Advancing Iris Biometric Technology

Mohammed A. M. Abdullah

Newcastle University

Newcastle-upon-Tyne, UK

A thesis submitted for the degree of

Doctor of Philosophy

2017

TO

my parents,

my beloved wife, **Maab**

AND

my loving sons, **Zakariya & Zain**.

Declaration

I, Mohammed Abdulmuttaleb M. Abdullah, hereby declare that this thesis is my own work and effort and that it has not been submitted anywhere for any award.

Signature:

Student: Mohammed Abdulmuttaleb M. Abdullah

Date:

Abstract

The iris biometric is a well-established technology which is already in use in several nation-scale applications and it is still an active research area with several unsolved problems. This work focuses on three key problems in iris biometrics namely: segmentation, protection and cross-matching. Three novel methods in each of these areas are proposed and analyzed thoroughly.

In terms of iris segmentation, a novel iris segmentation method is designed based on a fusion of an expanding and a shrinking active contour by integrating a new pressure force within the Gradient Vector Flow (GVF) active contour model. In addition, a new method for closed eye detection is proposed. The experimental results on the CASIA V4, MMU2, UBIRIS V1 and UBIRIS V2 databases show that the proposed method achieves state-of-the-art results in terms of segmentation accuracy and recognition performance while being computationally more efficient. In this context, improvements by 60.5%, 42% and 48.7% are achieved in segmentation accuracy for the CASIA V4, MMU2 and UBIRIS V1 databases, respectively. For the UBIRIS V2 database, a superior time reduction is reported (85.7%) while maintaining a similar accuracy. Similarly, considerable time improvements by 63.8%, 56.6% and 29.3% are achieved for the CASIA V4, MMU2 and UBIRIS V1 databases, respectively.

With respect to iris biometric protection, a novel security architecture is designed to protect the integrity of iris images and templates using watermarking and Visual Cryptography (VC). Firstly, for protecting the iris image, text which carries personal information is embedded in the middle band frequency region of the iris image using a novel watermarking algorithm that randomly interchanges multiple middle band pairs of the Discrete Cosine Transform (DCT). Secondly, for iris template protection, VC is utilized to protect the

iris template. In addition, the integrity of the stored template in the biometric smart card is guaranteed by using the hash signatures. The proposed method has a minimal effect on the iris recognition performance of only 3.6% and 4.9% for the CASIA V4 and UBIRIS V1 databases, respectively. In addition, the VC scheme is designed to be readily applied to protect any biometric binary template without any degradation to the recognition performance with a complexity of only $O(N)$.

As for cross-spectral matching, a framework is designed which is capable of matching iris images in different lighting conditions. The first method is designed to work with registered iris images where the key idea is to synthesize the corresponding Near Infra-Red (NIR) images from the Visible Light (VL) images using an Artificial Neural Network (ANN) while the second method is capable of working with unregistered iris images based on integrating the Gabor filter with different photometric normalization models and descriptors along with decision level fusion to achieve the cross-spectral matching. A significant improvement by 79.3% in cross-spectral matching performance is attained for the UTIRIS database. As for the PolyU database, the proposed verification method achieved an improvement by 83.9% in terms of NIR vs Red channel matching which confirms the efficiency of the proposed method.

In summary, the most important open issues in exploiting the iris biometric are presented and novel methods to address these problems are proposed. Hence, this work will help to establish a more robust iris recognition system due to the development of an accurate segmentation method working for iris images taken under both the VL and NIR. In addition, the proposed protection scheme paves the way for a secure iris images and templates storage. Moreover, the proposed framework for cross-spectral matching will help to employ the iris biometric in several security applications such as surveillance at-a-distance and automated watch-list identification.

Statement of Originality

This is to certify that to the best of my knowledge, the content of this thesis is my own work. This thesis has not been submitted for any degree or other purposes.

 This thesis has three contribution chapters and the publications arising from these chapters are listed below.

1. **Chapter 4: Iris Segmentation with the Active Contour Model**

   - **M. A. M. Abdullah**, S. S. Dlay, W. L. Woo and J. A. Chambers "Robust iris segmentation method based on a new active contour force with a noncircular normalization," *IEEE Transactions on System, Man and Cybernetics: Systems*, vol. In press, pp. 1-14, May, 2016.

   - **M. A. M. Abdullah**, S. S. Dlay and W. L. Woo "Fast and accurate method for complete iris segmentation with active contour and morphology," *2014 IEEE International Conference on Imaging Systems and Techniques (IST2014)*, pp.123-128, 2014.

   - **M. A. M. Abdullah**, S. S. Dlay and W. L. Woo "Fast and accurate pupil isolation based on morphology and active contour," *The 4th International conference on Signal, Image Processing and Applications*, pp. 418-420, 2014.

2. **Chapter 5: Iris Biometrics Protection with Watermarking and Visual Cryptography**

   - **M. A. M. Abdullah**, S. S. Dlay, W. L. Woo and J. A. Chambers "A framework for iris biometric protection: A marriage between watermarking and visual cryptography," *IEEE Access*, vol. 4, pp. 10180-10193, November, 2016.

   - **M. A. M. Abdullah**, S. S. Dlay and W. L. Woo "Securing iris images with a robust watermarking algorithm based on discrete cosine transform," *10th International Conference on Computer Vision Theory and Applications (VISAPP 2015)*, pp. 108-114, 2015.

3. **Chapter 6: Cross-spectral Iris Matching**

- **M. A. M. Abdullah**, R. R Al-Nima, S. S. Dlay, W. L. Woo and J. A. Chambers "Cross-spectral iris matching for surveillance applications," *Surveillance in Action*, Book section, Springer, In press, 2017.

- **M. A. M. Abdullah**, S. S. Dlay, W. L. Woo and J. A. Chambers "A novel framework for cross-spectral iris matching," *IPSJ Transactions on Computer Vision and Applications*, vol. 8, pp. 1-9, November, 2016. (**Invited**)

- **M. A. M. Abdullah**, S. S. Dlay, W. L. Woo and J. A. Chambers "Iris biometric: Is the near-infrared spectrum always the best?," *3rd Asian Conference on Pattern Recognition (ACPR2015)*, pp. 816-819, 2015.

4. **Other contributions**

- S.A.M.Al-Sumaidaee, **M. A. M. Abdullah**, R.R.O.Al-Nimaa, S.S. Dlay and J. A. Chambers "Multi-gradient features and elongated quinary pattern encoding for image-based facial expression recognition," Pattern Recognition, vol. 71, pp. 249-263, November, 2017.

- R.R.O.Al-Nima, **M. A. M. Abdullah**, M.T.S. Al-Kaltakchi, S.S. Dlay, W. L. Woo and J. A. Chambers "Finger texture biometric verification exploiting Multi-scale Sobel Angles Local Binary Pattern features and score-based fusion," Digital Signal Processing, vol. 70, pp. 178-189, November, 2017.

Acknowledgments

I am using this opportunity to express my sincere gratitude to many kind people around me who supported me throughout my PhD study. It would not have been possible to write this thesis without their help and support, to whom I would like to give particular mention here.

First and foremost I wish to thank my first supervisors, Prof. Jonathon Chambers and Prof. Satnam Dlay, for their inspirational guidance and constructive criticism which paved the way during my study. I received unlimited help and support, from them I learned how to think positively and how to be a successful researcher. I would also like to express my great appreciation to my third supervisor, Dr. Wai Woo, for his invaluable advices. I am sincerely grateful to all of my supervisors for being supportive and helpful since the days I began working on my project.

I would like to show my deepest appreciation to the Ministry of Higher Education and Scientific Research in Iraq for the award of a fully-sponsored scholarship that provided the necessary financial support during my PhD study. I also would like to acknowledge the academic and technical support of the Iraqi cultural attache in London and the University of Mosul and Ninevah University for providing me with study leave to gain the degree of PhD from Newcastle University. I also thank the School of Electrical and Electronic Engineering for their assistance and support since my first day in the school, especially the kind Postgraduate Research Coordinator, Gillian Webber and the lovely Receptionist, Deborah Alexander.

I owe a very important debt to my parents, brother and sisters who have given me their endless love and support throughout. Without their encouragement, this thesis would not have been written.

Last but not least, my heartfelt appreciation goes to my wife, Maab, and my sons, Zakariya & Zain for their support and great patience at all times. From them I stole great moments and special days for the sake of study. They offered me all these sacrifices without showing any grievance. My lovely family has been a constant source of love, motivation and energy, for which my mere expression of thanks is really inadequate.

Contents

List of Acronym

ANN	Artificial Neural Networks
AWGN	Additive White Gaussian Noise
BER	Bit Error Rate
BSIF	Binarized Statistical Image Feature
CDMA	Code Division Multiple Access
CHT	Circular Hough Transform
DCT	Discrete Cosine Transform
DET	Detection Error Trade-off
DoG	Difference of Gaussian
DWT	Discrete Wavelet Transform
DWT-PN	Discrete Wavelet Transform with Pseudo Noise
EER	Equal Error Rate
FAR	False Accept Rate
FFNN	Feed Forward Neural Network
FRR	False Reject Rate
GAR	Genuine Acceptance Rate
IDO	Integro-Differential Operator

JPEG	Joint Photograph Expert Group
LSB	Least Significant Bit
MICHIE	Mobile Iris Challenge Evaluation
MSW	Multi-Scale Weberface
NICE	Noisy Iris Challenge Evaluation
NIR	Near Infra-Red
NIST	National Institute of Standards and Technology
PSNR	Peak Signal to Noise Ratio
ROC	Receiver Operating Characteristic
SVD	Singular Value Decomposition
VL	Visible Light
VC	Visual Cryptography

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Introduction

Biometrics is the science of establishing human identity using physiological traits found in the face, a finger and the iris; or behavioral traits present in the voice and signature. The term Biometrics is derived from the Greek words "bios" and "metric" which means life measurement. Biometrics technologies generally involve measuring different sets of physiological and behavioral traits. The identity of an individual can be established by extracting measurable information from such traits which can be used later for authentication [1].

Basically, biometric systems operate in the same manner. Firstly, a biometric trait is captured then a set of unique feature are extracted which are then stored as biometric templates. To establish the identity, an individual unique feature is extracted and compared against a biometric database. A good biometric trait should have two characteristics: distinctiveness and stability. A distinctive biometric trait is unique to an individual whereas a stable one does not change over time [2].

This chapter gives a brief overview of biometric traits and their characteristics. In addition, biometric systems and their mode of functioning are presented. Finally, the contributions of this work are listed and the structure of the thesis is outlined.

1.2 Biometric Traits

Biometric systems use different human characteristics. In biometric society, these characteristics are known as traits, indicators or modalities which can be classified into two main categories: physical traits and behavioral traits. Biometric authentication using physical traits aims to measure unique human characteristics such as iris texture, sclera and retina blood vessel patterns and the shape or size of palm prints. On the other hand, behavioral biometrics measure learned traits such as gait pattern, keystroke, a person's signature and voice [2].

The choice of a suitable biometric trait can be difficult as a variety of biometric traits are available and each has its own advantages and disadvantages. Generally speaking, seven main factors should be considered when selecting a biometrics trait. These factors

can be summarized as follows [3]:

1. Universality: The trait should be available in every one accessing the system.

2. Permanence: The trait should be stable and not change significantly over time.

3. Uniqueness: The trait should be different among individuals. This means that it is possible to distinguish the individual with the available means.

4. Collectability: It should be possible to measure the trait within a reasonable amount of time.

5. Circumvention: Refers to the possibility of imitating the trait to get an unauthorized access.

6. Acceptability: This depends on how invasive is the process of collecting the biometric trait. For example, retina scan has a low acceptability due to its invasive collection method and also it may reveal some medical condition about the patients such as diabetes.

7. Performance: In general, a good biometric trait should have a reasonable accuracy.

No single biometric trait is considered to be ideal (meets all the aforementioned requirements) but some of these traits are admissible. In general, selecting a suitable trait often depends on the application.

1.3   Common Biometric Traits

Several biometric methods have been suggested during the last decades yet only a few have gained attention. Fig. 1.1 depicts the most commonly used biometric traits. A survey of these traits is presented in the next subsection.

1.3.1   Fingerprint Recognition

Fingerprint recognition is one of the most widely deployed biometrics. Fingerprint recognition operates by extracting unique features from a fingerprint such as ridges and minutia
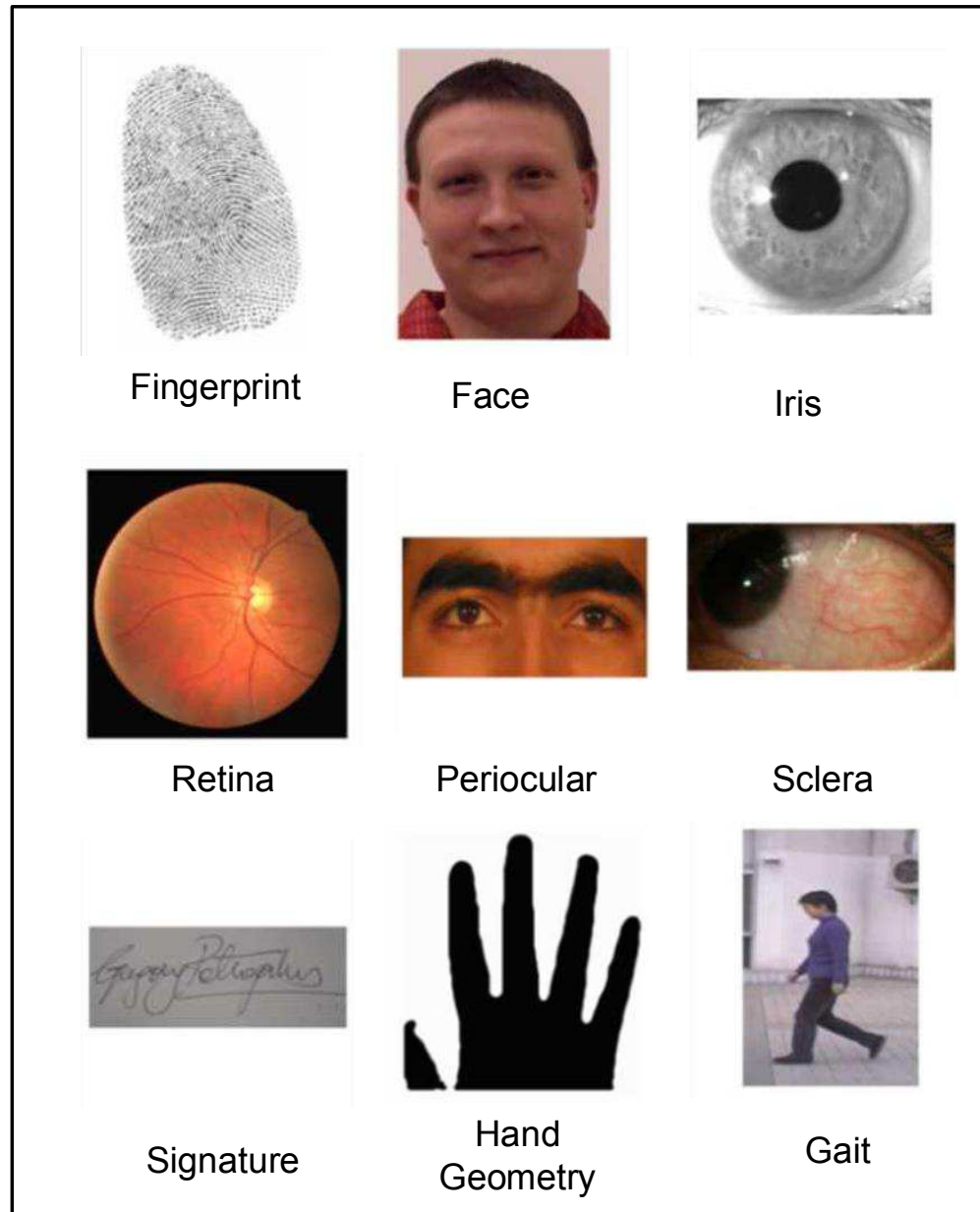
Figure 1.1: Commonly used traits in biometric systems [1].

points. After that, these features are enhanced and converted into templates to be stored in databases. Typically, multiple fingers are employed to establish a person's identity which forms a large scale identification system. However, a large scale finger print recognition system involves extensive computational requirements especially when working in the identification mode. In addition, fingerprints may be not stable due to several factors such as aging, skin disease and abrasion due to hard work [4].

1.3.2 Face Recognition

Face recognition is a non-intrusive recognition technology which is very common in surveillance systems since a person's face can be easily captured with video technology. Basically, face recognition either relies on geometric features such as the locations of the eyes, nose, mouth and their spatial relationships or exploits universal analysis of a face image and its intrinsic features. The face recognition performance is said to be reasonable under a controlled environment. However, in an uncontrolled environment face recognition performance degrades due to different factors such as illumination changes, background noise and pose variations. Therefore, it can be argued that using the face alone is not sufficient to achieve recognition with high level of confidence in a large scale environment [5]

1.3.3 Hand Geometry

A hand geometry recognition system operates by measuring certain feature in the hand such as the size and shape of the palm and fingers. The scanner of a hand geometry system cannot be used in small devices such as mobiles and laptops due to its large size. It could be argued that the geometry of the hand is not very distinctive therefore it cannot be scaled up for a large database. In addition, wearing jewelry and rings may affect the geometry information of the hand [1].

1.3.4 Iris Recognition

The iris is the colored ring that surrounds the pupil of the eye. Due to the unique characteristics of the iris pattern, it is considered as one of the most accurate means of human identification. The iris is a well-protected organ and appears to be stable over the life time [6]. Although the idea of utilizing the iris texture for personal identification was proposed by Frank Burch in 1936, the first working iris recognition system was implemented by Daugman in 1993 [7]. Large-scale identification systems adopt the iris biometric due to its high accuracy and speed. For example, the iris is employed as the primary biometric modality in several national identification systems such as the Aadhaar project in India, the national ID program in Mexico and the e-ktp program in Indonesia [8].

1.3.5 Periocular Recognition

The term periocular refers to the facial region that surrounds the eyes which consists of eyes, eyebrows and skin. The periocular region can be used to support iris recognition when the images are low resolution. In addition, the periocular biometric can be used to confirm the identity when part of the face image is occluded. A new sensor is not required for the periocular biometric as this region can be captured with the same face camera. Periocular recognition has a modest accuracy using good quality images with low intra-class variations [9].

1.3.6 Sclera Recognition

The sclera is the white and opaque protective layer of the eye. The sclera can be used for personal authentication because the structure of the blood vessels in the sclera is random and stable for each person [10]. Although the blood vessels of the sclera can be acquired at a distance under Visible Light (VL), sclera recognition is still challenging. This is because the vessels are often defocused and most importantly the vessels are noisy and have non-linear deformation due to the movement of the eye. Therefore, sclera recognition is often used with another biometric trait to boost the recognition performance [11].

1.3.7 Speaker Recognition

Speaker recognition refers to identifying persons based on the physiological and behavioral characteristics of their voice. Voice recognition can either refer to speaker recognition (who is speaking) or speech recognition (what is being said). A biometric system generally focuses on speaker recognition in order to identify a person. Speaker recognition can be dived into two types: text-dependent and text-independent. In text-dependent systems, the user is required to say a pass-phrase to complete the authentication while text-independent systems require a little cooperation from the user and hence they are more common in forensic applications as the enrollment could happen without the knowledge of the subject [2].

1.3.8 Signature Recognition

A signature belongs to the set of behavioral biometrics as each person has a unique writing style. Signature recognition can be divided into two main categories depending on the mode of operation: static and dynamic. In the static mode a scanner is used to digitize the signature and analyze its shape. This is also known as "off-line" signature recognition. On the other hand, in a dynamic or online recognition mode, the signature is acquired in real time by a digitized tablet which measures the number and length of stokes, pressure and acceleration. As a behavioral biometric, the signature is affected by time span and the emotional conditions of the person. In addition, professional forgers might imitate a person's signature to gain unauthorized access [2].

1.3.9 Gait Recognition

Gait recognition is a relatively new biometric method aims at identifying people by the way they walk. Gait recognition is appropriate in surveillance systems as it can be used for identifying people at a distance. However, the human gait is influenced by several factors such as the walking surface, footwear and walking speed. Therefore, a gait recognition system could be vulnerable to a high false rejection rate [12]. In addition, gait recognition systems involve a relatively high computation complexity as it is a video based recognition method [13].

1.4 Modes of Functioning

Regardless of the biometric trait, the biometric recognition process follows the procedure depicted in Fig. 1.2. After a biometric trait is captured, a suitable feature extraction is applied to derive the unique biometric characteristics and convert them into mathematical templates. After that, these templates are further compared against the ones stored in a database which were collected during the enrollment process. Then authentication is granted if the comparison between the current and stored template has enough similarity.

Depending on the number of comparisons between the biometric sample and templates, a biometric system can work in two modes namely, verification and identification [1].
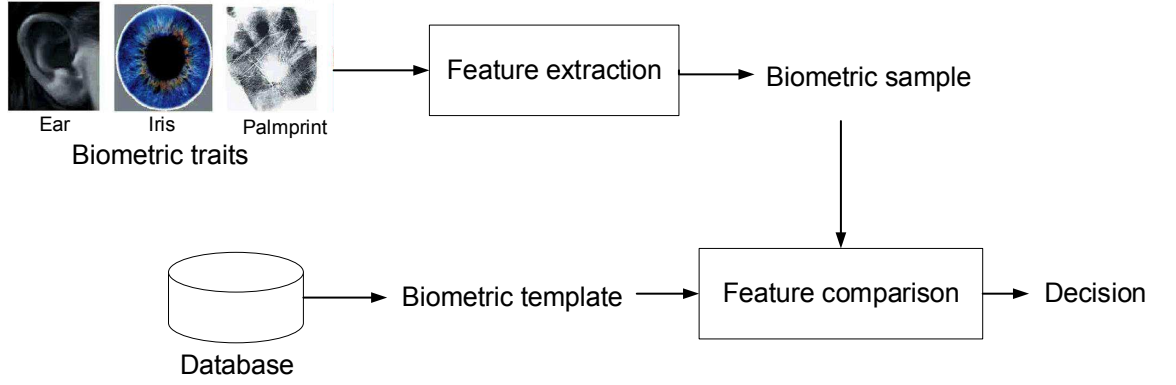
Figure 1.2: Typical stages of a biometric recognition system.

In the verification mode, the system verifies whether the enrolled identity is genuine or not. Therefore, the verification mode aims to answer the question: is this a person who s/he claimed to be? The user in this case is required to give an ID or a token along with the biometric sample. Therefore, the verification mode has low complexity as the comparison is carried out between the enrolled sample and the one in the database (1-to-1 match). Further, if the recognition rate is higher than a threshold value, the claim is accepted. Otherwise the enrolled sample is denied.

On the other hand, in the identification mode, the system is answering the question: is this person enrolled in the database? Since the biometric sample in the identification mode is compared against the entire database ($1-to-N$ match), it takes more time than the verification mode. The identification is known as screening which is often used for identity deduplication or in airports and forensics to match a subject against a watch-list.

1.5 Aims of the Work

The aims of this thesis are to investigate the open issues in iris recognition and propose novel methods to tackle these problems. In particular, three novel methods are proposed to address the problems of iris segmentation, image and template protection and cross-spectral iris matching.

