Bi-Modal Biometrics Authentication Based on Iris and Signature

by

Serestina Viriri

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

in the

School of Computer Science
University of KwaZulu-Natal
Durban, South Africa
September, 2010

UNIVERSITY OF KWAZULU-NATAL

FACULTY OF SCIENCE AND AGRICULTURE

The research described in this thesis was performed at the University of KwaZulu-Natal under the supervision of Professor Jules-Raymond Tapamo. I hereby declare that all materials incorporated in this thesis is my own original work except where acknowledgement is made by name or in the form of a reference. The work contained herein has not been submitted in part or whole for a degree at any other university.

Signed:

Serestina Viriri

Date: September 2010

As the candidate's supervisor, I have approved the dissertation for submission

Signed:

Prof. Jules-Raymond Tapamo

Date: September 2010

UNIVERSITY OF KWAZULU-NATAL

FACULTY OF SCIENCE AND AGRICULTURE

DECLARATION 1 - PLAGIARISM

I, ... declare that

1. The research reported in this thesis, except where otherwise indicated, is my original research.
2. This thesis has not been submitted for any degree or examination at any other university.
3. This thesis does not contain other persons' data, pictures, graphs or other information, unless specifically acknowledged as being sourced from other persons.
4. This thesis does not contain other persons' writing, unless specifically acknowledged as being sourced from other researchers. Where other written sources have been quoted, then:
    a. Their words have been re-written but the general information attributed to them has been referenced
    b. Where their exact words have been used, then their writing has been placed in italics and inside quotation marks, and referenced.
5. This thesis does not contain text, graphics or tables copied and pasted from the Internet, unless specifically acknowledged, and the source being detailed in the thesis and in the References sections.

Signed:

Serestina Viriri

UNIVERSITY OF KWAZULU-NATAL

FACULTY OF SCIENCE AND AGRICULTURE

DECLARATION 2 - PUBLICATIONS

DETAILS OF CONTRIBUTION TO PUBLICATIONS that form part and/or include research presented in this thesis (include publications in preparation, submitted, in press and published and give details of the contributions of each author to the experimental work and writing of each publication)

1. S. Viriri[1] and J-R. Tapamo[2], "Improving Iris-based Personal Identification using Maximum Rectangular Region Detection", *Proceedings of the IEEE Computer Society International Conference on Digital Image Processing*, Bangkok, Thailand, pp. 421-425, March 7-9, 2009.

2. S. Viriri and J-R. Tapamo, "Efficient Iris Pattern Recognition Based on Cumulative-Sums and Majority Vote Methods", *Proceedings of the* 20^{th} *Annual Symposium of Pattern Recognition Association of South Africa (PRASA)*, Cape Town, South Africa, pp. 117-120, November/December 30-1, 2009.

3. S. Viriri and J-R. Tapamo, "Signature Verification Based on Handwritten Text Recognition", *Communications in Computer and Information Science (CCIS)*, Springer-Verlag Berlin Heidelberg, pp. 98-105, 2009.

4. B. Schafer[3] and S. Viriri, "An Adaptive Off-line Signature Verification System", *Proceedings of the IEEE International Conference on Signal and Image Processing Applications*, Kuala Lumpur, Malaysia, November 18-19, 2009.

5. S. Viriri and J-R. Tapamo, "Biometrics and Banking Systems in the African Context", *Proceedings of the IST-Africa Conference*, Pretoria, South Africa, May 3-5, 2006.

6. S. Viriri and J-R. Tapamo, "Biometrics in Africa: A Comprehensive Survey", *South African Journal of Science (SAJS)*, (to be submitted).

7. S. Viriri and J-R. Tapamo, "Integrating Iris and Signature Traits for Personal Authentication using User-SpecificWeighting", *Proceedings of the* 21^{st} *Annual Symposium of Pattern Recognition Association of South Africa (PRASA)*, Cape Town, South Africa, pp. 293-298, November, 2010.

8. S. Viriri and J-R. Tapamo, "Enhanced Signature Verification Based on Handwritten Text Recognition", *SAIEE Africa Research Journal*, (submitted).

9. S. Viriri and J-R. Tapamo, "Iris Pattern Recognition Based on Cumulative-Sums and Majority Vote Methods", *South African Computer Journal (SACJ)*, (submitted).

The author's contributions in each of the above papers are as follow:
Author[1]: Literature review, design of algorithms, redaction of papers
Author[2]: Critical analysis of the models and algorithms, proof-reading manuscripts.
Author[3]: Literature review, implementation of algorithms, write-up of the paper.

Signed:

Serestina Viriri

To my family, at large,
my daughter, Vuyo Vongai.

Being wise is better than being strong;
yes, knowledge is more important than strength.
After all, you must make careful plans
before you fight a battle,
and the more good advice you get,
the more likely you are to win.

Table of Contents

List of Tables

List of Figures

List of Abbreviations

2ν-SVM	Dual ν-Support Vector Machine
AAD	Average Absolute Deviation
AMT	Ammar Matching Technique
CASIA	Chinese Academy of Sciences' Institute of Automation
E	Gabor Energy
EER	Equal Error Rate
FAR	False Acceptance Rate
FRR	False Rejection Rate
FTA	Failure To Acquire
FTE	Failure To Enroll
GAR	Genuine Acceptance Rate
GPDS	Grupo de Procesado Digital de Sennales
HD	Hamming Distance
HMM	Hidden Markov Model
ICA	Independent Component Analysis
LDA	Linear Discriminant Analysis
MD	Mahalanobis Distance
MLP	Multilayer Perceptrons
PCA	Principal Component Analysis

PDF	Probability Density Function
PIN	Personal Identification Number
RBF	Radial Basis Function
ROC	Receiver Operator Characteristics
ROI	Region Of Interest
SAM	Spectral Angle Mapper
SID	Spectral Information Divergence
SVM	Support Vector Machine
VQ	Vector Quantization
XOR	Exclusive-OR operator

Abstract

Multi-modal biometrics is one of the most promising avenues to address the performance problems in biometrics-based personal authentication systems. While uni-modal biometric systems have bolstered personal authentication better than traditional security methods, the main challenges remain the restricted degrees of freedom, non-universality and spoof attacks of the traits. In this research work, we investigate the performance improvement in bi-modal biometrics authentication systems based on the physiological trait, the *iris*, and behavioral trait, the *signature*.

We investigate a model to detect the largest non-occluded rectangular part of the iris as a region of interest (ROI) from which iris features are extracted by a cumulative-sums-based grey change analysis algorithm and Gabor Filters. In order to address the space complexity of biometric systems, we proposed two majority vote-based algorithms which compute prototype iris features codes as the reliable specimen templates. Experiments obtained a success rate of 99.6%.

A text-based directional signature verification algorithm is investigated. The algorithm verifies signatures, even when they are composed of symbols and special unconstrained cursive characters which are superimposed and embellished. The experimental results show that the proposed approach has an improved true positive rate of 94.95%.

A user-specific weighting technique, the *user-score-based*, which is based on the different degrees of importance for the *iris* and *signature* traits of an individual, is proposed. Then, an intelligent dual ν-support vector machine (2ν-SVM) based fusion algorithm is used to integrate the weighted match scores of the iris and signature modalities at the matching score level. The bi-modal biometrics system obtained a false rejection rate (FRR) of 0.008, and a false acceptance rate (FAR) of 0.001.

Acknowledgements

A thesis is a long cycle of self discovery and continuous process of knowledge acquisition. The author is deeply indebted to the following people for their support during the formulation of this thesis:

- My Lord and Saviour, **Jesus Christ**, *In everything you do, put God first, and He will direct you and crown your efforts with success.*
- My supervisor, Prof. Jules-Raymond Tapamo, for his guidance and support during the difficult times of this research. His passion for scientific discovery, perseverance and determination have been my inspirational tool for hope.
- My parents and family at large, for their undying love, prayers and encouragement.
- My fellow colleagues, Zygmunt, Jean-Vincent for their discussions and humor; Søren Greenwood, for his technical support; the research group of Computer Vision, Image Processing and Data Mining (CID), for the true teamwork spirit.
- The School of Computer Science, University of KwaZulu-Natal, for its overall support and encouragement.
- The National Laboratory of Pattern Recognition, Chinese Academy of Sciences, for granting me access to its CASIA Iris Database.
- The *Grupo de Procesado Digital de Sennales* (GPDS), the *Universidad de Las Palmas de Gran Canaria*, Spain, for allowing me to make use of its GPDS signature database.

Chapter 1

General Introduction

1.1 Introduction

For ages, human beings have been recognizing each other through various characteristics. We recognize each other by our faces, by the way we walk, and the way we speak [133]. There have been many efforts to implement computer systems that imitate the human abilities. Several such systems exist already, but there are still many unsolved problems. For computer systems to achieve good personal authentication or identification, there is a need to characterize automatically the given person. Biometrics offers automated methods of identity verification or identification on the principle of measurable physiological or behavioral characteristics such as a fingerprint, the iris, signature and voice sample.

The societal pervasiveness ultimately achieved by information technology is determined by the degree to which it secures and strengthens trust and privacy as cornerstones of a free society [71]. To date, information technology has demonstrated a tremendous potential to provide the framework for trusted processes on a global scale, while at the same time opening new opportunities for freedom of access to information, services, and products. However, realizing this potential in an environment of rising security requirements hinges critically upon achieving robust authentication of individual users, which moves beyond faceless logins to authentication mechanisms that tightly bind a user's actions to his/her individual physical identity or behavioral characteristics. Biometric systems uniquely provide the means to bind the physical presence of an individual user with his/her cyber actions such that it can firmly be established as the basis for a trusted process.

While it is widely acknowledged that the performance improvement in current biometrics-based personal authentication systems is necessary, it is not clear what mechanisms could be used to improve this performance [70]. Hence, the necessity to query whether a multi-modal biometrics system based on a physiological trait and a behavioral trait can improve performance of authentication systems?

Biometric systems can either be implemented as *uni-modal biometric systems* (based on a single biometrics trait) or *multi-modal biometric* (based on multiple biometric traits). Uni-modal biometric systems have got limitations such as non-universality and spoofing. Multi-modal biometrics are being explored to alleviate these problems.

1.2 Motivation

Biometric systems automatically measure physiological or behavioral biological characteristics of an individual, from which a decision is made based on the application to either authenticate or determine the identity of that individual. The main challenges in biometrics technology include determination of an analytical framework from which the performance of biometric systems can be modeled and predicted, removal of key biometric system performance barriers through research of multi-modal biometrics and effective vulnerability countermeasures, and understanding of the relationships between biometric applications, privacy and security, and user acceptance which is essential for both informed public policy and system design [71].

Several biometric technologies are available for personal recognition and identity authentication. Among them are the fingerprint, gait, face, voice, retina, iris, hand geometry and biometric signature. However, recognition based on any one of these modalities may not be sufficiently robust or acceptable to a particular user group or in a particular situation or instance. Biometric technologies are becoming the foundation of an extensive array of highly secured identification and personal verification solutions. As the level of security breaches and transaction fraud increases, the need for improved technologies for personal identification and verification is becoming apparent. The need for biometrics can be found in national,

regional and local governments, in the military, and in commercial applications. Enterprise-wide network security infrastructures, government identity documents (IDs), secured electronic banking, investing and other financial transactions, retail sales, law enforcement, and health and social services are already benefiting from these technologies.

Reliable personal recognition is critical to many business processes, for instance in the banking sector during a transaction, the primary goal of banking systems is to ensure that an account holder is who he says he is. The conventional knowledge-based and token-based methods do not really provide personal recognition because they rely on surrogate representations of the person's identity. Therefore, any system assuring reliable personal recognition must necessarily involve biometrics components. Biometrics are inherently secured since they are some unique features the person physically has. The science of biometrics is an elegant solution to identifying and authenticating an individual, and avoids problems faced by possession-based and knowledge-based security approaches. While small to medium scale commercial applications may still use single biometrics modality for verification and identification, the only obvious solution for building a highly accurate verification and identification system for large scale applications appears to be multi-modal biometric systems [85, 96, 112]. Multi-modal biometrics combine different biometric modalities to strengthen security, possibly reduce false rejections, and provide alternatives to the user. Multi-modal biometric systems are expected to be more reliable than uni-modal systems due to the presence of multiple, fairly independent pieces of evidence. In fact, multi-modal biometrics is a conventional decision fusion problem where the evidence provided by each biometric is combined to improve the overall accuracy [62, 83, 121].

While multi-biometric systems are being deployed in various sectors like banking and airports, this does not imply that multi-modal biometrics is a fully solved problem. In fact, multi-modal biometrics can be further improved by reducing the error rates; failure to enroll (FTE) rate, and false rejection rate (FRR) on a given false acceptance rate (FAR). Thus, the problem of biometrics recognition can be viewed as a *Grand Challenge*, given the expectations of high matching accuracy, ease of usability and efficient scalability in a variety of applications accessed by different segments of the general population [138].

1.3 Problem Statement

In this thesis, we aim to investigate methods and techniques to improve the performance in biometrics-based personal authentication systems. Multi-modal biometrics is one of the most promising avenues to address this problem, and it has been the subject of intense research in recent times. Based on this prospective advantage, is it possible to improve personal authentication in biometric systems, using bi-modal biometric techniques based on the *iris* (a physiological trait) and the *signature* (a behavioral trait)?

On one hand, the iris is proving to be one of the most reliable biometric traits for personal authentication, but the remaining challenges are the detection of the proper region of interest (ROI), and lack of effective and efficient feature extraction techniques. Furthermore, there is need to optimize the computational and storage complexities of iris-based biometric systems, for instance, minimizing storage of multiple templates per user.

On the other hand, signatures continue to be an important biometrics trait, widely used primarily for enforcing binding contracts, and authenticating and authorizing legal transactions. While handwritten recognition has reached its maturity level, there is still the need for novel techniques which verify signatures accurately, even when they are composed of symbols and special unconstrained cursive characters that are superimposed and embellished.

While uni-modal biometric systems, based on either the iris or signature can authenticate an individual, there is still room for enhancing the accuracy rate especially by fusing the iris and signature to form a bi-modal system. The appropriate fusion techniques are still a subject of concern today. Jain et. al. [70, 82, 83] presented a variety of fusion schemes which require further investigation of their effects with various biometric modalities.

1.4 Thesis Objectives

The main aim of this research work is to improve security threshold of personal authentication in bi-modal biometric systems through the fusion of the iris and signature traits. The specific objectives of this thesis are:

- To develop a framework for modeling bi-modal biometric systems based on the *iris* (a physiological trait) and the *signature* (a behavioral trait) for personal authentication.
- To reduce biometrics error rates using bi-modal biometric techniques.
- To improve the security threshold in bi-modal biometric systems using innovative techniques for automated biometrics authentication.
- To optimize the verification accuracy rate of biometric-based systems.

1.5 Contributions of the Thesis

The major contributions of this thesis include:

1. An extension of Droogenbroeck's algorithm [160] for openings of binary images to an algorithm that detects the largest non-occluded rectangular part of the iris as a region of interest (ROI). The iris features codes are extracted from the detected region of interest using a cumulative-sums-based grey change analysis method. This technique can possibly be utilized for partial iris recognition since it relaxes the requirement of using the whole part of the iris to produce an iris template.
2. Approaches to address the problem of computational and storage complexities in iris recognition systems, two majority vote-based algorithms have been proposed. These algorithms are used to compute a prototype code per individual as the representative specimen iris template.

3. An efficient text-based directional signature recognition algorithm which verifies signatures, even when they are composed of symbols and special unconstrained cursive characters that are superimposed and embellished has been investigated. This algorithm extends the character-based signature verification technique.

4. A user-score-based weighting technique of integrating iris and signature traits has been designed and implemented. The proposed approach calculates weights for individual biometric traits per user in proportion to the scores of the biometric traits of the same user. These weights indicate the importance of matching scores output by each biometrics trait. Thereafter, the fusion algorithms; 2ν-SVM and sum rule, are used to integrate the weighted iris and signature traits at the matching score level. This enhanced-user-specific weighting improves the accuracy rate of multi-modal biometric systems by reducing the false rejection rate (FRR) on a given false acceptance rate (FAR).

1.6 Thesis Outline

Chapter 2 presents the background on iris recognition, signature verification, and reviews the state-of-the-art of uni-modal and multi-modal biometrics. In Chapter 3, iris feature extraction, learning and classification methods are investigated. Basic image pre-processing algorithms and strategies for calculating the iris template are presented as well. Chapter 4 discusses signature feature extraction algorithms. In Chapter 5, multi-modal biometrics fusion algorithms and weighting techniques are designed and implemented. Experimental results and discussions are presented in Chapter 6. Chapter 7 draws conclusions and outlines future work.

Chapter 2

Background and Literature Review

2.1 Introduction

Research towards the study of biometrics has been around around for some time [70, 85, 128]. Most research is still in experimental phases [60, 70]. Several biometric techniques are available today, but many of them are at the experimental stage, while few have matured and are commercially available.

Most systems that control access to financial transactions, computer networks, or secured locations, identify authorized persons by recognizing passwords or personal identification numbers (PINs). The weakness of these systems is that unauthorized persons can discover others' passwords and PINs quite easily and use them without detection. Most of these systems require reliable personal authentication schemes to either confirm or determine the identity of individuals requesting their services. In the absence of robust authentication schemes, authentication systems are vulnerable to the wiles of an impostor. Biometric identification systems, which use physical features to check a person's identity, ensure much greater security than a password and number system [60].

Biometric systems are perceived to be better than traditional security methods in that they cannot be easily stolen or shared. Besides bolstering security, biometric systems also enhance user convenience by alleviating the need to design and remember passwords. Moreover, biometrics is one of the few techniques that can be used for negative recognition where the system determines whether the person is who he or she denies to be [83].

2.2 Biometric Technologies

There are several definitions of biometrics as well as different implementations and applications of biometric technologies. In general, biometrics can be defined as: ***the automated use of physiological or behavioral characteristics to determine or verify identity*** [65]. Other common definitions of biometrics are:

- The science of using biological properties to identify individuals; for example, fingerprints, iris, retina scan and voice recognition [120].
- The science and technology of authentication (i.e. establishing the identity of an individual) by measuring the subject person's physiological or behavioral features. The term is derived from the Greek words ***"bios"*** for life and ***"metron"*** for measure [120].
- A method of verifying an individual's identity based on measurement of the individual's physical feature(s) or repeatable actions where those features and/or actions are both unique to that individual and measurable [120].

Consequently, biometric systems exploit *automated methods of recognizing a person based on physiological or behavioral characteristics* [62]. Physiological biometrics are based on data derived from direct measurement of a body part (e.g. retina, iris, fingerprints, face), while behavioral biometrics are based on measurements and data derived from a human action (e.g. gait, signature). In fact, behavioral characteristics are traits that are learned or acquired. Biometric systems are being used to verify identities and restrict access to buildings, computer networks, and other secured sites. Recent global terrorism escalation is pushing the need for secure, fast and non-intrusive identification of people as a primary goal for homeland security [62].

While biometric systems have their limitations [135], they have an edge over traditional security methods in that it is significantly difficult to lose, steal or forge biometric traits. Biometric systems also introduce an aspect of user convenience that may not be possible when

using traditional security techniques. For example, users maintaining different passwords for different applications may find it challenging to recollect the password associated with a specific application. In some instances, the user might even forget the password, requiring the system administrator to intervene and reset the password for that user. Maintaining, recollecting, and remembering passwords can, therefore, be a tedious and expensive task. Biometrics addresses this problem effectively, thereby enhancing user convenience: a user can employ different biometric traits for different applications, with biometrics trait recollection not being an issue at all.

There are several biometric characteristics being used in various application systems. Each biometrics trait has its strengths and weaknesses, therefore, the choice of a biometrics trait depends on a variety of issues besides its matching performance [138]. Jain et al. [77] have identified factors that determine the suitability of a biometrics trait to be used in biometric systems [62, 133]:

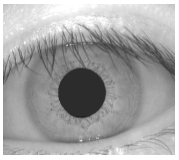
- *Uniqueness* - the given biometric trait should be sufficiently different across individuals.
- *Universality* - the trait type is present in as many people as possible.
- *Permanence* - the trait should be sufficiently invariant over time, or at least, it varies very slowly.
- *Measurability* - the possibility to measure the trait through the extraction of representative feature sets.
- *Performance* - the recognition accuracy should meet the constraints imposed by the application.
- *Acceptability* - the users should be willing to present their biometric traits to the system.
- *Circumvention* - the possibility to deceive the system by fraudulent methods is very tough.

Currently, there are many different biometric techniques that are either widely used or under intensive investigation, including fingerprint, iris, hand geometry, signature, facial

geometry, voice, palmprint, retina, vein structure, ear form, DNA, odor, keyboard strokes, and gait [62, 68]. Each of them has different accuracy, cost and a different fulfillment of the seven characteristics previously presented. Examples of these biometric techniques are shown in Figure 2.1.

(a) Face

(b) Fingerprint

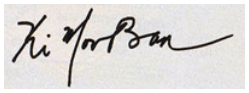


(c) Iris

(d) Gait

(e) Palmprint

(f) Hand-Geometry



(g) Signature

Figure 2.1: Examples of different biometric technologies

Fingerprint

Fingerprints have been used for personal identification for many years and the validity of fingerprint identification has been well-established. A fingerprint is the pattern of ridges and furrows on the surface of a fingertip whose formation is determined during the first seven months of fetal development [138]. It is formed by the accumulation of dead, cornified cells that constantly slough as scales from the exposed surface [68]. It has been empirically determined that the fingerprints of identical twins are different and so are the prints on each finger of the same person [110]. Fingerprint technology is so common in personal identification that

it has almost become the synonym of biometrics [44]. The main disadvantage with the fingerprint technology is its acceptability by users, because fingerprints have connotations of criminal investigations. Another problem with large-scale fingerprint recognition systems is that automatic fingerprint identification generally requires a large amount of computational resources. Multiple fingerprints of an individual provide additional information to enhance large-scale identification. The accuracy of fingerprint recognition systems has been shown to be very high [109].

Iris

Iris is the annular region of the eye bounded by the pupil and the sclera. The texture formation of iris in a human eye depends on the initial conditions of the embryonic mesoderm from which it develops [38]. The visual texture of the iris is formed during fetal development and stabilizes during the first two years of life [170]. Iris is inherently isolated from external environment and can not be modified surgically [171]. The complex iris texture carries very distinctive information useful for personal recognition [41]. The accuracy and speed of currently deployed iris-based systems is promising and support the feasibility of large-scale identification systems [138]. In fact, iris-based systems have a low FAR compared to other biometric traits, and the FRR is generally high [66].

Hand Geometry

Hand geometry recognition systems are based on a number of measurements taken from the human hand including its shape, size of palm, and lengths and widths of the fingers [182]. The main disadvantage of this technique is its low discriminative capability - it is very difficult for a hand geometry-based biometric system to achieve a very high identification accuracy, especially for a large population [68]. However, environmental factors such as dry weather or dry skin do not appear to adversely affect the authentication accuracy of hand geometry-based systems, but jewelry like rings may pose challenges in extracting the correct hand geometry information [138]. A variant of the hand geometry technique, the finger

geometry technique, which relies on a number of geometrical invariants of fingers such as the 3D shape of a finger has recently been investigated. It is claimed that finger geometry is more accurate in personal identification than hand geometry [68].

Signature

The way a person signs her name is known to be a characteristic of that individual [101, 115]. There are two approaches to signature verification: *off-line* and *on-line* verification. Off-line signature verification is based on the image properties and geometric features of a signature, while on-line signature verification uses the image properties, geometric features, and the dynamic features such as pressure exerted, time taken and trajectory profiles of the signature. Inherent advantages of a signature-based biometric system is that the signature has been established as an acceptable form of personal identification method, and it is impossible for an impostor to obtain the dynamics information from a written signature [68]. A signature is a behavioral biometrics trait that changes over a period of time and is influenced by the physical and emotional conditions of the signatories. Signatures of some people vary substantially, even successive impressions of their signature are significantly different [67, 138].

Face

Face recognition is a non-intrusive technique, and facial attributes are probably the most common biometric features used by humans to recognize one another [28]. Theoretically, it has the potential to become the most friendly and acceptable way to make personal identification [21]. The most popular approaches to face recognition [102, 151] are based on either (*i*) the location and shape of facial attributes, such as the eyes, eyebrows, nose, lips, and chin and their spatial relationship, or (*ii*) the overall analysis of the face image that represents a face as a weighted combination of a number of canonical faces. Although humans depend heavily on facial images and attributes to identify individuals, it is widely known that humans utilize a large amount of contextual information in performing face recognition [33]. Without the contextual information, it is questionable whether the face

itself is sufficiently effective to make a personal identification with high level of confidence.

Voice

Voice is a combination of physical and behavioral biometric characteristics. The vocal characteristics of humans are totally determined by the vocal tract, mouth, nasal cavities, and the other speech processing mechanisms of the human body [21]. The voice-print verification can either be a *text-dependent* which authenticates the identity of an individual based on a fixed predetermined phrase, or *text-independent* which verifies the identity of a speaker independent of the phrase [21]. Extensive studies have been conducted on voice recognition techniques. Currently, there are several voice-based recognition systems available in the market like Veritel, VoiceKey, SpeakEZ [21]. The main challenges with voice-based recognition is that the speech features may not be sufficiently unique to permit an identification of an individual from a large population, and voice features are sensitive to a number of factors such as background noise as well as the emotional and physical state of the speaker. Moreover, some people seem to be extraordinarily skilled in mimicking others' voice [21, 138].

Palmprint

The palms of the human hands contain larger area of pattern of ridges and valleys than fingerprints, as a result, palmprints are expected to be more distinctive than fingerprints [94, 176]. Human palms also contain additional distinctive features such as principals lines and wrinkles that can be captured even with a lower resolution scanner [54]. Palmprint recognition has the potential of achieving high accuracy rate, especially when all the features of the hand such as geometry, ridge and valley features, principal lines, and wrinkles are combined together to build a system.

Table 2.1: Comparison of biometric technologies (*H=High, M=Medium, L=Low*) [84, 85].

Biometrics Modality	Universality	Uniqueness	Permanence	Collectability	Performance	Acceptability	Circumvention
Face	H	L	M	H	L	H	L
Fingerprint	M	H	H	M	H	M	H
Hand Geometry	M	M	M	H	M	M	M
Keystrokes	L	L	L	M	L	M	M
Hand Vein	M	M	M	M	M	M	H
Iris	H	H	H	M	H	L	H
Retinal Scan	H	H	M	L	H	L	H
Signatures	L	L	L	H	L	H	L
Voice Print	M	L	L	M	L	H	L
Face Thermogram	H	H	L	H	M	H	H
Odor	H	H	H	L	L	M	L
DNA	H	H	H	L	H	L	L
Gait	M	L	L	H	L	H	M
Ear	M	M	H	M	M	H	M

Other Biometric Technologies

Besides the techniques mentioned above, other biometric techniques such as *keystroke, ear shape, retina, gait, DNA, and body odor,* have been investigated. Although each of these techniques has its own advantages, so far none of them has a strong potential to become a valid biometric technique to be used widely in the near future.

A brief comparison of fourteen different biometrics techniques provided by Jain et al [76, 84, 85] is shown in Table 2.1. Which biometrics technique should be used for a given application depends on the requirements and characteristics of that application, and the properties of the biometrics technology.

2.2.1 Biometric Applications

Biometrics has been widely used in forensic applications such as criminal identification and prison security. Biometrics technology is rapidly evolving and has a very strong potential to be widely adopted in civilian applications such as electronic banking, e-commerce, and access control. Due to a rapid increase in the number and use of electronic transactions, electronic banking and electronic commerce are becoming one of the most important emerging applications of biometrics [126]. These applications include credit card and smart card security, automated teller machine (ATM) security, check cashing and fund transfers, online transactions and web access. The physical access control applications have traditionally used token-based authentication. With the progress in biometrics technology, these applications will increasingly use biometrics for authentication. Remote login and data access applications have traditionally used knowledge-based authentication. These applications have already started using biometrics for personal authentication. The use of biometrics will become more widespread with time as the technology matures and becomes more trustworthy. Other biometric applications include welfare disbursement, immigration checkpoints, national ID, and voter and driver registration.

2.2.2 Biometric Systems

A typical biometrics system operates by acquiring biometric data from an individual, extracting a feature set from the acquired data, and comparing this feature set against the template feature set in the database.

A simple biometrics system has four basic modules [168]:

1. *Sensor Module*, which captures the biometric data of an individual. An example is a fingerprint sensor that captures fingerprint impressions of a user.

2. *Feature Extraction Module* in which the acquired data is processed to extract feature values. For example, the position and orientation of minutiae points in a fingerprint

image would be computed in the feature extraction module of a fingerprint system.

3. *Matching Module* in which the feature values are compared against those in the template by generating a matching score. For instance, in this module, the number of matching minutiae between the query and the template can be computed and treated as a matching score.

4. *Decision-Making Module* in which the user's claimed identity is either accepted or rejected based on the matching score generated in the matching module, this process is called *verification*. Alternately, the system may identify a user based on the matching scores, which is *identification*.

2.2.3 Uni-Modal and Multi-Modal Biometrics

Uni-modal biometrics are based on a single trait which sometimes has low accuracy rate for the identification of an individual. For instance, it is difficult to distinguish identical twins using their faces alone. Furthermore, using only one biometrics trait has several drawbacks, Frischholz et. al. [60] proved that about five percent of people have fingerprints that cannot be recorded because they are obscured by a cut or a scar, or they are too fine to extract distinctive features. Consequently, multi-modal identification systems seek to address the problem of non-universality and provide anti-spoofing measures which can lead to improved verification performance. In addition, multi-modal biometrics provides a possible viable way of overcoming the acceptability barriers to the widespread adoption of biometric systems.

Biometric systems using a single biometric trait for authentication purposes have the following limitations [135, 137]:

- *Noise in Sensed Data:* The sensed data maybe contaminated by noise due to the imperfect acquisition conditions like defective sensors or unfavorable environmental conditions like poor illumination. The variations in the sensed data can cause noise for example a scar on the fingerprint, or voice characteristics altered by the common cold. Noisy biometric data increase the False Rejection Rate (FRR).

- *Intra-Class Variations:* The biometric data acquired from an individual during verification may be different from the data that was used to generate the specimen template during enrollment, resulting in the increase of the FRR. This variation can be caused by either users who incorrectly interact with the sensor during biometric data acquisition or use of different sensors. Besides, the varying psychological makeup of an individual, may result in different behavioral traits of the same biometrics trait at various time instances.

