2010. Hierarchical Fusion of Face and Iris for Personal Identification 2010 International Conference on Pattern Recognition, August 23-26, 2010, 14, 217-220.

[96] Lumini, A. and Nanni, L. 2007. When Fingerprints Are Combined with Iris – A Case Study. International Journal of Network Security, 4, 27–34.

[97] Ong, M.G.K., Connie, T, Jin, A.T.B., Ling, D.N.C. 2003. A Single-sensor Hand Geometry and Palmprint Verification System ASEAN *Journal* on Science and Technology, 19, 100-106.

[98] kale, A. FUSION OF GAIT AND FACE FOR HUMAN identification. Proceedings of (ICASSP '04) IEEE International Conference. May 17-21, 2004 Maryland,USA, 5, 901-904.

[99] Derawi, M.O., Gafurov, D., Larseny, R., Busch, C. and Bours, P. Fusion of Gait and Fingerprint for User Authentication on Mobile Devices. Proceedings of the IEEE security and communication networks, Norway, May 26-28, 1, 1-6.

[100] Kisku1, D.R. Gupta, P. and Singh, J. K. Feature Level Fusion of Biometrics Cues: Human Identification with Doddington's Caricature. Proceedings of the 2010 international conference on Advances in computer science and information technology, USA, December 21-22, 1, 70-81.

[101]Ross, A. A., Nandakumar, K., and Jain, A. K. Handbook of Multibiometric (Springer Publisher), International Series on Biometrics, Vol. 6, 2006.

[102] Ross, A. A. and Jain, A. K. Information fusion in biometrics, Pattern Recognition Lett. **24**, 13, 2115–2125, 2003.

[103] Chang, K. I., K. W. Bowyer, and P. J. Flynn, "An evaluation of multi-modal 2D+3D face biometrics," IEEE Trans. on PAMI 27 (4), pp. 619-624, April 2005.

[104] Phillips, P.J., P. Grother R.J. Michaels, D.M. Blackburn and E. Tabassi and J.M. Bone, "FRVT 2002: overview and summary", March 2003.

[105] Ko, T.: Multimodal biometric identification for large user population using fingerprint, face and iris recognition. In: 34th Applied Imagery and Pattern Recognition Workshop, pp. 218–223 (2005).

[106] Sanderson C., and Paliwal, K. K. Information Fusion and Person Verification using speech and face information. Research Paper IDIAP-RR 02-33, IDIAP, September 2002.

[107] Toh, K.A., Yau, W.Y., Jiang, X., Chen, T.P., Lu, J., and Lim, E. Minutiae data synthesis for fingerprint identification applications, in Proc. Int. Conf. Image Processing (ICIP) (Greece), pp. 3:262–265, 2001.

[108] Willem, M. and Fmet, P. December 1997, Layped Biometric Verification, White paper, Keywm Technologies, December 1997.

[109] Kumar, A., Wong, D.C.M., shen, H.C. and Jain, A.K. Personal verification using palmprint and hand geometry biometric. In proceedings of the fourth International conference on audio and video based biometric person authentication, Pages 668-678, Guildford, U.K., June 2003.

[110] Ross A. and Govindrajan, R. Feature level fusion using hand and face biometrics. In proceeding of SPIE conference on Biometric technology for human identification, volume 5779, pages 196-204, Florida , U.S.A., March 2005.

[111] Jain, A.K., Nandakumar, K. and Ross, A. "Score normalization in multimodal biometric systems: Pattern Recognition" Vol. 38 pp. 2270 – 2285, 18 Jan 2005

[112] Huber, P.J. Robust Statistics. John Wiley & sons, 1981.

[113] Mathematical Index normalization available at: http://people.revoledu.com/kardi/tutorial/Similarity/Normalization.html

[114] Kittler, J., Hatef, M., Duin, R. P. and Matas, J. G. On Combining Classifiers. IEEE Transactions on Pattern Analysis and Machine Intelligence, 20(3):226–239, March 1998.

[115] Jain, A.K. Nandakumar, K. and Ross, A. "Score normalization in multimodal biometric systems: Pattern Recognition" Vol. 38 pp. 2270 – 2285, 18 Jan 2005

[116] Fuzzy logic toolbox for use with MATLB