The objectives of this thesis are as follows:

1. To investigate a new method for iris segmentation for both VL and Near Infra-Red (NIR) iris images with the following contributions:

8

- a novel iris segmentation method aimed at improving the recognition performance for iris images captured under both controlled and uncontrolled environment,

- a new shrinking-expanding active contour model which integrates a new pressure force to segment the iris accurately and

- a new method for discarding the images with an invalid iris and limiting the search region in the non-skin parts for irises captured with visible light.

2. To develop a new framework for iris image and template protection with the following contributions:

- protecting the evidentiary integrity of the iris images based on a novel watermarking algorithm by embedding text data as a contextual watermark in the iris image,

- a robust iris template protection method that neither involves pixel expansion nor quality loss in the iris template and

- protecting the integrity of the smart card and stored iris template using the hash function.

3. To develop a new framework for cross-spectral iris matching with the following contributions:

- evaluating the iris recognition performance under different channels,

- a new framework for cross-spectral matching capable of matching registered and unregistered iris images captured from the same subject and

- Enhancing the iris recognition performance by multi-channel fusion.

1.6   Contributions

This thesis offers three main contributions representing significant improvements in terms of iris biometric performance, iris biometrics protection and cross-spectral matching. These contributions can be outlined as the following:

1. The study introduces a new method for iris segmentation. Hence, a new active contour model for iris and image segmentation is developed by integrating a new pressure force within the Gradient Vector Flow (GVF) model which addresses the drawbacks of previous active contour models. The movement direction of the active contour is geared based on the eyelid location. This method is capable of accurately segmenting the iris from the eye image for images taken under both VL and NIR. In addition, a novel method for discarding the images with an invalid iris and limiting the search region in the non-skin parts for irises captured with visible light is proposed.

2. A novel framework for iris biometric protection is proposed. This framework incorporates two stages. The first stage is a robust watermarking algorithm to protect the evidentiary integrity of the iris images based on randomly exchanging four middle band coefficient pairs of the Discrete Cosine Transform (DCT) to embed text data as a contextual watermark in the iris image. The second stage is a Visual Cryptography (VC) scheme for iris template protection that neither involves pixel expansion nor quality loss in the iris template. The integrity of the stored iris template is also guaranteed by using the hash signatures.

3. A novel framework for cross-spectral iris matching. This framework is capable of matching registered and unregistered iris images in different lighting conditions. This work is amongst the first attempts in the literature to investigate the problem of VL to NIR iris matching (and vice versa) on iris images belonging to the same subject. In addition, the differences in iris recognition performance under NIR and VL imaging are investigated. Furthermore, enhancing the iris recognition performance with multi-channel fusion is attained.

1.7   Thesis Outline

Three novel methods are proposed in this work covering iris segmentation, protection and cross-spectral matching. These novel methods are discussed in Chapter 4, Chapter 5 and Chapter 6, respectively. The thesis is organized as follows:

Chapter 2 presents an overview of the anatomy and properties of the human iris from image acquisition to feature matching. Accordingly, a brief overview of camera types in the acquisition stage was given. In addition, the stages of the iris recognition system are presented in detail and the baseline algorithms in each stage are given.

Chapter3 presents the a brief introduction on performance evaluation for a biometric system. In addition, this chapter lists some of the public deployment iris based system used on a national scale. Moreover, a survey of the publicly available iris databases is given.

Chapter 4 presents the proposed iris segmentation method. A detailed literature review related to iris segmentation is given. The snake and the GVF active contours are presented along with their drawbacks. After that the proposed active contour is introduced based on adding a new pressure force to the GVF active contour to form a shrinking/expanding model for iris segmentation for iris images captured under both the visible and infra-red light. Moreover, a novel method is proposed for discarding the images with an invalid iris and limiting the search region in the non-skin parts for irises captured with visible light.

Chapter 5 presents the proposed iris image and template protection method. After the literature review, the chapter is divided into two parts. The first part presents the proposed watermarking algorithm for protecting the evidentiary integrity of the iris images based on exchanging multiple middle band coefficients of the DCT blocks using text data as a contextual watermark. The second part presents the template protection method which works by dividing the iris templates into two shares based on VC. After decomposing the iris template into two shares, one share is given to the user on a smart card and the other share is stored in the database along with a signature generated by a hash function. Furthermore, the integrity of the stored iris template is also guaranteed by using the hash signatures.

Chapter 6 focuses on cross-spectral iris matching. In this chapter a new framework is introduced for cross-spectral iris matching capable of matching registered and unregistered iris images taken under VL and NIR. Two methods are proposed for cross-spectral iris matching. The first method was designed to work with registered iris images which adopted a Feed Forward Neural Network (FFNN) to synthesize the corresponding NIR images from the VL images to perform the verification. The second method is capable

of working with unregistered iris images based on integrating the Gabor filter with different photometric normalization models and descriptors along with decision level fusion to achieve robust cross-spectral matching. In addition, this chapter investigates the performance of iris recognition under different channels. Furthermore, enhancing the iris recognition performance with multi-channel fusion is attained.

Finally, Chapter 7 draws the overall conclusions and provides directions for future work.

Chapter 2

Background of Iris Recognition

2.1 Background of Iris Recognition

"For purposes of rapid and reliable person identification,...it is hard to imagine one (unique identifier) better suited than a protected, immutable, internal organ of the eye (iris), that is readily visible externally and that reveals random morphogenesis of high statistical complexity" [7, p.1160].

2.1.1 History

Efforts to create a reliable means for human authentication based on the iris texture ago back to the early 1930s when the ophthalmologist Frank Burch noticed highly detailed and unique features in the iris which stayed unchanged over a long time. This idea remained as a science fiction until two ophthalmologists Leonard Flom and Aran Safir patented Burch's concept but they were unable to develop an automated recognition system. It was not until 1993 when John Daugman developed the first automated iris recognition system. Daugman's method is considered the baseline for all current iris recognition systems [14]. Fig. 2.1 shows the major milestones in the history of iris recognition.
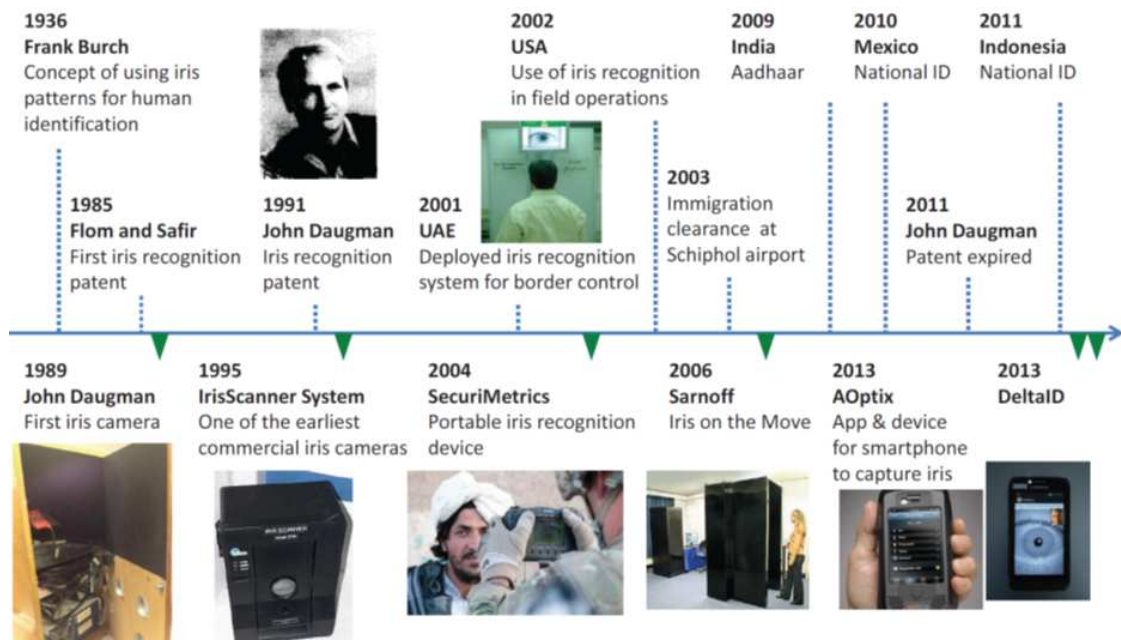
Figure 2.1: Major milestones in the history of iris recognition [1].

In 2002, iris recognition technology was manifested by disclosing the identity of the missing Afghan girl. This story goes back to 1984 when a photographer went to Pakistan to document the suffering of the Afghanistan's refugees following the bombing by the Soviet Union. During his visit he captured a photo of a young girl which then became very famous and printed on the cover of the National Geographic magazine [15].

Seventeen years later, National Geographic TV started a search for the Afghani girl but several women turned out and claimed to be that girl. Unfortunately, there was no way to establish the identity as there was no recorded name of the young Afghani girl and her face would have changed significantly due to aging. The team managed to confirm the correct identity with the help of iris recognition where the iris patterns were matched from the photograph of 1984 to a women called Sharbat Gula with a very tiny probability of error (10^{-15}) from her left eye [16].

2.1.2 Anatomy and Properties of the Human Iris

The iris is the colored ring that surrounds the pupil. A front view of an iris image is shown in Fig. 2.2. The iris controls the amount of light that enters the pupil. The pupil size can vary from 10% to 80% of the iris diameter. The average radius of the iris is around 6mm [6].
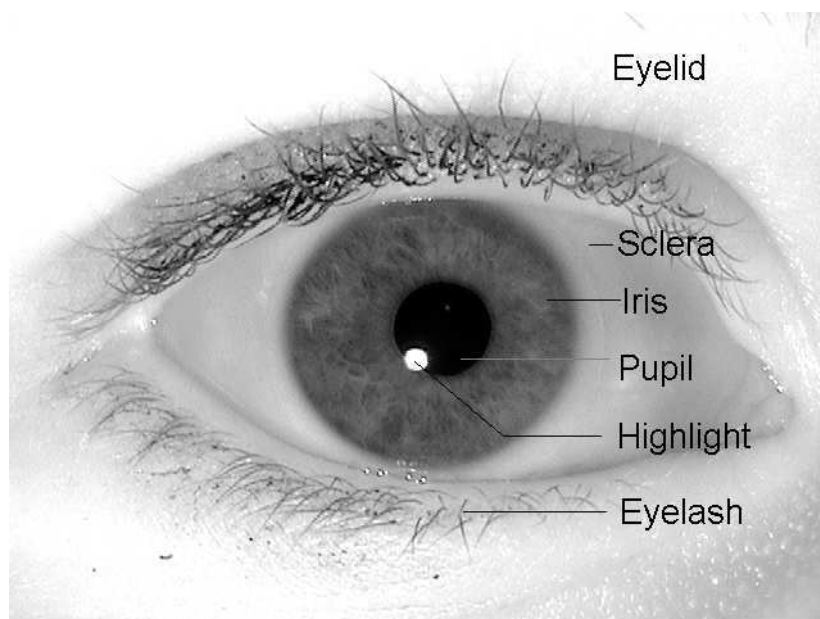
Figure 2.2: Eye image showing the iris and its surroundings.

The structure of the iris is completed by the eighth month of gestation. Although the color of the iris may change during the first postnatal years, the structure itself is stable throughout the human's life. The iris color is controlled by the density of the melanin pigment in its anterior layer. On the other hand, the meshwork of the elastic ligament forms the texture of the iris. The chromophore of the human iris is noticeable under VL and it becomes hidden under the NIR light. Therefore, with dark pigmented irides, stromal features of the iris are only revealed under NIR and they become hidden in VL so the information related to the texture is revealed rather than the pigmentation [14].

As mention is Section 1.2, a good biometric trait should have several characteristics to provide a reliable recognition. In addition to those characteristics, the iris enjoys further advantages over other biometric traits. For instance, the iris is a well-protected organ and its physiological response to light offers robustness to fake samples. Moreover, it cannot be surgically modified without risks to vision. Furthermore, iris technology is deemed to be very hygienic as there is no physical contact compared to other biometric based on finger or palm print. This property allows iris images to be captured from a distance without physical contact which makes the iris suitable for forensics applications. Besides, iris recognition technology is culturally accepted by the people of some countries where it is common to cover the face by Niqab. (Fig. 2.3).
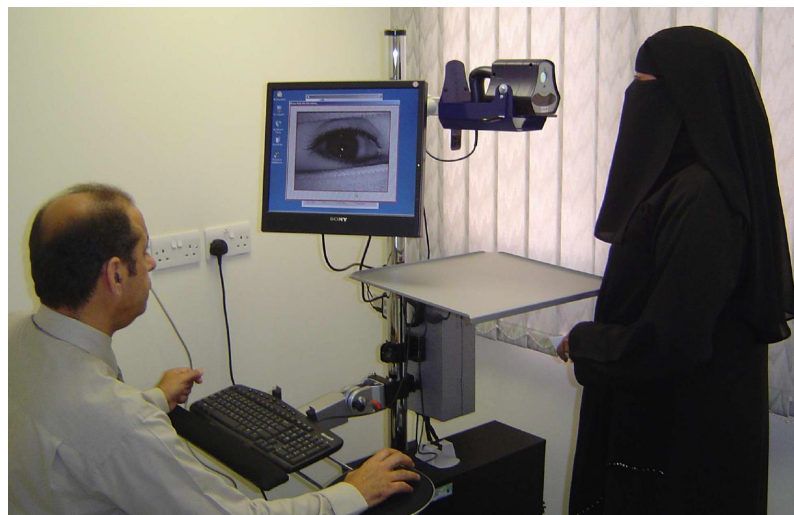
Figure 2.3: Scanning the iris for a female wearing Niqab without revealing the full face.

2.2   Iris Recognition System

Generally, an iris recognition system comprises of five main stages: image acquisition, iris segmentation, iris normalization, feature extraction and feature matching. Fig. 2.4 shows the main stages of an iris recognition system [7].
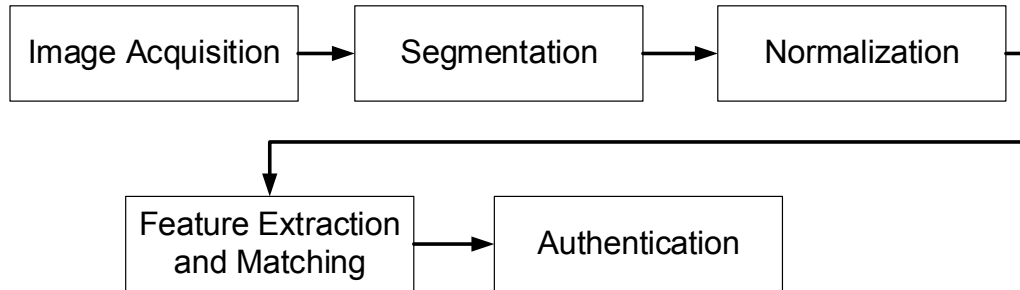
Figure 2.4: Block diagram showing the main stages in an iris recognition system.

2.3   Image Acquisition

Image acquisition plays a vital role in iris recognition. Poor image condition has been shown to degrade iris recognition performance and badly affect the intra-class similarity. Fig. 2.5 shows different types of iris camera. There are four main types of camera for iris acquisition [17]:

1. Access control: A wall-mounted camera that captures the iris with a medium focal length and requires user cooperation.

2. Handheld: A portable camera with a small focal length and typically used for access control.

3. Dual-eye visor: A mobile camera that covers both eyes and requires active user cooperation.

4. Stand-off camera: A camera with a large focal length which requires less user co-operation and can capture images on the move.

The aforementioned cameras have the same operation manner: An infra-red light is emitted from a source (with wavelengths between 700-900nm) and the iris image is cap-

17
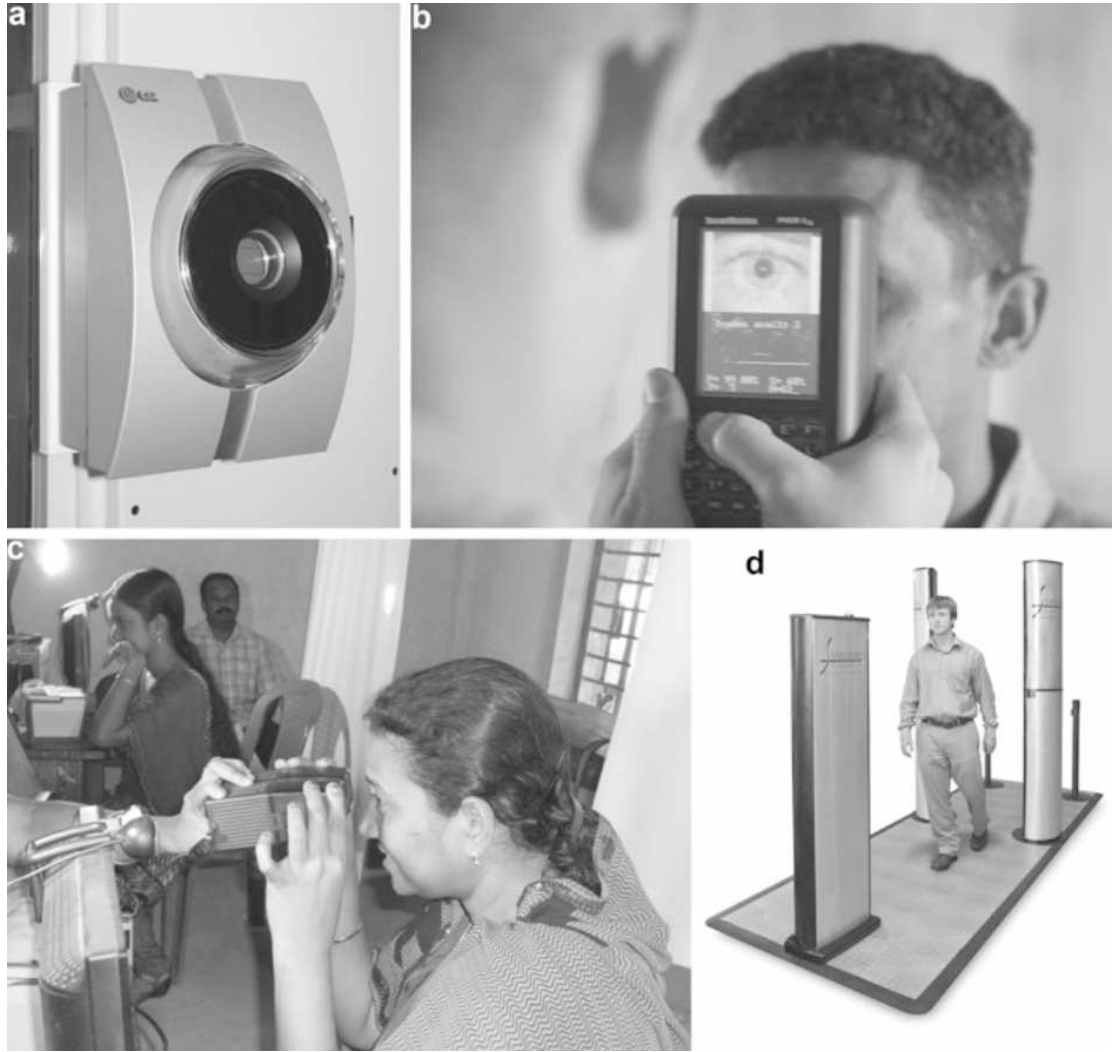
Figure 2.5: Iris camera types: (a) Wall-mounted, (b) Handheld, (c) Visor and (d) Stand-off (SRI Sarnoff IOM PassportTM system). Image source: [3].

tured with the camera. The human eye does not respond automatically to the NIR illumination compared with the VL in terms of blinking and pupil contraction. Therefore, there is an illumination limit to the NIR irradiance which has been set to 10mW per square centimeter. Hence, NIR devices should be placed relatively close to the subject. On the other hand, to avoid pupil dilation, iris recognition systems recommend that a specific illumination level is set.

2.4   Iris Segmentation

Iris segmentation is an essential module in an iris recognition system as the performance of the system is highly dependent on this step and errors can lead to misclassification during authentication. This step involves isolating the iris structure from other components in an eye image, including the pupil, sclera, eyelashes, eyelids and reflections. A robust segmentation technique is needed as the errors which happen at the segmentation stage cannot be corrected later and yield a false rejection.

Several iris segmentation algorithms have been proposed. These algorithms can be broadly classified into two categories of iris segmentation: 1) Iris segmentation with the classical circular approaches and their improvements, 2) Iris segmentation with noncircular approaches. A brief overview of the main methods for iris segmentation is given next.

2.4.1   Hough Transform

The Hough transform is a famous computer vision algorithm that can be employed for determining the parameters of different geometric shapes including lines and circles. For iris segmentation, the Circular Hough Transform (CHT) can be utilized for inferring the radius and center of the iris in images which are captured under a controlled environment.

Basically, the CHT involves these steps: After generating the edge map, a vote is cast in the Hough space for the parameters of circles passing through each edge point. Any circle can be defined with the center coordinates (x_c, y_c) and the radius r. Hence in the Hough space, a maximum point with the largest number of intersection will correspond to the radius and center coordinates of the best circle [18]. Although the CHT is robust to the gaps and noise presence in the image, it has a high computational complexity of $O(N^3)$ and suffers from the thresholding problem [19].

2.4.2 Integro-Differential Operator (IDO)

Daugman proposed to use the IDO for iris and pupil localization in the eye image. The IDO can be defined by:

$$max_{r,x_0,y_0} \left| G_\sigma(r) * \frac{\partial}{\partial r} \oint_{r,x_0,y_0} \frac{I(x,y)}{2\pi r} ds \right| \quad (2.1)$$

where $I(x,y)$ is the eye image, $*$ denotes the convolution operator, r is the radius of the search range, $G_\sigma(r)$ is a Gaussian smoothing function and s is the contour of the circle given by (x_0, y_0), and r. The IDO varies the radius and center position of the circular contour until finding a path where there is maximum change in pixel values. The operator is applied iteratively while reducing the amount of noise in order to attain a precise localization [7].

Although the IDO does not suffer from the thresholding problem, it can fail to detect circles in the presence of noise in the eye images especially when images are captured under VL.

2.4.3 Active Contour

Noncircular approaches are effective in iris segmentation because iris boundaries appear to be noncircular especially under uncontrolled environments and in the presence of eyelids. Therefore, an active contour is an ideal candidate for this purpose [20]. An active contour curve moves from initial mask until equilibrium is reached. The position of the active contour is changed by two opposing forces: an internal force, which controls the deformability of the curve, and an external force, which is derived from the image energy. Each vertex in the active contour force is moved between time t and $t+1$ by:

$$v_i(t+1) = v_i(t) + F_i(t) + G_i(t) \quad (2.2)$$

where F_i is the internal force, G_i is the external force and v_i is the position of vertex i. For segmenting the iris region, the internal force is initialized so that the contour evolves from initial state until the energy function is minimized when the curve is on the iris boundary [21].

2.4.4   Other segmentation methods

Other noncircular segmentation methods such as ellipse fitting and the parabolic Hough transform typically extend the previous segmentation methods [22, 23]. The thresholding based segmentation method works on the assumption that the iris/pupil can be separated from eye image based on the contrast difference. This method may work for the iris images captured under NIR because there is high contrast difference between the iris and pupil. However, it fails to segment visible iris images due to the low contrast difference and the presence of reflections. In addition, the thresholding based method requires a suitable threshold to be found for each imaging condition which could be challenging. Almost all the previously stated methods, however, require a fine tuning with large computation time and cannot be generalized for all the image conditions [24].

2.5   Normalization

After segmenting the iris, the next stage is to transform the segmented iris to the dimensionless polar coordinates in order to remove the dimensional inconsistency between the images due to pupil dilation with different lighting conditions. Other sources of inconsistency include camera or head rotation and varying capturing distance. The normalization stage aims to solve the inconsistency due to pupil dilation but inconsistency due to image rotation will be addressed at the matching stage [6]. Almost all the current iris recognition systems adopt the rubber sheet method or its modifications for iris normalization which is explained next.