- *Restricted Degrees of Freedom:* While a biometrics trait is expected to be sufficiently different across individuals, there can be similarities in the feature sets used to represent these traits. This limitation restricts the degrees of freedom provided by the biometrics trait.

- *Non-Universality:* While every user is expected to possess the biometrics trait being acquired, in reality the biometrics system may not be able to acquire meaningful data from a subset of individuals resulting in a failure-to-enroll (FTE) error associated with using a single biometrics trait. For example, an iris recognition system may fail to extract distinctive features from individuals with drooping eyelids or certain pathological conditions of the eye.

- *Spoof Attacks:* Behavioral traits such as voice and signature are vulnerable to spoof attacks by an impostor attempting to circumvent the system [55]. Physical traits such as fingerprints can also be spoofed by inscribing ridge-like structures on synthetic material such as gelatine [111, 129].

Some of these limitations imposed by uni-modal biometric systems can be overcome by including multiple sources of information for establishing identity [136]. Therefore, multi-modal biometric systems seek to alleviate some of these drawbacks by providing multiple evidences of the same identity that increase population coverage and deter spoofing attacks.

The performance of biometric systems is largely affected by the reliability of the sensor used and the degrees of freedom offered by the features extracted from the sensed signal. Multi-modal biometric systems are expected to be more reliable than uni-modal systems due to the presence of multiple pieces of evidence, and these systems are able to meet the

stringent performance requirements imposed by various applications because they are is based on different biometric traits [95]. Many studies [11, 62, 69] report an improvement in accuracy for multi-modal biometric systems with respect to uni-modal systems.

2.2.4 Fusion in Biometrics

Levels of Fusion

There are three levels of fusion in biometrics. Fusion in biometric systems integrates information presented by single or multiple biometric indicators. The information can be consolidated at three different levels. Ross and Jain in [137] described the three possible levels of fusion as illustrated in Figure 2.2. These levels include [136]:

1. *Fusion at the Feature Extraction Level:* Here, different features are extracted from the data obtained from each sensor. The features computed from different biometric indicators are concatenated into a single vector.
2. *Fusion at the Matching Score Level:* At that level, each system provides a similarity score indicating the distance between the input feature vector and the template vector. The similarity scores are combined to ascertain the veracity of the claimed identity.
3. *Fusion at the Decision Level:* Here, each system provides a similarity score per biometrics trait indicating the distance between the input feature vector and the template vector, which is individually classified into the two classes: *accept* or *reject*. A majority vote scheme is used to make the final decision [181].

Fusion Scenarios

Fusion of traits in multi-modal biometric systems can be done in a variety of scenarios depending on the number of traits, sensors, and feature sets used. It can be implemented in the following forms [137]:

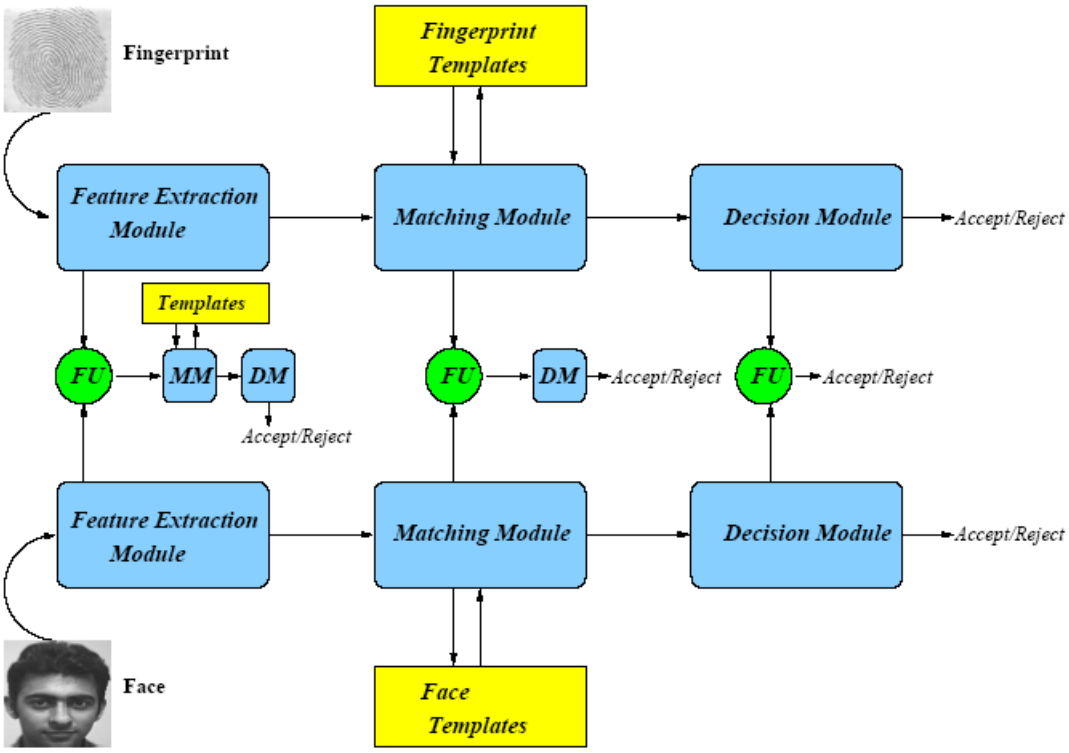


Figure 2.2: The three levels of fusion: Fusion Module (FU), Matching Module (MM), Decision Module (DM) [137].

- *Single Biometric Multiple Representations* - This fusion scenario involves using multiple representations of the same biometrics trait. Raw biometric data pertaining to different sensors are obtained, each representation has its own associated matcher or classifier, and the similarity scores calculated by these classifiers are then consolidated. Chang et. al. [26] acquire both 2D and 3D images of the face and combine them at the data level as well as the match score level to improve the performance of a face recognition system. Kumar et. al. [94] describe a hand-based verification system that combines the geometric features of the hand with palmprints at the feature and match score levels, and their experimental results at the match score fusion level are better than at the feature fusion level.

- *Single Biometric Multiple Matchers* - A single sensor is employed to obtain raw data which are then used by multiple classifiers. Each of these classifiers either operates on the same feature set extracted from the data or generates their own feature sets. Multiple matching strategies are incorporated in the matching module of a biometric system and combine the scores generated by these strategies. The logistic function, [80] is used to map the matching scores obtained from two different fingerprint matching algorithms into a single score. This type of fusion also takes place at the matching stage of a biometric system. Lu et. al. [106] extract three different types of feature sets from the face image of a subject using Principal Component Analysis (PCA), Linear Discriminant Analysis (LDA) and Independent Component Analysis (ICA); and integrate the output of the corresponding classifiers at the match score level.

- *Single Biometric Multiple Units* - In the case of some biometric traits like fingerprints (or the iris), it is possible to integrate information presented by two or more fingers (or both the irides) of a single user. This is a less expensive way of improving system performance since this neither entails deploying multiple sensors nor incorporating additional feature extraction or matching modules [137].

- *Multiple Biometric Traits* - Multiple biometric traits of an individual are used to establish his/her identity. Multi-modal systems employ multiple sensors to acquire data pertaining to different traits. The independence of the traits ensures that a significant improvement in performance is obtained [137]. These systems seek to improve

the speed and reliability of a biometric system [69] by integrating matching scores obtained from multiple biometric sources. Brunelli et. al. [20] use the face and voice traits of an individual for identification. A HyperBF network is used to combine the normalized scores of five different classifiers operating on the voice and face feature sets. A statistical framework based on Bayesian statistics is developed to integrate the speech (text-dependent) and face data of a user [9]. The estimated biases of each classifier is taken into account during the fusion process. Hong and Jain associate different confidence measures with the individual matchers when integrating the face and fingerprint traits of a user [69].

2.2.5 Operational Mode

Biometric systems can be used in two different modes: *verification* (authentication) mode and *identification* mode. Identity verification occurs on a *one-to-one matching*, when the biometric data obtained from the user are compared to the user's template in the database. Identification occurs on a *one-to-many matching*, when the identity of the user is *a priori* unknown [133]. In this case the user's biometric data are matched against all the records in the database. Verification (*am I who I claim to be*), and identification (*who am I*), are two different problems with different inherent complexities [135]. In this thesis, we have focused on multi-modal biometric systems, which operate in the verification mode.

Verification Mode

The biometric verification problem can be formulated as follows [135]: Given an input feature vector X_Q and a claimed identity I, determine if (I, X_Q) belongs to ω_1 or ω_2, where ω_1 indicates that the user is genuine and ω_2 indicates an impostor. Then, X_Q is matched against X_I, which is the template corresponding to user I, to determine the degree of similarity, as shown in equation (2.1).

$$(I, X_Q) \in \begin{cases} \omega_1 & if S(X_Q, X_I) \leq \eta, \\ \\ \omega_2 & otherwise, \end{cases} \tag{2.1}$$

where S is the function that measures the similarity between X_Q and X_I, and η is a computed local or global threshold. Every claimed identity is classified as genuine, ω_1 or impostor, ω_2, as shown in Figure 2.3.

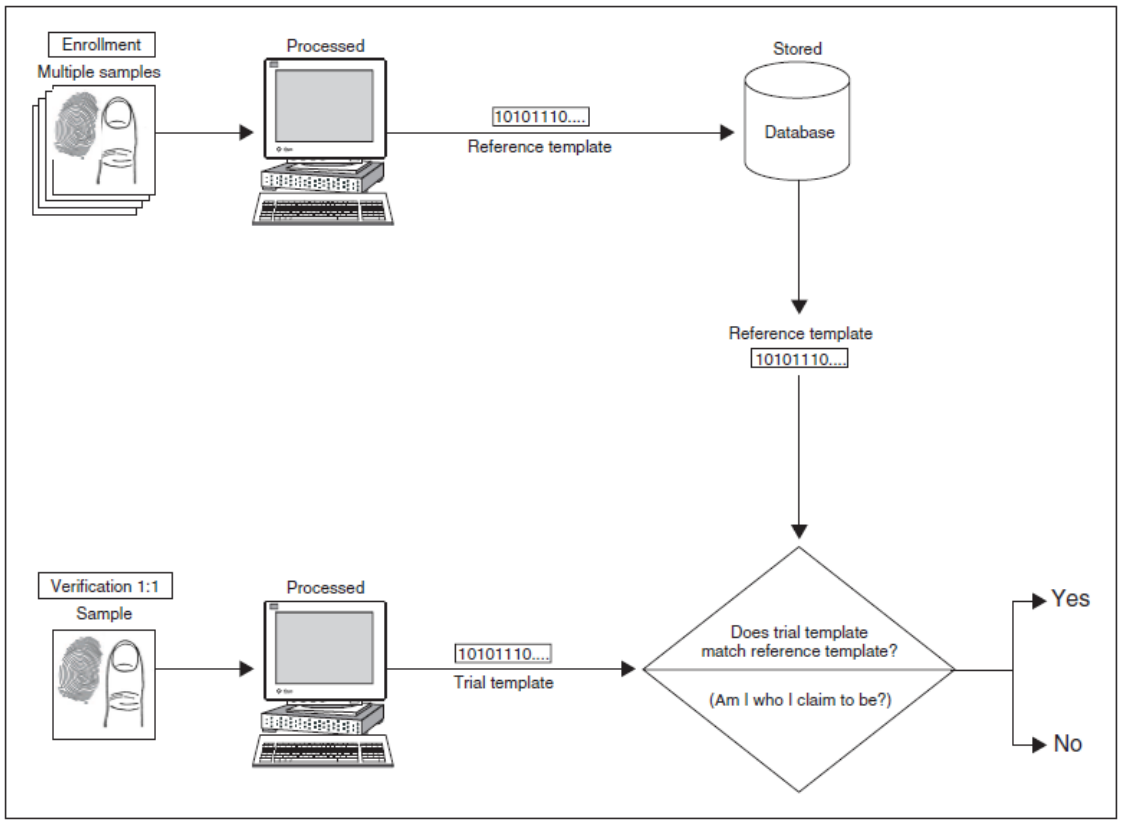


Figure 2.3: Biometrics: verification mode [131].

Identification Mode

The identification problem is formulated as follows: Given an input feature vector X_Q, determine the identity I_k, $k \in \{1, 2, ...N, N+1\}$; where I_1,I_2,...I_N are the identities enrolled in the system, and I_{N+1} indicates the reject case where no suitable identity is found, such that:

$$(X_Q) \in \begin{cases} I_k & if \max_k\{S(X_Q, X_{I_k})\} \leq \eta, \quad k = 1, 2, ...N, \\ \\ I_{N+1} & otherwise, \end{cases} \tag{2.2}$$

where X_{I_k} is the biometric template corresponding to identity I_k, and η is a computed local or global threshold, as illustrated in Figure 2.4.

2.2.6 Biometric Errors

In biometric systems, a similarity match score is *genuine* or *authentic* if it is a result of two matching samples of the same biometric trait of a user, otherwise it is an *impostor score*, resulting from comparing two biometric samples originating from different users [138]. A genuine score that falls below the threshold τ results in a *false rejection*, while an impostor score that exceeds the threshold τ results in a *false acceptance*. The *false rejection* and *false acceptance* are categorized in two types of biometric errors.

- ***False Rejection Rate*** (FRR) or (Type I error) - is a measure of the probability that an authorized user is rejected by the system. It is calculated by finding the ratio of the number of instances of false rejection to the total number of instances as defined in equations (2.3) and (2.4), [97]:

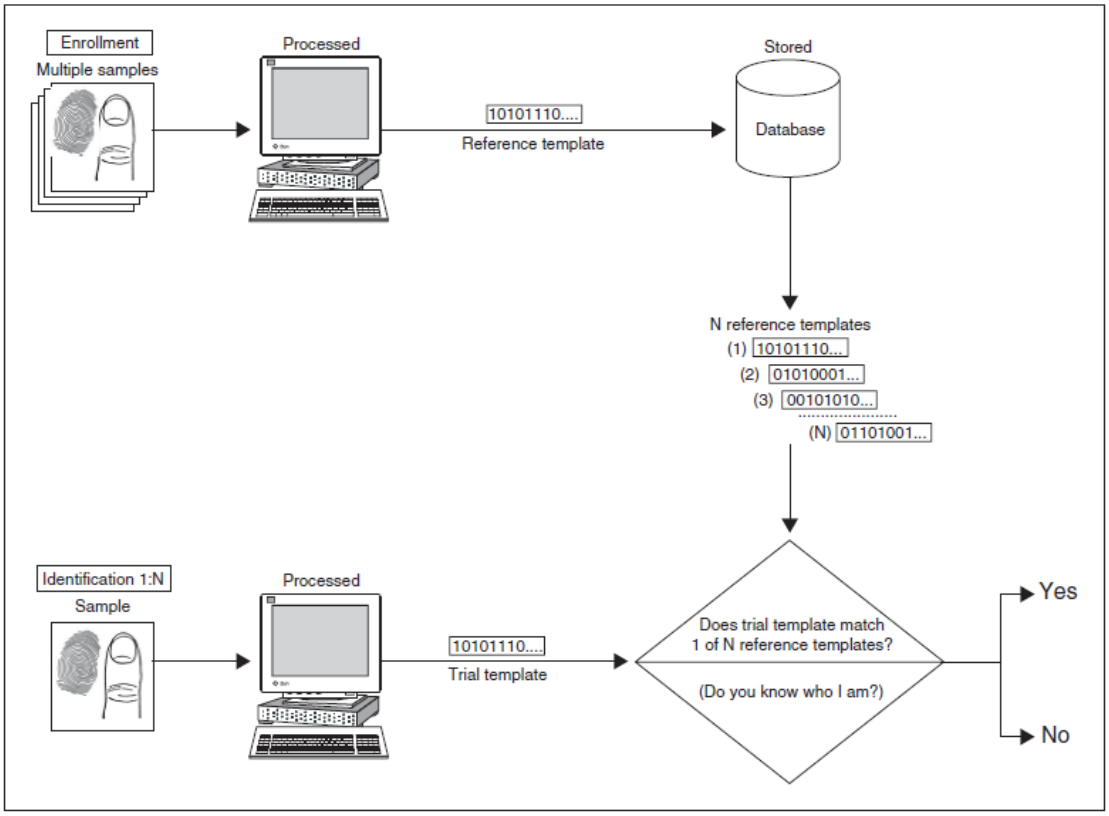


Figure 2.4: Biometrics: identification mode [131].

$$FRR(n) = \frac{Unsuccessful\ Authentication\ Attempts\ of\ Authorised\ User\ n}{Total\ Authentication\ Attempts\ of\ Authorised\ User\ n} \tag{2.3}$$

$$FRR = \frac{1}{N}\sum_{n=1}^{N} FRR(n) \tag{2.4}$$

where N is total number of individuals, and $FRR(n)$ is the number of unsuccessful authentication attempts of an authorised user n.

FRR is also defined as the fraction of genuine scores falling below the threshold τ, (equation (2.5)), resulting in a legitimate user being rejected because the biometrics system does not find the user's current biometric data similar enough to the master template stored in the database [138].

$$FRR(\tau) = \int_{-\infty}^{\tau} p(s|genuine)ds \tag{2.5}$$

where $p(s|genuine)$ is the estimated probability density function (or probability distribution) of the score s under the genuine condition; when a large number of genuine scores is available.

- ***False Acceptance Rate*** (FAR) or (Type II error) - is a measure of the probability that an unauthorized user is accepted by the system. It is expressed as a set of forgery attempts against a single individual as defined in equations (2.6) and (2.7), [97]:

$$FAR(n) = \frac{Successful\ Forgery\ Attempts\ of\ Unauthorised\ User\ n}{Total\ Forgery\ Attempts\ of\ Unauthorised\ User\ n} \tag{2.6}$$

$$FAR = \frac{1}{N}\sum_{n=1}^{N} FAR(n) \tag{2.7}$$

where N is total number of individuals, and $FAR(n)$ is the number of successful forgery attempts of an unauthorised user n.

FAR is also expressed as the fraction of impostor scores exceeding the threshold τ, (equation (2.8)), resulting in an impostor being accepted as a legitimate user because the biometrics system finds the impostor's biometric data similar to the master template of a legitimate user [138].

$$FAR(\tau) = \int_{\tau}^{\infty} p(s|impostor)ds \tag{2.8}$$

where $p(s|impostor)$ is the estimated probability density function of the score s under the impostor condition; when a large number of impostor scores is available.

The performance of a biometrics system is typically specified in terms of its FAR and a corresponding FRR. The decision scheme should establish a decision boundary, which minimizes the FRR for the specified FAR. There is a trade-off between the two types of errors and both the errors cannot be reduced simultaneously based on the operating point alone. In fact, these two errors are directly correlated. The given biometric application dictates the FAR and FRR requirements for the verification system. For example, access to an ATM machine generally needs a small FRR, but access to a secured military installation requires a very small FAR.

Besides the FAR and FRR, biometric systems encounter other types of errors. The *Failure to Acquire* (FTA) rate denotes the proportion of times the biometrics device fails to capture a sample when the biometrics characteristic is presented to it. This type of error typically occurs when the device is not able to locate a biometrics signal of sufficiently good quality [138]. The *Failure to Enroll* (FTE) rate is the proportion of users that can not be successfully enroled in a biometrics system. This necessitates the design of robust and efficient user interfaces that can assist users during enrollment [138].

Furthermore, the performance of a biometrics system can be provided by single-valued measures like the *Equal Error Rates* (EER) and the *d-prime value* [138]. The EER corresponds to the point where the FAR and FRR are equal; and a lower EER value indicates better performance. The d-prime value (d') measures the separation between the means of the genuine and impostor probability distributions in standard deviations units and is defined as [138]:

$$d' = \frac{\sqrt{2}|\mu_{genuine} - \mu_{impostor}|}{\sqrt{\sigma^2_{genuine} - \sigma^2_{impostor}}} \tag{2.9}$$

where $\mu_{genuine}$ and $\mu_{impostor}$ are the means, and $\sigma_{genuine}$ and $\sigma_{impostor}$ are standard deviations of the genuine and impostor distributions, respectively. The higher the d-prime value is, the better the performance of the system [153].

The performance of a biometrics system is also depicted visually in the *Receiver Operating Characteristics* (ROC) curves. The ROC curve displays how the FAR changes with respect

to the FRR and vice-versa. These curves can also be plotted using the genuine accept rate versus the false accept rate [17, 64].

2.3 Related Work

2.3.1 Iris Recognition

The idea of iris identification traces back to the Paris prison in the eighteenth century, where police discriminated criminals by inspecting their irides color [73]. Daugman [38] was the first to develop the fundamental algorithms, which now form the basis for current commercial iris recognition systems, after he was commissioned by Flom and Safir to conduct intensive and extensive research for implementing automated iris recognition.

One of the fundamental algorithms for iris recognition systems developed by Daugman [6, 38], is the 2-D Gabor Wavelet approach, which extracts discriminating information. Recognition is done by means of a test of statistical independence for two iris codes. A failure of the test implies a match. The matching system implements a normalized Hamming distance criteria. Furthermore, Daugman introduced an active contours method to enhance iris segmentation [42, 88]. The iris inner and outer boundaries are described in terms of active contours based on discrete Fourier series. This, enhanced iris segmentation by precisely detecting the upper and lower eyelid boundaries, and excluding any superimposed eyelashes or reflections from cornea or eyeglasses.

The active-contour models for the inner and outer iris boundaries support an isometric mapping of the iris. Let $(x_p(\theta), y_p(\theta))$ be the Cartesian coordinates of the contour model for the pupillary boundary, where the arc parameter $\theta \in [0, 2\pi]$, and the contour model $(x_s(\theta), y_s(\theta))$ describes the outer boundary of the iris at the sclera. A size-invariant, shape-flexible, and pupil-dilation-invariant dimensionless coordinate system for the iris region of interest of the image $I(x, y)$ is represented by the normalized mapping [42]:

$$I(x(r,\theta), y(r,\theta)) \rightarrow I(r,\theta) \tag{2.10}$$

where the dimensionless parameter $r \in [0,1]$, and

$$\begin{bmatrix} x(r,\theta) \\ y(r,\theta) \end{bmatrix} = \begin{bmatrix} x_p(\theta) & x_s(\theta) \\ y_p(\theta) & y_s(\theta) \end{bmatrix} \begin{bmatrix} 1-r \\ r \end{bmatrix} \tag{2.11}$$

The running time of the entire subroutine that fits active contours to both the inner and outer iris boundaries is relatively high. Figure 2.5 shows the normalization process of the iris image, where i and p represent the center of the iris and of the pupil, respectively.

In [43], Daugman and Downing investigated the effects of image compression on iris recognition performance. The compressed iris data are stored in the database, transmitted on the network, and embedded in media in the form of real images rather than as iris code templates generated with proprietary algorithms. The results showed that it is possible to compress iris images as severely as 150 : 1 from their original full-size formats with minimal impact on recognition performance rate [43, 130].

Other recent approaches to iris pattern recognition include: the Laplacian parameter approach by Wildes [1, 171]; the Zero-Crossing of the 1-D Wavelet Transform at various resolution levels by Boles et. al. [16]; the Independent Component Analysis (ICA) approach by Huang [73]; texture analysis using multi-channel Gabor filtering and Wavelet Transform by Zhu et. al. [180]; the Circular Symmetric filter approach by Ma et. al. [108], the Self-Organizing Neural Network approach by Liam et. al. [103], and the use of a partial iris for recognition using one-dimensional approach by Du [49].

Each of the above methods has its own advantages and disadvantages. Among them, Daugman's 2-D Gabor Wavelet approach has been successfully tested using a large scale iris

database and has been commercialized by Iridian, and the one-dimensional approach has been tested for use with partial iris identification.

To date, several research endeavors have proved that the iris can provide the most stable biometric signals for identification, with very distinctive texture that is formed during gestation. Compared with other biometric features such as the retina, fingerprint, voice and face, iris patterns are more stable, distinctive and reliable [51] for the following reasons [73]:

- The iris is formulated in the third month of gestation and the structures of its texture patterns are invariant.
- The formulation of the iris depends on the initial environment of the embryo, as a result, the iris texture patterns do not correlate with genetic determination.
- The right and left irides of any individual are different from each other.
- The iris is protected by aqueous humor and the cornea from any environmental disturbances.
- Iris recognition is non-intrusive.
- The iris is extremely difficult to modify through surgery.

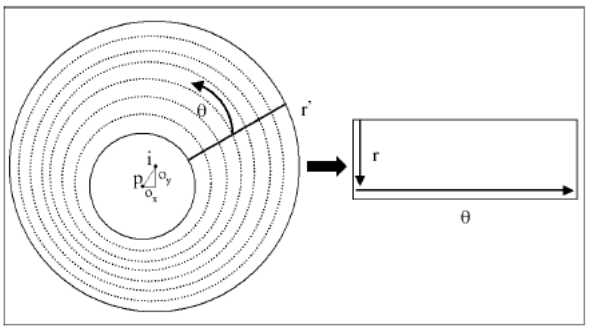


Figure 2.5: Normalization of the iris image from the Cartesian coordinate system into a pseudopolar coordinate system [41].

2.3.2 Signature Verification

A substantial amount of research work has been carried out in the area of signature recognition and verification. In fact, automatic handwriting based personal identification (HBPI) is an active research topic in computer vision and pattern recognition [179]. Signature verification poses a real challenge for researchers because of the many difficulties that can arise during the process of creating such a system [100]. Two approaches are used in signature verification:

- Off-line verification - based on the static image of the signature (the result of the action of signing).
- Online verification - the dynamic action of signing the signature itself.

Ammar [2] introduced a technique for off-line signature verification called *Ammar Matching Technique* (AMT). The AMT eliminates skilled forgeries with a very low rate of false rejections. Grey-level comparison technique [142] is used in off-line signature verification, to eliminate forged signatures created by photocopying or tracing. Justino et. al. [86] proposed an off-line signature verification system using a Hidden Markov Model (HMM). The system verifies signatures considering the three different forgery types in a HMM framework. The three types of forgery which are related to intra and inter-personal signature variability are random forgery, simple forgery and skilled forgery [48, 86].

The detection of every type of forgery requires an appropriate recognition approach. For instance, skilled forgery is better detected by methods based on a *pseudodynamic* approach [87, 132], which captures the handwriting motion properties and *graphometric* features [140].

Furthermore, Coetzer et. al. [35, 36] developed an HMM-based off-line signature verification system that uses Radon Transform (RT) to extract features from signature images. This HMM-based system outperforms human verifiers especially on bank cheques verification.

Since the properties of curvature, slant angle and total length of a signature are considered constant among different samples, Wilkinson et. al. [172] proposed slope histogram based

algorithm to detect forged signatures. Their results achieved an error rate of 7%, using a database of 500 genuine signatures and 306 forged ones. Furthermore, Krishnan and Jones [91] introduced an algorithm to detect traced forged signatures, using the gradient of the edges of the signature, because the gradients of the genuine signature and that of the traced forged signature are significantly different. They obtained a rejection rate of 85% for the traced forged signatures.

Neural networks have been used in signature segmentation [98], off-line signature verification [7, 141], and online signature verification [25]. Neural networks are trained to verify signatures and their characteristics. The main disadvantage of neural networks is, they require a large number of parameters to ensure that the network does in fact learn.

In [175] a handwritten signature verification system, based on Neural 'Gas' Vector Quantization (VQ) is proposed. The VQ technique employs a neural Gaussian model [158] to verify handwritten signatures. An overall verification rate of 92.0% was obtained.

Blumenstein et. al. [12, 13, 105] proposed a neural network-based technique for cursive character recognition. The proposed technique extracts direction information from the structure of character contours. The extracted direction information is integrated with the transitions between background and foreground pixels in the character image. The proposed technique improved the results achieved by the standard direction feature extraction technique [14, 15], reaching an accuracy rate of 81.58%.

There exist other approaches to off-line signature recognition and verification. A Support Vector Machine (SVM) approach based on the geometrical properties of the signature is proposed by Ozgunduz et. al. [123]. An Enhanced Modified Direction Feature with Single and Multi-classifier approaches are proposed by Armand et. al. [4]. Various classifiers have been successfully used in off-line signature verification, with SVM providing an overall better result than all others such as Hidden Markov Models. SVMs have achieved a true classification ratio of 0.95 [4].

Sabourin [139] designed a complete Automatic Handwritten Signature Verification System (AHSVS) based on directional Probability Density Function (PDF), Fuzzy Extended

Shadow Code, and Fuzzy ARTMAP, which is able to detect all classes of forgeries. The classes of forgeries include skilled, casual and random forgeries. This system integrates signature properties related to the geometric shape and to the effects of the writing dynamics like pressure and speed variations. The results obtained are very promising, but further research work is needed to find a signature representation based on local shape factors, and the intrinsic characteristics of each writer that is the writing dynamics.

Despite research over a long period, biometric approaches to authenticating personal identity have not achieved the degree of success in practical applications originally predicted [57]. Biometrics authentication based on personal handwritten signature has the following significant advantages [57]:

- Handwritten signature is the most traditionally recognized, natural and acceptable form of confirming personal identity.
- Signature is non-invasive and has no undesirable health connotations.
- The use of signature verification minimizes the disruption to accepted practices of personal authentication.

2.3.3 Multi-Modal Biometrics

A considerable number of researches has evidenced that multi-modal biometrics can achieve significant accuracy gains compared to uni-modal biometrics [10, 82, 136, 149], and can increase population coverage, while decreasing vulnerability to spoofing [77]. The key to multi-modal biometrics is the fusion of various biometric modality data at feature extraction, matching score or decision levels [110]. Several multi-modal fusion techniques have been proposed. Brunelli and Falavigna [20] used hyperbolic tangent (tanh) for normalization and weighted geometric average for fusion of voice and face biometric traits. They also proposed a hierarchical combination scheme for a multimodal identification system. Kittler et. al. [89] have conducted experiments with several fusion techniques for face and voice

traits. These fusion techniques include sum, product, minimum, median, and maximum rules. They found out that the sum rule outperformed others because it is not significantly affected by the probability estimation errors.

Bigun et. al. [9] developed a statistical framework based on Bayesian statistics to integrate information presented by the speech (text-dependent) and face data of a user. Hong and Jain [69] proposed an identification system based on face and fingerprint, where fingerprint matching is applied after pruning the database via face matching. Their system consolidates multiple cues by associating different confidence measures with the individual biometric matchers and achieved a significant improvement in retrieval time as well as identification accuracy [69], but they are all based on two physiological biometric modalities only, which can be correlated, unlike bi-modal systems based on physiological and behavioral modalities. Ben-Yacoub et. al. [8] considered several fusion strategies, such as SVM, tree classifiers and multi-layer perceptrons, for face and voice traits. The Bayes classifier is found to be the best method. Ross and Jain [136] combined face, fingerprint and hand geometry biometrics with sum, decision tree and linear discriminant-based methods. The authors report that the sum rule outperforms others. In [149], it is demonstrated that multi-modal fingerprint and face biometric systems can improve accuracy rates, even when using highly accurate Commercial Off-the-Shelf (COTS) systems on relatively large-scale populations. This improvement in accuracy rate is enhanced by an adaptive normalization method, and two fusion techniques: matcher weighting and user weighting.

The Dialog Communication Systems company developed BioID; a multi-modal identification system that uses three different features *(face, voice, and lip movement)* to verify personal identity [60]. The fused modalities of BioID achieved improved accuracy compared with single-feature systems based on either face, or voice or lip movement. In the case of failing to acquire biometric data from one of the modalities, the other two modalities can still lead to an accurate identification. BioID is the first identification system that uses a dynamic feature, *lip movement*. This feature makes BioID more secured against fraud than systems using only static physiological features such as fingerprints. The system acquires, preprocesses, and classifies each biometric feature separately. Then, using a strategy that depends on the level of security required by the application, it combines the classification results into

one result by which it recognizes persons. BioID uses a newly developed, model-based algorithm that matches a binary model of a typical human face to a binarized, edge-extracted version of the video image. The face extractor bases its comparison on the modified Hausdorff distance, which determines the model's optimal location, scaling, and rotation. The preprocessing module uses anthropomorphic knowledge to extract a normalized portion of the face, which scales all faces to a uniform size and crops the images uniformly for easier comparison. This procedure ensures that the appropriate facial features are analyzed. A 3D fast Fourier transformation of the 16 vector is used for training and classification of lip movement. In the training phase, all patterns are orthogonalized and normalized resulting in vectors called adjunct prototypes, which are used to produce a biometric template. The biometric technologies adopted in the BioID are highly correlated and dependent. This jeopardizes the performance of the system. For instance, if the user is angry, the facial expression, voice projection, and the lip motion are somehow affected.

Prabhakar and Jain [127] showed, in the context of a fingerprint verification system, that combining multiple matchers, multiple enrollment templates, and multiple fingers of a user can significantly improve the accuracy of a fingerprint verification system. They also argued that selecting matchers based on some "goodness" statistic may be necessary to avoid performance degradation when combining multiple biometric modalities [46, 165].

Currently, Japan is implementing biometric airport systems to enhance security and speed up passengers through check-in. These systems are based on facial and iris recognition technologies [96]. It is part of an E-Airport initiative announced by the Japanese government in June 2001 and designed to make Japan's international airports the most technologically advanced in the world. The E-Airport initiative is still at its infancy stage. In 2003 the International Civil Aviation Organization adopted a global plan for the implementation of machine-readable passports containing biometric components [56].

Another score-level fusion strategy based on quality measures for multi-modal biometric authentication is presented in [59]. In this method, the fusion is adapted every time an authentication claim is performed based on the estimated quality of the sensed biometric signals at this time. An operational procedure for dealing with degraded data in multi-modal

biometric authentication is presented and evaluated on real data. Experimental results combining written signatures and quality-labeled fingerprints are reported. The proposed scheme which does not consider the quality of the signal, outperforms significantly the fusion approach, but the computational overhead is compromised through the running time of the system.

Multi-Modal Biometric Fusion Techniques

Several multi-modal biometric fusion techniques have been proposed. They include: *simple-sum*, *min-score*, *max-score*, *matcher weighting* and *user weighting* [149]. The *matcher weighting* and *user weighting* methods take into account the performance of individual matchers in weighting their contributions.

Let the quantity n_i^m represents the normalized score for matcher $m, (m = 1, 2, ..., M)$, (where M is the number of matchers) applied to user $i, (i = 1, 2, ..., I)$, (where I is the number of individuals in the database). The fused score for user $i, (i = 1, 2, ..., I)$ is denoted f_i, and defined as follow [28, 149]:

1. **Simple-Sum**:

$$f_i = \sum_{m=1}^{M} n_i^m \tag{2.12}$$

2. **Min-Score**:

$$f_i = \min(n_i^1, n_i^2, ..., n_i^M) \tag{2.13}$$

3. **Max-Score**:

$$f_i = \max(n_i^1, n_i^2, ..., n_i^M) \tag{2.14}$$

4. **Matcher Weighting**: Weights are assigned to the individual matchers based on their Equal Error Rates (EER). The matcher weighting fused score for user i is calculated as:

$$f_i = \sum_{m=1}^{M} w^m n_i^m \tag{2.15}$$

where w^m is the weight associated with matcher m and

$$w^m = \frac{\left(1/\sum_{m=1}^{M} \frac{1}{e^m}\right)}{e^m} \tag{2.16}$$

and e^m is the EER of matcher m, $(m = 1, 2, ..., M)$. The weights for more accurate matchers are higher than those of less accurate matchers.

5. **User Weighting**: This fusion method assigns weights to individual matchers that may be different for different users. The user weighting fused score for user i is calculated as:

$$f_i = \sum_{m=1}^{M} w_i^m n_i^m \tag{2.17}$$

where w_i^m is the weight of matcher m for user i.

$$w_i^m = \frac{1}{\sum_{m=1}^{M} d_i^m}.d_i^m \tag{2.18}$$

and d_i^m is the *d-prime metric* [18], which is a measure of separation of the genuine and impostor distributions for user i and matcher m, (assuming that for every (i, m) pair, the mean and standard deviation of the associated genuine and impostor distributions are known):

$$d_i^m = \frac{\mu_i^m(gen) - \mu_i^m(imp)}{\sqrt{(\sigma_i^m(gen))^2 + (\sigma_i^m(imp))^2}} \tag{2.19}$$

where $\mu_i^m(gen)$ and $\mu_i^m(imp)$ denote the means of the genuine and impostor distributions respectively, and the respective standard deviations are $\sigma_i^m(gen)$ and $\sigma_i^m(imp)$.

2.4 Conclusion

The emergence of biometrics is a promising way to enhance security in verification systems and alleviate limitations of the traditional verification techniques. Biometrics technologies are perceived to bolster security levels in e-commerce at large, and all other public and private sectors. Multi-modal biometrics is a promising model that can improve accuracy rates in authentication systems. For instance, banking systems based on multi-modal biometrics can provide the means to bind the physical presence of an individual user with his cyber action such that intent can firmly be established as the basis for a trusted process.

In this research work, the proposed multi-modal biometrics system is based on both a physiological feature, the *iris* and a behavioral feature, the *signature*. These features are highly uncorrelated and independent, which guarantees a biometrics system with unrestricted degrees of freedom, high accuracy and efficiency. The following chapter investigates hybrid iris recognition techniques.

Chapter 3

Iris Pattern Recognition

3.1 Introduction

Iris recognition is becoming one of the most reliable biometric traits for personal identification. The iris is formed during gestation and the structures of its patterns are stable, invariant and have distinctive features for personal identification. In fact, its texture is very distinctive and does not correlate with genetic determination. The iris is well protected by aqueous humor, and it is almost impossible to modify it surgically without risk [51, 73, 166, 173]. Furthermore, the highest density of biometric degrees-of-freedom which are both stable and distinctive, is found in the iris texture patterns [40].

An efficient algorithm that detects the largest non-occluded rectangular part of the iris as region of interest (ROI) is investigated. Thereafter, a cumulative-sums-based grey change analysis algorithm is applied to the ROI to extract features for recognition. This method can be utilized for iris recognition based on part of the iris since it relaxes the requirement of using the whole iris to compute an iris template. Experiments carried out on a CASIA iris database, show that the approach is promisingly effective and efficient.

Most of the biometric authentication systems store multiple templates per user to account for variations in biometric data. Therefore, these systems suffer from storage space and computational overheads especially when searching for multiple templates of the same individual, and comparing them with the candidate to be authenticated. In order to address these issues, two majority vote-based algorithms are proposed, which calculate a string prototype iris features code as the reliable specimen template.

3.1.1 Motivation

One of the feature extraction techniques researched, cumulative-sums-based analysis, describes the variations in the grey values of iris patterns. In order to extract the real variations in the grey values features, the proper non-occluded ROI has to be detected. Hence, the algorithm thats detects the largest non-occluded rectangular part of the iris as region of interest (ROI) is investigated. Both the feature extraction and ROI detection methods are efficient in terms of computational complexity, since the cumulative sums are basically calculated by addition, and the ROI is detected using the linear accesses along a row in a 2-D array. In this research work, we investigate methods and techniques to improve the performance and security threshold of personal authentication in bi-modal biometrics systems. The time complexity of multi-modal systems is relatively high. Therefore, the investigated algorithms should be optimized.

3.2 Iris Recognition

An iris recognition system is made of two sub-systems: the *iris enrollment sub-system*, which enrolls the iris in the database, and the *iris identification / authentication sub-system*, which compares a newly input iris with the known irides in the database and decides if it is in the database. The iris recognition system architecture is depicted in Figure 3.1.

The basic modules for an iris recognition system include: (*preprocessing*, *feature extraction*, *template creation* and *matching*). These modules are discussed in the following subsections.

3.2.1 Image Preprocessing

An iris input image does not contain only the actual region of interest (ROI), the *iris* part, but also some *noisy* parts like eyelashes, pupil, skin. A change in the camera-to-eye distance results in variations in the size of the same iris [108]. Furthermore, the brightness of the iris

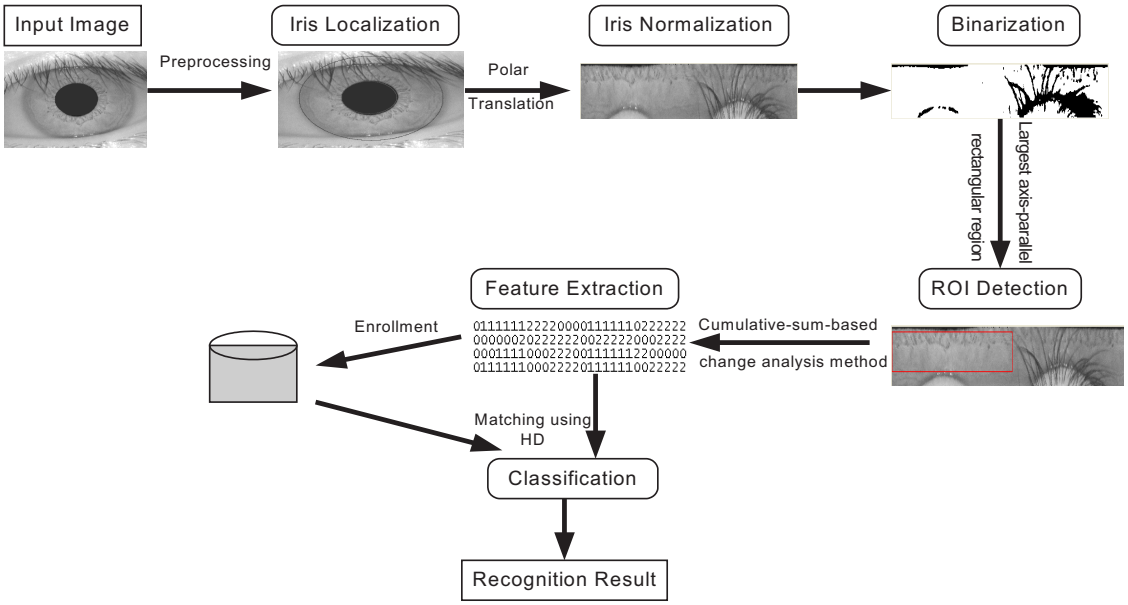


Figure 3.1: Iris recognition system

image is not uniformly distributed because of nonuniform illumination. Therefore, before features that characterize an iris are extracted, the original image needs to be preprocessed to localize the iris, normalize it, and reduce the influence of the noisy factors mentioned above.

3.2.2 Iris Localization

The iris is an annular part between the pupil and the sclera. Both the pupil and the sclera of a typical iris can approximately be taken as circles. However, the two circles are usually not concentric [108]. The inner and outer boundaries of the iris are precisely located using the integro-differential operator of the form [40, 41]:

$$\max_{(r,x_0,y_0)} \left| G_\sigma(r) * \frac{\partial}{\partial r} \oint_{r,x_0,y_0} \frac{I(x,y)}{2\pi r} ds \right| \tag{3.1}$$

where $I(x,y)$ is an image containing an eye. The operator searches over the image domain (x,y) for the maximum in the blurred partial derivative with respect to increasing radius r

of the normalized contour integral of $I(x, y)$ along a circular arc ds of radius r and centre coordinates (x_0, y_0). The symbol $*$ denotes convolution and $G_\sigma(r)$ is a smoothing function such as a Gaussian of scale σ. The complete operator behaves in effect as a circular edge detector, blurred at a scale set by σ, which searches iteratively for a maximum contour integral derivative with increasing radius at successively finer scales of analysis through the three parameter space of center coordinates and radius (x_0, y_0, r) defining a path of contour integration [39, 40]. Figure 3.2 shows the localized iris zone.

An alternative effective algorithm to localize the iris is sequenced as follows [108]:

1. Project the image in the vertical and horizontal direction to approximately estimate the center coordinates (x_p, y_p) of the pupil. Since the pupil is generally darker than its surroundings, the coordinates corresponding to the minima of the two projection profiles are considered as the center coordinates of the pupil.

2. Binarize a region centered at the point (x_p, y_p) by adaptively selecting a reasonable threshold using the gray-level histogram of this region. The centroid of the resulting binary region is considered as a more accurate estimate of the pupil coordinates.

3. Calculate the exact (x_{p0}, y_{p0}) centre and r_p radius of the pupil, and the exact (x_{i0}, y_{i0}) centre and r_i radius of the iris using Canny edge detection and the Hough Transform [63, 124].

3.2.3 Iris Normalization

Daugman solved the normalization problem by projecting the original iris in a Cartesian coordinate system into a doubly dimensionless pseudopolar coordinate system [38]. The iris in the new coordinate system can be represented in a fixed parameter interval. This method normalizes irides of different sizes to the same size by unwrapping anticlockwise the iris ring to a rectangular block with a fixed size. The dimensionless polar system assigns an r and θ value to each coordinate in the iris that will remain invariant to the possible stretching and skewing of the image.

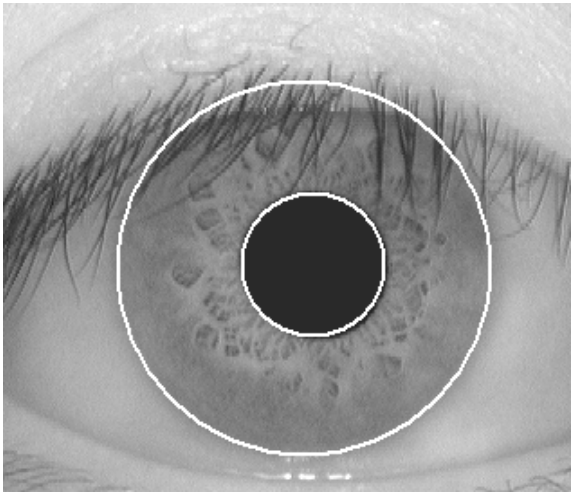


Figure 3.2: Segemented iris part

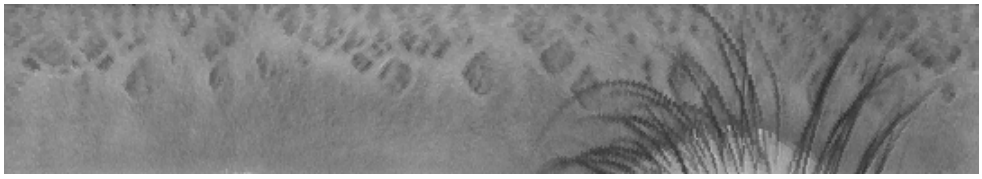


Figure 3.3: Normalized iris region

For the transformation, the r value ranges in $[0, 1]$ and the angular value θ spans the interval $[0, 2\pi]$. The remapping of the iris image, $I(x, y)$, from the raw Cartesian coordinates (x, y) to dimensionless non-concentric polar coordinate system (ρ, θ) is shown in Figure 3.3, and is defined by equations (3.2) to (3.5) [74, 157]:

$$I(x(\rho, \theta), y(\rho, \theta)) \rightarrow I(\rho, \theta) \tag{3.2}$$

which is implemented according to the following formulae

$$\begin{cases} x(\rho, \theta) = (1 - \rho)x_\rho(\theta) + \rho x_i(\theta) \\ y(\rho, \theta) = (1 - \rho)y_\rho(\theta) + \rho y_i(\theta) \end{cases} \tag{3.3}$$

where

$$\begin{cases} x_\rho(\theta) = x_{\rho 0}(\theta) + r_\rho cos(\theta) \\ y_\rho(\theta) = y_{\rho 0}(\theta) + r_\rho sin(\theta) \end{cases} \tag{3.4}$$

and

$$\begin{cases} x_i(\theta) = x_{i0}(\theta) + r_i cos(\theta) \\ y_i(\theta) = y_{i0}(\theta) + r_i sin(\theta) \end{cases} \tag{3.5}$$

The center of the pupil is denoted by $(x_{\rho 0}, y_{\rho 0})$ and (x_{i0}, y_{i0}) is the center of the iris; r_ρ is the radius of the pupil and r_i is the radius of the iris; and (x_ρ, y_ρ) and (x_i, y_i) are the coordinates of points bordering the pupil's radius and iris' radius, respectively.

3.2.4 Feature Extraction

Region of Interest (ROI)

The detection of the ROI, which is the actual iris component, is based on the algorithm which extends Droogenbroeck's algorithm [160] for openings of binary images. The investigated algorithm for the detection of the ROI combines Droogenbroeck's algorithm [160] with binarization and connected components algorithm using 4-connectivity. The extended algorithm extracts the biggest possible region of interest with minimum noise by scanning the binarized normalized-image horizontally and vertically to determine the length and width, respectively, of the largest possible axis-parallel rectangular region of the iris which is not occluded by the eye-lashes, skin, pupil, sclera. Figure 3.5 shows the accurate ROI detected from 6 different images using this algorithm. The algorithm is sequenced as follows:

1. The normalized image, I_{mn} with m rows and n columns is binarized as defined in equation (3.6):

$$B_{mn} = \{B_{ij} : 0 \leq i \leq m-1, 0 \leq j \leq n-1\} \tag{3.6}$$

where B_{ij} is defined as

$$B_{ij} = \begin{cases} 255 & \text{if } x_{ij} > \tau, \\ 0 & \text{otherwise.} \end{cases} \tag{3.7}$$

where τ, is the threshold calculated as follows:

$$\tau = k_1\sigma + k_2\mu \tag{3.8}$$

where σ and μ denote the standard deviation and mean of the original normalized image, I_{mn} respectively, k_1 and k_2 are real numbers chosen between 0 and 2, depending on the resolution quality [134]. In our case, an optimum binarization is achieved when

$k_1 = 0.25$ and $k_2 = 0.25$.

2. An algorithm based on 4-connectivity is applied to find the connected components of B_{mn} as classes of related pixels resulting in C_{mn} which is defined as

$$C_{mn} = \bigcup_{i=0}^{k-1} c_i \tag{3.9}$$

where $c_0, c_1, ..., c_{k-1}$, are k connected components. All tiny background components with total pixels less than a suitable threshold η, are regarded as minor noisy components within the foreground component, hence their labels are set to that of the pixel of the foreground component.

3. The foreground component of the image, C_{mn} is scanned horizontally from right to left resulting in matrix HOR, filled with the distance of each pixel contained in a foreground component to the right border of that foreground component.

4. VER, is the matrix whose elements are calculated by comparing the values in the columns of HOR, that is, $VER[i, j]$ is the length of the vertical segment of HOR in column j and within the neighborhood of i that has all its value greater or equal to $HOR[i, j]$.

5. $HOR[i, j]$, $VER[i, j]$, is the pair of elements representing the segments of an axis-parallel rectangle R_{ij}, defined as

$$R_{ij} = HOR[i, j] * VER[i, j] \tag{3.10}$$

where $HOR[i, j]$ and $VER[i, j]$ denote the length and width of R_{ij}, respectively, and $*$ denotes the multiplication operator. The rectangle R_{ij} with the maximum area is the largest area axis-parallel rectangle LR_{ij}, defined in equation (3.11).

$$LR_{ij} = \max(HOR[i, j] * VER[i, j]) \tag{3.11}$$

6. $LR_{i,j}$, denotes the largest area axis-parallel rectangle with top left coordinates **(i-c , j)**, and bottom right coordinates **(i +** $VER[i,j]$**-(c+1) , j +** $HOR[i,j]$**-1)**, where ***c*** is the total number of neighboring rows to row ***i*** in column ***j*** where $HOR[i,j] \leq HOR[k,j]$, when ***k*** = *[i-1, i-2,...,0].*

The results of the above mentioned algorithm are illustrated in Figure 3.4.

255	255	255	255	255	255	0	0	255
255	255	255	255	255	255	255	0	255
0	255	255	255	255	255	255	255	0
0	255	255	255	255	255	255	255	0
255	255	0	255	255	255	255	255	0
0	255	255	0	255	255	255	255	255
255	255	255	0	0	255	255	255	255

(a) Original Image

6	5	4	3	2	1	0	0	1
7	6	5	4	3	2	1	0	1
0	7	6	5	4	3	2	1	0
0	7	6	5	4	3	2	1	0
2	1	0	5	4	3	2	1	0
0	2	1	0	5	4	3	2	1
3	2	1	0	0	4	3	2	1

(b) HOR

2	4	4	5	6	7	0	0	2
1	3	3	4	5	6	6	0	2
0	2	2	3	4	5	5	5	0
0	2	2	3	4	5	5	5	0
1	7	0	3	4	5	5	5	0
0	6	2	0	1	2	2	2	2
1	6	2	0	0	2	2	2	2

(c) VER

12	20	16	15	12	7	0	0	2
7	18	15	16	15	12	6	0	2
0	14	12	15	16	15	10	5	0
0	14	12	15	16	15	10	5	0
2	7	0	15	16	15	10	5	0
0	12	2	0	5	8	6	4	2
3	12	2	0	0	8	6	4	2

(d) HOR*VER

Figure 3.4: (a) Original Binary Image, (b) HOR matrix, (c) VER Matrix, (d) HOR $*$ VER.

3.2.5 Feature Extraction using Cumulative-Sums

A cumulative-sums-based [90, 154] analysis method is used to extract features from the extracted rectangular region of interest. The contrast of the extracted region of interest is improved by a histogram stretching method, which results in a well-distributed image. The different sized regions of interest shown in Figure 3.5 are resized by averaging pixel values to $N(row) \times M(col)$ pixels size. The extraction of features is sequenced as follows [90]:

1. Divide the normalized iris image into basic cell regions for calculating cumulative sums.

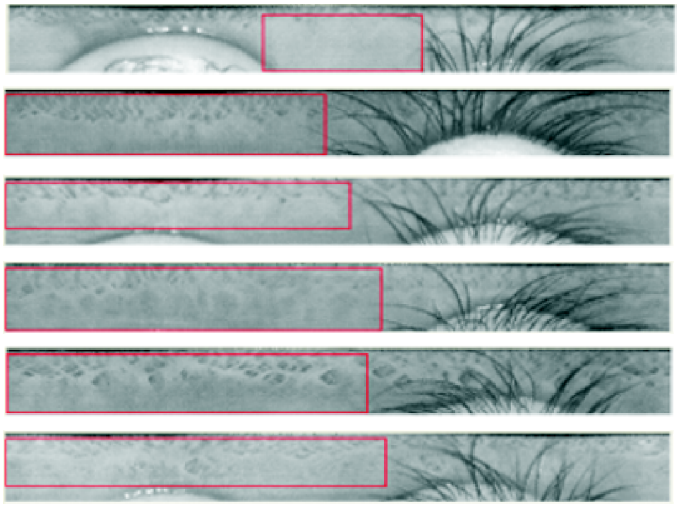


Figure 3.5: Detected regions of interest.

For instance, one cell region has 3(row) × 10(col) pixels size, (N = 3 and M = 10). An average or median grey value is used as a representative value of a basic cell region.

2. Basic cell regions are grouped horizontally and vertically as shown in Figure 3.6. Empirical experiments are conducted to determine the optimum way of grouping the cells. In our case, 3 cells are grouped horizontally, and 5 cells are grouped vertically.

3. Calculate cumulative-sums over each group as defined in equations (3.12) and (3.13).

4. Generate iris feature codes as shown in Figure 3.7.

The cumulative sums in *step 3* are computed following a sequence of steps. Suppose that $X_1, X_2, ..., X_n$ are n representative values of each cell region within a group, such that,

$$\overline{X} = \frac{1}{n}\sum_{i=1}^{n} X_i \tag{3.12}$$

where $\overline{X}$ is the mean grey value of each cell group.

$$S_i = S_{i-1} + (X_i - \overline{X})\ for\ i = 1, 2, ..., n. \tag{3.13}$$

where S_i is the cumulative sums over each group, with a constraint $S_0 = 0$.

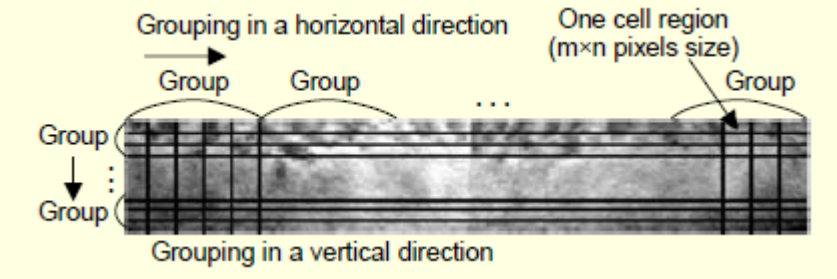


Figure 3.6: Grouping image cell regions horizontally and vertically [90].

Feature Coding - Cumulative-Sums

The iris codes are generated horizontally and vertically for each cell region by analyzing the cumulative-sums, (equation (3.13)), which describe the variations in the grey values of iris patterns. **Algorithm 1** shows how the iris codes are generated vertically. An upward slope of cumulative-sums (Figure 3.7(a)) means that the iris pattern changes from darkness to brightness, while a downward slope (Figure 3.7(b)) means the opposite. Figure 3.7 shows examples of iris codes generation. For instance, in (Figure 3.7(b)), the cumulative-sums change from maximum to minimum, which means that the variations in the grey values of iris patterns change from brightness to darkness. Therefore, the cumulative-sums values within the interval of the positions of the minimum and maximum , *[pos(MIN), pos(MAX)]*, are coded 2, and all other values outside the interval are coded 0.

This cumulative-sums-based feature extraction method is efficient in terms of computational complexity, since the cumulative sums are basically calculated by addition. Hence, it

(a) Upward slope

(b) Downward slope

Figure 3.7: Example of the iris code generation, (a)Darkness to brightness, (b)Brightness to darkness [90].

Algorithm 1 Iris code generation - vertically.

for {*vertical direction*} **do**
  $MAX \leftarrow \max(S_1, S_2, ..., S_n)$
  $MIN \leftarrow \min(S_1, S_2, ..., S_n)$
  if $MIN \geq S_i$ & $S_i \leq MAX$ **then**
    if S_i is upward slope **then**
      $IrisCode \leftarrow 1$
    end if
    if S_i is downward slope **then**
      $IrisCode \leftarrow 2$
    end if
  else
    $IrisCode \leftarrow 0$
  end if
end for

is appropriate to be implemented in multi-modal systems, where computational complexity is mainly a drawback.

Template Creation

After extracting iris features from various instances of the same iris taken in different contexts such as light intensity and distance, a prototype code or a representative iris feature code is calculated using the majority vote strategy. The extracted features are in the string format. An example of these iris features extracted in the string format is shown in Figure 3.8.

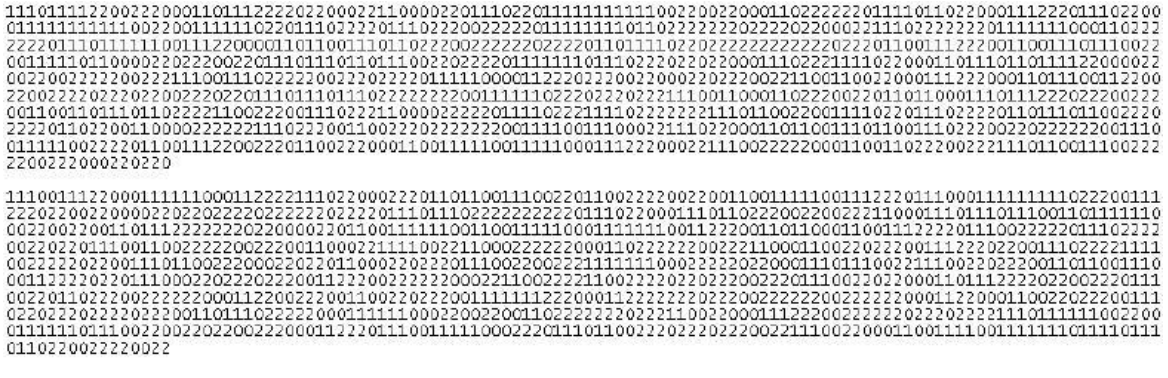


Figure 3.8: Example of the extracted iris feature codes in the string format

Let $S = \{0, 1, 2\}$ represents the gradient direction of the grey level, i.e. 1 is upward slope, 2 is downward slope, as shown in Figure 3.7(a) and 3.7(b), respectively, and 0 no slope. Each iris instance is represented by a string feature code $s = s_1, s_2, ..., s_l$, where $s_i \in S$ and $i = 1, ..., l$, which describes the variations in the grey values of that iris instance extracted using cumulative-sums as explained in [160]. From r samples of irides of the same eye, we calculate the prototype code for the class of the given iris using the majority vote strategy. Let s^i represents the i^{th} instance of a particular iris such that $s^i = s^i_1 s^i_2 ... s^i_l$, where s^i_j represents the j^{th} character of the i^{th} instance of an iris. The function P_k, which is the projection on the k^{th} character of each string feature code of r samples is defined as

$$P_k : \underbrace{S^l \times S^l \times ... \times S^l}_{r \ times} \longrightarrow \underbrace{S \times S \times ... \times S}_{r \ times} \tag{3.14}$$

such that for all $\alpha = (s^1, s^2, ..., s^r) \in S^l \times S^l \times ... \times S^l$

$$P_k(\alpha) = (s^1_k, s^2_k, ..., s^r_k) \tag{3.15}$$

Let $\omega = (a_1, a_2, ..., a_r)$ be the element of $S \times S \times ... \times S$. We define $f_a(\omega)$ as the frequency of a in the tuple $(a_1, a_2, ..., a_r)$. We can define a function, φ, in two different ways as either

$$\varphi(\omega) = \begin{cases} \underset{a \in \{0,1,2\}}{\operatorname{argmax}} f_a(\omega) & \text{if } \forall \underset{b \neq a}{b} \in S, f_a(\omega) > f_b(\omega), \\ 0 & \text{otherwise.} \end{cases} \tag{3.16}$$

or

$$\varphi(\omega) = \begin{cases} \underset{a \in \{0,1,2\}}{\operatorname{argmax}} f_a(\omega) & \text{if } \forall \underset{b \neq a}{b} \in S, f_a(\omega) > f_b(\omega), \\ \# & \text{otherwise.} \end{cases} \tag{3.17}$$

where equation (3.16) computes the majority vote and adopts no variations in the grey values of iris patterns as code 0, $(0 \in S)$, when there is no majority vote, and equation (3.17) computes the majority vote and adopts undefined variations in the grey values of iris patterns as symbol # when there is no majority vote.