2.5.1   Rubber Sheet Model

Daugman proposed to use the rubber sheet method for iris normalization [7]. This model remaps each point in the iris image to the polar coordinates (r, θ) where r has an interval $[0, 1]$ and θ is angle in $[0, 2\pi]$ as shown in Fig. 2.6:

This remapping from the Cartesian coordinates (x, y) to the normalized non-concentric
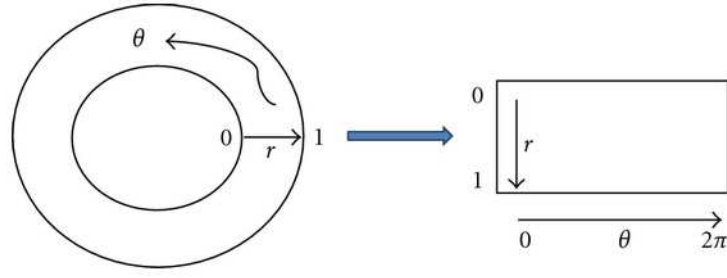
Figure 2.6: Rubber sheet model [4].

polar representation can be modeled by the following equations:

$$I(x(r, \theta), y(r, \theta)) \rightarrow I(r, \theta) \tag{2.3}$$

$$x(r, \theta) = (1 - r)x_p(\theta) + rx_i(\theta) \tag{2.4}$$

$$y(r, \theta) = (1 - r)y_p(\theta) + ry_i(\theta) \tag{2.5}$$

with

$$x_p(r, \theta) = x_{po}(\theta) + r_p cos(\theta) \tag{2.6}$$

$$y_p(r, \theta) = y_{po}(\theta) + r_p sin(\theta) \tag{2.7}$$

$$x_i(r, \theta) = x_{io}(\theta) + r_i cos(\theta) \tag{2.8}$$

$$y_i(r, \theta) = y_{io}(\theta) + r_i sin(\theta) \tag{2.9}$$

where $I(x, y)$ is the iris image, (x, y) are the original Cartesian coordinates and (r, θ) are the corresponding normalized polar coordinates. The radius of the pupil and iris are respectively defined by r_p and r_i while $x_p(\theta)$, $y_p(\theta)$ and $x_i(\theta)$, $y_i(\theta)$ represent the coordinates of the pupillary and iris boundaries in the direction θ. Further, (x_{p0}, y_{p0}) and (x_{i0}, y_{i0}) represent the centers of the pupil and iris respectively [7]. After that, a constant number of points are chosen along each radial lines to produce a fixed dimension normalized iris sheet. Examples of normalized iris images are shown in Fig. 2.7 .

As mentioned earlier, the rubber sheet method mitigates inconsistency due to the pupil dilatation but it does not compensate for rotational variations. Such rotational inconsistency will be addressed at the matching stage.

22
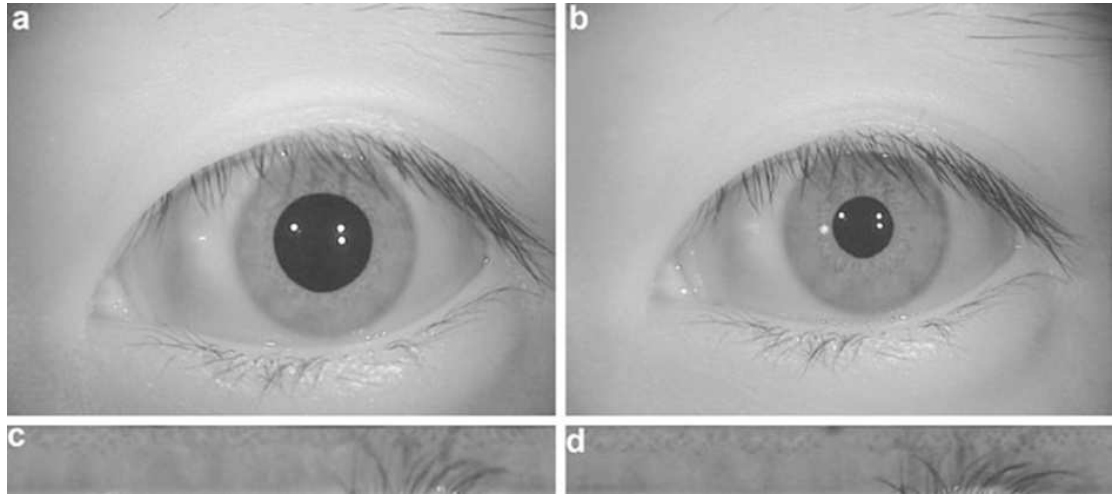
Figure 2.7: Iris normalization under different lighting conditions (a) Dilated pupil, (b) normal pupil, (c) and (d) iris images after normalization. Image source: [3].

2.5.2 Virtual Circles

Boles and Boashash [25] proposed to scale iris images to have a constant diameter to mitigate the dimensional inconsistency. After scaling, when the images to be compared have the same dimensions, concentric virtual circles are used as reference boundaries for feature extraction with the origin at the center of the pupil. After that, the same normalization resolution is assigned for the iris images so that each iris has the same number of data points. However, this method may fail when there is a big variation in pupil size within the iris images. In addition, it is not clear how to deal with the rotation invariance.

2.6 Feature Extraction

Feature extraction aims at extracting the most discriminating information from the iris image in order to provide accurate recognition. Nearly all iris recognition systems employ a band pass filter to generate the iris template and most of the currently deployed iris recognition systems adopt Daugman's method for feature extraction. Several alternative methods have been proposed but their performance is not as high as Daugman's and their recognition performance have not been tested on a large scale databases [24].

Most feature extractors used in iris recognition systems generate binary templates due to the following advantages[7]:

- Solid storage: iris templates (iriscode) have small storage (2048 bits in [6]) compared to other biometrics technologies which typically require more complex data representation.

- Fast comparison: rapid comparison can be executed when dealing with a binary representation. These operation can be executed in parallel to handle multi-millions comparison in one second.

Next, Daugman's method for feature extraction will be presented.

2.6.1 Gabor Filter

A Gabor filter is a linear filter used for feature extraction and texture analysis. A Gabor filter is created by modulating a sine/cosine wave with a Gaussian signal. This will provide a perfect conjoint localization in space and frequency [26].

Signal decomposition is achieved with a quadrature pair of Gabor filters. While the real part is constructed by modulating a Gaussian signal with a cosine, the imaginary part is constructed by modulating a Gaussian signal with a sine wave. The real and imaginary parts are also known as the even and odd components. The bandwidth of the filter is controlled by the width of the Gaussian signal while the frequency of the filter is specified by the frequency of the sine/cosine waves [26].

Daugman employed a 2D Gabor filter for encoding the iris texture [7]. A 2D Gabor filter can be represented as:

$$G(x,y) = e^{-\pi[(x-x_0)^2/\alpha^2 + (y-y_0)^2/\beta^2]} e^{-2\pi i[u_0(x-x_0)+v_0(y-y_0)]} \qquad (2.10)$$

where (x_0, y_0) represents the pixel coordinates in the iris image, (α, β) specify the effective width and length while (u_0, v_0) specify modulation which has a spatial frequency of $\omega = \sqrt{u_0^2 + v_0^2}$.

In Daugman's method, the phase output of the filter is quantized into four levels according to the quadrant of the complex plane of the filter phase information. Oppenheim

and Lim [27] show that the phase information provides the most significant information within an image. Hence, taking the phase information rather than amplitude in the iris image allows for robust encoding while discarding the redundant information such as illumination and lighting variations. These four levels are represented by two bits so that each pixel in the normalized iris image corresponds to two bits in the encoded template. Therefore, a normalized iris template with a resolution of 20×240 can be represented by a 9600 bit template. Therefore, the iris image can be represented by a compact 1200 byte template that allows an efficient and fast comparison of iris templates.

2.6.2 Log-Gabor Filters

A Gabor filter has the disadvantage that the even part of the filter will have a DC component [28]. To solve this drawback a Log-Gabor filter can be used. The frequency response of a Log-Gabor filter can be represented by:

$$G(f) = \exp[\frac{-(log(f/f_0))^2}{2(log(\sigma/f_0))^2}]$$

(2.11)

where f_0 represents the center frequency and σ gives the bandwidth of the filter [28].

2.7 Matching

After generating the iris templates, a metric should be employed to measure the similarity. This metric should give one range of values when comparing templates generated from the same eye (intra class) and another range when comparing templates belonging to different eyes (inter class). Based on this metric, a decision can be made to decide whether to authenticate the person or not. In principle, any type of classifier can be used for this purpose such as Euclidean distance or Hamming distance as explained next.

2.7.1   Weighted Euclidean Distance

The Weighted Euclidean Distance (WED) is used to measure the similarity between two integer templates. The WED is given by [29]:

$$WED(k) = \sum_{i=1}^{N} \frac{(f_i - f_i^{(k)})^2}{(\sigma^{(k)})^2} \qquad (2.12)$$

where f_i is the ith feature of the current iris template and $f_i^{(k)}$ is the ith feature of the compared template k while $\sigma^{(k)}$ is the standard deviation of the ith feature in the template k. The best match is found with the template corresponding to the minimum value of k.

2.7.2   Hamming Distance

The Hamming Distance (HD) is the matching metric employed by Daugman to measure the similarity between two templates. For the bit patterns X and Y, the HD can be defined as the sum of disagreeing bits over the total number of bits in template. For a binary template, the number of the disagreeing bits can be expressed as the sum of the exclusive-OR bits between X and Y divided by the total number of bits (N) as follows [6]:

$$HD = \frac{1}{N} \sum_{i=1}^{N} X_i (XOR) Y_i. \qquad (2.13)$$

If there is no correlation in the bits withing the templates, the HD between templates should be around 0.5. This is because the bits in independent patterns are random and therefore half of them will agree and half will disagree. On the other hand, if the two templates belong to the same eye the bits will be highly correlated and the HD should be close to zero.

In order to include the actual iris region and cancel the effects of eyelids and eyelashes, a noise masking is incorporated within the HD equation. This mask contains "0" bits which correspond to the true iris region and "1" bits which correspond to the noise. Hence, the modified HD equation is given by [6]:

$$HD = \frac{1}{N - \sum_{k=1}^{N} Xn_k (OR) Yn_k} \sum_{j=1}^{N} X_i (XOR) Y_i (AND) Xn_i' (AND) Yn_i' \qquad (2.14)$$

26

Template 1	11 00 11 00 10 01	
Template 2	00 11 00 10 01 10	HD=0.91

◄— Shift 2 bits left

Template 1	00 11 00 10 01 10	
Template 2	00 11 00 10 01 10	HD=0.00

—► Shift 2 bits right

Template 1	10 11 00 11 00 10	
Template 2	00 11 00 10 01 10	HD=0.25
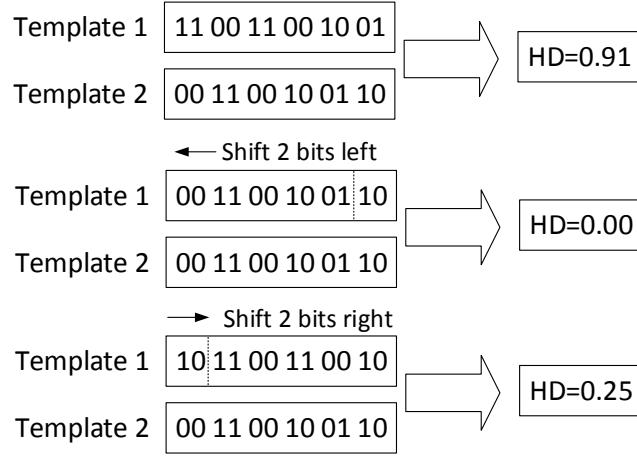
Figure 2.8: Shifting the reference template with one shift process (one left and one right) where the minimum Hamming distance is taken.

where X_i and Y_i are the two iris templates to be compared, Xn_i and Yn_i are the corresponding noise masks while N is the number of bits in each template.

To address the rotational inconsistencies, the iris template is shifted left and right multiple number of times and the HD is calculated then the minimum value is taken. Each filter generates two bits of data corresponding to one pixel in the iris pattern. Therefore, the number of bits to be moved in each shift equals twice the number of the employed filter. The actual number of shifts required to overcome the rotational inconsistencies is governed by the maximum angle of difference between the two normalized iris images [6]. Figure 2.8 illustrates the shift process.

2.8   Summary

In this chapter a brief history of iris recognition was presented showing the main milestones in iris recognition development. In addition, the anatomy and properties of the human iris were presented from image acquisition to feature matching. Accordingly, a brief overview of camera types in the acquisition stage was given. After that, the main stages in iris recognition namely: segmentation, normalization, feature extraction and matching were presented and their corresponding algorithms were explained.

The next chapter presents a brief overview on performance evaluation in a biometric system. In addition, a survey of the publicly available iris databases will be given.

Chapter 3

Performance Evaluation and Databases

3.1 Biometric System Evaluation

The evaluation of a biometric system is a challenging task as it not only involves engineering but also other fields such as computer science, statistics along with the end user community and system designers. Therefore, to establish a comprehensive understanding of a biometric system, the following points should be addressed [1]:

- The availability, maintainability and reliability of the biometric system.

- The error rates of the system in different applications (matching performance).

- The vulnerabilities of the biometric system and security issues.

- The user acceptability of the applied biometric system and privacy issues.

- The cost of implementing and running the system while judging the expected benefits.

There is no existing evaluation framework which can address all the aforementioned points simultaneously. The next section will focus on the matching performance of a biometric system.

3.2 Matching Performance

Biometric system performance can be measured by its ability to identify authorized subjects and reject unauthorized individuals. This can be achieved by measuring the similarity score for the output of a test. Hence, comparing the output score to a threshold results in an accept or reject decision. This decision could be erroneous in two cases. The first is false rejection when a true score is rejected and it is also known as False Reject Rate (FRR). The second case is false acceptance when an imposter is accepted and it is also known as False Accept Rate (FAR) [30].

An FRR of 1% is a result of one failed authentication attempt by the genuine user in each 100 authentication attempts. Most of the FRR error results from the incorrect interaction between the user and the biometric sensor. This can be easily corrected by asking the user to perform the authentication process again. This simulates entering a

wrong password in a password-based authentication system where the user is allowed to have another try. On the other hand, An FAR of 0.01% indicates that on average 1 in each 10000 authentication attempts by random imposters will be successful [30].

To generate the genuine scores in a biometric system which has N users and each user has m samples, the samples from the same user have to be compared . On the other hand, to generate the imposter scores, samples from two different users have to be compared. Therefore, the total number of genuine scores will equal to $(m(m-1)N)/2$ while the number of imposter scores will equal to $(N(N-1)m^2)/2$ [1].

The most common way of measuring the performance of biometric systems is by measuring the rate that both FAR and FRR become equal to each other which is known as the Equal Error Rate (EER). The EER is often used when the performance is needed to be summarized by a single number. The more accurate the biometric system the lower the EER. The distribution of FAR vs. FRR and EER are shown in Figure 3.1.
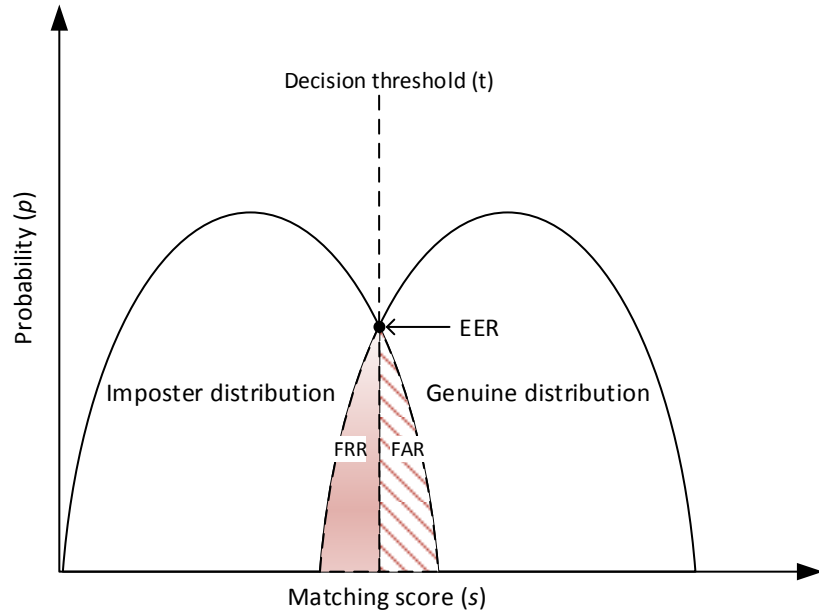
Figure 3.1: False rejection rate vs. false acceptance rate distribution [1].

3.3 Performance Graph

The FAR and FRR give the system performance at a specific score threshold. However, this evaluation is limited as the values of the threshold are only related to a specific algorithm and cannot be compared among different systems. In addition, it is often necessary to measure the performance over a range of thresholds. Therefore, it is essential to develop a method that is able to compare the performance independently of match scores [1].

This can be achieved by plotting the error rates over a range of thresholds with respect to the FAR and FRR. In this context, two standard plots are known in the literature namely: Receiver Operating Characteristic (ROC) curve and the Detection Error Trade-off (DET).

3.3.1 ROC Curves

In order to visualize the error trade-off, the FRR and FAR can be plotted over a range of thresholds. In this case all the scores should be normalized so that a unique threshold can be applied to all the genuine scores. This plot is known as the ROC curve. The ROC curve is a plot of the FAR versus the Genuine Acceptance Rate (GAR) which is calculated as:

$$GAR = 1 - FRR \tag{3.1}$$

A plot of ROC curve is depicted in Figure 3.2. In this figure the x-axis has a logarithmic scale to better distinguish the values of FAR.

3.3.2 DET Curves

The DET curve is similar to the ROC curve but the y-axis is the FRR as shown in Fig. 3.3. The choice between the ROC and DET curves is essentially aesthetic as both curves contain similar information. However, DET curves are often used in speaker recognition systems rather than ROC curves. This is because plotting error rates on both axes will give a uniform distribution to both errors and help to highlight the difference in a similarly performing systems [30].
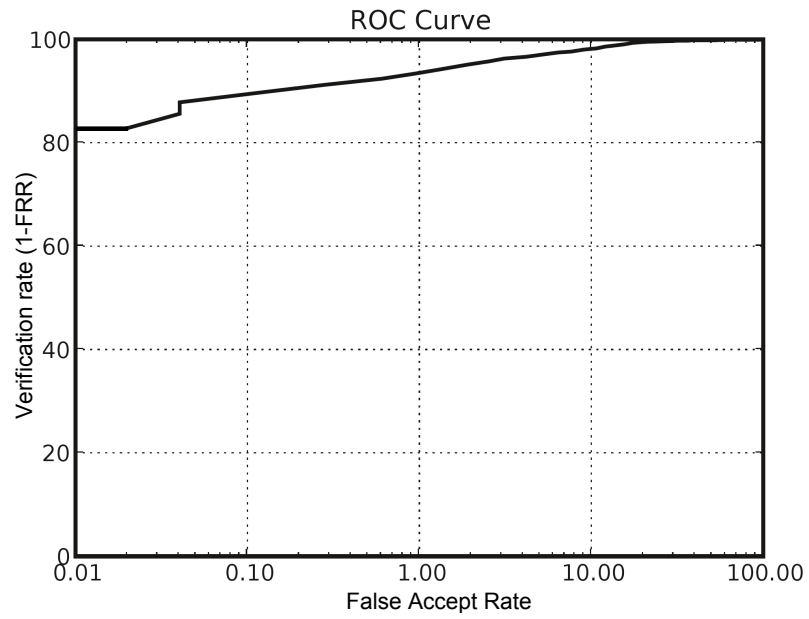
Figure 3.2: An example of ROC curve showing a verification rate of 90% at a false accept rate of 0.1%.
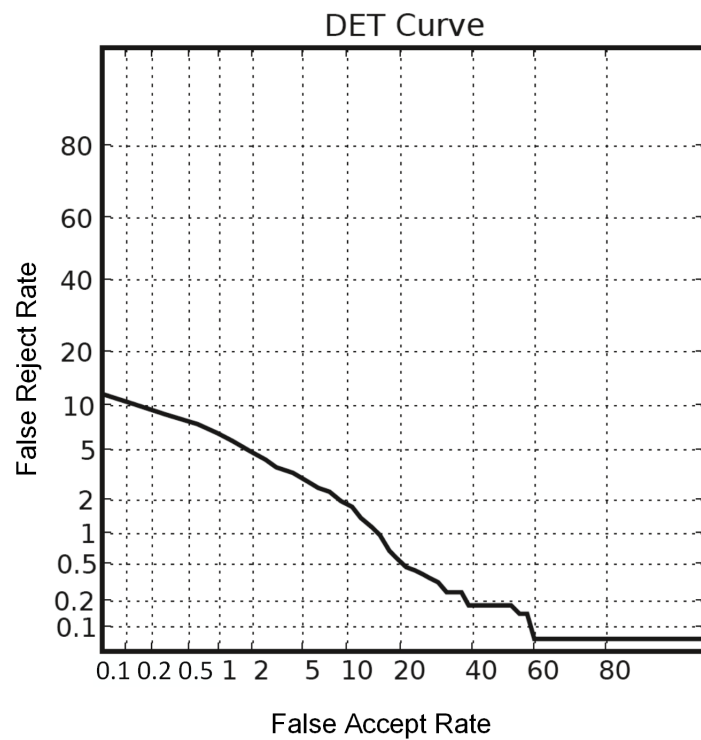
Figure 3.3: An example of DET curve showing a false reject rate of 5% at a false accept rate of 2%.

3.4 Biometrics Fusion

Biometric system that depends on a single source of data may fail to meet the requirements when working in challenging conditions. Therefore, fusion multiple level of sources can boost the performance and compromise for such limitations.

Generally speaking, fusion of biometric data can be divided into two broad categories: fusion before matching and fusion after matching (Fig. 3.4). Fusion before matching can be either performed at the sensor level or feature level. Sensor level fusion requires multiple sources of the biometric samples (raw data) and hence it can only be applied to a multi-sensors biometric system [1]. Feature level fusion works by combining multiple feature sets into a single feature vector. This feature vector can be either homogeneous (from the same feature extraction algorithm) or non-homogeneous (from different feature extraction algorithm). Feature from different sources need to be converted to the same representation to facilitate the fusion process [1].
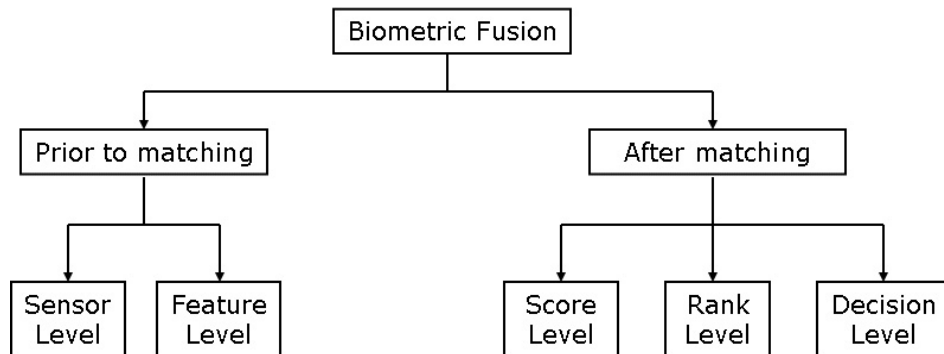
Figure 3.4: Biometric fusion classification [5].