The function ψ, that calculates the prototype code of the iris is defined as

$$\psi : \underbrace{S^l \times S^l \times ... \times S^l}_{r\ times} \longrightarrow S^l \tag{3.18}$$

such that for all $\beta \in \underbrace{S^l \times S^l \times ... \times S^l}_{r\ times}$

$$\psi(\beta) = q \tag{3.19}$$

where $q = q_1...q_k...q_l$, $(1 \leq k \leq l)$, with $q_k = \varphi(P_k(\beta))$. Then q represents the prototype code of the given iris. Figure 3.9 shows an example of an iris prototype code of an individual, where code 0 is adopted when there is no majority vote in the five iris feature codes. In this case, code 0, $(0 \in S)$, shows that there are no variations in the grey values of iris patterns neither from darkness to brightness nor brightness to darkness. Figure 3.10 shows an example of an iris prototype code of an individual, where the symbol # is adopted when there is no majority vote in the five feature codes. The symbol # denotes that there are either variations in the grey values of the iris patterns.

3.2.6 Feature Extraction using Gabor Filters

An alternative method for texture feature extraction, the multichannel filtering approach using Gabor Filters, is investigated in this research work. This texture feature extraction technique is implemented on a non-occluded iris region of interest. Moreover, Gabor filters are chosen as a comparative tool for the validation of the hybrid feature extraction technique;

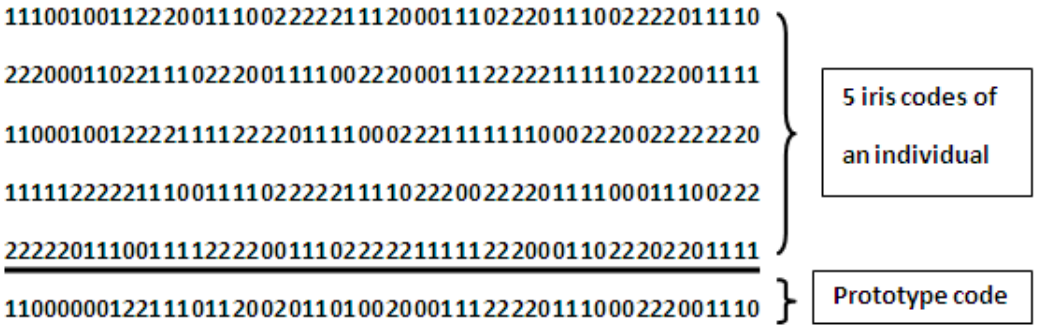


Figure 3.9: Example of the iris prototype code of an individual (with code **0** when there is no majority vote)

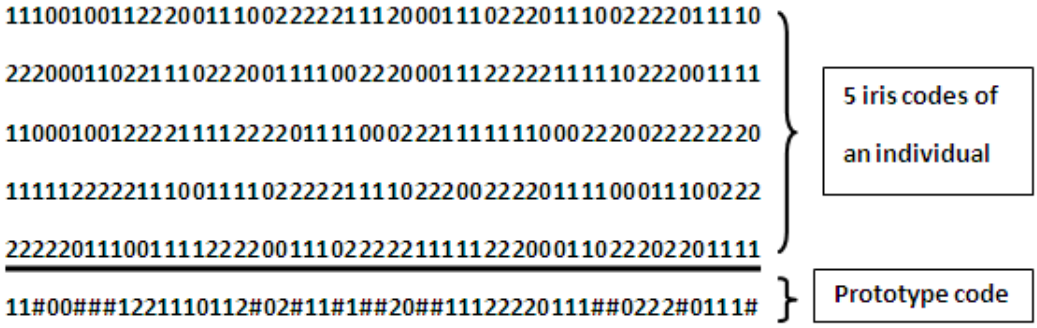


Figure 3.10: Example of the iris prototype code of an individual (with undefined code # when there is no majority vote)

the cumulative-sums. Gabor filters have proved to provide good performance in rotation-invariant texture classification. The multichannel filtering approach uses a multiresolution system to extract information that describes different characteristics of an image. These characteristics provide a description of image texture [119, 122, 125]. The visual cortex of a human has various cells that have spatial frequency and orientation selectivity when processing image signals. These cells can be viewed as mechanisms and detectors tuned to particular frequencies and orientations. Each detector is a single channel for signal processing. A set of such mechanisms tuned to a number of different frequencies and orientations constitutes a multichannel filtering system that models the human visual system [5].

The Gabor function can be implemented as a multichannel filter that mimics the human visual system. Two important aspects must be considered before designing a bank of Gabor

Filters. Firstly, the functional form of the set of filters must be specified, and the parameters must be carefully selected so that the filter is tuned to detect the different features and structures present in the image. Secondly, the filter outputs must undergo feature extraction in order to improve the feature set.

In the spatial domain, the Gabor function is a Gaussian modulated sinusoid. The complex Gabor Filter impulse response is

$$h(x,y) = \frac{1}{2\pi\sigma_x\sigma_y} \exp\left\{\frac{1}{2}\left(\frac{x^2}{\sigma_x^2} + \frac{y^2}{\sigma_y^2}\right)\right\} \exp\left(\frac{j2\pi x}{\lambda}\right) \tag{3.20}$$

where

$$j = \sqrt{-1}$$

In the spatial-frequency domain, its representation is

$$H(u,v) = \exp\left\{-2\pi^2\left[\left(u - \frac{1}{\lambda}\right)^2 \sigma_x^2 + v^2\sigma_y^2\right]\right\} \tag{3.21}$$

The frequency of the sinusoids is $\frac{1}{\lambda}$. The spread of the Gaussian in the x and y directions is controlled by σ_x and σ_y, respectively. The frequency bandwidth of the filter is represented by B_f and the angular bandwidth by B_θ. The x and y coordinates can be rotated spatially by a value θ to produce a filter for different orientations

$$x' = x\cos\theta + y\sin\theta \tag{3.22}$$

$$y' = -x\sin\theta + y\cos\theta \tag{3.23}$$

and substituting x' for x and y' for y. By variation of θ in equations (3.22) and (3.23), the filter can be tuned for orientation selectivity. σ_x can be computed by setting the frequency cutoff to -6db and σ_y by setting the cutoff in the angular direction to -6db as suggested in the literature [5, 34]:

$$\sigma_x = \frac{\sqrt{\ln 2}\left(2^{B_f}+1\right)}{\frac{\sqrt{2}\pi}{\lambda}\left(2^{B_f}-1\right)} \tag{3.24}$$

$$\sigma_y = \frac{\sqrt{\ln 2}}{\frac{\sqrt{2}\pi}{\lambda}\tan\left(\frac{B_\theta}{2}\right)} \tag{3.25}$$

Generally, B_f and B_θ are selected to match psycho-visual data.

A common technique is to use the real component of the complex Gabor function for filtering:

$$g(x,y) = \frac{1}{2\pi\sigma_x\sigma_y}\exp\left\{-\frac{1}{2}\left(\frac{x^2}{\sigma_x^2}+\frac{y^2}{\sigma_y^2}\right)\right\}\cos\left(\frac{2\pi x}{\lambda}\right) \tag{3.26}$$

This function has two symmetrically located Gaussians in the spatial frequency domain. The spatial-frequency representation is

$$\begin{aligned} G(u,v) = &\exp\left\{-2\pi^2\left[\left(u-\frac{1}{\lambda}\right)^2\sigma_x^2+v^2\sigma_y^2\right]\right\} \\ &+\exp\left\{-2\pi^2\left[\left(u+\frac{1}{\lambda}\right)^2\sigma_x^2+v^2\sigma_y^2\right]\right\} \end{aligned} \tag{3.27}$$

Gabor filters are also implemented in the following form [81, 93]

$$r(x,y) = \exp\left\{-\frac{1}{2}\left(\frac{x^2}{\sigma_x^2} + \frac{y^2}{\sigma_y^2}\right)\right\}\cos\left(\frac{2\pi x}{\lambda} + \phi\right) \tag{3.28}$$

where ϕ is the phase offset. If $\phi \in \{0, \pi\}$, the filter is symmetric; if $\phi \in \{\frac{\pi}{2}, -\frac{\pi}{2}\}$, the filter is antisymmetric. The parameters for the function are the same as discussed above.

Let $G(x,y)$ be a Gabor function, with form analogous to any of those discussed above. The response of $G(x,y)$ to a continuous input image $f(x,y)$ is computed by evaluating

$$R = G(x,y) * f(x,y) \tag{3.29}$$

$$= \iint_{\Omega} G(x,y) f(x,y)\, dx\, dy \tag{3.30}$$

where R is the filter output and Ω the image domain. The operator $*$ denotes convolution. For discrete image with M rows and N columns, the integral is evaluated using

$$R = \sum_{i=0}^{N-1}\sum_{j=0}^{M-1} G(i,j) f(i,j) \tag{3.31}$$

where G and f are discretized functions. The Gabor Filter response R undergoes further processing for feature extraction.

Gabor Filters must be tuned to detect the features in an image. For this purpose, parameters must be carefully selected for filter design. Methods for Gabor Filter selection and parameter estimation may be supervised or unsupervised [5]. Empirical information based on the analysis of the power spectrum of individual textures is also used [19]. Filter locations are determined by significant peaks and dominant directions in the frequency domain for oriented textures. The lower fundamental frequencies discriminate periodic textures. If the texture is non-oriented, the center frequencies of the two largest maxima are suggested. This approach is unreliable since images will contain different peaks in the power spectrum. Dunn

and Higgins [53] selected optimal filter parameters based on known sets of textures. They identify boundaries between two textures using a single filter. The filter is selected using an exhaustive search to find the center frequency and then applied to an image to partition it. This is not effective since a single filter will not be able to identify variations of the known sample textures. The most common approach for parameter estimation is the automated approach of filter banks [22, 78, 116]. Parameters are specified *ad hoc* and the filters are created so that they provide a reasonable coverage of the spatial-frequency domain. This avoids computing texture dependent parameters.

An important aspect of Gabor filtering is the post processing of filter outputs for feature extraction. A number of methods are mentioned in this regard in the literature [5, 92, 150], and these include

1. **Magnitude Response**: The simplest feature extraction method is to analyze the magnitude response of a set of filters [19]. Filters matching a particular texture will have large magnitudes. Their outputs are negligible when they do not match the texture.

2. **Spatial Smoothing**: Outputs from a Gabor Filter are generally sensitive to the noise in an image. Bovik et. al. [19] applied spatial smoothing to the filter output using a Gaussian with a spatial extent greater than that of the filter. If the Gaussian of the filter is $\chi(x, y)$, then the smoothing function is $\chi(\gamma x, \gamma y)$ with $\frac{2}{3}$ recommended for γ. Clausi [34] showed experimentally that spatial smoothing improves the performance of the filter for feature extraction.

3. **Real Component**: The real component $g(x, y)$, is implemented as an even-symmetric bank of filters in [78, 81]. This reduces the computational burden and their experiments achieved promising results.

4. **Sigmoidal Thresholding Function**: Jain et. al. [78, 81] subjected the filter outputs to a nonlinear transformation:

$$\varphi(R) = \tanh(\alpha R) = \frac{1 - e^{-2\alpha R}}{1 + e^{-2\alpha R}} \tag{3.32}$$

with an empirical value of 0.25 for α. This function changes the sinusoidal variations in the filtered image into square variations. Effectively, it behaves as a blob detector.

5. **Gabor Energy**: The outputs of two real Gabor Filters that differ in phase can be combined to yield a measure called the Gabor Energy (E) [93]. Specifically, one filter is symmetric and the other antisymmetric:

$$E = \sqrt{R_{even}^2 + R_{odd}^2} \tag{3.33}$$

The filtering and post processing produce feature images and the data in these images can be used directly as features for texture discrimination. In addition, each feature image F_k can be processed further for feature extraction. The following features can be derived for a point in F_k centered within a square window of width W

1. **Statistical Measures**: Statistical measures can be derived from the feature images. They include the mean $\overline{x}$, standard deviation s, variance s^2 and average absolute deviation (AAD)

$$\overline{x} = \frac{1}{N} \sum_{x,y \in W} F_k(x,y) \tag{3.34}$$

$$|\overline{x}| = \frac{1}{N} \sum_{x,y \in W} |F_k(x,y)| \tag{3.35}$$

$$s^2 = \frac{1}{N-1} \sum_{x,y \in W} [F_k(x,y) - \overline{x}]^2 \tag{3.36}$$

$$s = \sqrt{s^2} \tag{3.37}$$

$$AAD = \frac{1}{N} \sum_{x,y \in W} |F_k(x,y) - \overline{x}| \tag{3.38}$$

2. **Energy Measure**: In addition to deriving statistical features, we can compute a measure that is indicative of energy (E) in the variations of the Gabor responses

$$E = \frac{1}{N} \sum_{x,y \in W} [F_k(x,y)]^2 \tag{3.39}$$

where N is the number of points in the region W.

3.2.7 Iris Matching

The key to iris recognition is the failure of a test of statistical independence, which involves so many degrees-of-freedom that this test is virtually guaranteed to be passed whenever the

phase codes for two different eyes are compared, but to be uniquely failed when any eye's phase code is compared with another version of itself [41].

The test of statistical independence is implemented by the Boolean Exclusive-OR operator (XOR) applied to the phase vectors that encode any two iris patterns, masked by both of their corresponding mask bit vectors to prevent noniris artifacts from influencing iris comparisons. The XOR operator $\otimes$ detects disagreement between any corresponding pair of bits, while the AND operator $\cap$ ensures that the compared bits are both deemed to have been uncorrupted by eyelashes, eyelids, specular reflections, or other noise. The norms ($\| \ \|$) of the resultant bit vector and of the masked vectors are then measured in order to compute a fractional Hamming Distance (HD) as the measure of the dissimilarity between any two irides, whose two phase code bit vectors are denoted $\{codeA, codeB\}$ and whose mask bit vectors are denoted $\{maskA, maskB\}$ [41]. For the Gabor filters vectors, the HD is calculated using equation (3.40).

$$\mathbf{HD} = \frac{\|(codeA \otimes codeB) \cap maskA \cap maskB\|}{\|maskA \cap maskB\|} \tag{3.40}$$

For the cumulative-sums string iris codes, the HD is calculated using equation (3.41) [38, 90]. The smaller the HD is, the higher the similarity of the compared iris codes.

$$\mathbf{HD} = \frac{1}{2N}[(\sum_{i=1}^{N} A_h(i) \oplus B_h(i)) + (\sum_{i=1}^{N} A_v(i) \oplus B_v(i))] \tag{3.41}$$

where $A_h(i)$ and $A_v(i)$ denote the enrolled iris code over horizontal and vertical directions, respectively, $B_h(i)$ and $B_v(i)$ denote the new input iris code over the horizontal and vertical directions, respectively. N is the total number of cells, and $\oplus$ is the XOR operator.

3.2.8 The *DU* Measure

The *DU* measure is an alternative matching algorithm to verify the similarity between iris features. In fact, the *DU* measure is a hyper-spectral discrimination measure, which combines the Spectral Information Divergence (SID) and the Spectral Angle Mapper (SAM) into a mixed measure, hence it is referred to as the SID-SAM mixed measure [50]. The Spectral Angle Mapper (SAM) [24, 50, 52, 147] has been widely used as a spectral similarity measure for multi/hyper-spectral signals. The SAM measures the angle between the spectral vectors $\mathbf{r} = (r_1, r_2, ..., r_L)^T$ and $\mathbf{s} = (s_1, s_2, ..., s_L)^T$ and is given by:

$$SAM(\mathbf{r}, \mathbf{s}) = cos^{-1}\left(\frac{\langle \mathbf{r}, \mathbf{s} \rangle}{\|\mathbf{r}\| \times \|\mathbf{s}\|}\right) \tag{3.42}$$

where $\langle \mathbf{r}, \mathbf{s} \rangle$ is the inner product of vectors $\mathbf{r}$ and $\mathbf{s}$,

$$\langle \mathbf{r}, \mathbf{s} \rangle = \sum_{l=1}^{L} r_l s_l \tag{3.43}$$

and $\|*\|$ is the vector norm such that

$$\|\mathbf{r}\| = \sqrt{\langle \mathbf{r}, \mathbf{r} \rangle} \tag{3.44}$$

and

$$\|\mathbf{s}\| = \sqrt{\langle \mathbf{s}, \mathbf{s} \rangle} \tag{3.45}$$

Let $\mathbf{p} = (p_1, p_2, ..., p_L)^T$ and $q = (q_1, q_2, ..., q_L)^T$ be the two probability mass functions generated by vectors $\mathbf{r}$ and $\mathbf{s}$. The Spectral Information Divergence (SID) [24, 50, 52] between vectors $\mathbf{r}$ and $\mathbf{s}$ is defined as

$$SID(\mathbf{r}, \mathbf{s}) = D(\mathbf{p} \| \mathbf{q}) + D(\mathbf{q} \| \mathbf{p}) \tag{3.46}$$

where $D(\mathbf{p}\|\mathbf{q})$ is the relative entropy (also known as Kullback-Leibler information measure) of $\mathbf{q}$ with respect to $\mathbf{p}$, is defined as

$$D(\mathbf{p}\|\mathbf{q}) = \sum_{j=1}^{L} p_j \log(p_j/q_j) \tag{3.47}$$

and $D(\mathbf{p}\|\mathbf{q})$ is the relative entropy of $\mathbf{p}$ with respect to $\mathbf{q}$, where

$$D(\mathbf{q}\|\mathbf{p}) = \sum_{j=1}^{L} q_j \log(q_j/p_j) \tag{3.48}$$

Du et. al. [50, 52] developed the DU measure, also known as (SID,SAM)-mixed measure. This measure takes advantage of the strengths of both SID and SAM to measure the similarity between two iris signatures. It is defined as

$$DU(\mathbf{r},\mathbf{s}) = \frac{1}{N} \times \|r-s\|_1 \times [D(\mathbf{q}\|\mathbf{p}) + D(\mathbf{p}\|\mathbf{q})] \times \tan\left[cos^{-1}\left(\frac{\langle \mathbf{r},\mathbf{s}\rangle}{\|\mathbf{r}\| \times \|\mathbf{s}\|}\right)\right] \tag{3.49}$$

where N is the total number of nonzero pairs of r_i and s_i, and $\|r-s\|_1$ in the 1-norm.

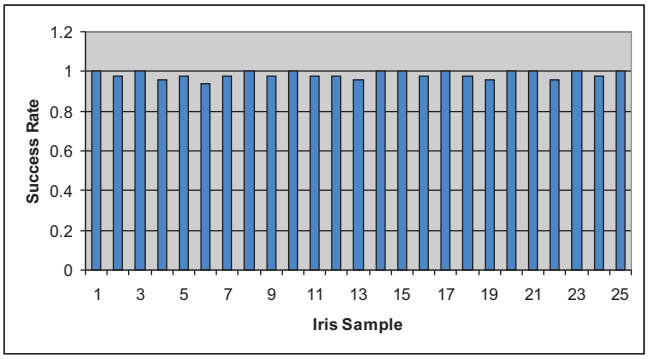


Figure 3.11: True positive rate from a sample of 25 people with 7 instances each, (CASIA).

3.3 Discussion of Results

The performance of an iris-based biometrics system which implements cumulative-sums feature extraction technique, is evaluated by analyzing its false acceptance rate (FAR) and false rejection rate (FRR) calculated at various thresholds. These two factors are computed by generating all possible genuine and impostor matching scores and then setting a threshold for deciding whether to accept or reject a match. The receiver operating characteristic (ROC) curve is used to plot the FRR or the genuine acceptance rate (GAR) against the FAR at different thresholds.

The test iris images used in the experiments were obtained from the CASIA iris database [23] with data from 108 people. Seven iris images of the same individual were obtained from a set of 108 individuals. Firstly, the ROI detection algorithm which extracts the largest possible axis-parallel rectangular iris region from the images tested, was applied to all 7 irides of the 108 individuals. Figure 3.5 shows how the algorithm detected accurately the ROI from 6 different iris images. The ROI with more than 80% of the valid iris patterns hidden mainly by eyelids and eyelashes, is rejected.

Secondly, the cumulative-sums technique is used to extract iris features from the detected region of interest without occlusions from obstacles like eyelashes, skin, pupil or sclera. Thus, non-iris pattern areas are completely discarded. On the other hand, the cumulative-sums algorithm is used to extract iris features from the whole iris images without excluding any occlusions from eyelashes, skin, pupil or sclera. Figure 3.12 shows that the cumulative-sums algorithm performs better when applied to non-occluded iris regions of interest than when applied to ROI with occlusions. The variations in the grey values of iris patterns are well defined in non-occluded ROI, hence, the cumulative-sums technique achieved a high recognition performance rate of 98.4%. Furthermore, Figure 3.11 shows the true positive rate of the cumulative-sums-based change analysis approach from a random sample of 25 individuals with 7 irides per individual. In conclusion, cumulative-sums algorithm is an efficiently effective technique in iris recognition, especially when performed on a non-occluded region of interest.

Thirdly, the two proposed algorithms for creating the specimen iris templates, defined in subsection 3.2.5, are used to create 2 prototype feature codes per individual. The first template is computed by applying the majority vote technique and adopting no variation in the grey values of iris patterns, when there is no majority vote, as defined in equation (3.16). The second prototype feature code is computed by applying the majority vote technique and adopting undefined variation in the grey values of iris patterns, when there is no majority vote, as defined in equation (3.17). The majority vote technique which adopts an undefined variation in the grey values of iris patterns, when there is no majority vote, slightly outperformed the other technique which adopts no variation in the grey values of iris patterns, when there is no majority vote, as shown in Figure 3.13. Furthermore, Figure 3.15 shows that a prototype feature code calculated from five instances of the same iris of an individual has an optimum true positive rate of 99.6%. Therefore, the performance rate of an iris recognition system based on the cumulative-sums is improved to 99.6% when the specimen iris template is created using the majority vote technique which adopts an undefined variation in the grey values of iris patterns, when there is no majority vote.

Lastly, further comparisons of the cumulative-sums-based change analysis approach, with the results of other iris feature extraction techniques in the literature, is shown in Table 3.1. The cumulative-sums achieved a recognition rate of 99.6%, while Gabor filters achieved an improved success rate of 99.8%, when both techniques employs the non-occluded ROI. The non-occluded iris ROI has proved that it can bolster the recognition rate of iris-based systems. Finally, iris matching algorithms: the Hamming Distance and the *DU* Measure, are compared in Figure 3.14, and there is no significant difference.

Table 3.1: Comparative table of recognition rate.

Methods	**Recognition rate (%)**
J.G. Daugman [38]	99.37
J-G. Ko [90]	98.21
Y. Wang [169]	97.25
Li Ma [108]	94.33
W.W. Boles [16]	92.61
Cumulative-sums	**99.6**
Gabor Filters	**99.8**

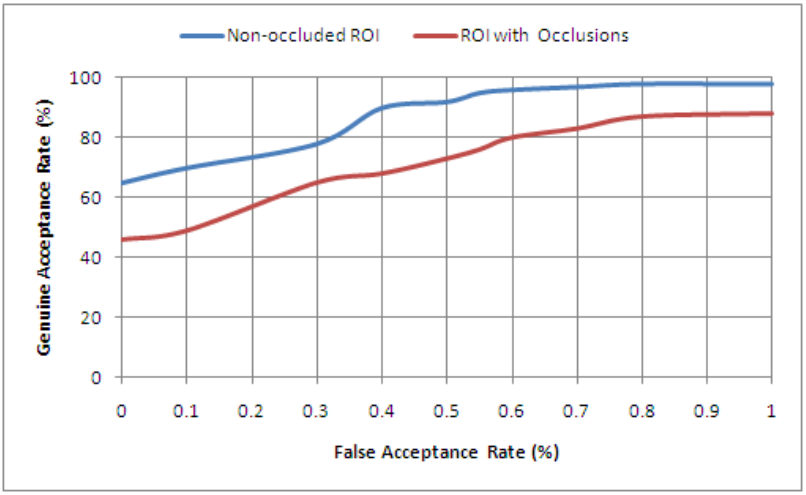


Figure 3.12: ROC curves: cumulative-sums applied on non-occluded ROI ***versus*** cumulative-sums applied on ROI with occlusions.

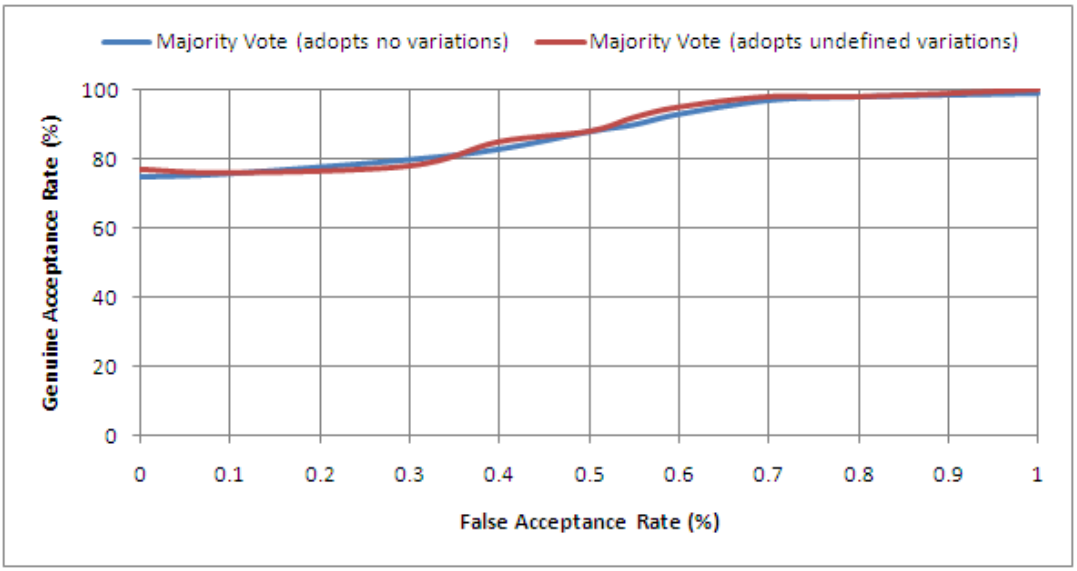


Figure 3.13: ROC curves: majority vote algorithm (adopts no variation in case of no majority vote) ***versus*** majority vote algorithm (adopts an undefined variation in case of no majority vote) cumulative-sums applied on ROI with occlusions.

3.4 Conclusion

An efficient approach of detecting the region of interest on a normalized iris image was presented. The algorithm extracts the largest axis-parallel rectangular region of the normalized

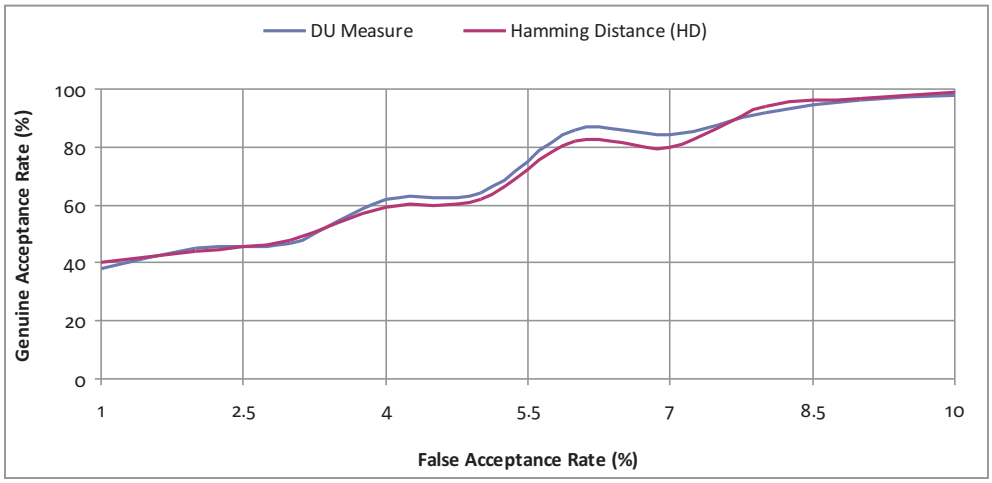


Figure 3.14: ROC curves: DU measure ***versus*** Hamming distance.

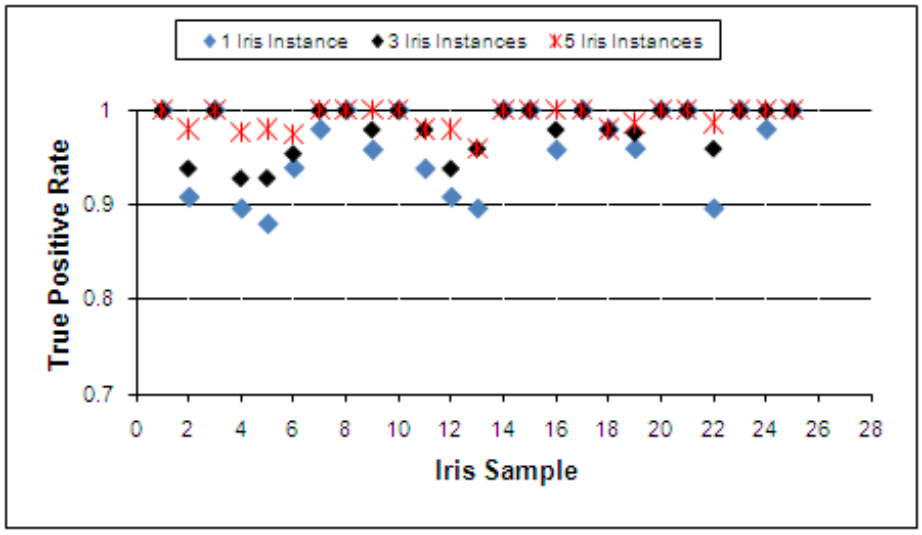


Figure 3.15: True positive rate from a sample of 25 people with a specimen template with 1 instance, 3 instances, and 5 instances each iris, (CASIA). (with an undefined variation)

iris image without occlusions from the eyelashes, pupil, sclera, or skin. The iris features codes are extracted from the detected region of interest using a cumulative-sums-based change analysis method. Then, two novel techniques based on majority vote are implemented to create specimen iris templates. Experimental results show that the proposed approach has a good success rate of 99.6%. Using the same ROI, Gabor filters achieved a high true positive rate of 99.8%. The following chapter explores the performance of signature verification based on handwritten text recognition.

Chapter 4

Signature Verification Based on Handwritten Text Recognition

4.1 Introduction

Signature verification has received extensive research attention in recent years. Signatures are widely used as the primary method for the identification and verification of human identity, and for authentication and authorization in legal transaction. In fact, signature is the most widely accepted biometric trait used for enforcing binding contracts in paper based documents for centuries [145]. Handwriting recognition has reached its maturity level; especially for the recognition of isolated characters, hand printed word recognition, and automatic address processing. Signatures are composed of special unconstrained cursive characters and symbols. In most cases they are superimposed and embellished, and as a result can be difficult to read.

The intrapersonal variations and interpersonal differences in signing make it necessary to analyze signatures absolutely as images instead of applying character and word recognition [123]. The other challenge of signature verification is that a signature is termed a behavioral biometric trait so it may change depending on behavioral characteristics such as mood and fatigue [4]. Hence innovative and accurate approaches need to be employed to improve the recognition and verification rates. For instance, when there are multiple known samples for a writer, it is more intuitive to use all of that information to learn the style of writing of that person in order to be able to classify a given questioned handwriting sample as belonging to the writer or not [152].

4.1.1 Motivation

Although artificial neural networks especially Multilayer Perceptrons (MLPs), have shown good results in character recognition, their performance is strongly affected by the quality of the representation of the characters. A large number of parameters are required to represent the character, which makes it difficulty to establish the rules for recognition. In fact, the MLPs become difficult to train, and as a result, the bigger the size of the network, the higher the computation time. Moreover, this can greatly restrict the practical use of neural networks especially in multi-modal systems, where various biometric modalities are trained independently.

Furthermore, signatures are composed of special unconstrained cursive symbols which are not necessarily alphabetical characters, and which are in most cases superimposed and embellished. This makes it difficult to apply alphabetical character recognition to all signatures. One of the main challenges poised by cursive alphabetical character recognition is the ambiguity and illegibility of the characters.

4.2 Signature Recognition

The basic modules for a signature recognition system investigated in this thesis include: *signature capturing, preprocessing*, *feature extraction, feature vector extraction*, and *classification*. These modules are depicted in Figure 4.1, and discussed in subsequent subsections.

4.2.1 Preprocessing

The preprocessing module is applied to both training and testing phases. It includes binarization, noise reduction, elimination of background [124] and skeletonization. A median filtering [63] noise reduction technique is used. There are several thinning algorithms [30, 99, 167, 174] in the literature, and among them, Hilditch's thinning algorithm based on a 3×3 mask size

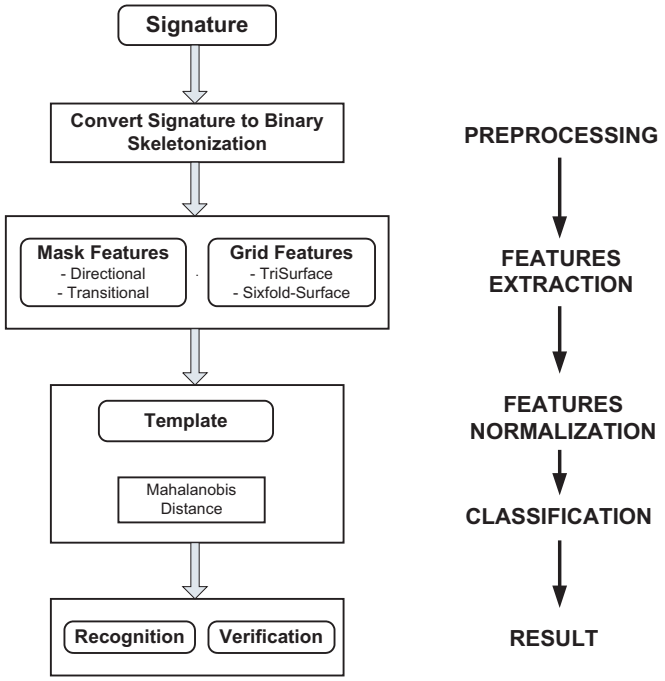


Figure 4.1: Signature recognition system

is adopted as the skeletonization technique in this research work. Hilditch's thinning algorithm guarantees that only a single layer of contour pixels is deleted in each iteration from the binary image, thereby resulting in a more precise skeleton without anomalies at the corners. The 8-neighborhood of the pixel P_0 is made up of the elements of $N_8 = \{P_1, P_2, ..., P_8\}$ represented as

P_4	P_3	P_2
P_5	P_0	P_1
P_6	P_7	P_8

Figure 4.2: 8-Neighborhood of Pixel P_0

The 4-neighborhood of the pixel P_0 is made up of the elements of $N_4 = \{P_1, P_3, P_5, P_7\}$ depicted as

	P_3	
P_5	P_0	P_1
	P_7	

Figure 4.3: 4-Neighborhood of Pixel P_0

The pixel P_0, is a point of the skeleton if and only if it complies with one of the five conditions of Hilditch's thinning algorithm. Let P_i be a pixel in a binarized signature image, where $i = 1, 2, ..., 8$, and $B(P_i)$ is the value of pixel P_i. Then, the five conditions of Hilditch's thinning algorithm are [75, 174]

1. The pixel P_0 is a point on the skeleton if

$$\sum_{i \in N_4} \{1 - |B(P_i)|\} \geq 1 \tag{4.1}$$

2. The pixel P_0 is boundary of one skeleton, therefore is not deleted if

$$\sum_{i \in N_8} |B(P_i)| \geq 2 \tag{4.2}$$

3. The pixel P_0 is not deleted because it is an isolated pixel if

$$\sum_{i \in N_8} C_i \geq 1 \tag{4.3}$$

where

$$C_i = \begin{cases} 1 & \text{for } B(P_i) = 1 \\ 0 & \text{for } B(P_i) \neq 1 \end{cases} \tag{4.4}$$

4. The pixel P_0 is a connective pixel, not deleted if

$$N_8^c(P_0) = 1 \tag{4.5}$$

where

$$N_8^c(P_0) = \sum_{i \in N_4} \{D(P_i) - D(P_i) \times D(P_{i+1}) \times D(P_{i+2})\} \tag{4.6}$$

and

$$D(P_i) = \begin{cases} 1 & \text{for } |B(P_i)| = 1 \\ 0 & \text{for } |B(P_i)| \neq 1 \qquad (i \in N_8) \end{cases} \tag{4.7}$$

5. One side is deleted when the width of skeleton is two pixels if

$$B(P_i) \neq 1 \qquad (i \in N_8) \tag{4.8}$$

and

$$N_8^c(P_0) = 1 \quad when \quad B(P_i) = 0 \tag{4.9}$$

Given the original signature in Figure 4.4(a), the resultant image after thinning is shown in Figure 4.4(b).

(a) Original signature

(b) Thinned signature

Figure 4.4: Signature skeletonization

4.2.2 Feature Extraction

The choice of a meaningful set of features is crucial in any signature verification system. Different feature methods have been studied to capture various structural and geometric properties of signatures. The extracted features are mask features and grid features. Mask features provide information about directions of the segments of the signature, while grid features give an overall signature appearance [123]. The extracted mask features are direction and transition features, and the grid features are trifold and sixfold features.

Direction Features

The direction feature technique was originally designed to simplify each alphabetical character's boundary or thinned representation through identification of individual stroke or line segments in the image [15]. Since signatures are composed of special unconstrained cursive symbols which are not necessarily alphabetical characters, it is not possible to apply alphabetical character recognition to all signatures. Hence, we have chosen to use a direction feature technique for handwritten text recognition, instead of the segmented alphabetical character recognition. The proposed text-based signature recognition approach explained below, is an extension of the alphabetical character-based direction feature technique [12].

Character-based Recognition

Character-based recognition is the recognition of alphabetical characters, that is, (lower case: a - z or upper case: A - Z), extracted from cursive handwriting. Blumenstein et. al. [12] proposed a neural network-based technique for cursive alphabetical character recognition implemented in segmentation-based word recognition systems. The technique integrates the direction information extracted from the structure of alphabetical character contours with the transition information between background and foreground pixels in the alphabetical character image. This cursive alphabetical character recognition technique is sequenced as follows [12]:

1. Cursive Character Processing

    - Character Extraction - character component analysis is used to sequentially locate all non-cursive or printed character components. Then vertical and horizontal boundaries of each character component is defined, respectively.
    - Preprocessing - character images are thresholded and slant corrected. The boundary detection on each character image is performed in order to facilitate direction feature extraction techniques.

2. Feature Extraction and Character Recognition

    - Direction Feature - simplifies each character's boundary through identification of line segments in the image. Features are extracted based on the direction of the line segments within a character image zoned into a window. This technique normalizes the line segments in order to discard spurious direction values. Contrarily, the spurious direction values could be very distinctive features for signature verification.

As a result, the accurate recognition of segmented characters is important in the context of segmentation-based word recognition [61]. Character-based recognition system handles formatting, performs correct segmentation into characters and finds the most plausible alphabetical characters. This process diminishes the extraction of all distinctive features especially from a signature. Moreover, character-based recognition is better suited for word verification than signature verification.

Text-based Recognition

In this thesis, text-based recognition involves the extraction of distinctive features from the whole signature text image without segmenting the individual characters contained in the signature. The extracted features represent the distinguishing cursive handwriting styles, which are formatted by character-based recognition.

The line segments, which give the direction transitions, are determined for the whole signature text image rather than on each character image, and categorized as *Vertical*, *Horizontal*, *Right diagonal* and *Left diagonal*. The intersection points between types of lines are located. The techniques for locating the starting point and intersection points, and labeling the line segments are discussed in [3, 4, 15]. The direction transitions are coded as indicated in Table 4.1.

Table 4.1: Direction transition codes

Direction Transition	**Code**
Vertical	2
Right Diagonal	3
Horizontal	4
Left Diagonal	5
Intersection	9

Line Segments Categorization. As mentioned above, four types of line segments are distinguished by following neighboring pixels along the thinned signature from the starting point. A semi 8-neighbourhood[1] based algorithm determines the beginning and end of individual line segments. This algorithm is described below.

In **Algorithm 2**, SOUTH, SOUTHWEST, WEST and NORTHWEST determine semi 8-neighbourhood values. After labeling the whole thinned signature using the codes defined in Table 4.1, the algorithm for extracting and storing line segment information first locates the starting point and then extracts the number of intersection points (equation (4.12)), and the number and lengths of line segments resulting in a set of nine feature values. The number and lengths features of line segments are extracted using equations (4.10) and (4.11), respectively.

$$Number = \frac{Number\ of\ Segments\ in\ a\ Particular\ Direction}{Area\ of\ Signature\ Bounding\ Box} \tag{4.10}$$

[1]In our context semi 8-neighborhood of a pixel I(i,j) is made of (i-1,j-1), (i,j-1), (i+1,j-1) and (i+1,j).

Algorithm 2 Line_Segments_Categorization(I).

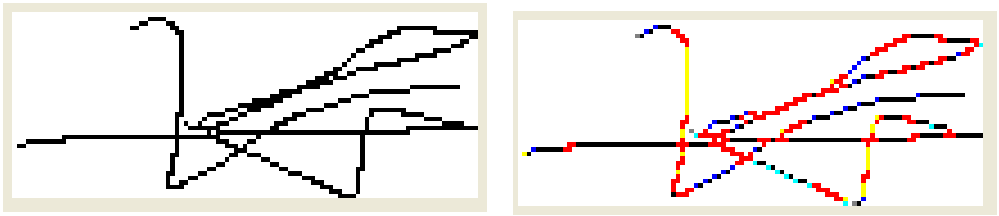
```
1: for (All foreground pixel (i,j)) do
2:   if I[i, j] == INTERSECTION then
3:     I[i, j] ← 9
4:   else
5:     if I[i + 1, j]) == FOREGROUND then
6:       I[i, j] ← 2
7:     end if
8:   else
9:     if I[i + 1, j − 1] == FOREGROUND then
10:      [i, j] ← 3
11:    end if
12:  else
13:    if I[i, j − 1] == FOREGROUND then
14:      I[i, j] ← 4
15:    end if
16:  else
17:    if [i − 1, j − 1]) == FOREGROUND then
18:      I[i, j] ← 5
19:    end if
20:  end if
21: end for
```

$$Length = \frac{Number\ of\ Pixels\ in\ a\ Particular\ Direction}{Area\ of\ Signature\ Bounding\ Box} \tag{4.11}$$

$$Intersection = \frac{Number\ of\ Intersection\ Points}{Area\ of\ Signature\ Bounding\ Box} \tag{4.12}$$

Transition Features

The transition feature (TF) extraction technique records the locations of the transitions between foreground and background pixels in the vertical and horizontal directions of binary images. The image is traversed in the following four directions: left to right, right to left, top to bottom and bottom to top. Each time there is a change from background to foreground or vice versa, then the ratio between the locations of the transition and the length/width of



(a) Original signature (b) Labeled signature

Figure 4.5: Original signature and its corresponding labeled signature *(Black=Horizontal, Yellow=Vertical, Red=Intersection, Blue=Right Diagonal, Cyan=Left Diagonal).*

the image traversed is recorded as a feature [4, 12, 118]. The average ratios of the X and Y positions of the transitions for each of the four directions are recorded, resulting in eight features. In addition, the total number of transitions is also recorded, resulting in two more features.

Grid Features

1. **Tri-Surface Feature** -The tri-surface area was implemented in an attempt to increase the accuracy of a feature describing the surface area of a signature [3, 4]. This is achieved by splitting up vertically the signature into three equal parts and calculating the proportion of the signature surface area of each part over the total surface area of the image using equation (4.13). This results in a set of three feature values. Figure 4.6 shows the tri-surface area.

2. **Sixfold-Surface Feature** -The concept of sixfold-surface feature is similar to the concept of the tri-surface feature. The signature image is split up vertically into three equal parts. Then, the center of gravity is calculated for each of the three parts, and the signature surface area above and below the horizontal line of the center of gravity is calculated [3, 4]. The result is a set of six feature values corresponding to the proportion of the signature surface area of each of the six parts over the total surface area of the entire signature image. The sixfold-surface feature is depicted in Figure 4.7.

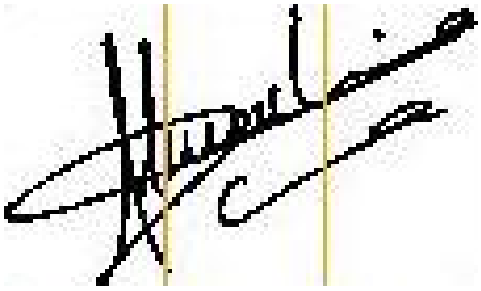


Figure 4.6: Tri-surface feature

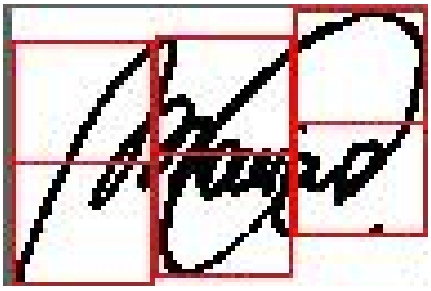


Figure 4.7: Sixfold-surface feature

$$Ratio = \frac{Area\ of\ Signature}{Area\ of\ Bounding\ Box} \tag{4.13}$$

4.2.3 Feature Normalization

Feature normalization aims at normalizing the individual components of the extracted feature vectors in such a way that the resulting (normalized) vectors are better suited for classification [159].

The extracted feature vector $\overrightarrow{v}$ of 28 dimensions is defined as follows:

$$\overrightarrow{v} = (v_0,\ v_1, ...,\ v_{27}) \tag{4.14}$$

where $\overrightarrow{v}$ is composed of 3 tri-surface, 6 sixfold-surface, 10 transitional, and 9 directional features. The scales of these individual features extracted are completely different. Firstly, this disparity can be due to the fact that each feature is computed using a formula that can produce a range of values. Secondly, the features may have the same approximate scale, but the distribution of their values has different means and standard deviations [104]. A statistical normalization technique is used to transform each feature in such a way that each transformed feature distribution has mean equal to 0 and variance of 1.

Let n be the number of features and m the size of the distribution, a features matrix X is defined in (4.15):

$$X = \begin{bmatrix} x_{11} & x_{12} & ... & x_{1n} \\ x_{21} & x_{22} & ... & x_{2n} \\ \vdots & & \ddots & \vdots \\ x_{m1} & x_{m2} & ... & x_{mn} \end{bmatrix} \tag{4.15}$$

where x_{ij} is the j^{th} feature of the i^{th} candidate for $(i = 1, 2, ..., m)$ and $(j = 1, 2, ..., n)$, the corresponding value is new_x_{ij} and is defined as (4.16):

$$new\_x_{ij} = \frac{x_{ij} - \overline{x}_j}{\sigma_j} \tag{4.16}$$

where $\overline{x}_j$ is the mean defined in equation (4.17) and σ_j is the standard deviation defined in equation (4.18)

$$\overline{x}_j = \frac{1}{m} \sum_{i=1}^{m} x_{ij} \tag{4.17}$$

$$\sigma_j = \sqrt{\frac{1}{m-1}\sum_{i=1}^{m}(x_{ij} - \overline{x}_j)^2} \tag{4.18}$$

4.2.4 Signature Verification

To verify the similarity of two signatures, Mahalanobis Distance (MD) based on correlations between signatures is used. It differs from Euclidean distance in that it takes into account the correlations of the data set and is scale-invariant. The smaller the MD is, the higher the similarity of the compared signatures. The MD is defined in equation (4.19).

$$MD(\overrightarrow{x}, \overrightarrow{y}) = \sqrt{(\overrightarrow{x} - \overrightarrow{y})^T S^{-1} (\overrightarrow{x} - \overrightarrow{y})} \tag{4.19}$$

where $\overrightarrow{x}$ and $\overrightarrow{y}$ denote the enrolled feature vector and the new signature feature vector to be verified, respectively, with the covariance matrix S.

Table 4.2: Verification rates *(D=Directional, T=Transitional, S=Sixfold, Tr=Trifold)*

	Verification Rate (%)	
Techniques	**GPDS Database**	**ePadInk Signatures**
D	94.76	95.14
DT	95.28	97.43
DTS	93.77	98.01
DTSTr	90.79	94.14

4.3 Discussion of Results

Our experiments were carried out using two data sets: the GPDS signature database [37], and a database created from signatures captured using the ePadInk tablet. The GPDS signature database contains data from 300 individuals: 24 genuine signatures for each individual, and 30 samples of forgeries per each genuine signature. The forgers were allowed to practice the

Table 4.3: Comparative table of datasets

	# Signers	**Genuine Samples**	**Forgery Samples**
Lv et. al. [107]	20	25	30
Huang et. al. [72]	21	24	24
Sansone et. al. [144]	49	20	10
Mitra et. al. [114]	20	10	10
Ferrer et. al. [58]	160	24	24
Vargas et. al. [163]	160	24	24
Our Dataset 1. [37]	300	24	30
Our Dataset 2.	20	10	10

Table 4.4: Comparative table of the proposed approach with other published techniques

	(%) FAR	**(%) FRR**	**(%) EER**
Lv et. al. [107]	28.30	27.50	27.90
Huang et. al. [72]	11.80	11.10	11.45
Sansone et. al. [144]	12.45	12.04	12.24
Mitra et. al. [114]	2.50	4.00	3.25
Ferrer et. al. [58]	12.60	14.10	13.35
Vargas et. al. [162]	14.66	10.01	12.33
Vargas et. al. [163]	7.35	5.05	6.20
Proposed on GPDS	5.34	5.20	5.27

signatures as many times as they wished. Each forger imitated 3 signatures of 5 individual signers in a single day writing session. The genuine signatures shown to each forger are chosen randomly from the 24 genuine ones. Therefore, for each genuine signature, there are 30 skilled forgeries made by 10 forgers from 10 different genuine specimens. The database created with ePadInk tablet comprises 400 signatures from 20 individuals, 10 genuine and 10 random forgeries per individual.

Firstly, the experiments were carried out using the text-based directional features alone, and the combination of the text-based directional features with one or more of the following features: transitional, sixfold and trifold as shown in Table 4.2. The verification rates of the two data sets: the GPDS signature database [37], and a database created from signatures captured using the ePadInk tablet are compared in Table 4.2. On the GPDS database, the combination of the text-based directional and transitional features achieved a high verification rate of 95.28%. On the other hand, the combination of the text-based directional,

Table 4.5: Comparison of directional feature extraction algorithms *(O=Original, D=Directional, F=Feature, M=Modified, E=Enhanced)*

Techniques	Verification Rate (%)	
	GPDS Database	**ePadInk Signatures**
ODF	83.65	80.02
MDF	84.57	85.50
EMDF	89.61	86.64
Our Approach	**94.76**	**95.14**

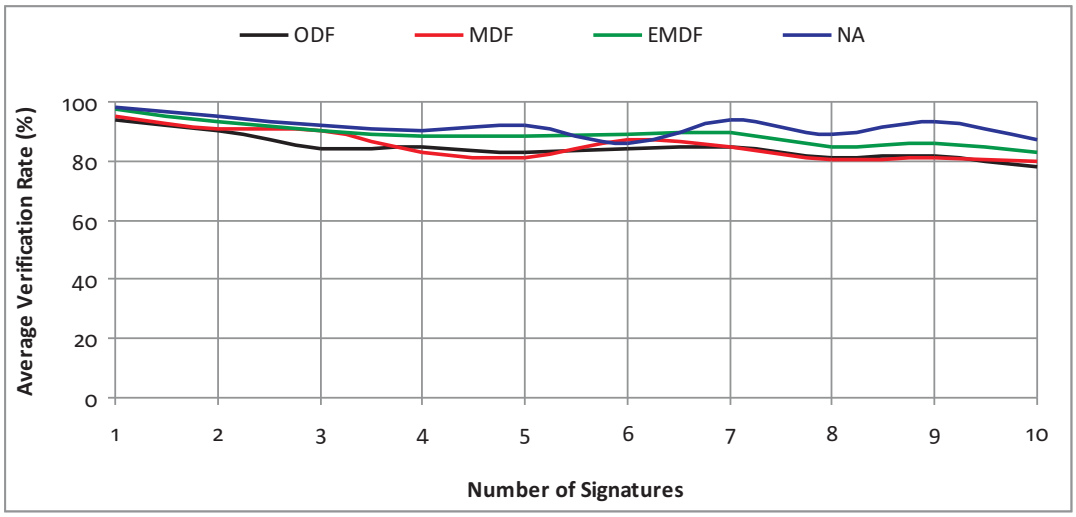


Figure 4.8: Average verification rate of directional feature extraction algorithms *(O=Original, D=Directional, F=Feature, M=Modified, E=Enhanced, NA=New Approach)*

transitional and sixfold features achieved the highest verification rate of 98.01%, when using the ePadInk database. This highest verification rate is obtained when both the mask and grid features are combined. The overall average verification rate of Table 4.2 is 94.92%.

Secondly, Tables 4.3 and 4.4 show the comparison of our datasets with the datasets used by other researchers, and the comparison of the results obtained by the proposed approach with other off-line related works in the literature, respectively. In fact, Ferrer et. al. [58], and Vargas et. al. [162, 163] used the same signature database as ours, the GPDS [37]. Table 4.4 presents the results in terms of Type I and Type II errors for forgeries. The Equal Error Rate (EER) value is calculated as the mean value between the False Acceptance Rate (FAR) and False Rejection Rate (FRR) values. Our approach obtained the lowest EER of 5.27%,

with the FAR of 5.34% and FRR of 5.20%, using the GPDS signature database. Vargas et. al. [163] obtained the EER of 6.20%, with the FAR of 7.35% and FRR of 5.05%, using the same GPDS database.

Further comparison of the results obtained by the proposed text-based feature extraction approach with character-based feature extraction approaches is presented in Table 4.5. Our approach, the text-based directional signature recognition technique obtained the following verification rates: 94.76% on GPDS database, 95.14% ePadInk signatures, and an average verification rate of 94.95%. The statistical normalization applied to the features as described in section 4.2.3, also enhanced the verification rate since it takes into account the correlations of the data set verified by Mahalanobis Distance.

Furthermore, the average variation of signature verification rates of the four directional feature extraction based algorithms is shown in Figure 4.8. For instance, the Enhanced Modified Directional Feature (EMDF) algorithm achieves an overall average verification rate of 97.4% when 1 signature per 39 individuals is considered, 89.8% with 7 signatures per 39 individuals, and an average of verification rate of 83.0% when 10 signatures per 39 individuals are considered. The New Approach (NA) achieves an average verification rate of 98.0% with 1 signature per 39 individuals, 94.2% with 7 signatures per 39 individuals, and an average of verification rate of 87.2% when 10 signatures per 39 individuals are considered.

4.4 Conclusion

The proposed algorithm improves the character-based directional feature extraction algorithm. Experimental results show that the proposed approach has an improved true positive rate of 94.95% compared to other character-based directional feature extraction algorithms as shown in Table 4.5. Further investigation of the effects of the proposed approach with other signature databases, and other alternative signature verification algorithms is to be carried out. The following chapter investigates various multi-modal fusion algorithms and user-specific weighting techniques of each biometrics trait.

Chapter 5

Bi-Modal Biometrics Fusion: Integrating Iris and Signature

5.1 Introduction

Multi-modal biometric systems are proposed to address the problems of uni-modal systems like non-universality. For example, the feature extraction module of a fingerprint authentication system may be unable to extract features from fingerprints associated with specific individuals, due to the poor quality of the ridges. In such instances, it is useful to acquire multiple biometric traits for verifying the identity. Multi-modal systems also provide anti-spoofing measures by making it difficult for an intruder to spoof multiple biometric traits simultaneously [136]. By asking the user to present a random subset of biometric traits, the system ensures that a *live* user is indeed present at the point of acquisition. Thus, a challenge-response type of authentication can be facilitated using multi-biometric systems.

However, an integration scheme is required to fuse the information presented by the individual modalities. Multi-modal biometric systems are expected to be more reliable due to the presence of multiple pieces of evidence [70]. Furthermore, multi-modal systems are able to meet the stringent performance requirements imposed by various applications [69]. In fact, the latest research indicates that using a combination of biometric techniques for human identification is more effective, and far more challenging [83]. Therefore, the problem of information fusion requires much attention in order to optimize the success rate of multi-modal biometric systems.

Multi-modal biometrics was pioneered by Anil K. Jain and there has been substantial research carried out in this area. A variety of biometric fusion schemes, which use classifiers, statistical frameworks, and other techniques have been described in the literature to combine

multiple biometric trait scores. These include majority voting, sum and product rules, k-NN classifiers, SVMs, HyperBF network, Bayesian statistics, decision trees, etc, [83, 89, 165]. For instance, Jain & Ross and Ross & Jain [82, 136] combine the matching scores of three traits (face, fingerprint and hand geometry) using three different techniques (sum rule, decision tree, linear discriminant analysis), to enhance the performance of a biometric system. Generally, experiments indicate that the fusion scheme using the sum rule with normalized scores gives the best performance. These results are further improved by learning user-specific matching thresholds and weights for individual biometric traits.

In this chapter, an enhanced user-specific weighting technique, which is based on the different degrees of importance for iris and signature biometric traits of an individual, to integrate a physiological trait, the *iris* and behavioral trait, the *signature* is proposed. The user-specific weights for individual biometric traits are calculated based on the score of each biometrics trait of an individual user. The proposed approach is an alternative to the estimation of user-specific weights by exhaustive search. Thereafter, an intelligent dual ν-support vector machine (2ν-SVM) based fusion algorithm is used to integrate the weighted match scores of iris and signature modalities at the matching score level.

5.2 Multi-modal Biometrics System

Multi-modal biometric systems are based on the consolidation of information presented by multiple evidences that stem from multiple traits. Some of the limitations imposed by uni-modal biometric systems can be alleviated by using multiple biometric modalities [9, 20, 83]. In fact, multi-biometric systems are expected to be more reliable due to the presence of multiple, fairly independent biometric traits.

A variety of factors should be considered when designing a multi-modal biometrics system. These include the choice and number of biometric traits; the level in the biometric system at which information provided by multiple traits should be integrated; the methodology adopted to integrate the information; and the cost versus matching performance trade-off.

A simple multi-modal biometrics system has five important components as depicted in Figure 5.1, in which different biometric traits are fused at match score level

1. **Sensor Module**, acquires the biometric data of an individual. An example is the ePadInk tablet that captures the signature.
2. **Feature Extraction Module**, the acquired biometric data is processed to extract distinctive feature values.
3. **Matching Module**, the extracted feature values are compared against those in the template by generating a matching score.
4. **Fusion Module**, combines the biometric traits.
5. **Decision Module**, a claimed identity is either accepted or rejected based on the fusion matching score generated in the fusion module.