On the other hand, fusion after matching can be divided into score level, rank level and decision level. Combining the final output scores of multiple biomtric matchers is known as score level fusion. It is easy to consolidate the scores resulted from similar classifier as these scores are homogeneous. However, if the output scores of matchers are of different numerical scale, or have different probability distribution; score fusion may become challenging and a normalization stage is needed [1].

Decision level fusion takes the decision of the classifiers independently and fuse them based on "AND" and "OR" rules or a voting scheme such as majority voting or weighted voting. This fusion scheme is common when building a multi-biometric system based on

commercial biometric systems because such systems allow access to the final recognition decisions only. Rank level fusion is relevant with biometric systems that work in the identification mode where the classifier set a rank for each identity based on likelihood of being correct. Combining the rank from multiple classifiers should result in boosting the performance. Hence, higher rank corresponds to better match [1].

3.5   Iris Biometrics Potential

As stated previously, the texture of the iris differs significantly from subject to subject even between monozygotic twins. Deployed iris recognition systems have an outstanding accuracy even in large scale applications. Daugman performed a study which included 200 billion cross-comparisons conducted on a database from the United Arab Emirates border crossing system. The experiment achieved remarkable results with a FAR of 10^{-6} and a FRR of 1% [31]. The potential of iris biometrics has also been affirmed with 1.2 trillion comparison by tests carried out by the National Institute of Standards and Technology (NIST) which confirmed that iris biometrics has the best balance between accuracy, template size and speed compared to other biometric traits [32].

In addition to the high recognition rate, an iris recognition system has an extremely rapid matching speed of hundreds of thousands persons per second on a single 3GHz server due to the binary nature of the iris template [6].

3.5.1   Public deployments

This section presents some of the large public deployments that adopt the iris as the main biometric modalities.

3.5.1.1   The United Arab Emirates Border Crossing

One of the first major deployments of iris recognition was the iris-based border security system in the United Arab Emirates which started in 2001. There are several million registered persons in this project with about 14 billion comparison carried out daily. The average time to carry out the comparison is only around two seconds [33].

3.5.1.2 The Unique Identification Authority of India

The unique identification authority of India was launched in 2009 in order to solve the identity problem as hundreds of millions have no official ID in India. The objective of the project is to collect the biometric and demographic data of residents while issuing a 12-digit unique number called Adhaar to each person. It is the world largest national identification project where more than one billion residents have enrolled as of July, 2016 [8].

The data are collected via 36000 portable enrollment stations where about a million new people are enrolled daily. In total 10^{15} all-to-all check operations are carried out daily for the sake of identity de-duplication. This would not be possible without the rapid matching speed that iris recognition technology enjoys [33].

3.5.1.3 Other Deployments

Other large-scale national identification systems have emerged recently such as the Indonesias e-ktp program and Mexico's national ID program where the iris serves as the main modality [8].

Iris recognition technology is also deployed in several other crossing/identity programs. For example, iris recognition based immigration systems have been in use at the Amsterdam Schiphol airport, the USA-Canada border and at a couple of major airports in the United Kingdom for more than ten years [33]. However, the one in the United Kingdom was decommissioned in 2013. In addition, iris recognition technology has been used by the USA military for entry control and people identification in Iraq and Afghanistan (Fig. 3.5).

3.6 Public Iris Databases

In order to confirm the results of a biometric trait, the results should be based on a large number of samples. Regarding iris biometrics, there are several freely available databases captured under different conditions. An overview of the main iris databases is given in the following subsection.

Figure 3.5: American solder performs identity check using iris recognition technology [2].

3.6.1 CASIA Database

The CASIA iris image database is constantly growing and released by the Institute of Automation from the Chinese Academy of Sciences. The current version (CASIA-IrisV4) contains a total of 54,601 iris images from more than 1,800 genuine subjects and 1,000 virtual subjects with synthesized irides. The database is divided into six subsets namely: CASIA-Iris-Interval, CASIA-Iris-Lamp, CASIA-Iris-Twins, CASIA-Iris-Distance, CASIA-Iris-Thousand, and CASIA-Iris-Syn [34].

CASIA-Iris-Interval contains 2639 images with extremely clear iris texture details. CASIA-Iris-Lamp contains 16212 images with nonlinear deformations due to light variations. CASIA-Iris-Twins contains 3183 irides taken from identical twins. CASIA-Iris-Distance accommodates 2567 face images with high quality iris details. CASIA-Iris-Thousand is considered the first available iris database with more than one thousand subjects. Finally, CASIA-Iris-Syn has 10,000 synthesized iris images. Figure 3.6 shows image samples from this database.
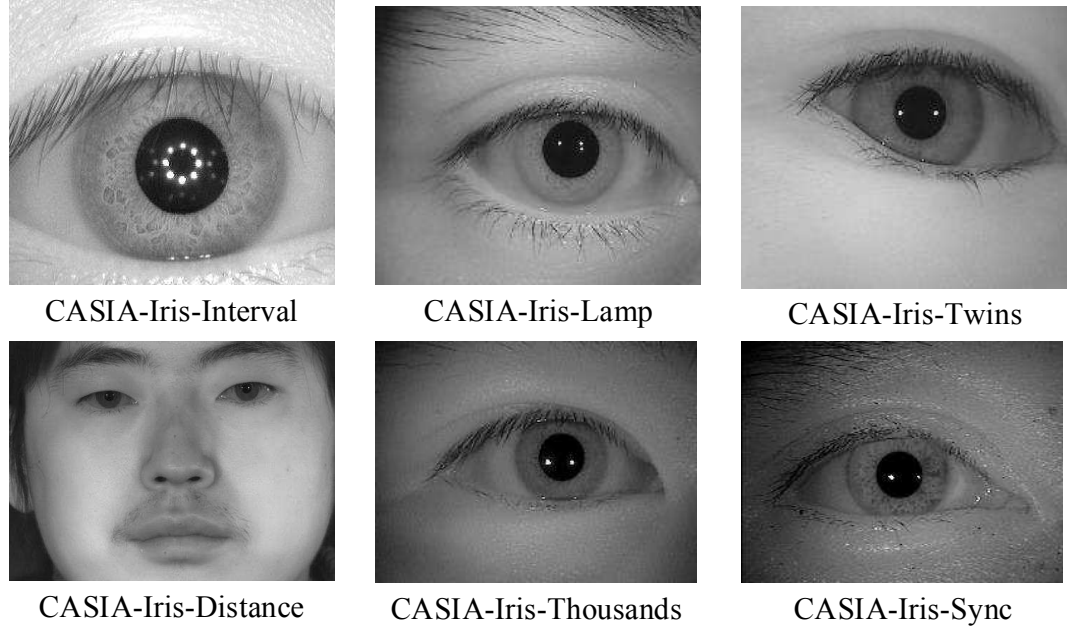
Figure 3.6: Iris samples from the CASIA V4 database.

3.6.2 MMU Database

The MMU iris databases were provided by the Malaysian Multimedia University in two versions MMU1 and MMU2. The MMU2 iris database [35] consists of 995 iris images which have been collected with distance of 47-53cm away from the user. Unlike MMU1 which contains a smaller number of samples with few noise factors, the captured iris images in MMU2 contain severe obstructions by eyelids/eyelashes, specular reflection, nonlinear deformation, low contrast and illumination changes. Figure 3.7 shows samples from the MMU1 and MMU2 databases.

3.6.3 UBIRIS Database

UBIRIS was introduced by the University of Beira in 2004 to test iris recognition performance under less constrained environments whilst simulating different noise factors such as defocusing, blurring, occlusions and specular reflections [36]. It contains 1877 images from 241 subjects in two different sessions. All images are taken under visible light. The images are stored with JPEG format with a color depth of 24 bits and a resolution of 800×600 pixels.

The database was collected during two sessions using a Nikon E5700 camera. While
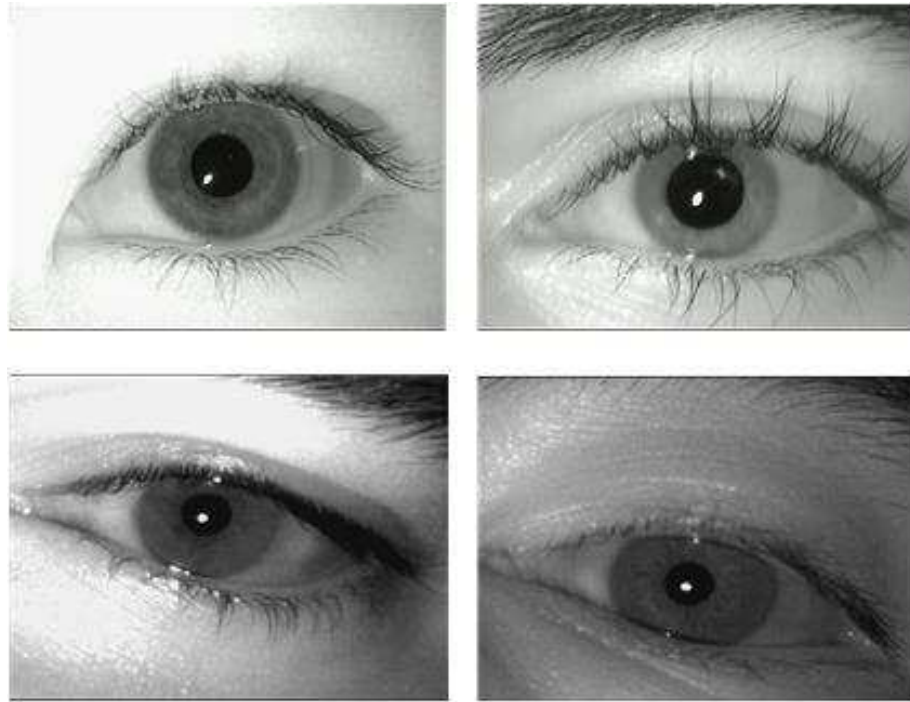
Figure 3.7: Iris samples from the MMU1 (first row) and MMU2 (second row) databases.

the first session contains relatively good quality images, several realistic noise factors were introduced to the second session of the UBIRIS V1 database such as reflections, defocus and oblique views to simulate non-cooperative conditions. Figure 3.8 shows samples from the UBIRIS V2 databases.
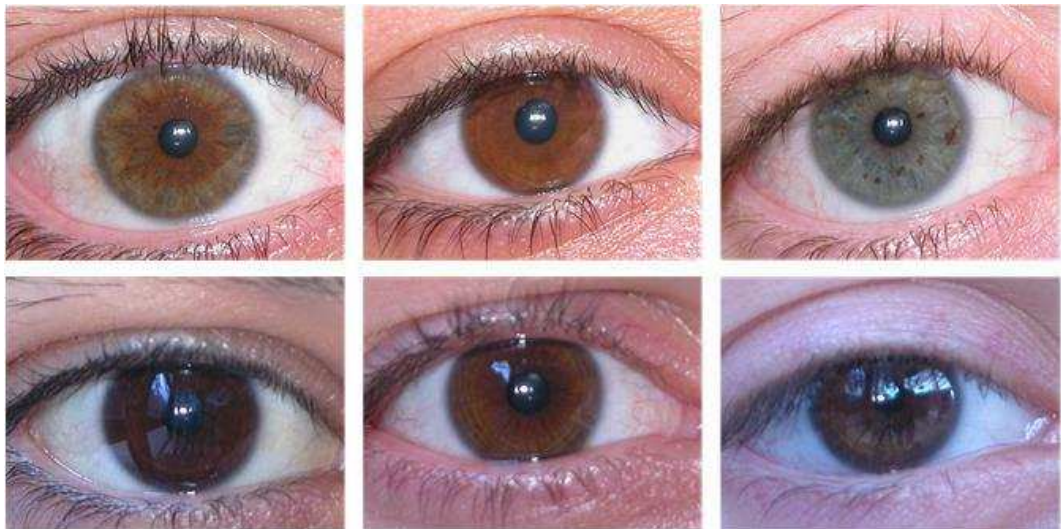
Figure 3.8: Iris samples from the UBIRIS V1 databases.

On the other hand, the UBIRIS V2 iris image database was also released by the University of Beira [37]. These images were captured under visible light in unconstrained conditions with more severe noise factors. In addition, the images were captured with a standoff distance of 4 to 8 meters with a rate of three images per meter while the subjects were walking toward the camera. Besides the noise factors introduced in UBIRIS V1, additional factors were added including head rotation, poor illumination, dark irides and obstructions due to glasses, contact lenses and hair.

The database has 522 left and right iris images collected from 261 subjects to produce 11,102 images in total. Similar to UBIRIS V1, the images were collected in two sessions with a resolution of 400×300 pixels. Figure 3.9 shows samples from the UBIRIS V2 databases.
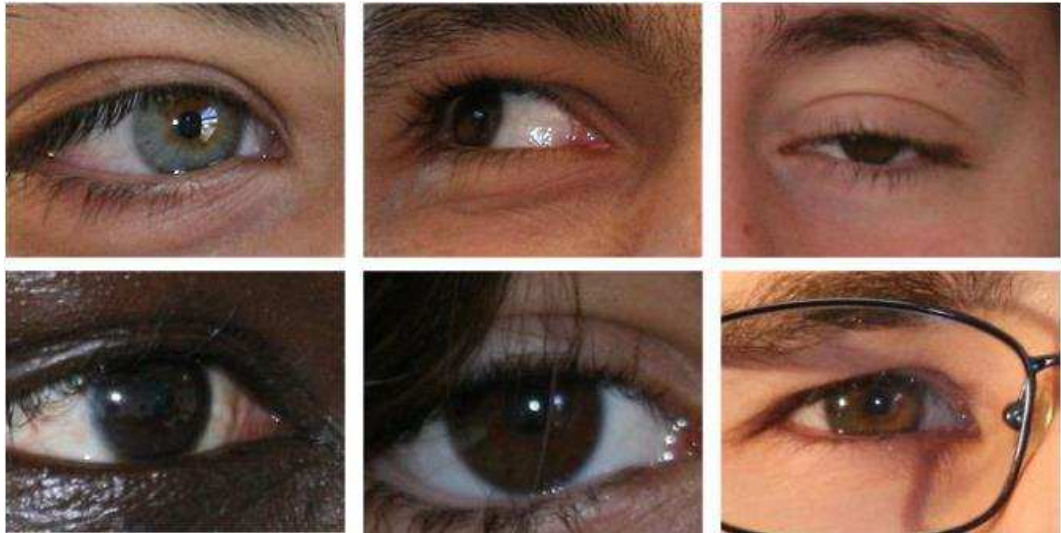
Figure 3.9: Iris samples from the UBIRIS V2 databases.

3.6.4 Other Iris Databases

There are several iris databases which were generated to study iris biometrics under special conditions. For example, the PolyU iris database [38] contains bi-spectral iris images which are captured under NIR and VL simultaneously from both right and left eyes of 209 subjects. Each image has a resolution of 640×480 and is available in both NIR and VL with pixel correspondences. Similarly, the UTIRIS database [39] contains two sessions with 1540 images; the first session was captured under VL while the second session was

captured under NIR. Each session has 770 images taken from the left and right eyes of 79 subjects where each subject has an average of 5 iris images.

The UPOL [40] iris database which was generated by the Palacky University Olomouc and contains a high quality iris images captured by an optometric framework. This made the UPOL database suitable to study the texture details of the iris and to assess the iris recognition performance under a noise-free environment.

The ND-Iris-Contact-Lenses database was released by the University of Notre Dam to study the effects of wearing contact lenses on the iris recognition performance [41]. The ND-Iris-Template-Aging database was also released by University of Notre Dam to study the effect of aging on iris recognition performance over two years time span [42]. On the other hand, the ATVS-FakeIris Database [43] was released to help in developing methods for iris liveness detection. This database contains two sessions: the first one with real iris images while the second has fake iris images which were printed on paper. Figure 3.10 shows iris samples from different iris databases.
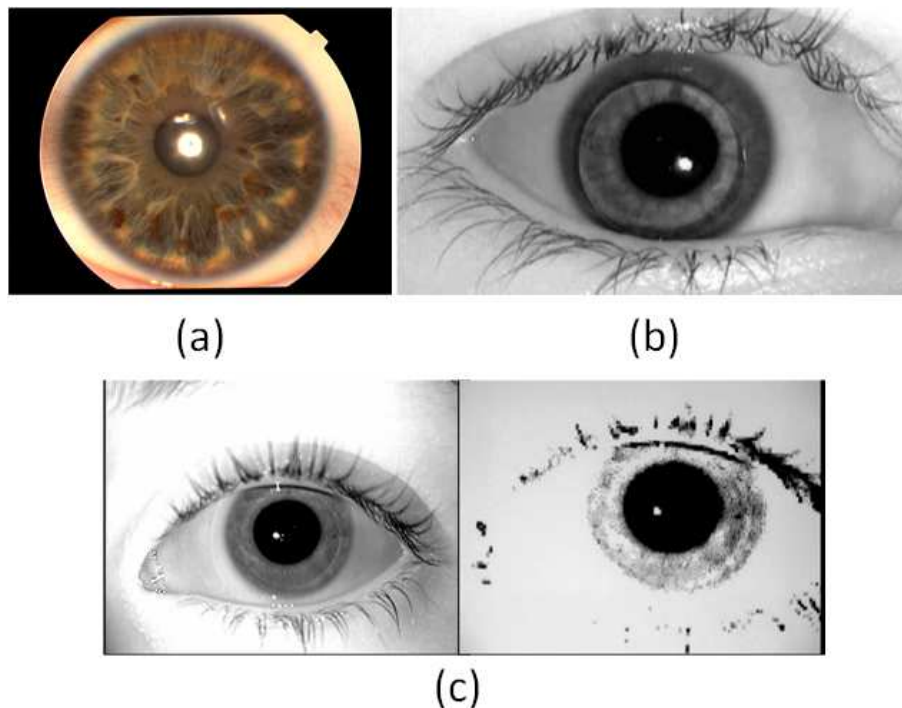
Figure 3.10: Iris samples from: (a) the UPOL database, (b) the ND-Iris-Contact-Lenses database and (c) the ATVS-FakeIris database.

3.7   Summary

In this chapter a brief introduction to performance evaluation for a biometric system was provided. In addition, this chapter shed light on the iris biometric potential along with the public deployments for a national scale iris based recognition system. Moreover, a survey of the publicly available iris databases was given.

The next chapter introduces the proposed segmentation method and the developed active contour model for image and iris segmentation.

Chapter 4

Iris Segmentation with the Active Contour Model

4.1 Introduction

Iris segmentation is an essential module in an iris recognition system as the performance of the system is highly dependent on this step and errors can lead to misclassification during authentication. This step involves isolating the iris structure from other components in an eye image, including the pupil, sclera, eyelashes, eyelids and reflections.

For iris segmentation, several researchers [7, 18] assume that the inner and outer iris boundaries are circular. This is a source of error, since the pupil boundary is not exactly a circle even in cooperative recognition [44]. In addition, Proenca and Alexandre [45] observed a significant degradation of iris recognition rates, especially in the presence of translation errors of the segmented pupil border. On the other hand, the outer iris boundary appears to be noncircular and nonelliptical in nonideal images such as off-axis iris images [46]. Moreover, simple shape assumptions for iris segmentation are not effective as the iris is partially deformed by eyelids, eyelashes and reflections.

All of these challenges explain the importance of using a noncircular approach for iris segmentation. The active contour is an ideal candidate for this purpose [20]. However, there are various drawbacks in the previous active contour models which make them inefficient for a precise iris segmentation. For instance, the snake active contour [47] is sensitive to the initial curve and cannot detect nonconvex objects [21]. Although the problems associated with the snake active contour were alleviated by Xu and Prince [21] in the GVF active contour, the GVF active contour still suffers from the formation of minimum energy points and stopping at spurious edges. In addition, the traditional snake and the GVF models are designed to shrink to reach the target boundary. Therefore, the contour is going to shrink and disappear if the initial mask lies inside of the target object [48].

In this chapter, a new active contour model for iris and image segmentation is proposed with robust initialization by integrating a new pressure force within the GVF model which addresses the drawbacks of previous active contour models. The movement direction of the active contour is geared based on the eyelid location.

This chapter is organized as follows. The next section presents a literature review on the iris segmentation methods. Section 4.3 presents a brief overview of the active contour models. Following this the proposed active contour model is introduced in Section 4.4.

Section 4.5 discusses the iris segmentation method in detail. The results are presented and discussed in Section 4.6. Finally, Section 4.7 summarizes this chapter.

4.2 Related Work

Many iris segmentation algorithms have been proposed. These algorithms can be broadly classified into three categories of iris segmentation; 1) Iris segmentation with the classical circular approaches and their improvements, 2) Iris segmentation with noncircular approaches and 3) Iris segmentation with active contour models.

Several traditional iris segmentation algorithms have been suggested including the well-known algorithms proposed by Daugman [7] and Wildes [18]. Daugman [7] used the IDO to find the assumed circular boundaries of the iris. On the other hand, Wildes [18] applied an edge detector followed by a CHT to localize the iris. Later, several others [49, 50] also proposed iris segmentation methods based on the CHT. Other methods based on the approximation of circular iris boundaries have also been implemented such as the least squares method proposed by Zhu et al. [51] and the Hough transform with IDO proposed by Abidin et al. [23].

The above classical approaches achieved good performance when the original iris images were captured in ideal conditions. However, there are major drawbacks with these algorithms. For instance, all these methods locate the iris by considering it as a standard circle which causes errors in terms of segmentation. The need for an exhaustive search for circles over a large N^3 parameter space also makes the procedure time consuming [19]. To solve the drawbacks of the previous traditional algorithms, some improved iris segmentation algorithms have been proposed. As a case in point, Tan et al. [52] estimate a coarse location of the iris using a clustering algorithm then the iris is segmented with a modified IDO which has lower computation time. Sahmoud and Abuhaiba [23] proposed an iris segmentation algorithm which starts by determining the expected region of the iris using the K-means clustering algorithm to reduce the search region, then the CHT is applied in order to estimate the iris radius and center. Radman et al. [53] adopted an improved IDO to segment the iris. In their approach the approximate position of the pupil center is determined using the circular Gabor filter to reduce the search time. Then, the iris

and pupil circles are localized using the IDO. Hong-Lin et al. [54] presented circle-based iris segmentation wherein a Laplace pyramid is incorporated to save computation time. Noise and reflections are removed by anisotropic diffusion and morphological operations, then the innovated curve evolution is used to detect the exterior boundary. Although the processing time is improved in the aforementioned methods, the application of these algorithms is limited to ideal iris images as they have adopted a circular model assumption.

Later other researchers employed noncircular iris segmentation approaches. For instance, He et al. [55] extracted an approximate position for the iris using an Adaboost-cascade iris detector followed by an elastic model called pulling and pushing for iris segmentation. Jan et al. [56] adopted a two-fold scheme based on a circu-differential accumulator and gray statistics to localize a coarse iris region. However, they tested their method on relatively easy iris databases acquired under a controlled environment. More recently, Frucci et al. [57] adopted the watershed transformation and circle fitting for iris segmentation. Although a noncircular method is adopted for the outer iris boundary, the pupil is segmented using a circular approach. Unfortunately, this may not provide an accurate segmentation as the pupil appears to be noncircular especially in the nonideal iris images. In addition, they only tested their method on visible light iris images.

Ryan et al. [22] adopted the starburst algorithm to locate pupillary and limbic pixels which are then used to fit a pair of ellipses for the iris localization. Good results are reported but the number of parameters to adjust and search increased (major and minor axis length, center coordinates and rotation angle). Ghodrati et al. [58] used morphology and the arched Hough transform to segment the iris. The results show an improvement in the precision of the iris localization but it should also be noted that the database used to test the methodology is the CASIA version 1.0 which is considered as a non-challenging database.

Recently, work using an active contour emerged in the literature and several researchers proposed different nonideal iris recognition schemes. For example, Daugman [59] proposed the Fourier active contour approach to model the pupil and the iris boundaries. This method, however, requires good quality iris images with high contrast [59]. Vatsa et al. [60] proposed an iris segmentation algorithm that uses a modified energy function and computes the exact iris boundaries by evolving an initial contour in a close region within

5 to 10 pixels. The problem with this algorithm is that the method could not segment the iris if the initial contour was placed far from the actual iris boundaries. Shah and Ross [61] proposed a method to detect the boundary of the iris based on a geodesic active contour. Unfortunately, because the stopping criterion of this method does not take into account the amount of edge detail, the evolving contour might not stop at the desired iris boundaries [61]. Talebi et al. [62] used a balloon active contour to segment the iris images from the CASIA version 1.0 database. However, the drawback with this method is that the initial mask for the active contour is set manually.

On the other hand, others [63, 64] proposed an automated method to estimate the approximate boundaries of the iris then they implemented the active contour to find the accurate pupil and iris boundaries. As a case in point, Roy et al. [63] applied direct least squares based elliptical fitting to obtain an initial curve for the active contour. Similarly, [64] took advantage of the CHT to initialize the active contour. Although these methods achieved good results, the main limitation is the complexity of the methods that are used to initialize the active contour compared with the simple approach that is adopted in this chapter, and is later explained.

Research in iris segmentation has been gaining more attention in recent years due to the interest in iris recognition at a distance [37]. In addition, competitions such as the Mobile Iris Challenge Evaluation (MICHE) [65] focus on the processing of visible light iris images. This has sparked more work on iris segmentation as the traditional iris segmentation algorithms cannot cope with such imaging [66, 67]. One of the main aims of this work is to design a robust iris segmentation algorithm to address this challenge.

4.3   Active Contour Model

An active contour is a curve that can move within an image from an initial state into a position where its energy is minimized under the influence of internal forces and image forces that pull it towards features such as lines and edges. These curves are called snakes because of the way the contours move while the energy is minimized. The active contour has become popular in computer vision fields such as edge extraction, image segmentation, motion tracking and 3D reconstruction [20]. In the next subsections, active contour

models and the proposed model will be discussed in detail.

The active contour models can be broadly classified into two types: parametric active contours [47, 21] and geometric active contours [68, 69]. Parametric active contour models depend on image gradients to stop the curve evolution on the object boundary [47] whereas geometric region based active contour models depend on partitioning the image domain by fitting statistical models such as intensity, colour or texture in each set of regions [69].

4.3.1 Active Contour Model

The snake is represented by a curve $v(s) = [x(s), y(s)]$ in which $s \in [0, 1]$. The variation s represents the length of the curve. The snake energy is defined as:

$$E_{snake} = \int_0^1 E_{int}(v(s)) \, \mathrm{d}s + \int_0^1 E_{ext}(v(s)) \, \mathrm{d}s. \tag{4.1}$$

The terms $E_{int}(v(s))$ and $E_{ext}(v(s))$ represent respectively the internal and external energy of the snake. The internal energy is used to control the deformability of the snake, and is written as:

$$E_{int}(v(s)) = \frac{1}{2}(\alpha(s) \, |v_s(s)|^2 + \beta(s) \, |v_{ss}(s)|^2) \tag{4.2}$$

where v_s is the first spatial derivative which represents elasticity, or membrane-like behavior, while the second term v_{ss} is the second spatial derivative and represents rigidity or thin-plate behavior. The coefficients α and β are weighting parameters that control respectively the elasticity and rigidity of the contour.

The external energy function is derived from the image energy. For example, in the case where edges of the image are of interest, the energy can be defined as:

$$E_{ext}(v(s)) = - \, |\nabla(G_\sigma(x, y) * I(x, y))|^2 \tag{4.3}$$

where $G_\sigma(x, y)$ is a Gaussian function with standard deviation σ, ∇ is the gradient operator and $*$ represents convolution while $I(x, y)$ is the image intensity function. This convolution smoothes the image to eliminate noise.

Substituting (4.2) and (4.3) in (4.1), gives us the whole expression of the snake:

$$E_{snake} = \int_s (1/2(\alpha(s)|v_s(s)|^2 + \beta(s)|v_{ss}(s)|^2) \qquad (4.4)$$
$$-(\nabla G_\sigma(x,y) * I(x,y))^2)\mathrm{d}s.$$

A snake minimizing (4.4) must satisfy the following Euler equation [21]:

$$\alpha v_{ss} - \beta v_{ssss} - \nabla E_{ext} = 0. \qquad (4.5)$$

Solution of the above equation gives the final contour minimizing E_{snake}. This equilibrium function could be considered as the force equilibrium function and is written as:

$$F_{int} + F_{ext} = 0. \qquad (4.6)$$

The internal force discourages stretching and bending while the external force pulls the snake towards the desired image edges. Therefore, when the original contour evolves and deforms into the final contour ($F_{int} = -F_{ext}$) this means that for every point along the curve the internal and external forces are equal and act in opposite directions to each other giving a stable state.

In order to solve (4.5) the curve is made to be dependent on an artificial parameter t (time) as follows:

$$\frac{\partial E}{\partial t}(t,s) = \alpha v_{ss} - \beta v_{ssss} - \nabla E_{ext} \qquad (4.7)$$
$$E(0,s) = E_0(s) \qquad (4.8)$$

where $E_0(s)$ is the initial curve. To allow the local minimum to be reached smoothly, the initial contour should be chosen sufficiently close to the object to be detected [21].

The snake active contour proposed by Kass et al. [47] has deficiencies. The two main drawbacks are the sensitivity to the initial curve and failure to detect nonconvex objects [21]. A partial solution to these problems were provided by Xu and Prince [21] in the GVF active contour which will be discussed in the next subsection.

4.3.2   Gradient Vector Flow Active Contour

The traditional snake model has drawbacks as discussed earlier. Much of the reason for poor performance was attributed to the external force. To ameliorate this problem, Xu and Prince proposed a new snake known as the GVF snake. The basic model for the GVF snake was the same as the traditional snake but with a new external force field ($E_{ext} = V$) known as the GVF field which was more suitable than the external potential force field and overcame the deficiencies of the previous model [21].

The GVF snake is defined as a contour $v(s) = (x(s), y(s))$ which satisfies the following Euler equation

$$\alpha v_{ss} - \beta v_{ssss} - V = 0 \tag{4.9}$$

where $V(x, y) = (u(x, y), v(x, y))$ is the vector field which substitutes the external vector force field E_{ext} of the traditional snake. The internal forces are defined similar to the original model consisting of elastic and bending forces. The edge map $f(x, y)$ of the image can be defined as follows:

$$f(x, y) = |\nabla(G_\sigma(x, y) * I(x, y))|^2. \tag{4.10}$$

$V(x, y)$ is then defined to be a vector field which minimizes the following energy function.

$$\iint \mu(u_x^2 + u_y^2 + v_x^2 + v_y^2) + |\nabla f|^2 \, |V - \nabla f|^2 \, dx \, dy \tag{4.11}$$

where u_x, u_y, v_x and v_y are the partial derivatives of $u(x, y)$ and $v(x, y)$ in the x and y directions.

With reference to (4.11) it can be seen that when the contour is far from the object boundary, ∇f becomes small and the first term of the equation dominates yielding a slowly varying field. On the other hand, when the contour is near the object boundary, ∇f becomes large and the second term dominates. This equation can be minimized by setting $V = \nabla f$. The parameter μ is a regularization parameter governing the trade-off between the first term and the second term which should be set higher in noisy images.

The GVF field can be found with the calculus of variation by solving the following

Euler equations:

$$\mu\nabla^2 u - (u - f_x)(f_x^2 + f_y^2) = 0 \qquad (4.12)$$

$$\mu\nabla^2 v - (v - f_y)(f_x^2 + f_y^2) = 0 \qquad (4.13)$$

where ∇^2 is the Laplacian operator. Therefore, the desired vector field $V(x, y)$ is the one that satisfies the above Euler equations. In homogeneous regions, f_x and f_y are both zero (because the gradient is zero). So, the vector field $V(x, y)$ is given by the first term and hence the resulting vector field is obtained by diffusing the boundary vectors into smooth areas using the Laplacian equation.

Equations (4.12) and (4.13) can be solved iteratively by treating u and v as a function of time. Therefore, the Euler equations now become:

$$u_t(x, y, t) = \mu\nabla^2 U(x, y, t) - (U(x, y, t) - \qquad (4.14)$$

$$f_x(x, y)).(f_x(x, y)^2 + f_y(x, y)^2)$$

and

$$v_t(x, y, t) = \mu\nabla^2 V(x, y, t) - (V(x, y, t) - \qquad (4.15)$$

$$f_x(x, y)).(f_x(x, y)^2 + f_y(x, y)^2).$$

The steady-state solution of these linear parabolic equations is the desired solution of the Euler equations and is found when $(t \rightarrow \infty)$. This functions as a stopping condition.

The GVF active contour solved the problems associated with the traditional active contour because the new model is less sensitive to initialization and can detect nonconvex objects. However, the GVF active contour still suffers from the formation of minimum energy points in the case of noisy images and stopping at spurious edges. In addition, the traditional snake model and the GVF model are designed to shrink to reach the target boundary. Therefore, they must be initialized outside the object boundary or else the contour would not reach the object boundary; if it lies inside of the target contour it is going to shrink and disappear [48].

To solve these drawbacks, a pressure force is integrated within the GVF active contour

model as described in the next subsection.

4.4   Proposed Active Contour Model

It is difficult to segment the outer iris boundary because the iris is often occluded by eye-lids or eyelashes and there is low contrast difference between the iris and sclera in some cases. Therefore, methods based on a non-parametric curve such as an active contour are appropriate, however, these methods need to be adapted to achieve an accurate iris segmentation.

Applying the traditional snake active contour will not give good results even if a GVF model is used as the contour will not stop at the desired boundary. This is because both models need to be initialized outside the object boundary in order to converge correctly. Therefore, in the case of an outer iris boundary segmentation, the contour would be trapped at the eyelids and never reach the zone of interest even if the "GVF" model is used as shown in Fig. 4.1.

In order to handle these problems, a new model with an added pressure force is proposed. Hence, the initial mask of the active contour is set to lie inside the iris boundary *(see Section 4.5.2)* and another force is added to the external force of the GVF active contour model. This force acts as a pressure force that pushes the contour to the object boundary. Without this pressure force, even if perfect edge detection was possible, the curve will shrink and vanish. Moreover, this force also solves the problem of contour stopping at the weak edges since it urges the contour to override them.

In this new model, the external force consists of the GVF force and an internal pressure force which acts in a direction normal to the curve to push it outward. So, (4.9) can be rewritten as follows:

$$\alpha v_{ss} - \beta v_{ssss} - V + K\overline{n_{(s)}} = 0 \qquad (4.16)$$

where $\overline{n_{(s)}}$ is the unit vector normal to the contour at point $v(s)$ and K is the amplitude of this force. The amount of the pressure forces can be controlled by adjusting the value of K.

In some applications a shrinking active contour model is required. This can be achieved
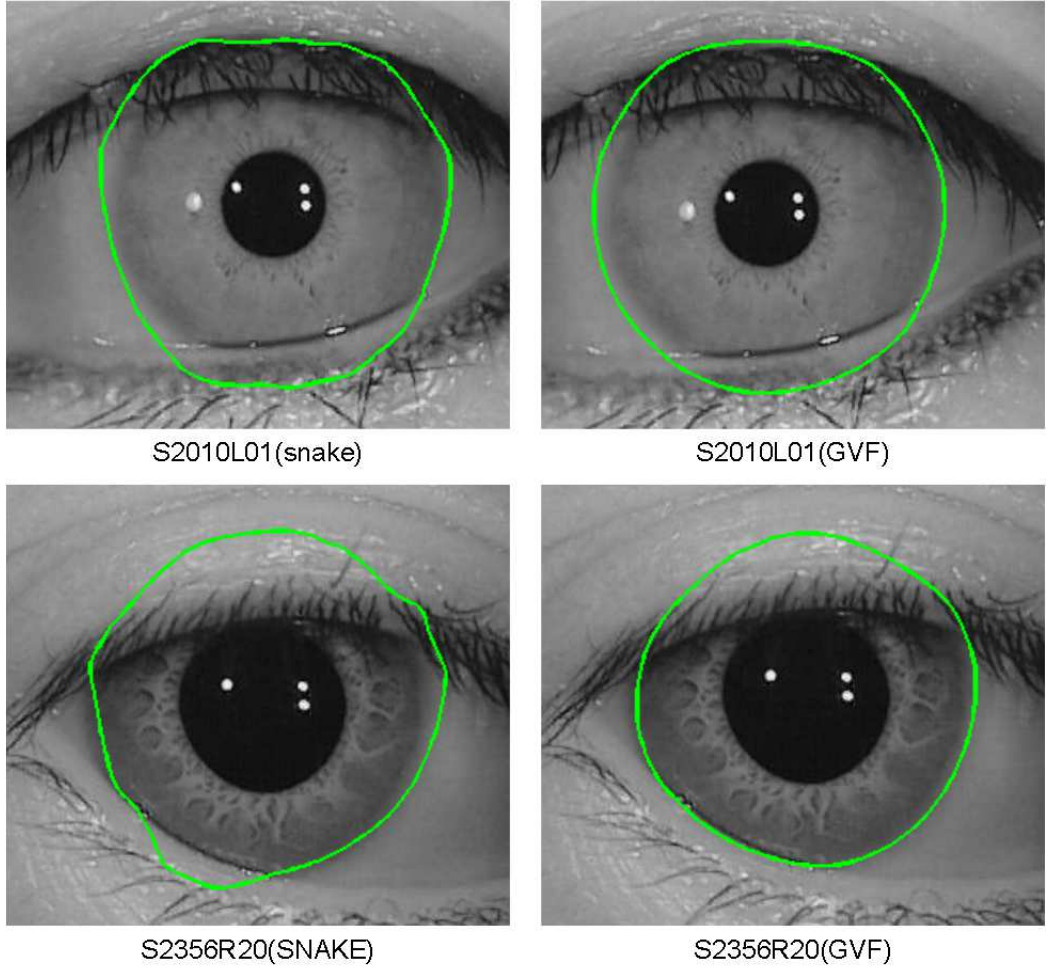
Figure 4.1: Segmenting different iris images from the CASIA-Iris Lamp V4 with the traditional snake (left column) and the GVF model (right column). The images are cropped for illustration purpose.

by changing the sign of the pressure force in 4.16 so the new equation can be written as:

$$\alpha v_{ss} - \beta v_{ssss} - V - K\overline{n_{(s)}} = 0. \tag{4.17}$$

A unit normal vector of a curve is perpendicular to the curve at a given point. This means a normal vector of a curve at a given point is perpendicular to the tangent vector at the same point. In summary, a normal vector of a curve is the derivative of the tangent vector of a curve divided by its amplitude as follows:

$$\overline{n_{(s)}} = \frac{T'(s)}{||T'(s)||} \tag{4.18}$$

where $T(s)$ is the unit tangent vector, $T'(s)$ is its derivative and $||.||$ defines the Euclidean norm. This pressure force not only pushes the contour outward, but also it prevents the curve from being trapped by spurious edge points.

It can be argued that the proposed pressure force is similar to the adaptive force proposed in [70]. This force was however added to the original snake model which makes it susceptible to well-known snake deficiencies [21]. In addition, the traditional snake and GVF models can only move in one direction (shrink). The proposed model in this chapter addresses the aforementioned drawbacks of the previous models and allows the GVF model to move in both directions (expand or shrink) which makes it adequate for various image segmentation applications including iris segmentation. The proposed active contour model is integrated with the proposed iris segmentation method as explained in the following section.

4.5 Proposed Iris Segmentation Method

The proposed method in this chapter is designed to achieve robust and accurate iris segmentation with high recognition rates for iris images where both the pupil and iris appear to be noncircular, and there are several occlusions by eyelashes and eyelids.

The iris segmentation algorithm proposed in this chapter has been divided into two main stages. The first stage is pupil segmentation (in Section 4.5.1). The second stage is iris segmentation (in Section 4.5.2). In order to complete the iris recognition system and evaluate the results of the iris segmentation algorithm, a noncircular iris normalization scheme is discussed in Section 4.5.3 and finally feature extraction and matching are presented in Section 4.5.4.

4.5.1 Pupil Segmentation

The target is to cover all the possible conditions for iris image capture. Therefore, the experiments in this chapter are conducted over two types of iris images: one for iris images which are captured under NIR light and the second for images captured under visible light.

If the iris image is taken under NIR light, the pupil will appear darker than its surrounding with high contrast between the pupil and the iris region (see Fig. 4.2 (a)) [71]. Hence, methods based on thresholding are convenient for isolating the pupil from the rest of the iris image and finding its coarse parameters. However, if the iris images are captured under visible light, the contrast difference between the pupil and the iris is low as shown in Fig. 4.5 (a). Therefore, a different approach should be adopted to find the pupil coarse parameters. Accordingly, the proposed pupil segmentation method in this chapter can work with two different types of iris images: 1) segmentation of the pupil captured under NIR light and 2) segmentation of the pupil captured under visible light.
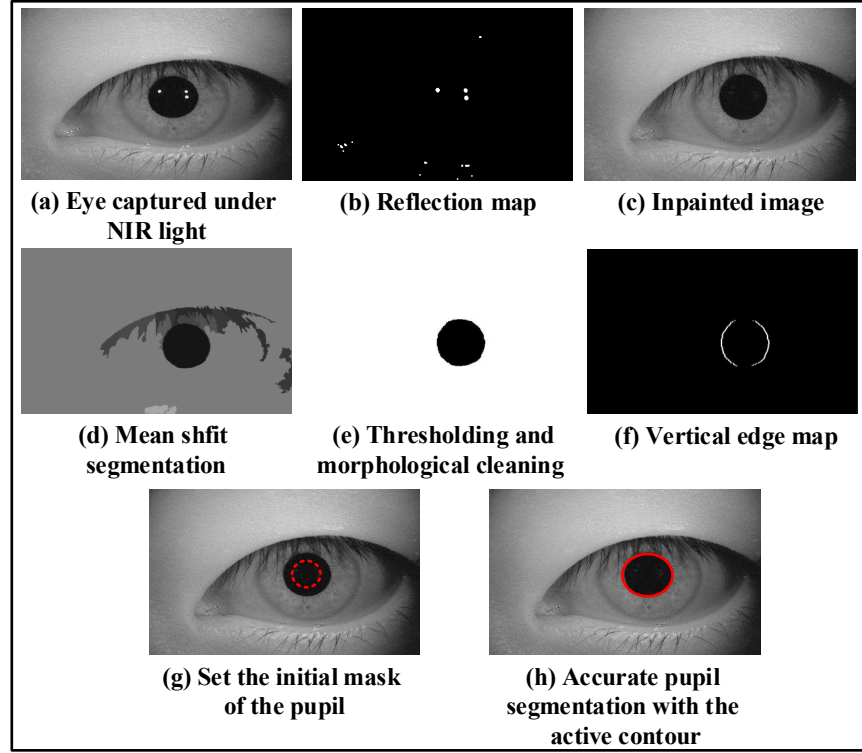
Figure 4.2: The steps of the pupillary detection algorithm for the iris images captured under near infrared light.

4.5.1.1 Segmentation of the Pupil Captured under NIR Light

In this subsection a fast and accurate method is proposed to segment the pupil in iris images captured under NIR light as in the CASIA V4.0 and MMU2 databases. The mean shift and morphological operations are combined with the proposed active contour to segment the pupil accurately. Mean shift is used to cluster the iris image while the mor-

phological operations are used to determine the approximate boundary of the pupil region then the proposed active contour is used to find the precise boundary.

For illustration purposes, Fig. 4.2 shows the major steps involved in the processing procedures and the obtained results. More specifically, the module broadly consists of the following sub-steps: *a)* Reflection Removal, *b)* Mean Shift, *c)* Detecting the Coarse Parameters of the Pupil and *d)* Pupil Accurate Segmentation with Active Contour. Detailed description of the signal processing procedures involved in each step are given in the next subsections.

(a) Reflection Removal   The pupil region has some light reflection spots which typically have the highest values in the iris images taken under the NIR light as shown in Fig. 4.2 (a). Local adaptive thresholding is used to build the binary reflection map (Fig. 4.2 (b)) by calculating an individual threshold for each pixel within a window of 30×30 pixels based on the intensity values of the local neighborhood of that pixel. Next, those reflection regions are filled with image inpainting from the nearest neighbors as shown in Fig. 4.2 (c).

(b) Mean Shift   Mean shift is a nonparametric space analysis technique for determining the maxima of a density function. Mean shift can be widely adjusted to different applications including clustering, image segmentation and object tracking [72]. The mean shift is therefore exploited for image clustering and applied in this chapter with a multivariate kernel. The eyelashes are mitigated in the resultant image while large objects such as the pupil are retained as shown in Fig. 4.2 (d). The number of clusters is regulated by the kernel bandwidth parameters (h_s, h_r) as in [72] which are set empirically to be (4,3). In addition, spatial regions containing less than 700 pixels are eliminated to reduce the noise in the resultant image.

(c) Detecting the Coarse Parameters of the Pupil   After applying the mean shift, the pupil can be easily isolated by adaptive thresholding based on Otsu's method [73]. Then, a morphological dilation operation with a square structuring element is applied to the binary image in order to eliminate the effect of eyelashes.

Once the pupil is isolated, the CHT can be applied on the resultant binary image to detect the pupil's coarse parameters. After applying the Canny edge detector, only the vertical edges of the pupil are used as an input to the CHT (Fig. 4.2 (f)) in order to reduce the influence of the eyelids. The search region for the CHT will be limited to the pupil part. This will not only reduce the processing time of CHT significantly, but also reduce the errors of the false circle detection by CHT due to removal of unwanted edges.
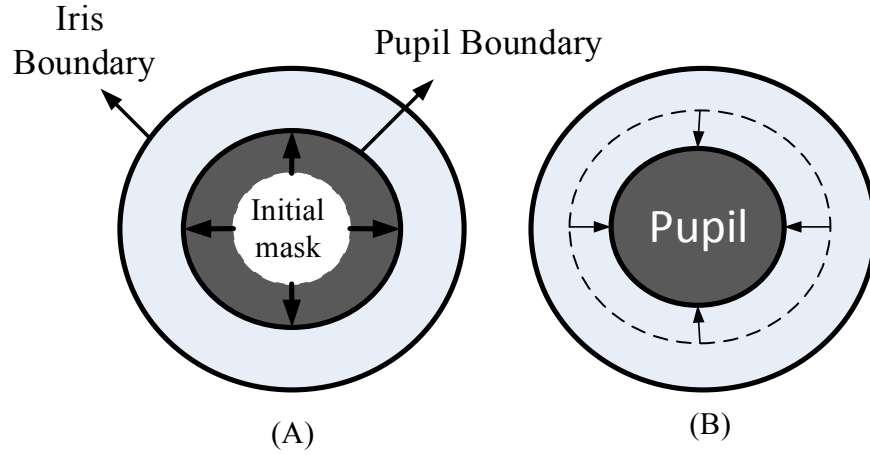
Figure 4.3: Initial mask evolving toward the final pupil boundary with (a): the proposed expanding active contour for pupil segmentation in the NIR iris images and (b) the proposed shrinking active contour for pupil segmentation in visible light iris images.