5.3 Integrating the Iris and Signature Traits

There are various levels of fusion for combining biometric traits. The three possible levels of fusion are [136]: *fusion at the feature extraction level*, *the matching score level*, and *the decision level*. These fusion levels are described in detail in section 2.2.4.

The iris and signature traits are fused at the matching score level, where the matching scores output of each of these two traits are weighted and combined. Fusion at the matching score level is usually preferred, as it is relatively easy to access and combine the scores presented by the different modalities [83]. There are two distinct approaches for the match score level fusion: the *classification problem* approach [165], where a feature vector is constructed using the matching scores output by the individual matchers, and the *combination problem* approach, where the individual matching scores are combined to generate a single scalar score, which is then used to make the final decision. The *combination* approach is used in this research work because it is shown in the literature [136] that it performs better than the *classification* approach.

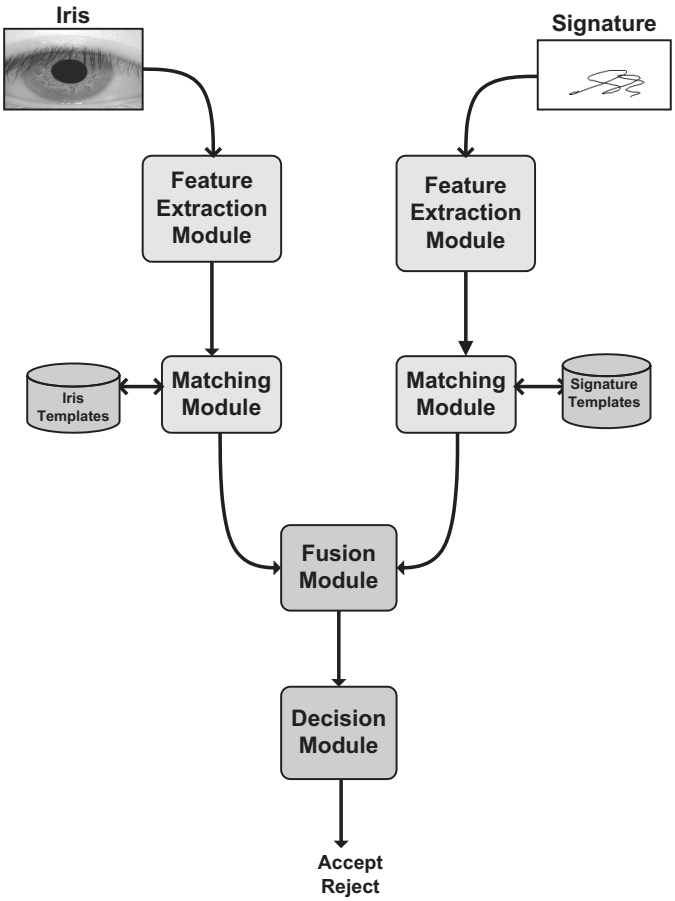


Figure 5.1: Bi-modal biometrics system (iris and signature)

5.3.1 Score Generation

Iris Score

Iris matching scores are generated from string iris feature codes extracted by the cumulative-sum-based grey change analysis technique. To verify the similarity of two iris codes, Hamming Distance (HD) based on the matching algorithm [38] is used. The smaller the HD, the higher the similarity of the compared iris codes. The HD denotes the iris raw matching score, $s_{iris} \in [0, 1]$, which is computed as

$$s_{iris} = \frac{1}{2N}[(\sum_{i=1}^{N} A_h(i) \oplus B_h(i)) + (\sum_{i=1}^{N} A_v(i) \oplus B_v(i))] \tag{5.1}$$

where $A_h(i)$ and $A_v(i)$ denote the enrolled iris code over horizontal and vertical directions, respectively, $B_h(i)$ and $B_v(i)$ denote the new input iris code over the horizontal and vertical directions respectively. N is the total number of cells, and $\oplus$ is the XOR operator.

Signature Score

Signature matching scores are generated from the signature feature vectors. To verify the similarity of two signatures, Mahalanobis Distance (MD) based on correlations between signatures is used. It differs from Euclidean distance in that it takes into account the correlations of the data set and is scale-invariant. The smaller the MD is, the higher the similarity of the compared signatures. MD represents the signature's raw matching score, $s_{sig} \in [0, 1]$, which is computed as follows

$$s_{sig}(\overrightarrow{x}, \overrightarrow{y}) = \sqrt{(\overrightarrow{x} - \overrightarrow{y})^T S^{-1} (\overrightarrow{x} - \overrightarrow{y})} \tag{5.2}$$

where $\overrightarrow{x}$ and $\overrightarrow{y}$ denote the enrolled feature vector and the new signature feature vector to be verified, with the covariance matrix S.

5.3.2 Score Normalization

Given a set of n raw matching scores S_n, (iris or signature scores), the corresponding set, S'_n of normalized scores, is obtained by calculating for each score $s \in S_n$ the equivalent normalized score $s' \in S'_n$, using one of the following normalization methods.

- *Min-Max Normalization*: retains the original distribution of scores and maps all the scores into the $[0, 1]$ range.

$$s' = \frac{s - \min(S_n)}{\max(S_n) - \min(S_n)} \tag{5.3}$$

  where $\min(S_n)$ and $\max(S_n)$ are the minimum and maximum, respectively, of the given set S_n of matching scores.

- *Z-Score Normalization*: transforms the scores to a distribution with arithmetic mean of 0 and standard deviation of 1.

$$s' = \frac{s - \mu}{\sigma} \tag{5.4}$$

  where μ and σ are the mean and standard deviation, respectively, of the set S_n.

- *Tanh Normalization*: is a robust statistical technique [79] which maps the raw scores into the $[0, 1]$ range.

$$s' = \frac{1}{2}\left\{\tanh\left(0.01\left(\frac{s - \mu}{\sigma}\right)\right) + 1\right\} \tag{5.5}$$

  where μ and σ are the mean and standard deviation, respectively, of S_n.

5.3.3 Score Weighting

Let s'_{iris} and s'_{sig} be the normalized scores of the iris and signature traits, respectively. The fusion score, s_{fus} is computed as

$$s_{fus} = w_{iris}s'_{iris} + w_{sig}s'_{sig} \tag{5.6}$$

where w_{iris} and w_{sig} are the *weights* associated with the degrees of importance of the two traits per individual, and

$$w_{iris} + w_{sig} = 1 \tag{5.7}$$

The different iris scores and signature scores are given different degrees of importance for different users. For instance, by reducing the weight w_{iris} of an occluded iris and increasing the weight w_{sig} associated with the signature trait, the false reject error rate of the particular user can be reduced. The biometric system learns user-specific parameters by observing system performance over a period of time [83]. Two techniques are used to compute the user-specific weights: *an exhaustive search technique*, and *a user-score-based technique*.

The Exhaustive Search Technique

Let w^i_{iris} and w^i_{sig}, be the weights associated with the i^{th} user in the database. The algorithm operates on the training set as follows [82]:

- For the i^{th} user in the database, vary weights w^i_{iris} and w^i_{sig} over the range $[0, 1]$, with the constraint $w^i_{iris} + w^i_{sig} = 1$. Compute $s^i_{fus} = w^i_{iris}s'_{iris} + w^i_{sig}s'_{sig}$. This computation is performed over all scores associated with the i^{th} user.
- Choose that set of weights that minimizes the total error rate. The total error rate is

the sum of the false acceptance and false rejection rates pertaining to this user.

The set of weights, $\{w^i_{iris}, w^i_{sig}\}$, that minimize the total error rate, with the constraint $w^i_{iris} + w^i_{sig} = 1$, do not necessarily associate the degrees of importance for iris and signature biometric traits of the i^{th} individual in the fusion score: $s^i_{fus} = w^i_{iris} s'_{iris} + w^i_{sig} s'_{sig}$. An alternative user-score-based weighting technique, which computes the weights, $\{w^i_{iris}, w^i_{sig}\}$, by associating them with the degrees of importance for iris and signature biometric traits, respectively, is proposed. In this method, the weights, $\{w^i_{iris}, w^i_{sig}\}$, which are not constrained to $w^i_{iris} + w^i_{sig} = 1$, are computed in consideration of how close the scores, s'^i_{iris} and s'^i_{sig} are, to the thresholds of the iris and signature traits, respectively. The user-score-based weighting technique is described below.

The User-Score-Based Technique

Let s'^i_{iris} and s'^i_{sig}, be the normalized scores associated with the i^{th} user in the database, and τ_1 and τ_2 are the thresholds of the iris and signature traits, respectively. The preliminary weights w'^i_{iris} and w'^i_{sig} per trait are computed as

$$w'^i_{iris} = \begin{cases} 0.5 & \text{if } s'^i_{iris} = \tau_1 \\ \frac{s'^i_{iris}}{\tau_1 + s'^i_{iris}} & \text{otherwise} \end{cases} \tag{5.8}$$

and

$$w'^i_{sig} = \begin{cases} 0.5 & \text{if } s'^i_{sig} = \tau_2 \\ \frac{s'^i_{sig}}{\tau_2 + s'^i_{sig}} & \text{otherwise} \end{cases} \tag{5.9}$$

where w'^i_{iris} and w'^i_{sig} are the initial weights associated with the iris and signature, respectively, **without** the constraint $w'^i_{iris} + w'^i_{sig} = 1$. These weights are assigned to the scores,

s'^{i}_{iris} and s'^{i}_{sig} after analyzing how close or farther away the scores are from their respective thresholds, τ_1 and τ_2. Then, the fusion weights for the i^{th} user are computed respectively, for the iris and signature as

$$w^{i}_{iris} = \frac{w'^{i}_{iris}}{w'^{i}_{iris} + w'^{i}_{sig}} \tag{5.10}$$

$$w^{i}_{sig} = \frac{w'^{i}_{sig}}{w'^{i}_{iris} + w'^{i}_{sig}} \tag{5.11}$$

with the constraint $w^{i}_{iris} + w^{i}_{sig} = 1$, and the fusion score is computed in equation (5.12).

$$s^{i}_{fus} = w^{i}_{iris} s'^{i}_{iris} + w^{i}_{sig} s'^{i}_{sig} \tag{5.12}$$

5.3.4 Fusion Algorithms

Sum Rule

Given the normalized matching scores of iris s_{iris} and signature s_{sig}, the iris-signature fusion score s_{fus} is calculated by linearly combining the two scores [27, 31].

$$s_{fus} = \beta s_{iris} + (1 - \beta) s_{sig} \tag{5.13}$$

where β is a fusion weight computed using the training data, and is dependent on the degree of similarity of each of the modalities [113, 117, 143].

User-Specific Parameters

Two types of parameters are considered, thresholds and weights [82].

User-Specific Thresholds

The user-specific thresholds verify the matching score of an individual. The matching thresholds for the i^{th} user in the database are computed using a cumulative histogram of impostor scores for the iris and signature traits as follows [82]

1. Let $\tau_i(\omega)$ be the threshold in the cumulative histogram that retains ω fraction of scores, $0 \leq \omega \leq 1$.

2. Compute $\{FAR_i(\omega), GAR_i(\omega)\}$, using $\{\tau_i(\omega)\}$ as the matching threshold, where $FAR_i(\omega)$ is the false acceptance rate corresponding to ω fraction of scores of the i^{th} user, and $GAR_i(\omega)$ is the genuine acceptance rate corresponding to ω fraction of scores of the i^{th} user.

3. Compute the FAR and GAR as

$$FAR(\omega) = \sum_i FAR_i(\omega) \tag{5.14}$$

$$GAR(\omega) = \sum_i GAR_i(\omega) \tag{5.15}$$

4. Generate the ROC curve from $\{FAR(\omega), GAR(\omega)\}$.

Table 5.1 shows the user-specific thresholds corresponding to a FAR of 1% of 10 users. The ω corresponding to a specified FAR is used to compute the set of user-specific thresholds, $\{\tau_i(\omega)\}$.

Table 5.1: User-specific thresholds corresponding to a FAR of 1%

User	Iris	Signature
1	0.25	0.32
2	0.27	0.31
3	0.30	0.35
4	0.27	0.29
5	0.28	0.32
6	0.27	0.31
7	0.28	0.31
8	0.30	0.33
9	0.29	0.30
10	0.29	0.32

Matching Score Weighting

Weights indicate the importance of matching scores of each biometrics trait, the iris and signature. The two algorithms used to compute the user-specific weights: *an exhaustive search technique*, and *a user-score-based technique* are described in section 5.3.3. The alternative technique (special case) of weighting the matching scores is to assign equal weights for all the traits. The fusion matching score s_{fus} is defined in (5.16)

$$s_{fus} = \frac{1}{2}(s'_{iris} + s'_{sig}) \tag{5.16}$$

where s'_{iris} and s'_{sig} are normalized matching scores of iris and signature traits, respectively.

2ν-SVM

Support Vector Machine (SVM) has been used in different domains, particulary in biometrics recognition [155, 161]. SVM is a classifier that constructs hyperplanes in a multidimensional space and separates the data points into different classes [164]. SVM implements an iterative training algorithm which maximizes the margin between two classes. However, it has been proven that margin maximazation does not always lead to minimum classification errors

[29, 146]. For instance, dual ν-SVM (2ν-SVM) is used to address the challenges of classifying fuzzy data [32]. In this research work, the 2ν-SVM fusion algorithm is used to integrate the iris and signature traits. The dual ν-SVM (2ν-SVM) is defined below.

Let $\{\mathbf{x}_i, y_i\}$ be a set of N vectors with $\mathbf{x}_i \in \Re^d$, $y_i \in \{+1, -1\}$, and $i = 1, ..., N$. $\mathbf{x}_i$ is the i^{th} vector that belongs to a binary class y_i [32]. The hyperplane that maximizes the margin between two classes is defined as

$$\mathbf{w}\varphi(\mathbf{x}) + b = 0 \tag{5.17}$$

such that,

$$y_i(\mathbf{w}\varphi(\mathbf{x}_i) + b) \geq (\rho - \psi_i), \qquad \rho, \psi_i \geq 0 \tag{5.18}$$

to minimize,

$$\frac{1}{2}\|\mathbf{w}\|^2 - \sum_i C_i(\nu\rho - \psi_i) \tag{5.19}$$

where ρ gives the marginal position of the hyperplane and ν denotes the error. $\varphi(\mathbf{x})$ is the function which maps the data space to the feature space, and provides generalization for the decision function. $C_i(\nu\rho - \psi_i)$ computes the rate of errors, b is the bias, $\mathbf{w}$ is the normal vector, and ψ_i is the slack variable for classification errors [164]. ν is the error which is computed using ν_+ (positive error) and ν_- (negative error) [164].

$$\nu = \frac{2\nu_+\nu_-}{\nu_+ + \nu_-}, \;\; 0 < \nu_+ < 1 \;\; and \;\; 0 < \nu_- < 1 \tag{5.20}$$

The cost of errors C_i, is computed as [164]

$$C_i = \begin{cases} C_+, & \text{if} \quad y_i = +1 \\ C_-, & \text{if} \quad y_i = -1 \end{cases} \tag{5.21}$$

given that

$$C_+ = \left[n_+ \left(1 + \frac{\nu_+}{\nu_-} \right) \right]^{-1} \tag{5.22}$$

$$C_- = \left[n_- \left(1 + \frac{\nu_-}{\nu_+} \right) \right]^{-1} \tag{5.23}$$

and n_+ and n_- are the signed number of training points for the classes. Further, 2ν-SVM training can be formulated as [32]

$$max_{\alpha_i} \left\{ -\frac{1}{2} \sum_{i,j} \alpha_i \alpha_j y_i y_j K(\mathbf{x}_i, \mathbf{x}_j) \right\} \tag{5.24}$$

where

$$0 \leq \alpha_i \leq C_i \tag{5.25}$$

$$\sum_i \alpha_i y_i = 0 \tag{5.26}$$

$$\sum_i \alpha_i \geq \nu \tag{5.27}$$

$i, j \in 1, ..., N, \alpha_i, \alpha_j$ are Lagrange multipliers and the Kernel function is [32]

$$K(\mathbf{x}_i, \mathbf{x}_j) = \varphi(\mathbf{x}_i)\varphi(\mathbf{x}_j) \tag{5.28}$$

where

$$K(\mathbf{x}_i, \mathbf{x}_j) = \exp(-\gamma \|\mathbf{x}_i - \mathbf{x}_j\|^2), \qquad \gamma > 0. \tag{5.29}$$

The Kernel $K(\mathbf{x}_i, \mathbf{x}_j)$ is the Radial Basis Function (RBF) [161]. An iterative optimized training algorithm is used to train 2ν-SVM [32]. This optimization algorithm divides the problem into a two-variable decision problem. Chew et. al. [32] proved that the optimized 2ν-SVM has a better complexity of $O(N)$ than $O(N^2)$ of the SVM.

The 2ν-SVM fusion algorithm is used to integrate the matching scores of the iris s_{iris} and signature s_{sig}, together with their corresponding weights, w_{iris} and w_{sig}. The weighted iris matching score m_{iris} is defined as

$$m_{iris} = s_{iris} * w_{iris} \tag{5.30}$$

and the weighted signature score m_{sig} is defined as

$$m_{sig} = s_{sig} * w_{sig} \tag{5.31}$$

The weighted matching scores and their labels are used to train the 2ν-SVM for bimodal fusion. Let the training data be

$$Z_{iris} = (m_{iris}, y) \tag{5.32}$$

and

$$Z_{sig} = (m_{sig}, y) \tag{5.33}$$

where $y \in \{+1, -1\}$, such that $+1$ represents the authentic class and -1 denotes the intruder class. The 2ν-SVM error parameters are calculated using equation (5.34) and (5.35).

$$\nu_+ = \frac{n_+}{n_+ + n_-} \tag{5.34}$$

$$\nu_- = \frac{n_-}{n_+ + n_-} \tag{5.35}$$

where n_+ and n_- are the number of authentic and intruder, respectively. $\varphi(.)$ is used to map the training data into a higher dimension feature space such that $Z \rightarrow \varphi(Z)$. The optimal hyperplane which separates the training data in the higher dimensional feature space is computed as the solution of problem (5.24).

In the classification phase, the multi-modal fusion matching score s_{fus} is computed in equation (5.36),

$$s_{fus} = f_{iris}(m_{iris}) + f_{sig}(m_{sig}) \tag{5.36}$$

where

$$f_{iris}(m_{iris}) = a_{iris}\varphi(m_{iris}) + b_{iris} \tag{5.37}$$

$$f_{sig}(m_{sig}) = a_{sig}\varphi(m_{sig}) + b_{sig} \tag{5.38}$$

where a_{iris}, a_{sig}, b_{iris} and b_{sig} are parameters of the hyperplane. The solution of equation (5.36) is the signed distance of s_{fus} from the separating hyperplane given by the two 2ν-SVM for the two biometric modalities. The decision function defined in equation (5.39) verifies the identity.

$$Decision(s_{fus}) = \begin{cases} Accept, & \text{if } s_{fus} > 0 \\ Reject, & \text{otherwise} \end{cases} \tag{5.39}$$

Table 5.2: User-specific scores and weights of different traits for 10 users

User	**Iris Score**	**Signature Score**	**Normalized Iris Score**	**Normalized Signature Score**	**Iris Weight**	**Signature Weight**
1	0.192	0.001	0.487	0.488	0.80	0.20
2	0.277	0.001	0.490	0.488	0.86	0.14
3	0.625	2.054	0.505	0.505	0.50	0.50
4	0.446	2.438	0.506	0.496	0.44	0.56
5	0.232	0.005	0.486	0.492	0.83	0.17
6	0.473	2.383	0.498	0.507	0.47	0.53
7	0.071	0.028	0.484	0.493	0.67	0.33
8	0.522	2.474	0.505	0.507	0.47	0.53
9	0.366	1.358	0.497	0.502	0.48	0.52
10	0.451	1.774	0.502	0.506	0.50	0.50

5.4 Discussion of Results

Our experiments were carried out using three data sets: the *CASIA* iris database [23] which is further expounded in section 3.3, and *GPDS* signature database [37] and a database created from signatures captured using the ePadInk tablet, which are explained in section 4.3. Firstly, the matching scores of the iris and signature traits are computed as defined in equations (5.1) and (5.2). These matching scores are normalized and weighted as defined in subsections 5.3.2 and 5.3.3, respectively. Various normalization techniques were investigated.

The ROC curves depicting the performance of the individual score normalization techniques is shown in in Figure 5.2. The *Tanh Normalization* technique performs better than the *Min-Max* and *Z-Score* techniques.

Table 5.2 shows the scores for the iris and signature biometric traits, and their respective weights, for the sample of ten different individuals. The raw scores are normalized by the tanh technique, and the weights are computed using equations (5.10) and (5.11).

Figure 5.3 shows the average true positive rates achieved by the exhaustive search technique and the user-score-based approach, respectively, on uni-modal biometric traits based

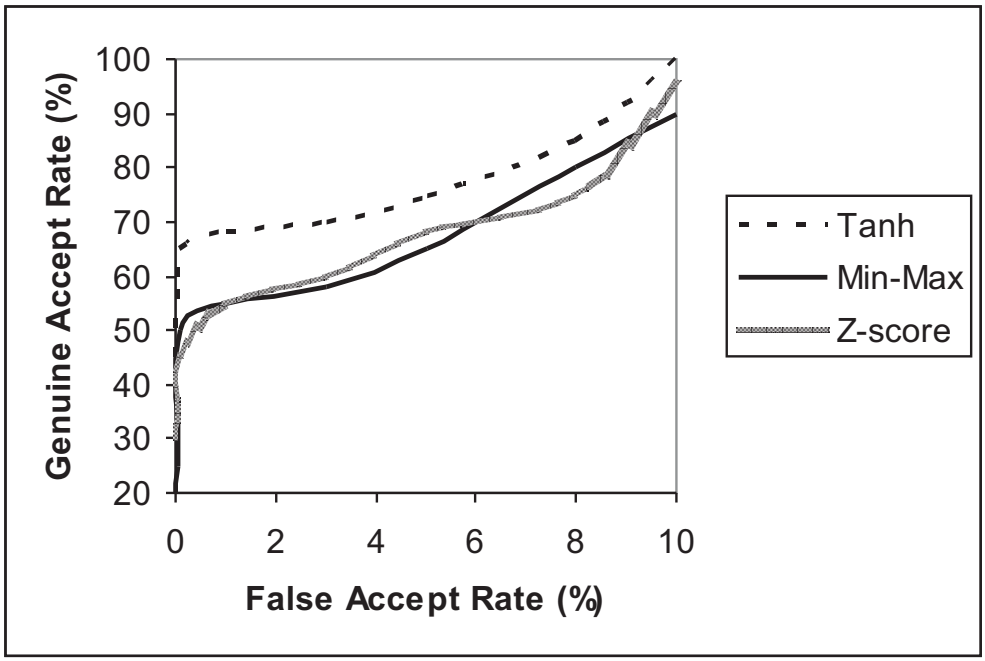


Figure 5.2: ROC curves showing the performance of each of the three normalization techniques on the iris trait

on iris and signature. The exhaustive search technique obtained true positive rates of 92.4% and 82.0% on the iris and signature traits, respectively. The user-score-based approach obtained true positive rates of 99.25% and 94.0% on the iris and signature traits, respectively. The overall average true positive rate achieved by the exhaustive search technique is 87.2%, compared to 96.63% which is obtained by the user-score-based algorithm. Therefore, the results show an improvement in accuracy when the user-score-based weighting technique is used.

5.5 Conclusion

In this chapter, an enhanced user-specific weighting technique of integrating a physiological biometrics trait, the *iris*, and a behavioral trait, the *signature* is proposed. The proposed user-score-based approach calculates weights for individual biometric traits per user in proportion to the scores of the biometric traits of the same user. The user-specific weights

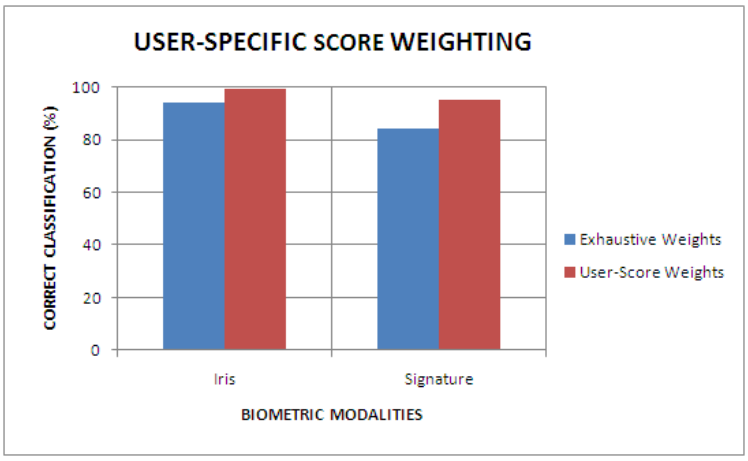


Figure 5.3: Average true positive rate of the iris and signature modalities

and their corresponding matching scores are fused using the sum rule algorithm and 2ν-SVM based learning technique. The experimental results and statistical evaluation of the investigated user-specific weight based fusion algorithms are discussed in chapter 6.

Chapter 6

Performance Improvement and Discussions

6.1 Introduction

In this chapter, we present experimental results and discussions of the designed bi-modal biometrics system. Fusion algorithms, various weighting and normalization techniques, and their results are discussed. An analysis and comparison of the results achieved are carried out, and the description of the data sets used in the experiments and the overall system, is presented.

6.2 Experimental Environment

6.2.1 Software Development Environment

The algorithms for the multi-modal biometrics system are entirely implemented in Borland C++ Builder 6.0. The algorithms were developed and executed on an Intel Core 2 Quad Q9650 (3GHz, 1333MHz, 12MB). The ePadInk tablet used to create an alternative database has the following specifications: (Monochrome LCD, Touchpad resolution of 1200 x 1600 ppi (points per inch), and Tethered passive stylus).

6.2.2 Data Set

The images used in this research project are taken from three data sets: the *CASIA iris database* [23], *GPDS signature database* [37], and a database created from signatures captured using the ePadInk tablet. The CASIA iris database contains iris images from 108 people, each person has 7 images of the same eye acquired on different instances.

The GPDS signature database contains data from 300 individuals: 24 genuine signatures for each individual, and 30 samples of forgeries per each genuine signature. The forgers were allowed to practice the signatures as many times as they wished. Each forger imitated 3 signatures of 5 individual signers in a single day writing session. The genuine signatures shown to each forger are chosen randomly from the 24 genuine ones. Therefore, for each genuine signature, there are 30 skilled forgeries made by 10 forgers from 10 different genuine specimens. The database created with ePadInk tablet comprises 400 signatures from 20 individuals, 10 genuine and 10 forgeries per individual.

6.3 System Overview

The design and implementation of a multi-modal biometrics system require analysis of the biometric traits involved. This analysis gives an insight of the appropriate basic algorithms that can result in an effective system. The multi-modal biometrics authentication system architecture is depicted in Figure 6.1. The basic modules for this system are: *image acquisition*, *preprocessing*, *feature extraction*, *template creation*, *matching*, *fusion* and *decision*.

6.3.1 Iris Subsystem

An iris image is acquired as input to the subsystem. In the localization module, the inner and outer boundaries of the iris are precisely located using the integro-differential operator defined in equation (3.1) and shown in Figure 6.2(a).