(d) Pupil Accurate Segmentation with Active Contour   The detected pupil parameters from the CHT in the previous sub-step are used to set the initial mask of the pupil which lies inside the pupillary region as shown in Fig. 4.3 (a). Finally, the pupil's accurate boundary is detected with the proposed active contour. Hence, the previously estimated mask is used as an initial mask for the expanding active contour. This, consequently, will improve the accuracy of the final contour and reduce the number of iterations.

4.5.1.2   Segmentation of the Pupil Captured under Visible Light

As mentioned earlier, isolating the pupil by thresholding will probably fail when the iris image is captured under visible light because of the low contrast difference between the pupil and the iris especially in dark pigmented iris images. There has been increasing attention for iris images taken with the visible wavelength under an uncontrolled environment due to different applications such as surveillance [37]. The irises in such images

vary in size and location and contain multiple noise factors as in the UBIRIS V1 and UBIRIS V2 databases. Therefore, to segment the pupil and find its coarse parameters the following approaches are adopted. Firstly, a novel method is proposed to discard the images that contain an invalid iris such as in the cases of closed or severely occluded iris based on the sclera presence. Next, after removing the reflection spots, a skin detection method is adopted in order to reduce the search region for the pupil within the non-skin regions. Later, the CHT is applied on the vertical edges of the non-skin regions to find the coarse parameters of the pupil and set the initial mask for the active contour. Finally, the proposed shrinking active contour is applied to segment the pupil accurately. Details of these operations are described in the next subsections.

(a) Closed Eye Detection   When the iris images are captured in an uncontrolled environment, it is likely that there are some cases where the eyelids are occluding the iris partially or completely. Therefore, the following method is proposed in order to discard these bad images. Since the sclera is the most easily distinguishable part in the eye image captured under visible light [74], the HSI color model is utilized in sclera isolation. The HSI color model represents every color with three components: hue (H), saturation (S) and intensity (I). The saturation component (S) indicates how much the color is affected by white color. Therefore, this component can be used as an indication for the sclera presence. First, the eye image is converted to the HSI color space then histogram equalization is applied to enhance the contrast of the sclera region in the S component of the eye image. Experimental analysis showed that the saturation value in the sclera region varies from 0 to 0.31 so Otsu's adaptive thresholding method is used to select the correct value which separates the sclera in each eye image. After thresholding, if the white pixels count is less than 1000 pixels the eye image is discarded. This value is set empirically because it is noticed that the iris in this case is very small and not usable. Fig. 4.4 illustrates the proposed closed eye detection method. While the first row of this figure shows a valid eye image with good number of pixels in the thresholded S component, the second row shows a heavily occluded eye image which has been discarded due to the limited pixels count in the resultant thresholded image. It should be noted that this method can be used efficiently to detect the presence of the sclera in an eye image, nevertheless, it may not

(a) Original image	**(b) _S_ component of the HIS color space**	**(c) Thresholded image**
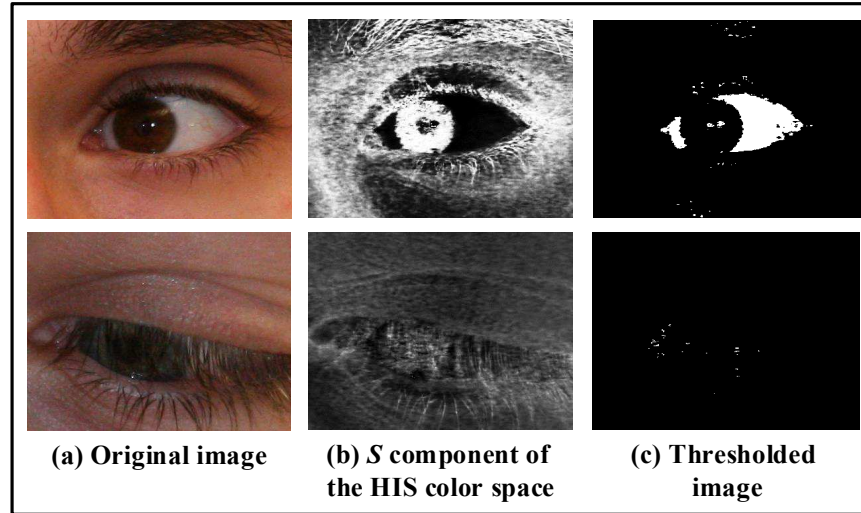
Figure 4.4: Sclera detection to discard the closed eye images; the eye image in the bottom row is discarded because the iris and sclera are heavily occluded.

provide an accurate segmentation for the sclera in all the cases.

(b) Skin Detection   A skin detector model is proposed to limit the search for the pupil in the non-skin regions only. The discrimination between the skin and non-skin pixels is carried out by introducing a skin color model which calculates the distance of the pixel color to skin color. Following the works of [75, 76], a non-parametric skin model is created using manually annotated skin and non-skin pixels. The pre-trained model for skin detection accommodated 138571957 pixels in total. The former model is used to estimate the skin color distribution without deriving an explicit model. Next, a Bayes' classifier is used to calculate the skin probability of each pixel (Fig. 4.5 (b)) and the skin likelihood image is computed with respect to the trained data. Finally, this likelihood image is thresholded at the zero level to generate the skin map as shown in Fig. 4.5 (c) and morphological image closing is used to close the small gaps in the resultant skin map.

(c) Detecting the Coarse Parameters of the Pupil   The YCbCr color space is utilized because it is capable of maximizing the contrast between the sclera and iris [74]. The histogram equalization is applied to the original image then the red chroma component of the YCbCr color space is extracted and the histogram equalization is applied again (Fig. 4.5 (d)). Next, the Canny vertical edge detector is applied on the non-skin regions as
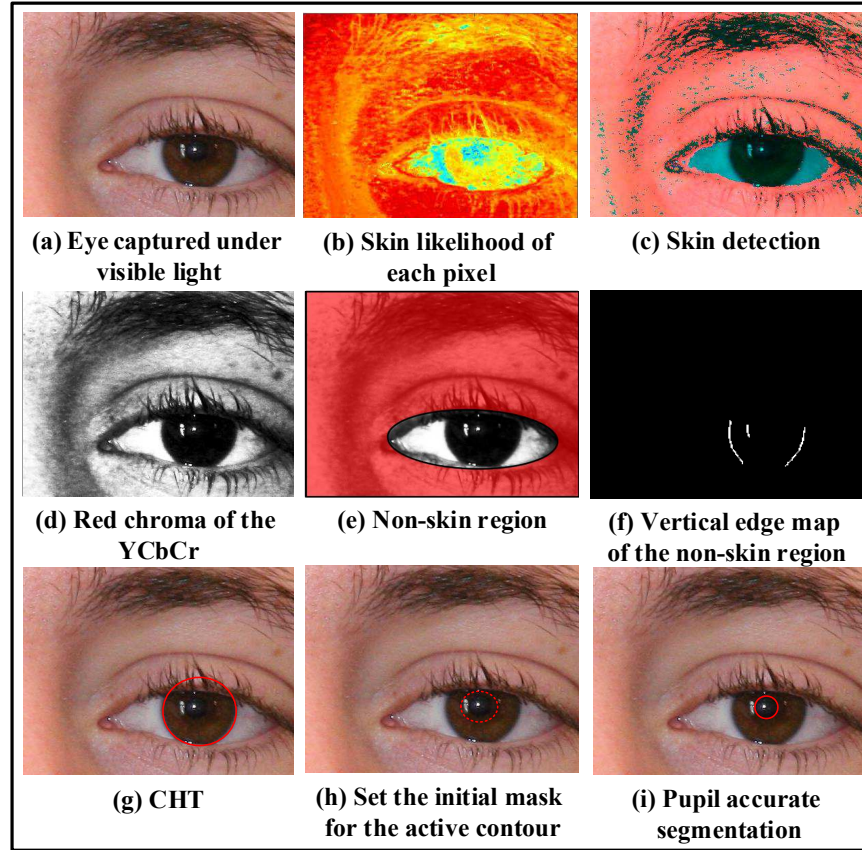
Figure 4.5: The steps of the pupillary detection algorithm for the iris images captured under visible light.

illustrated in Fig. 4.5 (e) and Fig. 4.5 (f). Later, the CHT is applied to the resultant edge image to determine the coarse pupil parameters.

(d) Pupil Accurate Segmentation with Active Contour The circle parameters obtained from the previous step are used to initialize the active contour. Accordingly, the center of the initial mask is set to be the same center of the iris obtained from the previous step. Although the pupil and iris centers are known to be non-concentric, this small translation of the initial mask will not affect the active contour convergence.

On the other hand, for calculating the radius of the initial mask (Fig. 4.5 (h)), the iris radius obtained previously from the CHT is utilized. From physiology, the ratio between the radii of the iris and the pupil is approximately 3:1 [77]. Hence, the radius of the initial circle is set to be $2/3$ of the iris radius to make sure that the initial circle always lies outside the pupil boundary even under low illumination conditions when the pupil becomes dilated. Then the proposed shrinking active contour model (Fig. 4.3 (b)) is

employed to segment the pupil accurately as shown in Fig. 4.5 (i).

4.5.2 Iris Segmentation with the Proposed Active Contour

Segmenting the outer iris boundary is a challenging task as the contrast difference between the pupil/iris or iris/sclera is not very high. Moreover, the appearance of eyelids and eyelashes hinders the segmentation process. Therefore, a robust segmentation method should be designed to achieve an accurate iris segmentation. The proposed iris outer boarder segmentation algorithm consists of the following steps:

4.5.2.1 Eyelashes Removal

Eyelashes need to be removed before applying the active contour to detect the iris boundary as they affect the contour convergence. To cure this problem, 2D order-statistic filtering is applied on the iris images. Experiments indicate that setting the size of the window to $[2 \times 10]$ with an order of 16 removes most of the eyelashes as shown in Fig. 4.6. The remaining eyelashes are either eliminated or weakened so the proposed active contour model is able to pass them due to the added pressure force.
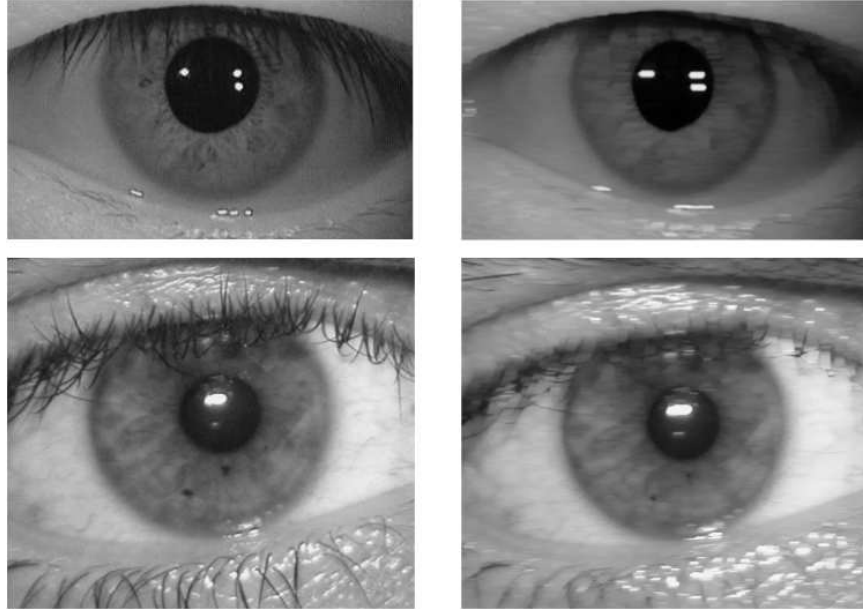
Figure 4.6: Attenuation of eyelashes with 2D order-statistic filter. Left column shows the original iris images while the right column shows the processed images.
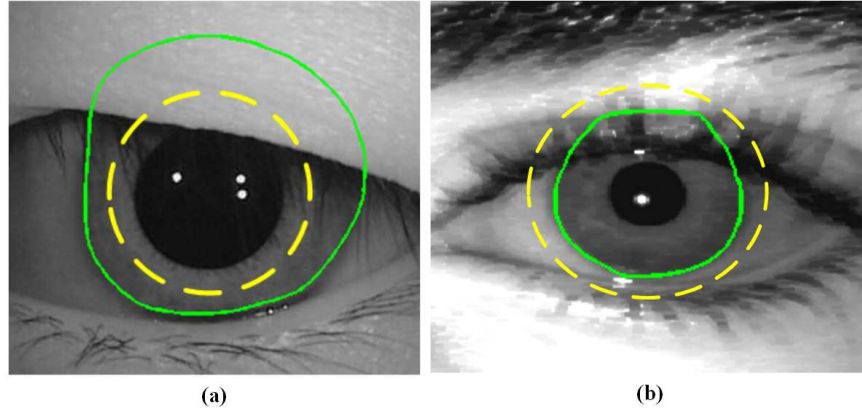
Figure 4.7: Unsuccessful iris segmentation with: (a) the expanding active contour and (b) the shrinking active contour.

4.5.2.2 Active Contour Initialization

After the pupil has been segmented, the active contour is initialized by a new circular mask which is created outside the pupil. The radius of this new mask is set to be larger than the radius of the final contour obtained from the segmentation of the pupil. This ensures the initial curve lies outside the pupil boundary in order to converge easily to the iris boarder.

The initial contour is evolved using the proposed active contour model from the initial mask until the energy function is minimized when the curve is on the iris boundary. This grants good segmentation if the eyelids are far from the pupil. However, there are some cases where the upper eyelid is near or covering the pupil; applying the active contour with an initial curve lying outside the pupil for such images will result in the contour bulging outward towards the eyelids as shown in Fig. 4.7 (a). This problem cannot be solved by using only the shrinking active contour because the contour will be trapped at the eyelashes and the fold of the eyelid as shown in Fig. 4.7 (b) which causes false segmentation.

4.5.2.3 Utilizing the Eyelid Position

To deal with this issue, a novel approach is proposed. A Hough line transform is applied to the upper portion of the iris image to detect the upper eyelid as shown in Fig. 4.8. Hence, if a line is found in the region of the initial contour, then the proposed shrinking
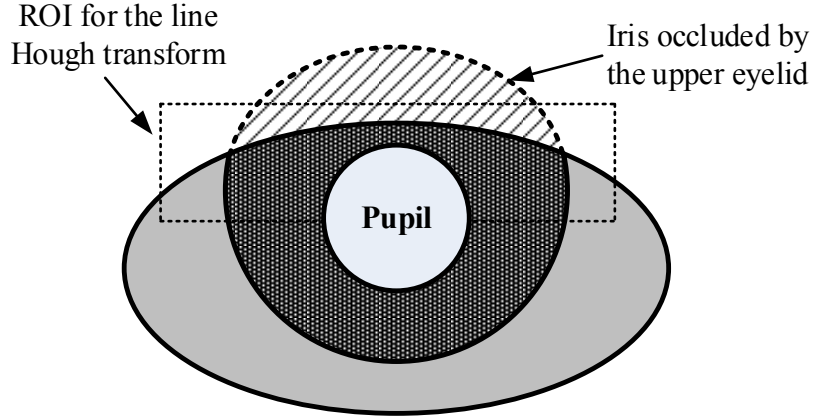
Figure 4.8: Utilizing the Hough line transform to check the occlusion by the upper eyelid to determine whether to use the proposed shrinking or expanding active contour.

active contour in equation (4.17) is applied. In this case, the initial mask for the active contour is set to be larger than the iris radius so it can converge correctly to the final contour shown in Fig. 4.9 (a). On the contrary, if the eyelids are not close to the pupil, then the expanding active contour is evolved from the initial mask which lies within the iris as depicted in Fig. 4.9 (b).

4.5.2.4 Eyelids Removal

This approach has the advantage that no separation algorithm is needed in finding the eyelids. Once the contour has converged to its final state, the last estimates of the iris boundaries can be used for removing the eyelids.

4.5.3 Noncircular Normalization

Once the segmentation is complete, the next stage is iris normalization. This stage is essential because the size of iris varies from person to person; even for the same person it can change, due to variation in illumination, pupil size and standoff distance. The normalization process involves unwrapping the iris and converting it into the dimensionless polar coordinates as proposed by Daugman [7]. However, the classical normalization approach requires both the iris and pupil to be circular in shape and share the same reference point for iris unwrapping. Since the pupil and the iris can be nonconcentric, a remapping formula is proposed by Masek [49] to rescale the centers. Nevertheless, when using non-

62
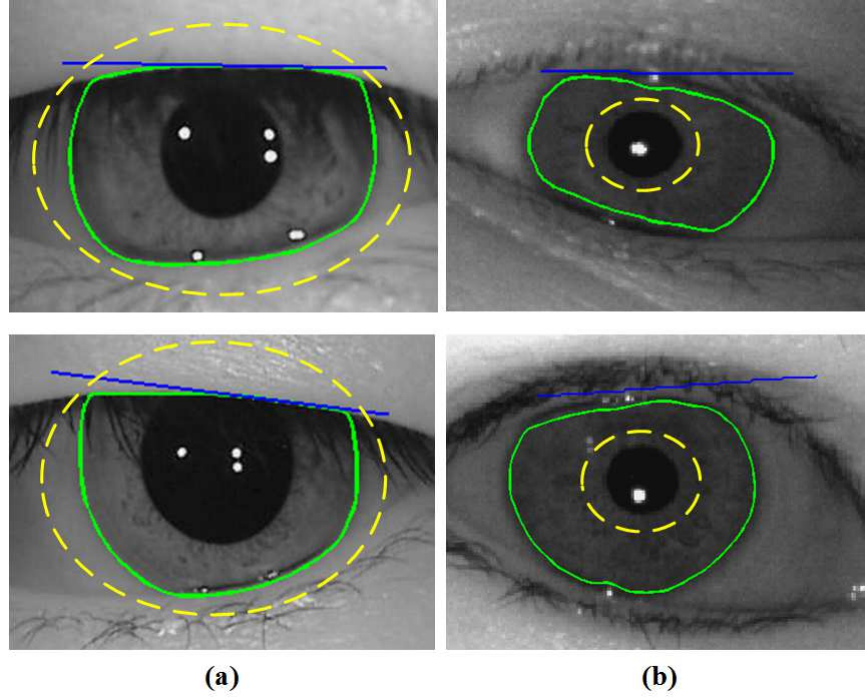
Figure 4.9: Initial mask moving toward the final iris boundary, where the blue line represents the detection of the upper eyelid by the Hough line transform and the dotted yellow line represents the initial mask in: (a) the shrinking active contour and (b) the expanding active contour.

circular approaches for iris segmentation, iris boundaries could be any kind of curve and finding a reference point becomes difficult so the traditional iris normalization method is inadequate.

Here, non-circular iris normalization method from [78] is adopted. Instead of representing the iris and the pupil by circles and finding a reference point, the boundaries obtained by the active contour are used directly for this purpose regardless of the iris or pupil centers. Hence, radial lines pass from the pupil contour to the iris contour and are traced back to the pupil center (X_{pupil}, Y_{pupil}) as shown in Fig. 4.10. After that, a number of data points are selected along each radial line.

The length of each radial line is calculated as the distance between the two contours (pupil boarder to iris boarder) which can be found as follows:

$$R_i = \sqrt{(x_i - x_p)^2 + (y_i - y_p)^2} \tag{4.19}$$

where x_i, y_i and x_p, y_p correspond to the iris and pupil contours respectively. Experiments

63
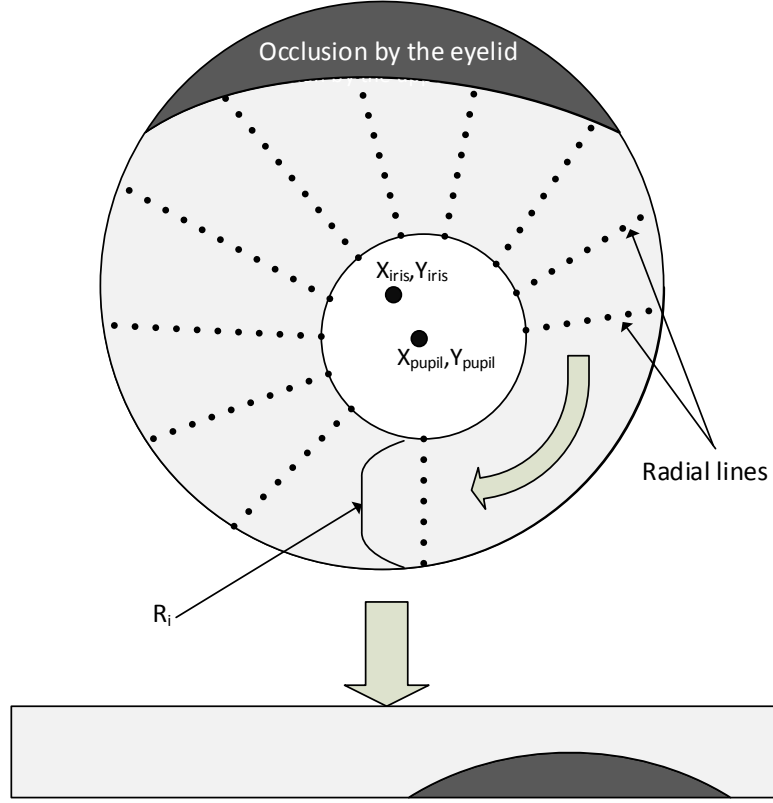
Figure 4.10: Diagrammatic representation of the noncircular normalization method for an off-axis iris image.

indicate that choosing 350 radial lines with 50 points in each gives the best result.

This normalization method can be used with any iris segmentation approach and the efficiency of noncircular normalization method can be seen from the improvement of the EER compared to the traditional circular normalization method as will be illustrated in Fig. 4.14, Fig. 4.15 and Table 4.2.

It is worth mentioning that although some researchers [61, 62] used active contour models for iris segmentation; for iris normalizing, a traditional circular method was employed. Consequently, this reduced the efficiency of their segmentation methods.

4.5.4 Feature Extraction and Matching

Feature encoding is implemented by convolving the normalized iris template with a 1D Log-Gabor filter [49]. Only the phase information is used to encode the iris pattern, because of its robustness to illumination, imaging contrast and camera gain [7]. The output of filtering is then phase quantized to four levels using the Daugman method [7], with

each filter producing two bits of data for each phase. At the matching stage, the Hamming distance has been applied as a metric for recognition. The Hamming distance algorithm also incorporates noise masking so that only significant bits are used in calculating the Hamming distance between two iris templates. The normalization, feature extraction and matching are adopted from the iris recognition system in [49].

4.6   Results and Discussions

Experiments were conducted on four iris databases namely: CASIA-IrisV4-Lamp, MMU2, UBIRIS V1 and UBIRIS V2. Most of the images in these databases are challenging and captured under different conditions from a wide variety of ethnicity.

The CASIA-IrisV4-Lamp was released by the Institute of Automation, Chinese Academy of Sciences [34]. It contains 16212 images from 819 classes. It was collected in an indoor environment with nonlinear deformation due to variations in visible illumination. In addition, it contains many images with heavy occlusion and poor contrast.

The MMU iris databases were provided by the Malaysian Multimedia University in two versions MMU1 and MMU2. The MMU2 iris database [35] consists of 995 iris images which have been collected with distance of 47-53cm away from the user. Unlike MMU1 which contains a smaller number of samples with few noise factors, the captured iris images in MMU2 contains severe obstructions by eyelids/eyelashes, specular reflection, nonlinear deformation, low contrast and illumination changes.

On the other hand, the UBIRIS V1 iris image database was released by the University of Beira, Portugal [36]. It contains 1877 images from 241 subjects in two different sessions. All images are taken under visible light. Several realistic noise factors were introduced to the session 2 of the UBIRIS V1 database such as reflections, defocus and oblique views to simulate non-cooperative conditions.

Finally, the UBIRIS V2 iris image database was also released by the University of Beira [37]. These images were captured under visible light in unconstrained conditions with more realistic noise factors. In addition, the images were captured on the move with a standoff distance of 4 to 8 meters. The database has 11,102 images in total taken from 261 subjects. A subset of this database that consists of 2250 images from 50 subjects

was employed in the experiments because the ground truth of these images are available from the work of Hofbauer et al. [66] so the segmentation performance can be measured accurately. Forty images were discarded by the proposed close eye detection method because the iris in these images is either occluded severely or completely. It is noteworthy that the NICE.I iris segmentation competition was based on only 500 images taken from the UBIRIS V2 database [79]. Therefore, this work exploits approximately four and half times the number of the iris images used in the NICE.I competition.

To evaluate the proposed segmentation algorithm, segmentation accuracy, recognition performance and computational time are assessed. Moreover, comparisons with different state-of-the-art iris segmentation algorithms in the literature are performed.

4.6.1 Segmentation Evaluation

The evaluation of iris segmentation results is a challenging issue because the ground truth is not available for all the images. Therefore, visual inspection is used to judge the performance where the ground truth in not available for the iris databases of CASIA V4, MMU2 and UBIRIS V1. On the other hand, the ground truth for 2250 images from the UBIRIS V2 was made available by the work of Hofbauer et al. [66]. A mathematical model was used to measure the segmentation performance as illustrated later in this subsection. In addition, the overall performance of the biometric system was measured with the ROC curves and the EER as illustrated later in Subsection 4.6.2.

Since the visual inspection is subjective, and different annotators give various results, measures of visual evaluation are adopted, namely: the maximum offset from the pupil boundary O_p and the maximum offset from the iris boundary O_i as shown in Fig. 4.11. Thus, the segmentation results are divided into three groups correct, fair and bad:

- Correct: the maximum offset between final contour and the actual iris or pupil boundary is no more than three pixels.

- Fair: $3 < O_i$ and $O_p <= 10$ pixels.

- Bad: O_i and $O_p > 10$ pixels.

After applying the proposed method to the iris images, the segmentation results are
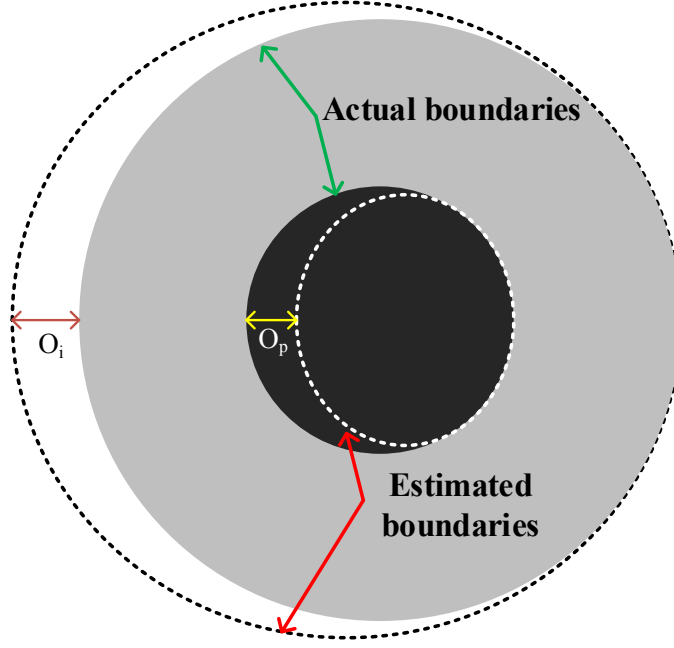
Figure 4.11: Visual evaluation criteria.

Table 4.1: Visual Segmentation Results of the Images in the CASIA V4, MMU2 and UBIRIS V1 Databases

Database	Correct	Fair	Bad
CASIA-IrisV4-Lamp	95.1%	2.9%	2%
UBIRIS V1 Session 1	96.5%	2.2%	1.3%
UBIRIS V1 Session 2	94.4%	3.3%	2.3%
MMU2	93.7%	4.1%	2.2%

considered "correct" if the final contour falls on the actual iris and pupil boundaries. On the other hand, "fair" segmentation is achieved when the maximum offset between the real boundary and the final contour boundary is within 3 to 10 pixels. Anything other than that is treated as "bad". Fig. 4.12 shows examples of different segmentation results. The iris segmentation results with the proposed method using the visual inspection are depicted in Table 4.1. According to Table 4.1, the highest and lowest percentage of correct segmentation are respectively recorded with the UBIRIS V1 session 1 and MMU2 databases. This is because most of the iris images in the MMU2 database contain severe obstructions by the eyelids/eyelashes, specular reflection and blured iris region. On the contrary, unlike session 2 of the UBIRIS V1 database, the iris region in session 1 of the same database are not occluded severely by the eyelids or blured. On the other hand,

67
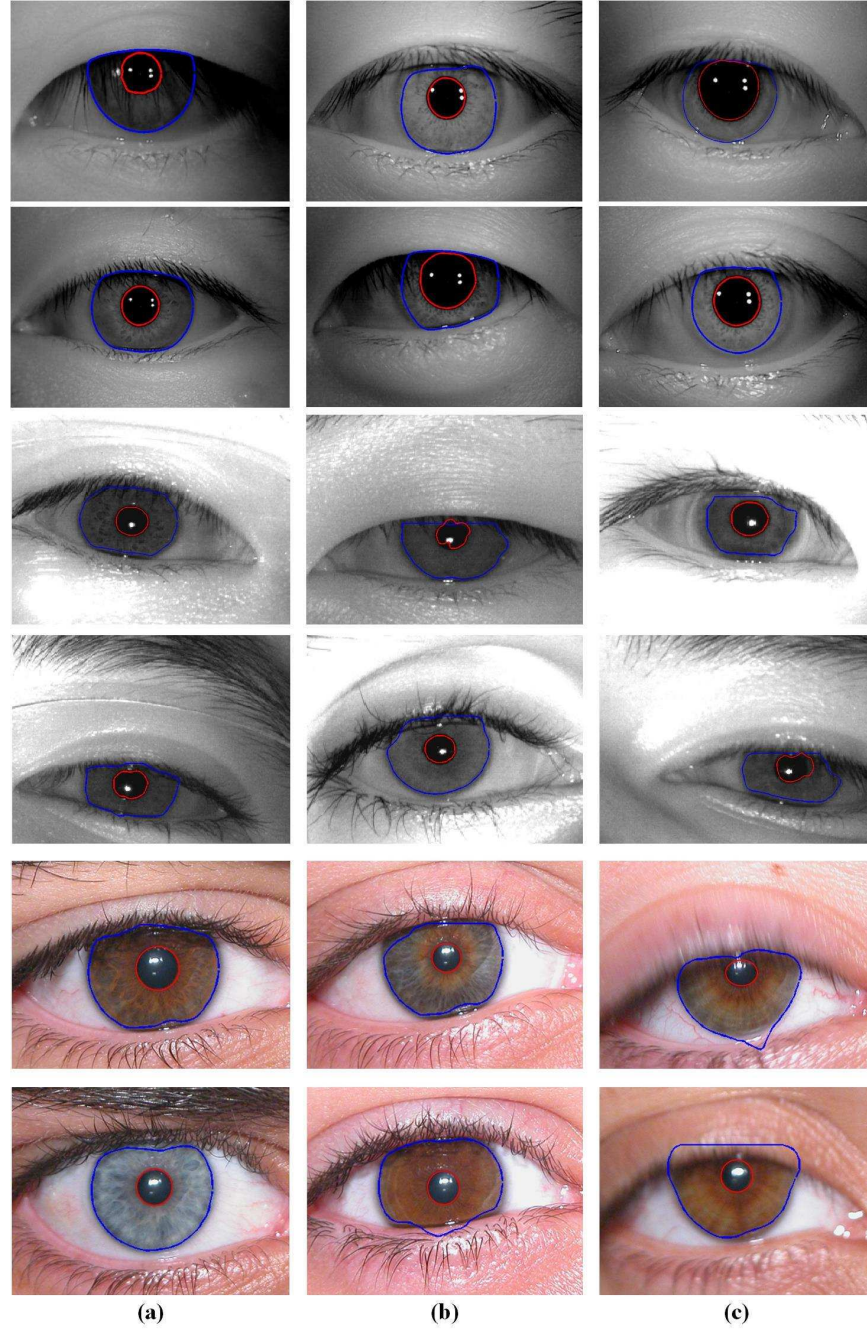
Figure 4.12: Segmentation classification results from the CASIA V4, MMU2 and UBIRIS V1 databases: (a) correct, (b) fair and (c) bad.

since the ground truth for the UBIRIS V2 database is available, a mathematical method based on the total number of the disagreeing pixels between the segmented image mask and its ground truth is adopted. Let I_i be the input image, $O(c', r')$ the output image segmentation mask and $C(c', r')$ its ground-truth. All the images of I_i, O and C have the same dimensions. Hence, the classification error rate (E_i) can be calculated as the

Figure 4.13: Iris segmentation results for images from the UBIRIS V2 database using the proposed method.

proportion of correspondent disagreeing pixels between the output image and its ground truth as follows [79]:

$$E_i = \frac{1}{c \times r} \sum_{c'} \sum_{r'} O(c', r') \oplus C(c', r') \qquad (4.20)$$

where c' and r' are the pixels of the output image and its ground truth; r and c are respectively the number of rows and columns of the image while $\oplus$ is the logical XOR operator. The total classification error ($E1$) is given by the average of all the errors (E_i):

$$E1 = \frac{1}{n} \sum_{i} E_i \qquad (4.21)$$

where n is the total number of images. The error $E1$ for the subset of the UBIRIS V2 database segmented with the proposed method is 2.95%. Examples of these segmentation results are shown in Fig. 4.13. Table 4.3 shows the efficiency of the proposed method compared to others. It can be clearly seen that the proposed iris segmentation method outperforms state-of-the-art methods in terms of the total classification error and processing time. For the outer iris boundary, the proposed active contour with prior contour initialization converges easily with average number of 75 iterations. As for the inner boundary, only 25 iterations are needed. This is because the initial contour is set to be very close to the actual pupil's shape. For iris segmentation, extensive experiments have been performed to determine a common set of parameters that can be used for accurate iris

extraction. Accordingly, the values of theses parameters to be used in (4.16) and (4.17) are $\alpha = 0.4$, $\beta = 0.2$, and $K = 0.3$. Using these values accurate segmentation results were sustained for iris images.

4.6.2 Performance Comparison

In order to evaluate the efficiency of the proposed method, it was compared with the previously quoted techniques in terms of recognition performance and processing time for the CASIA V4, MMU2 and UBIRIS V1 databases. As for the UBIRIS V2 database, the proposed algorithm performance is compared with the reported results in the works of Luengo-Oroz et al. [80], Chen et al. [81], Labati et al. [82] and Tan et al. [83] in terms of the total classification error ($E1$) and the processing time. This set of iris images and their respective ground truths are available from the works of [66, 79].

For the CASIA V4, MMU2 and UBIRIS V1 databases, the iris segmentation algorithms proposed [21, 61, 62, 69, 84, 85][1] are re-implemented and compared with the proposed algorithm through recognition performance. Only the segmentation approaches in the previously stated algorithms are implemented, and then the iris images are processed with the same normalization, encoding and matching procedures presented in this chapter. Furthermore, to evaluate the recognition performance, an ROC curve of the proposed algorithm is plotted and the EER is obtained from the ROC curve. Intuitively, the more accurate the segmentation, the higher the recognition performance.

Fig. 4.14, Fig. 4.15 and Table 4.2 illustrate the performance of the proposed algorithm against the performance of the previously stated algorithms [61, 62, 21, 69, 84, 85] on the images in the CASIA V4, MMU2 and UBIRIS V1 databases. It can be seen from Fig. Fig. 4.14, Fig. 4.15 and Table 4.2 that the proposed algorithm achieves the lowest EER. The classical circular approaches for iris segmentation fail in terms of detecting the iris in the nonideal iris images especially under the presence of noise or occlusion. In addition, the circular segmentation methods locate the iris considering it as a standard circle which causes errors in segmentation when the iris appears to be noncircular in nonideal conditions. The high EER reported in the work of Radman et al. [53] is also

---

[1]The source code of the active contour models used to replicate these works is available:
http://uk.mathworks.com/matlabcentral/fileexchange/28149-snake—active-contour/content/Snake2D.m
http://uk.mathworks.com/matlabcentral/fileexchange/24998-2d-3d-image-segmentation-toolbox
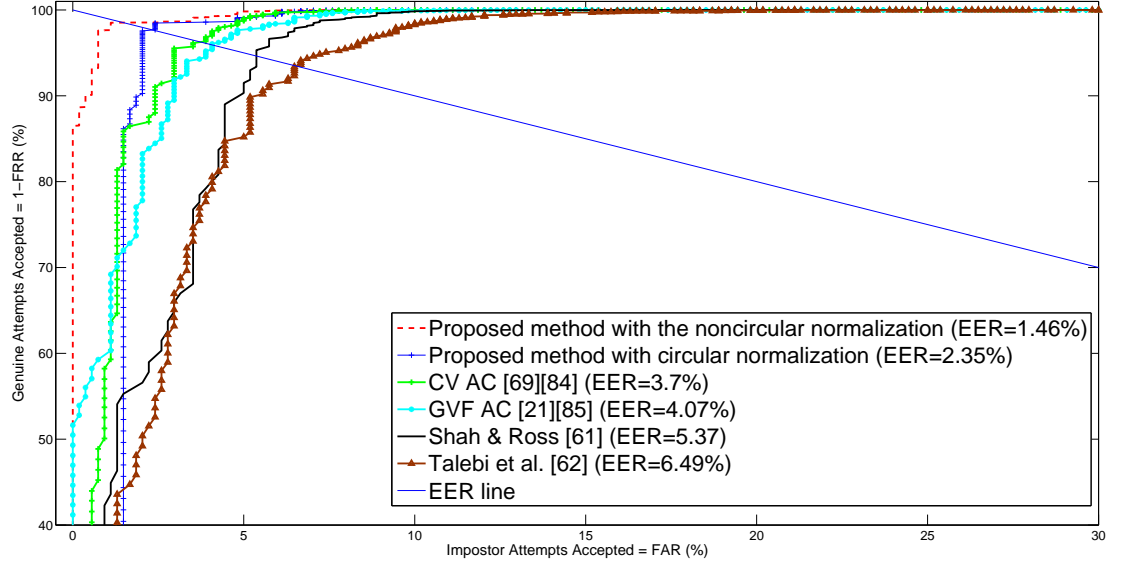
(a)
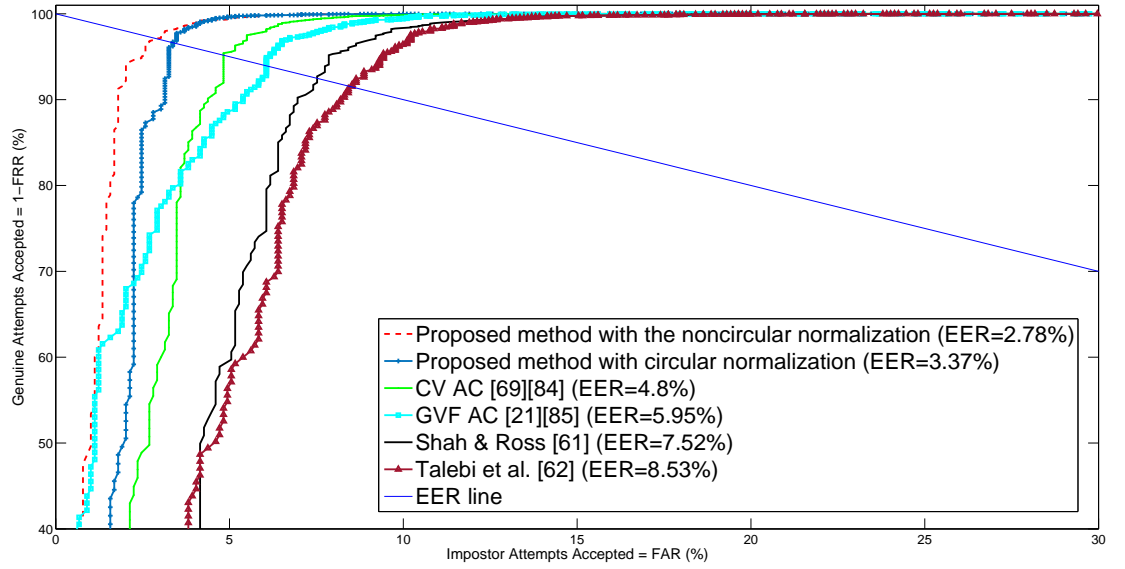
(b)

Figure 4.14: ROC curves and EERs illustrate the recognition performance of different iris segmentation methods: (a) CASIA-LAMP V4 database and (b) MMU2 database
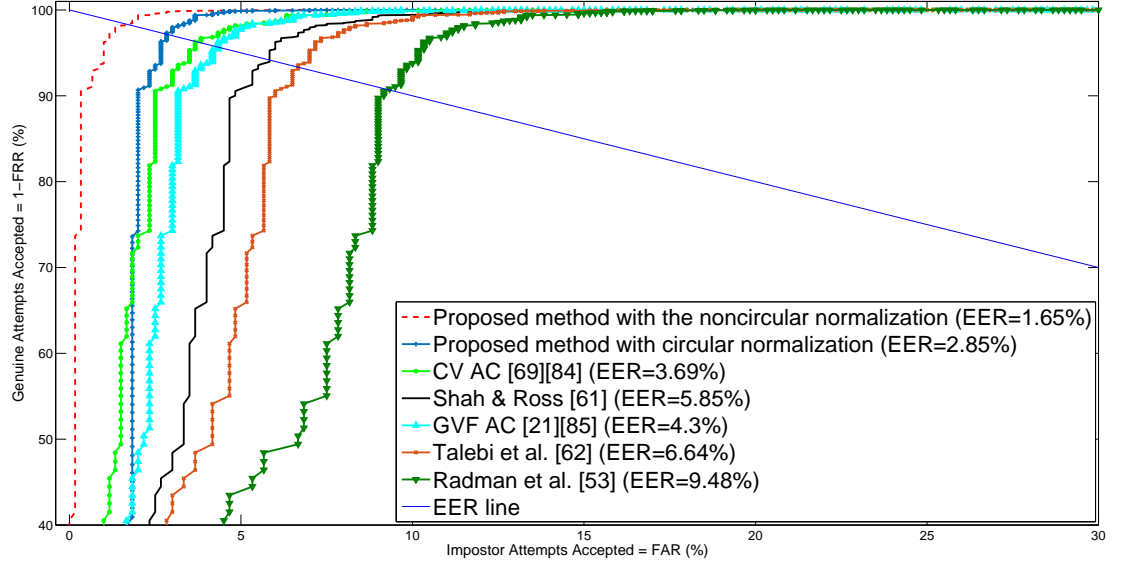
(a)
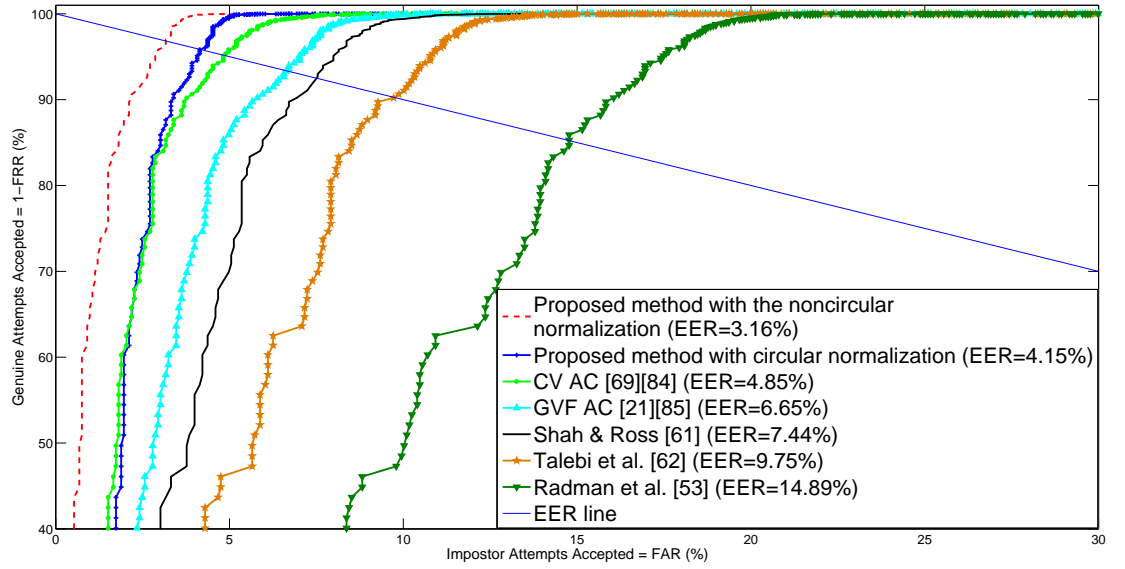
(b)

Figure 4.15: ROC curves and EERs illustrate the recognition performance of different iris segmentation methods: (a) UBIRIS V1 Session 1 and (b) UBIRIS V1 Session 2

Table 4.2: Performance comparison of the proposed method on the images from different databases in terms of EER.

Method	CASIA V4	MMU2	UBIRIS V1	
			Session 1	Session 2
Proposed with the noncircular normalization	**1.46%**	**2.78%**	**1.65%**	**3.16%**
Proposed with circular normalization	2.35%	3.37%	2.85%	4.15%
Shah and Ross [61]	5.37%	7.52%	5.82%	7.44%
Talebi et al. [62]	6.49%	8.53%	6.64%	9.75%
Chan-Vese AC [69, 84]	3.70%	4.80%	3.69%	4.85%
GVF AC [21, 85]	4.07%	5.95%	4.30%	6.65%
Radman et al. [53]	-	-	9.48%	14.89%

believed to be the result of adopting a circular approach (IDO) for iris segmentation.

Moreover, the recognition performance of the proposed method is better than the other methods based on classical active contour models [21, 61, 62, 69, 84, 85]. Several aspects contribute to this. Firstly, the coarse iris parameter estimations allow accurate mask initialization for the active contour and hence reduce the convergence time. Second, the integration of the pressure force with the active contour yields an effective curve evolving mechanism. Third, introducing the shrinking and expanding active contour contributes to more efficient iris segmentation for iris images with eyelids which lie close to the pupil. Fourth, adopting noncircular normalization has effectively normalized the segmented portion of the iris. All of these points have resulted in a more accurate and robust iris segmentation and, hence, higher recognition ratio.

On the other hand, the efficiency of the noncircular normalization method can be seen from Fig. 4.14, Fig. 4.15 and Table 4.2. The achieved improvements in the EER by this normalization method on CASIA V4, MMU2, UBIRIS V1 session 1 and UBIRISV1 session 2 are 37.87%, 17.5%, 42.1% and 23.85%, respectively.