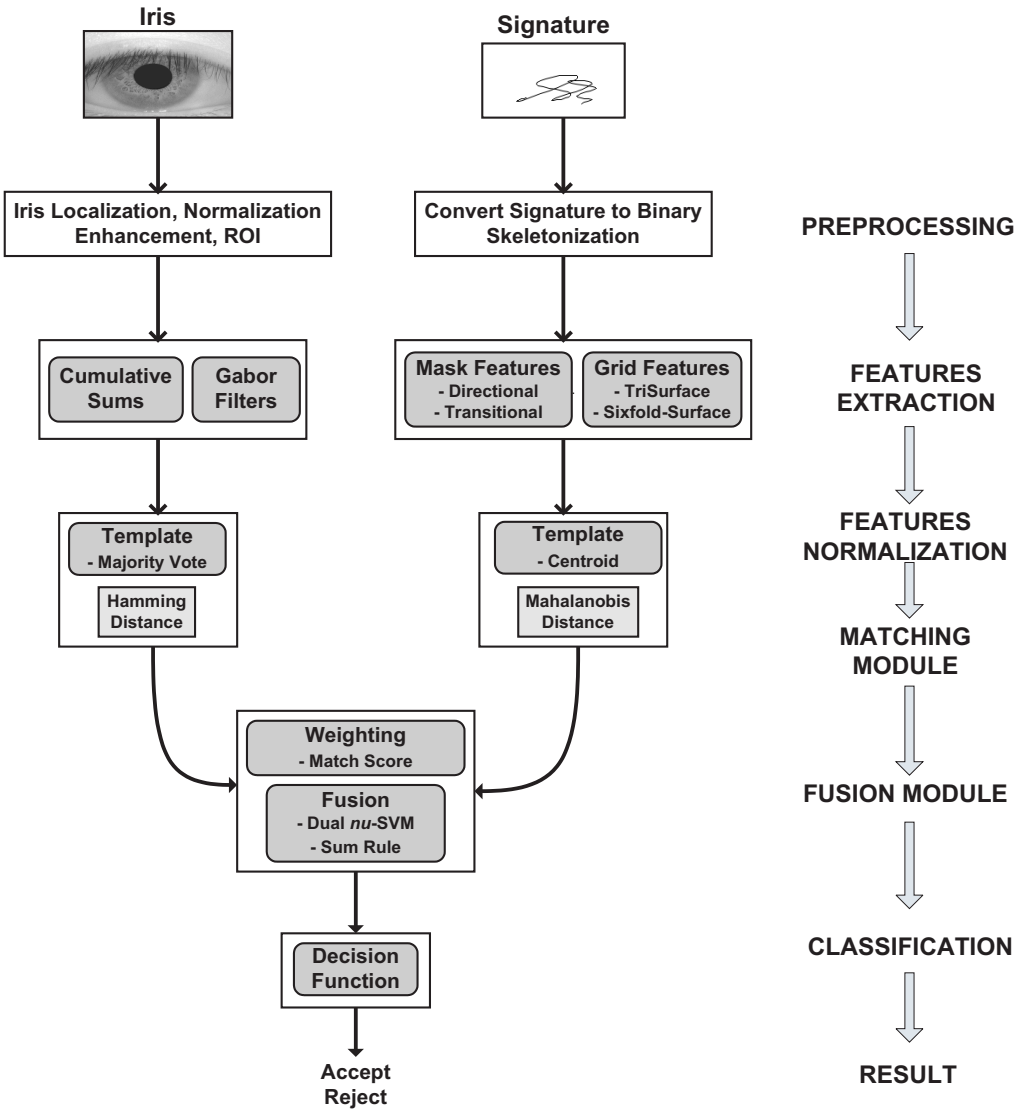
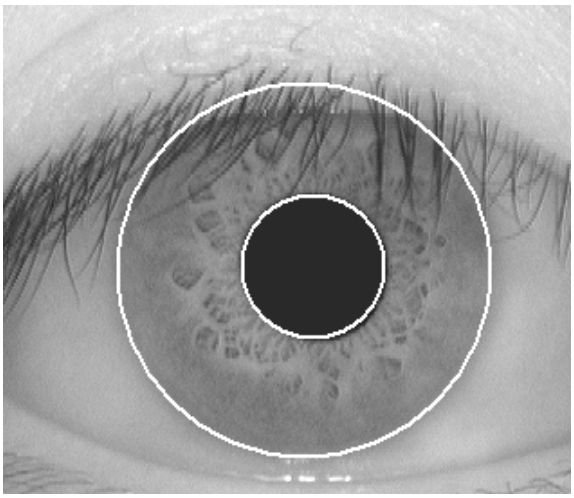
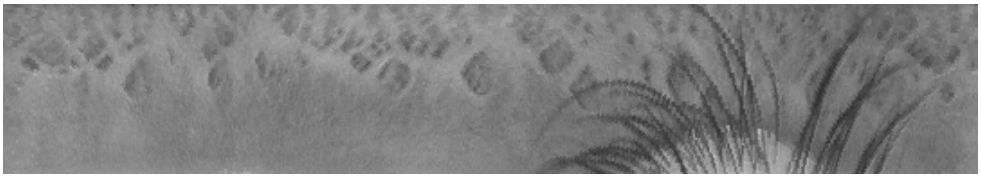


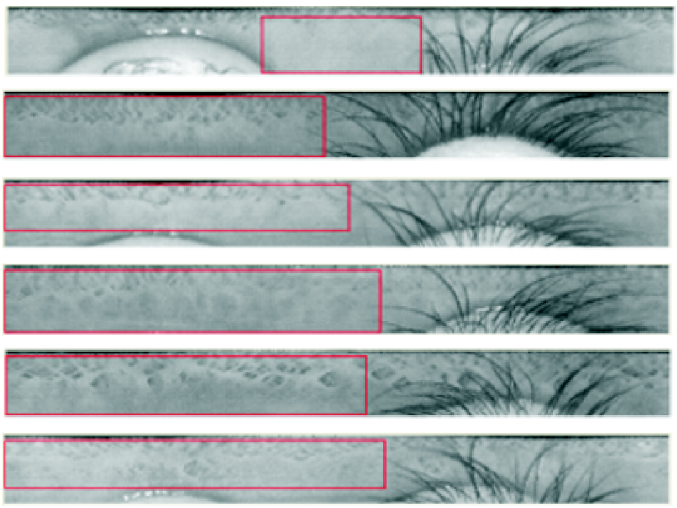
Figure 6.1: An architecture of bi-modal biometrics system based on the *iris* and *signature*



(a) Localized iris



(b) Normalized iris region



(c) Region of interest

Figure 6.2: Iris preprocessing

The localized iris region is transformed into a dimensionless polar system by projecting the original iris in a Cartesian coordinate system into a doubly pseudopolar coordinate system [38]. This method normalizes irides of different sizes to the same size by unwrapping anticlockwise the iris ring to a rectangular block with a fixed size as illustrated in Figure 6.2(b).

The algorithm for extracting the biggest possible region of interest (ROI) with minimum noise scans the binarized normalized-image horizontally and vertically to determine the length and width of the largest possible axis-parallel rectangular region of the iris without occlusions from the eye-lashes, skin, pupil, scaler, as depicted in Figure 6.2(c). Contrast enhancement is performed on the extracted iris region using a histogram based approach, which results in a well-distributed image with a more uniform histogram.

Cumulative-Sums Feature Representation

A cumulative-sums-based analysis method is used to extract features from the detected rectangular region of interest (ROI). After extracting string features from various instances of the same iris taken in different contexts such as light intensity, and distance, a prototype code or a representative iris feature code is calculated using the majority vote strategy.

In our implementation, a prototype iris feature code f is defined in equation (6.1),

$$f = (f_0 f_1, ..., f_{1023}) \tag{6.1}$$

f is a string iris feature code of dimension 1024, such that 512 characters of f are calculated horizontally and the other 512 characters are extracted vertically, where $f_i \in \{0, 1, 2\}$ and $i = 1, ..., 1023$. Examples of iris feature codes of two individuals are shown in Figure 6.3.

The matching score of the cumulative-sums iris codes, which is the Hamming Distance (HD), is calculated using equation (6.2) [38, 90]. The smaller the HD is, the higher the similarity of the compared iris codes.

$$\mathbf{HD} = \frac{1}{2N}[(\sum_{i=1}^{N} A_h(i) \oplus B_h(i)) + (\sum_{i=1}^{N} A_v(i) \oplus B_v(i))] \tag{6.2}$$

where $A_h(i)$ and $A_v(i)$ denote the enrolled iris code over horizontal and vertical directions, respectively, $B_h(i)$ and $B_v(i)$ denote the new input iris code over the horizontal and vertical directions, respectively. N is equal to 512, which is the length of either the horizontal or vertical string code component; and $\oplus$ is the XOR operator.

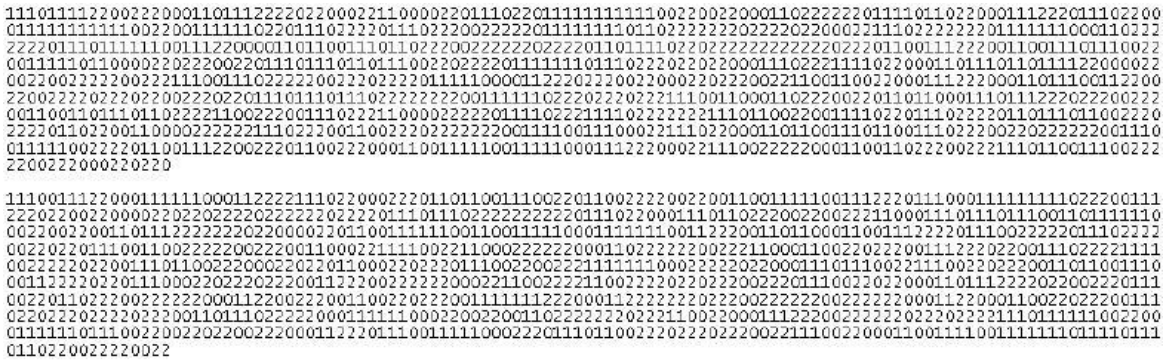


Figure 6.3: Examples of the extracted iris feature codes of two individuals

Gabor Filters Feature Representation

Alternatively, Gabor Filters are used to extract iris features from the detected region of interest. The iris texture features are extracted in the form of vectors of dimension 80 each. The iris ROI is convoluted with 40 Gabor Filters (8 orientations and 5 frequencies). Each orientation, θ_k is defined as:

$$\theta_k = \frac{\pi}{n}(k-1) \qquad k = 1, 2, ..., n \tag{6.3}$$

where n denotes the number of orientations. The radial center frequency, ω_l is given by equation (6.4).

$$\omega_l = \omega_{max}\lambda^{l-1} \qquad l = 1, 2, ..., m \tag{6.4}$$

where m is the number of frequencies, $\omega_{max} = \frac{\pi}{2}$ is the maximum value of radial frequency, and $\lambda = \sqrt{2}$ is the spacing factor between different frequencies [45, 148, 178].

The feature vector $\overrightarrow{v}$ of dimension 80 is defined as:

$$\overrightarrow{v} = (\mu_{0,0}, \sigma_{0,0}, \mu_{0,1}, \sigma_{0,1}, ..., \mu_{4,7}, \sigma_{4,7}) \tag{6.5}$$

where $\mu_{i,j}$ is the mean, and $\sigma_{i,j}$ the standard deviation, respectively, of the magnitude of Gabor coefficients at frequency ω_i and orientation θ_j. The magnitudes of Gabor coefficients represent the energy of the image at different frequencies and orientations, and are used to extract the texture properties of the image [177].

For the Gabor Filter vectors, the measure of the similarity between any two iris codes, $\overrightarrow{p} = (p_0, p_1, ..., p_{79})$ and $\overrightarrow{q} = (q_0, q_1, ..., q_{79})$, is calculated using either equation (3.40), the DU measure given by equation (3.49), or the Euclidean distance defined in equation (6.6) as:

$$D(\overrightarrow{p}, \overrightarrow{q}) = \sqrt{\sum_{i=0}^{n-1}(p_i - q_i)^2} \tag{6.6}$$

where $n = 80$, the dimension of iris feature vectors. The smaller the $D(\overrightarrow{p}, \overrightarrow{q})$ is, the higher the similarity of the compared irides.

6.3.2 Signature Subsystem

Signature images are acquired as input to the subsystem. In the preprocessing module, Hilditch's thinning algorithm, a 3×3 window version is used as the skeletonization technique [167, 174].

Then, mask and grid features that capture various structural and geometric properties of the signatures, are extracted. The extracted mask features are direction and transition features, while the grid features are tri-surface and sixfold features. The extracted 28-dimensional feature vector, $\overrightarrow{v}$, is defined as follows:

$$\overrightarrow{v} = (\underbrace{v_0,\ v_1,\ v_2}_{Tri-Surface}, \underbrace{v_3,\ v_4, ...,\ v_8}_{Sixfold}, \underbrace{v_9,\ v_{10}, ...,\ v_{18}}_{Transitional}, \underbrace{v_{19},\ v_{20}, ...,\ v_{27}}_{Directional}) \tag{6.7}$$

where $\overrightarrow{v}$ is composed of 3 tri-surface, 6 sixfold-surface, 10 transitional, and 9 directional features.

The statistical normalization technique used to transform each feature vector into a distribution with mean equal to 0 and variance of 1, is described in *subsection* 4.2.3.

The matching score between two signatures is calculated using Mahalanobis Distance (MD) as defined in equation (6.8) as:

$$MD(\overrightarrow{x}, \overrightarrow{y}) = \sqrt{(\overrightarrow{x} - \overrightarrow{y})^T S^{-1} (\overrightarrow{x} - \overrightarrow{y})} \tag{6.8}$$

where $\overrightarrow{x} = (x_0, x_1, ..., x_{27})$ and $\overrightarrow{y} = (y_0, y_1, ..., y_{27})$ denote the enrolled template and the candidate signature feature vector to be verified, respectively, with the covariance matrix S. If S is an identity matrix, the MD distance reduces to the Euclidean distance, such that:

$$MD(\overrightarrow{x}, \overrightarrow{y}) = \sqrt{\sum_{i=0}^{27} (x_i - y_i)^2} \tag{6.9}$$

However, if S is a diagonal matrix, the MD distance reduces to the normalized Euclidean

distance, defined as:

$$MD(\overrightarrow{x}, \overrightarrow{y}) = \sqrt{\sum_{i=0}^{27} \frac{(x_i - y_i)^2}{\sigma_i^2}} \tag{6.10}$$

where σ_i is the standard deviation of the x_i over the template feature vector.

The iris and signature matching scores of an individual are weighted and integrated within the *fusion module* as described below.

6.3.3 Fusion: Iris and Signature

Let ms^i_{iris} and ms^i_{sig}, be the *Tanh* normalized matching scores of iris and signature traits of the i^{th} user, respectively, with corresponding user-score-based weighted values of w^i_{iris} and w^i_{sig}, such that $w^i_{iris} + w^i_{sig} = 1$. The fusion module of the multi-modal system is based on the following algorithms:

- **Sum Rule**: The linear combination of the matching scores with their respective weights is defined as:

$$s^i_{fus} = w^i_{iris} s^i_{iris} + w^i_{sig} s^i_{sig} \tag{6.11}$$

- **2ν-SVM**: The user-specific weighted matching scores and their labels are used to train the 2ν-SVM for bimodal fusion. The fusion weighted matching score s^i_{fus} is computed in equation (6.12), and is defined in detail in section 5.3.4.

$$s^i_{fus} = f_{iris}(s^i_{iris} w^i_{iris}) + f_{sig}(s^i_{sig} w^i_{sig}) \tag{6.12}$$

where

$$f_{iris}(s^i_{iris} w^i_{iris}) = a_{iris} \varphi(s^i_{iris} w^i_{iris}) + b_{iris} \tag{6.13}$$

$$f_{sig}(s^i_{sig} w^i_{sig}) = a_{sig} \varphi(s^i_{sig} w^i_{sig}) + b_{sig} \tag{6.14}$$

where a_{iris}, a_{sig}, b_{iris} and b_{sig} are parameters of the hyperplane. The decision function defined in equation (6.15) verifies the identity of the i^{th} user using the signed distance of s^i_{fus} from the separating hyperplane given by the two 2ν-SVM for the two biometric modalities.

$$Decision(s^i_{fus}) = \begin{cases} Accept, & \text{if } s^i_{fus} > 0 \\ Reject, & \text{otherwise} \end{cases} \tag{6.15}$$

6.4 Experimental Results and Discussions

The performance of the investigated bi-modal biometrics system is evaluated by calculating its false acceptance rate (FAR) and false rejection rate (FRR) at various thresholds. These two factors are integrated together in a receiver operating characteristic (ROC) curve that plots the FRR or the genuine acceptance rate (GAR) against the FAR at different thresholds. The FAR and FRR are computed by generating all possible genuine and impostor matching scores and then setting a threshold for deciding whether to accept or reject a match.

The bi-modal database used in the experiments was constructed by merging the CASIA iris database with the GPDS signature database. An alternative bi-modal database was constructed from the CASIA iris database and a database created from signatures captured using the ePadInk tablet. Seven iris images of the same user were obtained from a set of 50 users from the CASIA database. Fifteen signatures (10 genuine and 5 forgeries) were drawn from a different set of 50 users from the GPDS database, and additional signatures were captured using ePadInk tablet. The mutual independence assumption of these biometric traits allows us to randomly pair the users from the two different sets. In this way, two bi-modal databases consisting of 50 users were constructed, either from CASIA with GPDS, or CASIA with signatures captured using ePadInk tablet.

Firstly, a thorough discussion of the results for the proposed techniques for the iris pattern recognition is carried out in subsection 3.3, while the results for the investigated signature verification is presented in subsection 4.3. The final experimental results for the

investigated bi-modal biometrics system are divided into three parts. The first experiment evaluates the performance of the two weighting techniques; the exhaustive search and the user-score-based. The second experiment compares and contrasts the performance of the three fusion algorithms investigated, (sum-rule, threshold-specific, and 2ν-SVM) when implemented with each of the weighting techniques. Finally, in the last experiment, we compare the performance of the proposed bi-modal biometric system and the other existing bi-modal systems.

6.4.1 Validation of the User-Score-Based Weighting Algorithm

In this experiment, the performance of the uni-modal biometric traits based on the iris and signature, respectively, and bi-modal traits combined using the exhaustive search technique and the user-score-based approach, respectively, is evaluated as shown by the ROC curves in Figure 6.4. The overall results show an improvement in performance when scores are combined using the user-score-based weighting technique. Furthermore, Table 6.1 shows that for a given FAR of 0.001, user-score-based weighting technique obtained a very low FRR of 0.008, compared to exhaustive search weighting with a FRR of 0.015.

The user-score-based weighting algorithm computes the weights of the iris and signature traits by analyzing how close the two matching scores are to their respective thresholds, hence associating the weights with the different degrees of importance for the bi-modal biometric traits involved. Comparatively, the exhaustive search weighting technique calculates weights that simply minimize the total error rate. This minimum error rate (the sum of FAR and FRR) does not necessarily reflect the different degrees of importance for the bi-modal biometric traits fused.

Table 6.1: Exhaustive search versus user-score-based technique on a given FAR

Weighting Technique	**FAR**	**FRR**
Exhaustive search	0.001	0.015
User-score-based	0.001	0.008

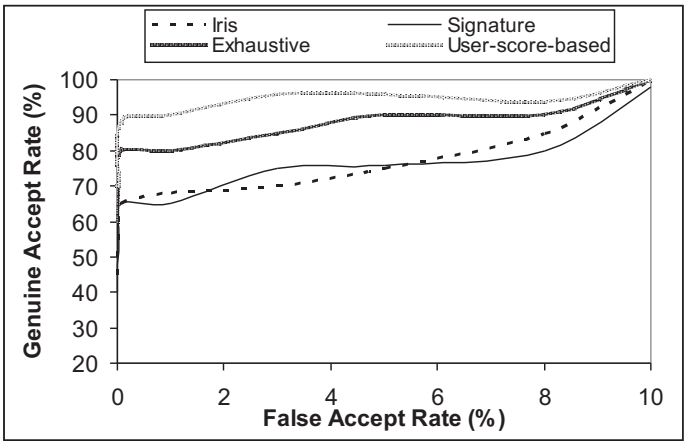


Figure 6.4: Tanh normalized-based ROC curves showing the performance of using the *iris*, *signature*, *iris + signature* (exhaustive), and *iris + signature* (user-score-based)

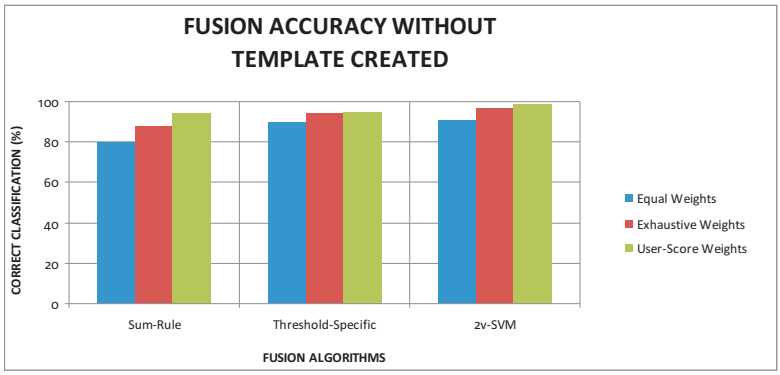


Figure 6.5: Average true positive rate without creating an iris specimen template

6.4.2 Comparison of the Fusion Algorithms

In the second experiment, we compare the performance of each of the three fusion algorithms investigated, (*sum-rule, threshold-specific, and* 2ν*-SVM*) when implemented with each of the three different weighting techniques: (the exhaustive search, the user-score-based, and the equal weights). In fact, we evaluate the performance of each fusion algorithm when implemented with each of the three weighting techniques. Figure 6.5 shows the results obtained by integrating the iris and signature traits, when the iris matching score is not computed from the specimen template. The Figure 6.5 shows that the sum-rule, threshold-specific, and 2ν-SVM fusion obtain the best success rates of 96.8%, 97.2%, and 98.0%,

respectively, when implemented with the proposed user-score-based weighting approach.

Furthermore, Figure 6.6 shows the results achieved by the three fusion algorithms, when the iris matching score is computed from the specimen template created using the majority vote based strategy as described in subsection 3.2.6. The 2ν-SVM fusion algorithm achieves the best success rate of over 99.0%, when implemented with the proposed user-score-based weighting approach as compared to the other fusion techniques.

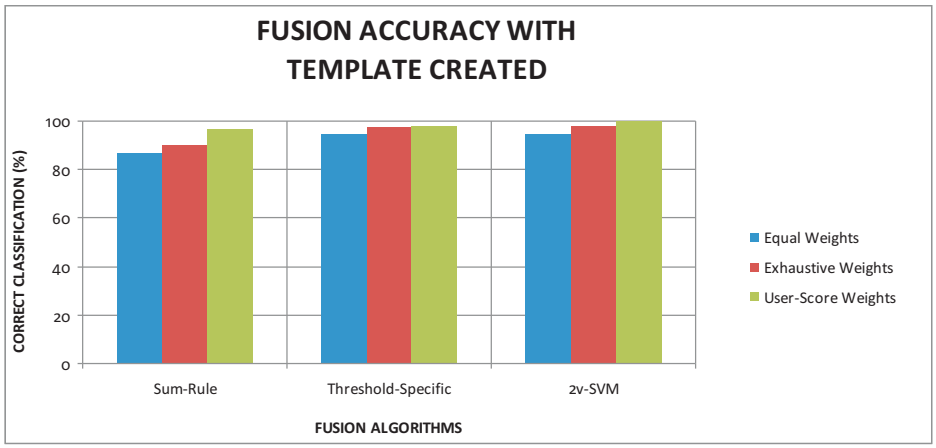


Figure 6.6: Average true positive rate with an iris specimen template created

6.4.3 Comparison with Existing Bi-modal Biometric Systems

Table 6.2 shows the performance of the user-score-based weighted fusion algorithms: sum-rule and 2ν-SVM, compared to other bi-modal biometric fusion algorithms in the literature. The quality based sum-rule [164] obtained an accuracy rate of 97.39%, when used to fuse the face and iris modalities, whereas the fusion of the iris and signature modalities based on the user-score-based weighted sum-rule achieves an accuracy rate of 97.44%. Furthermore, the Table 6.2 shows that the 2ν-SVM fusion algorithm improves the verification accuracy rates of the sum-rule fusion based on (face + iris), and (iris + signature) by 1.52% and 2.32%, respectively.

Table 6.2: Comparative table of the weighted based fusion algorithms

Biometric Modalities	**Weighted Fusion Algorithm**	**Verification Accuracy (%)**
Face + Iris	Quality based Sum-rule [164]	97.39
Face + Speech	k-NN based fusion [156]	99.72
Face + Iris	Quality based [164]	98.91
Iris + Signature	User-Score-based Weighted Sum-rule	97.44
Iris + Signature	User-Score-based Weighted 2ν-SVM	99.76

6.4.4 Statistical Evaluation of the Proposed Bi-modal Biometrics System

In order to validate the verification accuracy rates presented in this thesis, and to compare the proposed and existing techniques investigated, we used the McNemar test [47]. The McNemar test is a nonparametric statistical test which determines whether the null hypothesis holds or not. For two given algorithms, the null hypothesis, H_0, states that there is no difference between the accuracy rates of the two algorithms [47].

Let T_1 be the fusion algorithm based on the exhaustive weighting approach, and T_2 the fusion algorithm based on the proposed user-score-based weighting technique. Given the following number of cases:

- T_1 is correct and T_2 is also correct = a
- T_1 is correct and T_2 is wrong = b
- T_1 is wrong and T_2 is correct = c
- T_1 is wrong and T_2 is also wrong = d

The McNemar test computes the difference between the expected number of cases in which T_1 and T_2 provide conflicting results, and the actual number of conflicting cases using equation (6.16) [47].

$$\chi^2 = \frac{(|b-c|-1)^2}{b+c} \tag{6.16}$$

where χ^2 has a chi-squared distribution with 1 degree of freedom.

From equation (6.16), if $\chi^2 > 3.841$, the null hypothesis, H_0, is rejected, therefore, the accuracy rates obtained by the fusion algorithm based on the exhaustive weighting approach, and the fusion algorithm based on the user-score-based weighting technique are statistically different with 95% confidence [47]. However, if $\chi^2 \leq 3.841$, then the null hypothesis is accepted and the accuracy rates of the two algorithms are statistically not different.

In our case, we compared the accuracy rates obtained by each fusion algorithm when two different weighting techniques, the exhaustive approach, T_1, and the user-score-based technique, T_2, are implemented. The statistical results obtained are shown in Table 6.3. Table 6.3 shows that using the McNemar test, the accuracy rate of the user-score-based weighted 2ν-SVM fusion algorithm is statistically different from the exhaustive-based weighted 2ν-SVM fusion algorithm. Therefore, the 2ν-SVM fusion algorithm obtained better accuracy rate when the bi-modal matching scores are weighted using the proposed user-score-based technique.

Table 6.3: Statistical comparative table of the exhaustive-weighted fusion algorithms, T_1, with the user-score-weighted fusion algorithms, T_2

Algorithm		T_2 **correct**	T_2 **wrong**	χ^2	**Statistical Result**
Sum rule	T_1 **correct** T_1 **wrong**	87 9	2 2	3.273	Not Quite Statistically different
2ν-SVM	T_1 **correct** T_1 **wrong**	91 8	0 1	6.125	Statistically different

6.5 Conclusion

The experimental results of the designed bi-modal biometrics system have been presented. Statistics have been drawn to compare and contrast the effect of the investigated algorithms and techniques with related works. Innovative iris recognition techniques and novel signatures verification algorithms are consolidated to enhance the security threshold of personal authentication in bi-modal biometric systems. Hence, an efficient iris recognition algorithm that detects the largest non-occluded rectangular part of the iris as region of interest (ROI) has been investigated. A hybrid feature extraction method, cumulative-sums-based grey change analysis algorithm is used. Then, two novel techniques based on majority vote are implemented to create the specimen iris templates. Furthermore, a text-based directional signature verification algorithm, which verifies signatures even when they are composed of special unconstrained cursive characters that are superimposed and embellished, is designed.

An enhanced user-specific weighting strategy has been proposed to integrate the iris and signature traits at the matching score level using both the 2ν-SVM and sum-rule. The performance of the multi-modal biometrics system is evaluated by analyzing its error rates; false rejection rate (FRR), false acceptance rate (FAR) and the receiver operating characteristic (ROC) curves, at various user-specific thresholds.

The following chapter concludes the whole research work carried out, and highlights the shortcomings of the designed multi-modal biometrics system. The identified limitations of the system pave the way for further investigation.

Chapter 7

Conclusion and Future Work

7.1 Summary of Work

In this thesis, a framework for modeling and implementing bi-modal biometric authentication systems based on a physiological trait, the *iris* and a behavioral trait, the *signature* has been presented. Firstly, a comprehensive literature survey of the-state-of-the-art of iris recognition, signature verification, and multi-modal systems was carried out. The challenges addressed, and the novel techniques designed and investigated include:

- An algorithm that detects the largest non-occluded rectangular part of the iris as a region of interest (ROI) has been developed. The iris features codes are extracted from the detected region of interest using a cumulative-sum-based grey change analysis method. This technique can be utilized for partial iris recognition since it relaxes the requirement of using the whole part of the iris to produce an iris template.

- A solution to address the problem of computational and space complexities in iris recognition systems, a majority vote strategy has been developed in order to calculate a prototype code per individual as the representative specimen iris template.

- An efficient text-based directional signature recognition algorithm which verifies signatures, even when they are composed of special unconstrained cursive characters that are superimposed and embellished has been proposed. This algorithm extends the character-based signature verification technique.

- A user-score-based weighting technique of integrating iris and signature traits has been designed and implemented. The proposed approach calculates weights for individual

biometric traits per user in proportion to the scores of the biometric traits of the same user. The user-specific weights and their corresponding matching scores are fused using the 2ν-SVM based learning technique.

Finally, a comparative study of the above proposed approaches with the other existing techniques in the literature has been carried out. The proposed framework for modeling bi-modal biometrics system based on the *iris* (a physiological trait) and the *signature* (a behavioral trait) achieved an improved security threshold of personal authentication. For instance, the results obtained showed that the 2ν-SVM fusion algorithm achieves an accuracy rate of 99.76% when the bi-modal matching scores are weighted using the proposed user-score-based technique. The McNemar test proved that the accuracy rate of the user-score-based weighted 2ν-SVM fusion algorithm is statistically different from the other fusion approaches investigated in this research work. Furthermore, low biometrics error rates have been obtained as shown in Table 6.1.

7.2 Limitations of the System and Recommendations for Future Work

The following is a list of limitations and suggestions for improvements and future work regarding the bi-modal biometrics system based on iris and signature:

- **Data set**: The data sets used to conduct experiments are restricted to particular groups of people. For instance, the iris images are taken only from the Chinese ethnic group, various ethnic groups would possibly provide interesting insights of iris recognition. Furthermore, signature images do not include specialized handwritings like Arabic and Chinese.

- **Fusion**: Our fusion centered on matching score level only. Further investigation of the effect of other levels of fusion like feature extraction and decision is envisioned. Moreover, the extension of the multi-modal framework to other biometric traits is recommended.

- **Biometric traits**: Other atypical traits like color of eyes, gender and height of individual could be considered in conjunction with typical physiological and behavioral biometric traits to enhance performance.

Further investigation of extending the proposed framework for modeling bi-modal biometric systems to rather multi-modal biometric systems is envisioned.

Bibliography

[1] J.M.H Ali and A.E. Hassanien. An iris recognition system to enhance e-security environment based on wavelet theory. *Advanced Modelling and Optimization (AMO)*, 5, 2003.

[2] M. Ammar. Elimination of skilled forgeries in off-line systems: A breakthrough. *Proceedings of the 11th IAPR International Conference on Pattern Recognition*, pages 415 – 418, 1992.

[3] S. Armand, M. Blumenstein, and V. Muthukkumarasamy. Off-line signature verification using the enhanced modified direction feature and neural-based classification. *IEEE Proceedings, Neural Networks*, pages 684 – 691, 2006.

[4] S. Armand, M. Blumenstein, and V. Muthukkumarasamy. Off-line signature verification using an enhanced modified direction feature with single and multi-classifier approaches. *IEEE Computational Intelligence Magazine*, 2:18 – 25, 2007.

[5] A.K. Bachoo. *Comparison of Segmentation Methods for an Accurate Iris Extraction*. MSc Thesis, University of KwaZulu-Natal, 2006.

[6] A.K. Bachoo and J-R Tapamo. Texture detection for segmentation of iris images. *Proceedings of SAICSIT*, pages 236 – 243, 2005.

[7] S. Barua. Neural networks and their applications to computer security. *Proceedings of SPIE - International Society of Optical Engineering*, pages 735 – 742, 1992.

[8] S. Ben-Yacoub, Y. Abdeljaoued, and E. Mayoraz. Fusion of face and speech data for person identity verification. *IEEE Transactions on Neural Networks*, 10(5):1065 – 1075, 1999.

[9] J. Bign, E.S. Bigun, B. Duc, and S. Fischer. Expert conciliation for multimodal personal authentication systems using bayesian statistics. *International Conference on Audio and Video-Based Biometric Person Authentication (AVBPA)*, pages 291 – 300, 1997.

[10] J. Bigun, J. Fierrez-Aguilar, J. Ortega-Garcia, and J. Gonzalez-Rodriguez. Multimodal biometric authentication using quality signal in mobile communications. *IEEE Computer Society Press*, pages 2 – 11, 2003.

[11] D.A. Black. Forgery above a genuine signature. *Journal of Criminal Law, Criminology and Police Science*, 50:585 – 590, 1962.

[12] M. Blumenstein, X.Y. Liu, and B. Verma. A modified direction feature for cursive character recognition. *IEEE Proceedings, Neural Networks*, 4:2983 – 2987, 2004.

[13] M. Blumenstein and B. Verma. Neural-based solutions for the segmentation and recognition of difficult handwritten words from a benchmark database. *Fifth International Conference on Document Analysis and Recognition (ICDAR'99)*, pages 281 – 284, 1999.

[14] M. Blumenstein and B. Verma. A new segmentation algorithm for handwritten word recognition. *Proceedings of the International Joint Conference on Neural Networks (IJCNN '99)*, pages 2893 – 2898, 1999.

[15] M. Blumenstein, B. Verma, and H. Basli. A novel feature extraction technique for the recognition of segmented handwritten characters. *Proceedings of the IEEE Conference on Document Analysis and Recognition*, 1:137 – 141, 2003.

[16] W.W. Boles and B. Boashsh. A human identification technique using images of the iris and wavelet transform. *IEEE Transactions Signal Processing*, 46(4):1185 – 1188, 1998.

[17] R. Bolle, J.H. Connell, S. Pankanti, N.K. Ratha, and A.W. Senior. The relationship between the roc curve and the cmc. *Proceedings of IEEE Workshop on Automatic Identification Advanced Technologies*, pages 15 – 20, 2005.

[18] R.M. Bolle, S. Pankanti, and N.K. Ratha. Evaluation techniques for biometrics-based authentication systems. *Proceedings of International Conference on Pattern Recognition*, 2:831 – 837, 2000.

[19] A.C. Bovik, M. Clark, and W.S. Geisler. Multichannel texture analysis using localized spatial filters. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 12:55 – 73, 1990.

[20] R. Brunelli and D. Falavigna. Person identification using multiple cues. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 17(10):955 – 966, 1995.

[21] Jr. J. Campbell. Speaker recognition: A tutorial. *Proceedings of IEEE*, 85(5):1437 – 1462, 1997.

[22] D.P. Casasent, J.S. Smokelin, and A. Ye. Wavelet and gabor transforms for detection. *Optical Engineering*, 31:1893 – 1898, 1992.

[23] Casia Iris Image Database (CASIA). *<http://www.sinobiometrics.com/>*, (URL accessed on June 8, 2005).

[24] C.I. Chang. An information theoretic-based approach to spetral variability, similarity and discriminability for hyperspectral image analysis. *IEEE Transactions on Information Theory*, 46:1927 – 1932, 2000.

[25] H. D. Chang, J. F. Wang, and H. M. Suen. Dynamic handwritten chinese signature verification. *Proceedings of ICDAR'93: International Conference on Document Analysis and Recognition*, pages 258 – 261, 1993.

[26] K.I. Chang, K.W. Bowyer, and P.J. Flynn. Face recognition using 2d and 3d facial data. *Proceedings of Workshop on Multimodal User Authentication*, page 25 32, 2003.

[27] V. Chatzis, A.G. Bors, and I. Pitas. Multimodal decision-level fusion for person authentication. *IEEE Transactions on Systems, Man and Cybernetics-Part A: Systems and Humans*, 29(6):674 – 680, 1999.

[28] R. Chellappa, C.L. Wilson, and S. Sirohey. Human and machine recognition of faces: A survey. *Proceedings IEEE*, 85:705 – 740, 1995.

[29] P. H. Chen, C.J. Lin, and B. Scholkopf. A tutorial on ν-support vector machines. *Applied Stochastic Models in Business and Industry*, 21:111 – 136, 2005.

[30] Y. Chen and W. Hsu. An interpretive model of line continuation in human visual perception. *Pattern Recognition*, 22(5):619 – 639, 1989.

[31] M.C Cheung and M. Mak. A two-level fusion approach to multimodal biometric verification. *IEEE International Conference: Acoustics, Speech, and Signal Processing (ICASSP)*, 5:485 – 488, 2005.

[32] H. G. Chew, C.C. Lim, and R.E. Bogner. An implementation of training dual-nu support vector machines. *Kluwer*, 2004.

[33] R. Clarke. Human identification in information systems: Management challenges and public policy issues. *Information Technology and People*, 7:6 – 37, 1994.

[34] D.A. Clausi and M.E. Jernigan. Designing gabor filters for optimal texture separability. *Pattern Recognition*, 33:1835 – 1849, 2000.

[35] J. Coetzer, B. M. Herbst, and J. A. du Preez. Off-line signature verification using the discrete radon transform and a hidden markov model. *Eurasip Journal on Applied Signal Processing - Special Issue on Biometric Signal Procesing*, 2004(4):559 – 571, 2004.

[36] J. Coetzer, B. M. Herbst, and J. A. du Preez. Off-line signature verification: A comparison between human and machine performance. *Tenth International Workshop on Frontiers in Handwriting Recognition*, 2006.

[37] GPDS Signature Database. *<http://www.gpds.ulpgc.es/download/index.htm/>*, (URL accessed on February 20, 2008).

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

[39] J. Daugman. The importance of being random: statistical principles of iris recognition. *Pattern Recognition*, 36:279 – 291, 2002.

[40] J. Daugman. Demodulation by complex-valued wavelets for stochastic pattern recognition. *International Journal of Wavelets, Multiresolution and Information Processing*, 1:1 – 17, 2003.

[41] J. Daugman. How iris recognition works. *IEEE Transactions on Circuits and Systems for Video Technology*, 14:21 – 30, 2004.

[42] J. Daugman. New methods in iris recognition. *IEEE Transactions on Systems, MAN, and Cybernetics*, 37(5):1167 – 1175, 2007.

[43] J. Daugman and C. Downing. Effects of severe image compression on iris recognition performance. *IEEE Transactions on Information Forensics and Security*, 3(1):52 – 61, 2008.

[44] S.G. Davies. Touching big brother: How biometric technology will fuse flesh and machine. *Information Technology and People*, 7(4):38 – 47, 1994.

[45] H.B. Deng, L.W. Jin, L.X. Zhen, and J.C. Huang. A new facial expression recognition method based on local gabor filter bank and pca plus ida. *International Journal of Information Technology*, 11(11):86 – 96, 2005.

[46] U. Dieckmann, P. Plankensteiner, and T. Wagner. Sesam: A biometric personal identification system using sensor fusion. *Pattern Recognition Letters*, 18:827 – 833, 1997.

[47] T. G. Dietterich. Approximate statistical tests for comparing supervised classification learning algorithms. *Neural Computation*, 7(10):1895 – 1924, 1998.

[48] J.P. Drouhard. A neural network approach to off-line signature verification using directional pdf. *Pattern Recognition*, 29(3):415 – 424, 1996.

[49] Y. Du, B. Bonney, R. Ives, D. Etter, and R. Schultz. Analysis of partial iris recognition using a 1-d approach. *Proceedings of IEEE International Conference on Acoustics, Speech, and Signal Processing*, 2:961 – 964, 2005.

[50] Y. Du, C.I. Chang, H. Ren, C.C. Chang, J.O. Jensen, and F.M. D'Amico. A new hyperspectral discrimination measure for spectral characterization. *Optical Engineering*, 43:1777 – 1786, 2004.

[51] Y. Du, R. Ives, D. Etter, and T. Welch. A new approach to iris pattern recognition. *Proceedings of SPIE*, 5612:104 – 116, 2004.

[52] Y. Du, R. Ives, D. Etter, T. Welch, and C.I. Chang. A one-dimensional approach for iris identification. *Proceedings of SPIE*, 5404:237 – 247, 2004.

[53] D.F. Dunn and W.E. Higgins. Optimal gabor filter for texture segmentation. *IEEE Transactions on Image Processing*, 4:947 – 964, 1995.

[54] N. Duta, A.K. Jain, and K.V. Mardia. Matching of palmprints. *Pattern Recognition*, 23(4):477 – 485, 2002.

[55] A. Eriksson and P. Wretling. How flexible is the human voice? a case study of mimicry. *Proceedings of the European Conference on Speech Technology*, pages 1043 – 1046, 1997.

[56] B. Erin. Biometric passports set to take flight. *<http://www.pcworld.com/>*, (URL accessed on June 8, 2005).

[57] M. C. Fairhurst. Signature verification revisited: Promoting practical explotation of biometric technology. *Electronics and Communication Engineering Journal*, pages 273 – 280, 1997.

[58] M. Ferrer, J. Alonso, and C. Travieso. Off-line geometric parameters for automatic signature verification using fixed-point arithmetic. *IEEE Transaction on Pattern Analysis and Machine Intelligence*, 27(6):993 – 997, 2005.

[59] J. Fierrez-Aguilar, J. Ortega-Garcia, J. Gonzalez-Rodriguez, and J. Bigun. Discriminative multimodal biometric authentication based on quality measures. *Pattern Recognition Society*, 38:777 – 779, 2004.

[60] R.W. Frischholz and U. Deickmann. Bioid: A multi-modal biometric identification system. *IEEE Computer Society*, 33(2):64 – 68, 2000.

[61] P. D. Gader, M. Mohamed, and J-H. Chiang. Handwritten word recognition with character and inter-character neural networks. *IEEE Transactions on Systems, Man, and Cybernetics*, 27:158 – 164, 1997.

[62] M. Gamassi, M. Lazzaroni, M. Misino, V. Piuri, D. Sana, and F. Scotti. Accuracy and performance of biometric systems. *Instrumentation and Measurement Technology Conference*, 2004.

[63] R. Gonzalez and R. Woods. *Digital Image Processing.* Addison-Wesley Publishing, 1993.

[64] P. Grother and P.J. Philips. Models of large population recognition performance. *Proceedings of IEEE Computer Society Conference on Vision and Pattern Recognition*, 2:68 – 75, 2004.

[65] International Biometric Group. *<http://www.biometricgroup.com/reports/public/reports/>*, (URL accessed on February 20, 2006).

[66] International Biometric Group. Independent testing of iris recognition technology: Final report. *<http://www.biometricgroup.com/reports/public/ITIRT.html/>*, (URL accessed on May 15, 2008).

[67] W.R. Harrison. *Suspect Documents, their Scientific Examination.* Nelson-Hall Publishers, 1981.

[68] L. Hong. Automatic personal identification using fingerprints. *PhD Thesis, Michigan University*, 1998.

[69] L. Hong and A.K. Jain. Integrating faces and fingerprints for personal identification. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 20:1295 – 1307, 1998.

[70] L. Hong, A.K. Jain, and S. Pankanti. Can multibiometrics improve performance? *Proceedings of AutoID'99, NJ, USA*, pages 59 – 64, 1999.

[71] L. A. Hornak, S. Schuckers, A.K. Jain, and M. Schuckers. Biometric - performance, security, and societal impact statement of work. *ITR Collaborative Research, West Virginia University*, 2004.

[72] K. Huang and H. Yan. Off-line signature verification based on geometric feature extraction and neural network classification. *Pattern Recognition Letters, Elsevier*, 30(1):9 – 17, 1997.

[73] Y. Huang, S. Luo, and E. Chen. An efficient iris recognition system. *Proceedings of the First International Conference on Machine Learning and Cybernetics*, 2002.

[74] B. Jahne, H. Haubecker, and P. Geibier. *Handbook of Computer Vision and Applications*. Academic Press, 1999.

[75] A.K. Jain. *Fundamentals of Digital Image Processing*. Prentice Hall, 1988.

[76] A.K. Jain, R. Bolle, and S. Pankanti. *Biometrics, Personal Identification in Networked Society*. Kluwer Academic Publishers, 1998.

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

[78] A.K. Jain and F. Farrokhnia. Unsupervised texture segmentation using gabor filters. *Pattern Recognition*, 24:1167 – 1186, 1991.

[79] A.K. Jain, K. Nandakumar, and A. Ross. Score normalization in multimodal biometrics systems. *Pattern Recognition Letters*, (38):2270 – 2285, 2005.

[80] A.K. Jain, S. Prabhakar, and S. Chen. Combining multiple matchers for a high security fingerprint verification system. *Pattern Recognition Letters*, 20:1371 – 1379, 1999.

[81] A.K. Jain, N.K. Ratha, and S. Lakshmanan. Object detection using gabor filters. *Pattern Recognition*, 30:295 – 309, 1991.

[82] A.K. Jain and A. Ross. Learning user-specific parameters in a multi-biometric system. *Proceedings International Conference on Image Processing*, pages 22 – 25, 2002.

[83] A.K. Jain and A. Ross. Multibiometric systems. *Communications of the ACM*, 47, 2004.

[84] A.K. Jain, A. Ross, and S. Pankanti. Biometrics: A tool for information security. *IEEE Transactions on Information Forensics and Security*, 1(2):125 – 143, 2006.

[85] A.K. Jain, A. Ross, and S. Prabhakar. An introduction to biometric recognition. *IEEE Transactions on Circuits and Systems for Video Technology*, 14:4 – 20, 2004.

[86] E.J.R. Justino, F. Bortolozzi, and R. Sabourin. Off-line signature verification using hmm for random, simple and skilled forgeries. *International Conference on Document Analysis an Recognition*, 1:169 – 181, 2001.

[87] E.J.R. Justino, A.E. Yacoubi, F. Bortolozzi, and R. Sabourin. An off-line signature verification system using hmm and graphometric features. *IAPR International Workshop on Document Analysis Systems*, pages 211 – 222, 2000.

[88] M. Kass, A. Witkin, and D. Terzopoulos. Snakes: Active contour models. *International Journal on Computer Vision*, 1(4):321 – 331, 1988.

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

[90] J.G. Ko, Y.H. Gil, J.H. Yoo, and K.IL. Chung. A novel and efficient feature extraction method for iris recognition. *ETRI Journal*, 29(3):399 – 401., 2007.

[91] G. Krishnan and D. Jones. Machine verification of traced signatures. *Proceedings of SPIE - International Society of Optical Engineering*, pages 563 – 572, 1991.

[92] P. Kruizinga, N. Pekov, and S.E. Grigorescu. Comparison of texture features based on gabor filters. *International Conference on Image Analysis and Processing, Proceedings*, pages 142 – 147, 1999.

[93] P. Kruizinga and N. Petkov. Nonlinear operator for orientated texture. *IEEE transactions on image processing*, 8:1395 – 1407, 1999.

[94] A. Kumar, D.C.M. Wong, H.C. Shen, and A.K. Jain. Personal verification using palmprint and hand geometry biometric. *International Conference on Audio and Video-Based Biometric Person Authentication (AVBPA)*, pages 668 – 678, 2003.

[95] L.I. Kuncheva, C.J. Whitaker, and R.P.W. Duin. Is independence good for combining classifiers? *Proceedings of International Conference on Pattern Recognition*, 2:168 – 171, 2000.

[96] M. Kuriko. Japanese airport tests biometric security. *<http://www.pcworld.com/>*, (URL accessed on June 8, 2005).

[97] C. Lakshmi and A. Kandaswamy. An algorithm for improved accuracy in unimodal biometric systems through fusion of multiple features sets. *ICGST-GVIP Journal*, 9(3):33 – 40, 2009.

[98] M. Lalonde and J. J. Brault. A neural network approach to handwritten curve partitioning. *Proceedings of Vision Interface*, pages 136 – 141, 1989.

[99] L. Lam, S.W. Lee, and C.Y. Suen. Thinning methodologies-a comprehensive survey. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 14(9):869 – 886, 1992.

[100] F. Leclerc and R. Plamondon. Automatic signature verification: The state of the art - 1989-1993. *International Journal of Pattern Recognition and Artificial Intelligence: Special Issue on Signature Verification*, 8(3):643 – 660, 1994.

[101] L. Lee, T. Berger, and E. Aviczer. Reliable on-line human signature verification systems. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 18(6):643 – 647, 1996.

[102] S.Z. Li and A.K. Jain. *Handbook of Face Recognition*. Springer-Verlag, 2005.

[103] S. Lim, K. Lee, O. Byeon, and T. Kim. Efficient iris recognition through improvement of feature vector and classifier. *ETRI Journal*, 23(2):61 – 70, 2001.

[104] M.W. Lin, J.R. Tapamo, and B. Ndovie. A texture-based method for document segmentation and classification. *South African Computer Journal*, 36:49 – 56, 2006.

[105] X.Y. Liu and M. Blumenstein. Experimental analysis of the modified direction feature for cursive character recognition. *Ninth International Workshop on Frontiers in Handwriting Recognition (IWFHR'04)*, pages 353 – 358, 2004.

[106] X. Lu, Y. Wang, and A.K. Jain. Combining classifiers for face recognition. *IEEE Proceedings Inernational Conference on Multimedia and Expo (ICME)*, 3:13 – 16, 2003.

[107] H. Lv, W. Wang, C. Wang, and Q. Zhuo. Off-line chinese signature verification based on support vector machine. *Pattern Recognition Letters, Elsevier*, 26:2390 – 2399, 2005.

[108] L. Ma, T. Tan, Y. Wang, and D. Zhang. Personal identification based on iris texture analysis. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 25, 2003.

[109] D. Maio, D. Maltoni, J.L. Wayman, and A.K. Jain. Third fingerprint verification competition. *Proceedings of International Conference on Biometric Authentication*, pages 1 – 7, 2004.

[110] D. Maltoni, D. Maio, A.K. Jain, and S. Prabhakar. *Handbook of Fingerprint Recognition*. Springer, 2003.

[111] T. Matsumoto, H. Matsumoto, K. Yamada, and S. Hoshino. Impact of artficial gummy fingers on fingerprint systems. *Proceedings of SPIE on Optical Security and Counterfeit Deterrence Techniques*, 4677:275 – 289, 2002.

[112] A. Maura. The business case for biometrics: Bank systems and technology. *<http://www.banktech.com/>*, (URL accessed on June 29, 2005).

[113] U. Meier, W. Hurst, and P. Duchnowski. Adaptive bimodal sensor fusion for automatic speech reading. *IEEE International Conference: Acoustics, Speech, and Signal Processing (ICASSP)*, pages 833 – 836, 1996.

[114] A. Mitra, P. Kumar, and C. Ardil. Automatic authentication of handwritten documents via low density pixel measurements. *International Journal of Computational Intelligence*, 2(4):219 – 223, 2006.

[115] V.S. Nalwa. Automatic on-line signature verification. *Proceedings of IEEE*, 85(2):215 – 239, 1997.

[116] K.R. Namuduri, R. Mehrotra, and N. Ranganathan. Efficient computation of gabor filter based multiresolution responses. *Pattern Recognition*, 27:925 – 938, 1994.

[117] C. Neti, G. Potamianos, J. Luettin, I. Matthews, H. Glotin, D. Vergyri, J. Sison, A. Mashari, and J. Zhou. Audio-visual speech recognition. *Final Workshop 2000 Report, Center for Language and Speech Processing, The Johns Hopkins University, Baltimore*, 2000.

[118] V. Nguyen, M. Blumenstein, V. Muthukkumarasamy, and G. Leedham. Off-line signature verification using enhanced modified direction features in conjuction with neural classifiers and support vector machines. *IEEE Proceedings, Document Analysis and Recognition*, 2:734 – 738, 2007.

[119] M. Nixon and A. Aguado. *Feature Extraction and Image Processing, Second Edition.* Academic Press, 2008.

[120] Glossary of Terms. *<http://www.data-core.com/glossary-of-terms.html/>*, (URL accessed on February 20, 2006).

[121] L. O'Gorman. *Guarding Your Business: An Architecture for Security.* Kluwer Press, 2004.

[122] L. O'Gorman, M.J. Sammon, and M. Seul. *Practical Algorithms for Image Analysis, Second Edition.* Cambridge University Press, 2008.

[123] E. Ozgunduz, T. Penturk, and M. E. Karslygil. Off-line signature verification and recognition by support vector machine. *Eusipco Proceedings*, 2005.

[124] J.R. Parker. *Algorithms for Image Processing and Computer Vision.* Wiley Computer Publishing, 1997.

[125] M. Petrou and P. Garcia Sevilla. *Image Processing, Dealing with Texture.* John Wiley and Sons, Ltd, 2006.

[126] S Prabhakar. *Fingerprint Classification and Matching using a Filterbank.* PhD Thesis, Michigan University, 2001.

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

[128] S. Prabhakar, S. Pankanti, and A.K. Jain. Biometric recognition: Security and privacy concerns. *IEEE Security and Privacy Magazine*, 1(2):33 – 42, 2003.

[129] T. Putte and J. Keuning. Boimetric fingerprint recognition: Dont get fingers burned. *Proceedings of IFIP Conference on Smart Card Research and Advanced Applications*, pages 289 – 303, 2000.

[130] S. Rakshit and D.M. Monro. An evaluation of image sampling and compression for human iris recognition. *IEEE Transactions on Information Forensics and Security*, 2(3):605 – 612, 2007.

[131] K. A. Rhodes. Information security: Challenges in using biometrics. *GAO-03-1137T*, 2003.

[132] G. Rigoll and A. Kosmala. A systematic comparison between on-line and off-line methods for signature verification with hidden markov models. *International Conference on Pattern Recognition*, 2:1755 – 1757, 1998.

[133] Z. Riha and V. Matyas. Biometric authentication systems. *FIMU Report Series*, 2000.

[134] G. Ritter and J. Wilson. *Handbook of Computer Vision Algorithms in Image Algebra,* Second Edition. CRC Press, 2001.

[135] A. Ross. Information fusion in fingerprint authentication. *PhD Thesis, Michigan University*, 2001.

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

[137] A. Ross and A.K. Jain. Multimodal biometrics: An overview. *Proceedings of European Signal Processing Conference*, pages 1221 – 1224, 2004.

[138] A. Ross and A.K. Jain. Human recognition using biometrics: An overview. *Annals of Telecommunications*, 62:11 – 35, 2007.

[139] R. Sabourin. Off-line signature verification: Recent advances and pespectives. *Proceedings of the First Brazilian Symposium on Advances in Document Image Analysis*, pages 84 – 98, 1997.

[140] R. Sabourin and G. Genest. An extended -shadow-code based approach for off-line signature verification: Part i evaluation of the bar mask definition. *IAPR International Conference on Pattern Recognition*, pages 450 – 455, 1994.

[141] R. Sabourin and R. Plamondon. Off-line signature verification using directional pdf and neural networks. *Proceedings of the 11th IAPR International Conference on Pattern Recognition*, pages 321 – 325, 1992.

[142] R. Sabourin, R. Plamondon, and G. Lorette. Off-line identification with handwriteen signatures image: Survey and pespectives. *Proceedings of SSPR'90: Syntactic and structural Pattern Recognition*, pages 377 – 391, 1990.

[143] C. Sanderson and K. K. Paliwal. Noise compensation in a person verification system using face and multiple speech features. *Pattern Recognition Letters*, 36:293 – 302, 2003.

[144] C. Sansone and M. Vento. Signature verification: Increasing performance by a multi-stage system. *Pattern Analysis and Applications, Springer*, 3:169 – 181, 2000.

[145] B. Schafer and S. Viriri. An adaptive off-line signature verification system. *Proceedings of IEEE International Conference on Signal and Image Processing Applications*, 2009.

[146] B. Schlkopf, B. Scholkopf Gmd, A.J. Smola, R. Williamson, and P. Bartlett. New support vector algorithms. *Neural Computation*, 12:1083 – 1121, 2000.

[147] R.A. Schowengerdt. *Remote Sensing: Models and Methods for Image Processing, Second Edition*. Academic Press, 1997.

[148] L. Shen and L. Bai. Information theory for gabor feature selection for face recognition. *Journal on Applied Signal Processing*, 2006(1):1 – 11, 2006.

[149] R. Snelick, U. Uludag, A. Mink, M. Indovina, and A.K. Jain. Large-scale evaluation of multimodal biometric authentication using state-of-the-art systems. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 27(3):450 – 455, 2005.

[150] M. Sonka, V. Hlavac, and R. Boyle. *Image Processing, Analysis and Machine Vision*. PWS Publishing, 1999.

[151] C. Soutar. Biometric system security white paper, bioscrypt [online]. *<http://www.bioscrypt.com/>*, (URL accessed on September 20, 2009).

[152] H. Srinivasan, S.N. Srihari, and M.J. Beal. Signature verification using kolmogorov-smirnov statistic. *Proceedings of International Graphonomics Society Conference (IGS)*, pages 152 – 156, 2005.

[153] J.A. Swets, W.P. Tanner, and T.G. Birdsall. Decision processes in perception. *Psychological Review*, 68(5):301 – 340, 1961.

[154] W.A. Taylor. Change-point analysis: A powerful new tool for detecting changes. *<http://www.variation.com/cpa/tech/changepoint.html>*, (URL accessed on November 10, 2007).

[155] A. Tefas, C. Kotropoiilos, and I. Pitas. Using support vector machines to enhance the performance of elastic graph matching for frontal face authentication. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 23(7):735 – 746, 2001.

[156] A. Teoh, S. A. Samad, and A. Hussain. Nearest neighbourhood classifiers in a bimodal biometric verification system fusion decision scheme. *Journal of Research and Practice in Information Technology*, 36(1), 2004.

[157] C. Tisse, L. Martin, L. Torres, and M. Robert. Personal identification technique using human iris recognition. *Proceedings of Vision Interface*, pages 294 – 299, 2002.

[158] T.M.Martinetz and K.J.Schulten. A neural gas network learns topologies, in artificial neural networks. *Elsevier Science Publishers*, pages 397 – 402, 1991.

[159] V. truc and N. Paveic. A comparison of feature normalization techniques for pca-based palmprint recognition. *Proceedings of the international conference MATHMOD 2009*, pages 2450 – 2453, 2009.

[160] M. van Droogenbroeck. Algorithms for openings of binary and label images with rectangular structuring elements. *Proceedings of ISMM2002, CSIRO Publishing*, pages 197 – 207, 2002.

[161] V. Vapnik and S.E. Golowich. Support vector method for function approximation, regression estimation and signal processing. *Advances in Neural Information Processing Systems*, 9:281 – 287, 1997.

[162] J. Vargas, M. Ferrer, C. Travieso, and J. Alonso. Off-line signature verification based on high pressure polar distribution. *International Conference on Frontiers in Handwriting Recognition, ICFHR 2008*, 2008.

[163] J. Vargas, M. Ferrer, C. Travieso, and J. Alonso. Off-line signature verification based on pseudo-cestral coefficients. *International Conference on Document Analysis and Recognition, ICDAR 2009*, pages 126 – 130, 2009.

[164] M. Vatsa, R. Singh, and A. Noore. Integrating image quality in 2ν-svm biometric match score fusion. *International Journal of Neural Systems*, 17(5):343 – 351, 2007.

[165] P. Verlinde and G. Cholet. Comparing decision fusion paradigms using k-nn based classifiers, decision trees and logistics regression in multi-modal identity verification application. *International Conference on Audio and Video-Based Biometric Person Authentication (AVBPA)*, pages 188 – 193, 1999.

[166] S. Viriri and J-R. Tapamo. Improving iris-based personal identification using maximum rectangular region detection. *IEEE Computer Society, Digital Image Processing, Proceedings*, 11:421 – 425, 2009.

[167] S. Viriri and J-R. Tapamo. Signature verification based on handwritten text recognition. *Lecture Notes in Computer Science (LNCS) - Springer-Verlag Berlin Heidelberg*, pages 98 – 105, 2009.

[168] S. Viriri and J-R. Tapamo. Biometrics and banking systems in the african context. *IST-Africa Conference Proceedings, P. Cunmingham and M. Cunmingham(eds), IIMC International Information Management Coorporation*, May 2006.

[169] Y. Wang and J. Han. Iris recognition using independent component analysis. *International Conference on Machine Learning and Cybernetics*, pages 18 – 21, 2005.

[170] H.P. Wasserman. *Ethinc Pigmentation*. Elsevier, 1974.

[171] R. Wildes. Iris recognition: An emerging biometric technology. *Proceedings of IEEE*, 85(9):1348 – 1363, 1997.

[172] T. S. Wilkinson and J. W. Goodman. Slope histogram detection of forged handwritten signatures. *Proceedings of SPIE - International Society of Optical Engineering*, pages 293 – 304, 1990.

[173] S. Yang and I. Verbauwhede. Secure iris verification. *IEEE, Acoustics, Speech and Signal Processing, Proceedings*, 2:133 – 136, 2007.

[174] M. Yin and S. Narita. Speedup method for real-time thinning algorithm. *International Conference on Digital Image Computing Techniques and Applications*, 2002.

[175] B. Zhang, M. Fu, and H. Yan. Handwritten signature verification based on neural 'gas' based vector quantization. *IEEE International Joint Conference on Neural Networks*, 2:1862 – 1864, 1998.

[176] D. Zhang, W.K. Kong, J. You, and M. Wong. Online palmprint identification. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 25(9):1041 – 1050, 2003.

[177] D. Zhang, A. Wong, M. Indrawan, and G. Lu. Content-based image retrieval using gabor feature texture features. *Proceedings of First IEEE Pacific-Rim Conference on Multimedia*, pages 1 – 9, 2001.

[178] M. Zhou, H. Wei, and S. Maybank. Gabor wavelets and adaboost in feature selection for face verification. *Proceedings of Applications of Computer Vision*, pages 101 – 109, 2006.

[179] Y. Zhu, T. Tan, and Y. Wang. Biometric personal identification based on handwriting. *Chinese Academy of Sciences*, 1999.

[180] Y. Zhu, T. Tan, and Y. Wang. Biometric personal identification based on iris patterns. *Proceedings of IEEE Pattern Recognition*, 2:801 – 804, 2000.

[181] Y. Zuev and S. Ivanon. The voting as a way to increase the decision reliability. *Foundations of Information/Decision Fusion with Applications to Engineering Problems*, pages 206 – 210, 1996.

[182] R. Zunkel. *Hand Geometry Based Authentication*. Kluwer Academic Publishers, 1999.