As for the UBIRIS V2 database, Table 4.3 confirms that the proposed method is superior to the works of Luengo-Oroz et al. [80], Chen et al. [81] and Labati et al. [82] in terms of the total classification error ($E1$) and the computation times.

The smaller classification error reported in the work of [83] can be attributed to the smaller number of iris images employed in their experiment compared to this work. In addition, significant amount of time is required to complete their segmentation procedure whereas the proposed method achieved improvement of 96.6% in terms of the segmentation time.

Table 4.3: The average computation times and the $E1$ error reported with different segmentation methods for the UBIRIS V2 database.

	Total classification error ($E1$)	Time (sec)
Proposed algorithm	**2.95%**	**0.5**
Luengo-Oroz et al. [80]	3.05%	3.5
Chen et al. [81]	2.97%	6.77
Labati et al. [82]	3.01%	120
Tan et al. [83]	2.05%	130

4.6.3 Computation Time

All experiments were conducted on a 3.2 GHz core i5 processor with 8 GB of RAM under the Matlab environment. In addition, the time consuming stages such as the CHT are implemented under a C++ environment which is then called by Matlab with the help of a MEX-file in order to reduce the running time. As for the works of [80, 81, 82, 83] the experiments were conducted on a 2.2 GHz Intel processor with 2 GB of RAM to achieve a similar environment to the aforementioned works.

The proposed iris segmentation method can be divided into three main stages: pupil segmentation, eyelid detection and iris-limbic segmentation. Table 4.4 shows the average computation time for each stage of the proposed algorithm which is obtained from averaging the times of the segmentation process of 100 images taken from each database. The variations in the computation times among databases are due to the different images size.

Table 4.5 and Table 4.3 illustrate the average times of different iris segmentation algorithms. As mentioned before, the circle detection approaches are the most time consuming process especially if they are applied directly on the whole image without modification. The long computation time in the Shah and Ross method [61] can be attributed to the circle fitting method used for pupil localization before the active contour is applied. Similarly, Hilal et al. [64] applied the CHT to set the initial mask of the active contour. On the other hand, Talebi et al. [62] achieved lower time than the previous two methods because no circle fitting is used in their method however, the initial mask of the active contour is set manually. The significant computation time in the Tan et al. [83] method can be attributed to the calculation of the localized Zernike features for every single pixel in the iris image [86].

The proposed method is superior in terms of the computation time of the previous iris

Table 4.4: The Average Computation Times (in Sec) of Each Stage in the Proposed Segmentation Algorithm

	CASIA V4	MMU2	UBIRIS V1	UBIRIS V2
Pupil segmentation	0.32	0.28	0.4	0.24
Eyelid localization	0.01	0.01	0.02	0.01
Iris segmentation	0.31	0.23	0.35	0.25
Total average time	0.65	0.52	0.77	0.5

Table 4.5: Comparison among the Average Computation Times (in Sec) for Different Iris Segmentation Methods

	CASIA V4	MMU2	UBIRIS V1
Proposed algorithm	**0.65**	**0.52**	**0.77**
Radman et al. [53]	-	-	1.09
Shah and Ross [61]	5.1	4.2	6.2
Talebi et al. [62]	1.8	1.2	2.2
Hilal et al. [64]	4.8	3.9	5.8

segmentation methods [53, 61, 62, 64, 80, 81, 82, 83] and segmented the iris in less than a second which implies that it is suitable for real time applications.

4.7 Summary

In this chapter, a novel method for iris segmentation has been proposed. A new pressure force was designed and integrated with the GVF active contour to allow the contour to expand or shrink, which in turn helps to achieve robust iris segmentation.

The proposed iris segmentation process consists of two models: pupil segmentation and iris segmentation. For pupil segmentation, two schemes were proposed to determine the approximate parameters of the pupil in the iris images which are captured under visible and near infrared light. These parameters were then used to set the initial mask for the active contour. Initializing the active contour near the desired object boundary helps not only to reduce the execution time by minimizing the number of iterations, but also achieves robust segmentation as the search region is limited by the desired object. On the other hand, for iris segmentation, the Hough line transform was employed for eyelid detection. Hence, if the eyelid is closed or covering the pupil, the contour will shrink from the initial mask which is set to be larger than the iris. In contrast, if the eyelid is

not close to the pupil, the contour will expand from the initial mask which is set outside the pupil boundary. The proposed scheme is robust in finding the exact iris boundary and isolating the eyelids of the iris images. Moreover, noncircular iris normalization helped to effectively unwrap the segmented iris. Therefore, instead of representing the iris and the pupil in terms of circles, the obtained boundaries from the active contour are used.

The experimental results on the CASIA V4, MMU2, UBIRIS V1 and UBIRIS V 2 databases showed that the proposed scheme achieves state-of-the-art iris results in terms of segmentation accuracy and recognition performance while being computationally more efficient.

The next chapter presents the proposed iris image and template protection method. After the literature review, the chapter is divided into two parts. The first part presents the proposed watermarking algorithm for protecting the evidentiary integrity of the iris images while the second part presents the template protection method which along with the related analysis and comparisons.

Chapter 5

Iris Biometrics Protection with Watermarking and Visual Cryptography

5.1 Introduction

Despite the fact that biometric systems offer reliable techniques for personal identification, their usage could be hampered by the lack of a proper protection scheme that guarantees the security and privacy of the biometric traits. When biometric images or templates are transmitted through insecure channels or stored as raw data, they run risks of being stolen or modified. Hence, it is imperative that robust and reliable means of biometric protection are implemented [87].

Ratha et al. [88] described eight types of attacks that are possible in a biometric system, such as database template tampering, template modification, matcher override of the final decision and attack on the channel between the feature extractor and the matcher, or attack on the channel between the database and matcher. Moreover, due to the wide spread use of biometric technology in many applications, it is very likely that biometric data are being transmitted over non-secure channels. Hence, for a biometric system to work properly, the system must guarantee that the biometric data came from a legitimate person at the time of enrollment.

Several means are employed to protect biometric data such as only encryption, or watermarking and encryption. Encryption can be used as one potential mechanism of protecting the biometric features as in [89]. However, encryption may limit the capacity of large scale biometric systems because it can be computationally expensive. In addition, encryption cannot provide complete protection as the templates must be decrypted before matching. Jain et al. [90] emphasized this by suggesting that if only cryptographic techniques are used for the protection of biometric data, security of such data is not fully maintained because this data has to be decrypted somewhere.

Hence, the use of watermarking technology has emerged. Since watermarking involves hiding information within the host data, it can provide security even after decryption. On the other hand, VC can be utilized for biometric template protection. The most commonly used template for an iris recognition system is the so called *IrisCode* which is a binary compact representation of the iris [6]. This template is usually stored as raw data in databases or transmitted over unsecure channels. It was believed in the biometric community that this type of iris representation does not reveal adequate information to re-

generate the iris image as the encoding process is a one-way function. However, recently researchers [91, 92] were able to propose a reversibility scheme for the *IrisCode*. For instance, the authors in [92] proposed a reconstruction method for iris images from a binary template using a probabilistic approach based on genetic algorithms where they analyzed the vulnerabilities of commercial iris recognition systems by matching the reconstructed synthetic images with the original ones. Their experiments showed the fragility of such systems against this type of attack. Hence, it is imperative to find robust template protection methods.

In this chapter, the first work which considers enhancing the security of the iris biometric through both watermarking and VC is proposed. As such, a framework for iris image and template protection which incorporates two stages is introduced. The first stage is a robust watermarking algorithm to protect the evidentiary integrity of the iris images based on randomly exchanging four middle band coefficient pairs of the DCT. The aim of this stage is to embed text data as a contextual watermark in the iris image. The second stage is a VC scheme for iris template protection that neither involves pixel expansion nor quality loss in the iris template. Therefore, after decomposing the iris template into two shares, one share is given to the user on a smart card and the other share is stored in the database along with a signature generated by a hash function. Furthermore, the integrity of the stored iris template is also guaranteed by using the hash signatures.

This chapter is organized as follows. The next section presents a literature review on the related works while Section 5.3 gives an overview of the watermarking algorithms and visual cryptography. The proposed method is explained in Section 5.4. Experimental design and performance analysis are given in Section 5.5. Finally, Section 5.6 summarizes this chapter.

5.2   Related Work

Various algorithms have been suggested to protect biometric data and templates using watermarking or VC. In terms of watermarking, integrating watermarking with a biometric for the sake of protection has been achieved in two scenarios. The first scenario is when watermarking is applied to hide biometric data or a template inside a host signal (template watermarking) [93]. The other is using watermarking techniques for embedding owner-

ship information in the biometric data to protect the integrity of such biometric features (sample watermarking) [94].

Indeed, the first type (template watermarking) is limited to a secure channel transmission between the local matcher and the database. Consequently, the embedded biometric data could be degraded if the host signal suffers from attacks during the transmission and hence this could affect the biometric system recognition performance. On the other hand, the second type (sample watermarking) can be used effectively for database ownership protection and to ensure the biometric trait has come from a legitimate user by embedding user information inside the biometric trait [24]. Therefore, part of the work in this chapter is of the second type.

Most of the work reported on biometric protection by watermarking often focuses on fingerprints. On the contrary, a few relevant works have been undertaken so far for iris protection and the vast majority of them target hiding the iris template inside a cover image. For instance, Jain et al. [95] proposed a method to authenticate a fingerprint image with facial information using watermarking. The eigen coefficients of the user's face were embedded into the fingerprint image using a secret key with spatial domain watermarking. However, the fingerprint minutia could be reasonably impaired by embedding such face information inside it. In [96] the authors proposed a protection algorithm for the fingerprint image by watermarking it with a password extracted from the palm print of the same person. However, no experiments were performed by the authors to show the algorithm robustness against attacks. Later work in [97] proposed a watermarking algorithm for protecting the biometric image. In their paper the face images were watermarked using the watermarking algorithm due to Cox [98] which is based on the DCT. The face image acted as the username for identification while the watermark acted as a password for authentication. However, the problem with this watermarking scheme is that the original image is needed at the watermark detector stage.

In terms of iris protection with watermarking, Park et al. [99] proposed a watermarking method to embed the iris feature inside a face image and tested their method under different attacks. Bartlow et al. [100] proposed a scheme that encodes voice feature inside raw iris images stored in a database in order to provide additional level of authentication. Hassanien et al. [101] suggested a watermarking technique based on the Discrete Wavelet

Transform (DWT) to embed iris code data into the content of a digital image, which can be used eventually to identify the owner. However, no experiments have been undertaken on the effect of the watermarking on the iris recognition performance. Later, the authors in [102] applied biometric watermarking by taking the DWT and the Singular Value Decomposition (SVD) of the host image to obtain an eigen value vector. Next the iris features were extracted with the DCT to obtain 200 coefficients and then embedded in the eigen vector derived from the host image. Despite the good results reported by the authors, the drawback of this approach is that the feature extraction algorithm for the iris cannot be changed. The work in [103] applied watermarking to hide the fingerprint and iris features in a cover image. The cover image is divided into blocks then each block is transformed with a two-dimensional DCT and classified as a smooth block or edge block. The biometric features are embedded in the low frequency coefficients of the 8×8 DCT blocks while the edge blocks are eliminated. However, removing the edge blocks could unfortunately result in quality degradation of the original image. A watermarking algorithm is proposed in [104] to protect the iris images based on interchanging fixed locations of the DCT middle band coefficients. However, there is a possibility that an attacker can predict these fixed locations and destroy the watermark information or embed false watermark data. In addition, the iris template is still not protected as the aim of that work was to protect only the iris images.

It is evident from the previous work that watermarking can be used effectively to protect the integrity of biometric images. However, watermarking cannot be used for biometric template protection because watermarking introduces some degradation to the host medium. In a biometric system, any degradation is not acceptable because such degradation can affect the system performance significantly. Therefore, alternative approaches are needed. Hao et al. [105] presented a scheme for integrating the iris biometric into cryptographic applications. The iris code is encoded with binary keys using the XOR operation while Hadamard and Reed-Solomon codes are used to resolve the variability in the iris code. Good performance is reported in term of FRR however, the iris images were ideal and according to [106] a high FRR was recorded when the approach is implemented on the ICE database. In addition, the 44 security bits used in this method is inadequate in the current cryptographic applications [107]. Cimato et al. [108] proposed a multi-biometric

system which extracts an identifier (ID) from the templates of left and right irises of each user with the help of a hash function and pseudo random permutation function. In the verification phase, both templates and the user's ID are required to complete the authentication. Although the proposed method can offer a secure ID generation, the iris template is still not protected. In addition, this method requires two biometric traits to generate the ID which adds more complexity.

More recently, Yan et al. [107] proposed a method to preserve the privacy of the biometric credential. Their method fuses the user's biometrics (iris image) with a reference subject using keys extracted from the user's biometrics to generate a BioCapsul which could be used later instead of the biometric template for the authentication. However, this method degrades the iris recognition performance. In addition, generating the BioCapsul requires more complex operation compared to the simple VC scheme that is proposed in this chapter. Rathgeb et al. [109] proposed a scheme for iris template protection based on Bloom filters. Although the usage of Bloom filters enables irreversibility for a uniform iris template, the scheme does not provide unlinkability. This concern is reinforced by the work of Hermans et al. [110] which demonstrated that the scheme is vulnerable to cross-matching attacks.

VC is a robust way of protecting an image without complicated mathematical operations or any knowledge of cryptography. Although there are some methods for protecting the biometric traits with VC [111, 112], few enhance the security of the iris biometric through VC. The authors in [111] proposed a method to secure the face image with the help of stenography and VC to decompose the image into two shares where each share is stored in a different database so that the original image can be revealed only when both shares are available. The drawback with the previous method is the additional cost of having two database servers for saving the shares and the possibility of tampering of the templates in these databases. In [112] the authors proposed a method to improve the privacy of the face images using half-toning and VC to split the face images into two encrypted parts. However, the efficiency and robustness of this method was not supported with experimental results or security analysis. In addition, no information was given on how to deal with the loss in contrast or the problem of resolution expansion of the resultant image in the aforementioned methods.

In this work, the gap in iris biometrics protection is filled by proposing a two stage framework for iris image and template protection. The first stage is a robust watermarking algorithm to protect the evidentiary integrity of the iris images based on exchanging multiple middle band coefficients of DCT blocks using text data as a contextual watermark. The second stage is protecting the iris template with VC by dividing the template into two secret shares.

5.3   Watermarking Algorithms and Visual Cryptography

As the proposed approach is based on two main schemes, namely watermarking and visual cryptography, this section prepares the reader by giving a brief overview of watermarking and visual cryptography algorithms and highlights why the DCT has been selected as the transform basis of the proposed watermarking algorithm.

5.3.1   Watermarking Algorithms

A number of watermarking techniques are available for embedding information securely within an image. Watermarking algorithms can be classified according to their embedding domain into transform domain techniques [113] and spatial domain techniques [114]. In the spatial domain the pixel values are directly modified to embed the watermark using different approaches such as Least Significant Bit (LSB) [114] or the correlation-based technique [115]. While the spatial domain techniques have least complexity and highest payload, they cannot withstand low pass filtering, image compression and common image processing attacks [116]. Therefore, transform domain watermarking has emerged because it is robust against image manipulations and compression. In the frequency domain, the host image is segmented into multiple frequency chains using several transformations such as DWT or DCT [113]. Then, the inverse transform is applied to obtain the watermarked image.

In principle, any frequency domain transform can be used for image watermarking, however, frequency transformation in the DCT domain allows an image to be divided into different frequency bands, so they facilitate embedding the watermarking information in a specific frequency band [117]. It has been found that the middle frequency bands are

most suitable for embedding the watermark because the low frequency band carries the most visually important parts of the image while the high frequency band is exposed to removal through compression and noise attacks on the image. Therefore, embedding the watermark in the middle frequency band neither affects the visual important parts of the image (low frequency) nor overexposes them to removal through attacks when high frequency components are targeted [117].

5.3.2 Watermarking Requirements from a Biometric Prospective

A number of distinctive properties should be available in any watermarking algorithm [98]. Nonetheless, additional constraints are needed when dealing with a biometric system. These characteristics can be summarized as:

- Perceptibility: in the invisible watermarking, the watermarking algorithm should not affect the quality of the underlying host image or introduce visible distortions.

- Robustness: the watermark should be detectable even after the host image undergoes a variety of manipulations and attacks such as filtering, noise and compression. However, increasing the robustness of the watermarking algorithm will affect the perceptibility of the host image.

- Capacity: the watermarking capacity is a measure of how much watermarking data can be embedded in the host image.

- Recognition performance: a good watermarking algorithm should not introduce considerable degradation on the recognition performance of the biometric system.

5.3.3 Visual Cryptography

Visual cryptography is a secret sharing scheme which was introduced by Naor and Shamir [118] to decompose an image into n random shares such that, when all these shares are superimposed, the original image is revealed again. However, the secret image will not be revealed if the number of stacked shares is less than n.

In the case of (2,2) VC, each pixel in the binary image I of size $(M \times N)$ is encoded into two subpixels called shares $SR1$ and $SR2$ as illustrated in Fig. 5.1. If the pixel

Pixel	Shares		SR1 (OR) SR2	SR1 (XOR) SR2
	SR1	SR2		
White	▢■	■▢	▢	▢
▢	■▢	▢■	▢	▢
Black	■▢	■▢	■▢	■
■	▢■	▢■	▢■	■

Figure 5.1: (2,2) visual cryptography; the 50% loss in contrast can be solved when using the XOR operation.

is white, one of the two rows in Fig. 5.1 corresponding to the white pixel is randomly chosen to generate $SR1$ and $SR2$ and vice versa for a black pixel. Therefore, neither $SR1$ nor $SR2$ divulges any information about the binary image I. The original image can be reconstructed again by superimposing $SR1$ and $SR2$ together. However, the resulting image will be of size $(M \times 2N)$. Although traditional VC is a simple and a powerful protection scheme, unfortunately, it has not been widely used due to the increase in image size and the 50% loss in contrast [119]. The problem of contrast loss can be solved by superimposing the shares together using the XOR operation instead of the OR (as shown in Fig. 5.1) and hence no loss in quality will occur in the original image. Nevertheless, the generated image is still twice the size of the original one. An approach to remedy this problem is proposed in the next section.

5.4 The Proposed Method

In this section, a two-layer iris images and templates protection scheme is proposed. The first stage is a robust watermarking algorithm to protect the iris images based on randomly exchanging the middle band coefficients of the DCT blocks using text data as a contextual watermark while the second stage is focused on protecting the iris template with VC.

5.4.1 Stage one: iris images watermarking

The proposed watermarking algorithm is designed in a way which will not degrade the iris image or the recognition performance while it retains robustness to malicious attacks and

noise. Hence, the proposed algorithm encodes one-bit of the binary watermark text into each 8×8 sub-block of the host image by ensuring that the difference of two mid-band coefficients is positive in the case the encoded value is 1. Otherwise, the two mid-band coefficients are exchanged. Accordingly, after the DCT is applied to the image, an 8×8 block is taken. Each DCT block consists of three frequency bands as illustrated in Fig. 5.2. F_L and F_H denote the low and high frequency components of the block respectively, while F_M is the middle frequency band and is chosen for embedding watermark information. This avoids significant modifications to the cover image while providing additional resistance to lossy compression techniques which target the high frequency components [120].
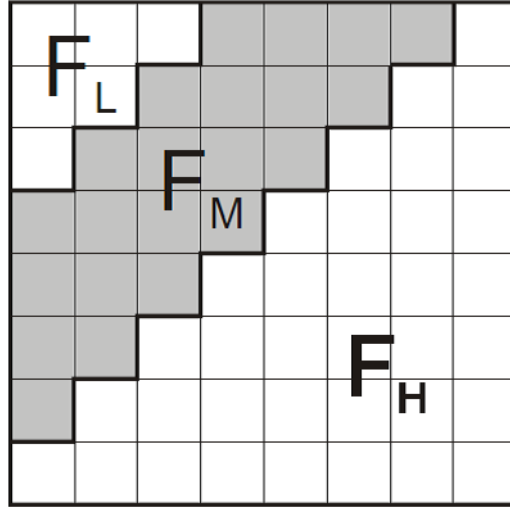
Figure 5.2: Frequency regions in an 8×8 DCT block [1].

The proposed scheme targets the middle band frequency F_M so that two locations from the DCT block ($DCT_{u1,v1}$ and $DCT_{u2,v2}$) are chosen as the region for comparison. Firstly, the watermark text is converted to a binary image and each pixel inside the watermark text is checked so the coefficients are swapped if the size of each coefficient does not agree with the bit that is to be encoded. Thus, if the pixel value in the binary text is 1, the DCT coefficient are swapped such that $DCT_{u1,v1} > DCT_{u2,v2}$. On the other hand, if the pixel value is 0, coefficients are swapped so that $DCT_{u2,v2} > DCT_{u1,v1}$.

Hence, instead of degrading the image by inserting data, this scheme hides the watermark by interpreting 0 or 1 with the relative values of the two fixed locations in the F_M region ($DCT_{u1,v1}$ and $DCT_{u2,v2}$). It is known that the DCT coefficients of the middle

frequencies generally have similar magnitudes [121] so swapping of such coefficients will not alter the watermarked image significantly.

During the watermark extraction, the 8×8 DCT of the cover image is taken again, and the watermarking algorithm will decode a 1 if $DCT_{u1,v1} > DCT_{u2,v2}$; otherwise it will decode a 0 to form the watermark.

Yet, if only one pair of coefficients is used to hide the watermark data, it will become vulnerable to noise and attacks. Therefore, the watermark can be destroyed by image manipulations and compression (as it is demonstrated in Section 5.5.1.5). In addition, an attacker can analyze some watermarked copies of the same image to predict the locations of these coefficients as well as destroy them. To solve these problems, exchanging multiple coefficient pairs is performed by selecting random locations from the F_M frequency band for the embedding purpose. Exchanging more than one pair will increase redundancy and make the scheme robust to different attacks. In addition, the random selection of the embedding locations in each DCT block makes it almost impossible for the attacker to predict these locations and destroy the watermarking information or embed false information inside the watermarked image.

16	11	10	16	24	40	51	61
12	12	14	19	26	58	60	55
14	13	16	24	40	57	69	56
14	17	22	29	51	87	80	62
18	22	37	56	68	109	103	77
24	35	55	64	81	104	113	92
49	64	78	87	103	121	120	101
72	92	95	98	112	100	103	99

Figure 5.3: JPEG quantization table and the selected embedding locations.

Empirical results have shown that exchanging four pairs from the middle frequency band gives a good trade-off between robustness and perceptibility. Basically, any of the 22 middle band locations (F_M) shown in Fig 5.2 can be utilized for the embedding purpose. Nevertheless, to make the algorithm robust to Joint Photograph Expert Group (JPEG) compression, eight embedding pairs have been selected based on the recommended JPEG quantization table. It can be seen from Fig. 5.3 that these locations are suitable for embed-

Table 5.1: The locations array (L) used for selecting the watermarking embedding locations

p	1	2
1	(1,4)	(3,3)
2	(2,3)	(4,1)
3	(1,6)	(3,5)
4	(1,5)	(3,4)
5	(3,4)	(6,1)
6	(4,3)	(5,2)
7	(4,2)	(5,1)
8	(2,6)	(3,6)

ding because they have almost the same value in the JPEG quantization table. Therefore, a scaling applied to any of these coefficients will scale the other one with the same factor. This in turn will preserve the relative size of the coefficients to be exchanged.

Thence, the location of the pairs to be exchanged will be selected randomly from the eight shaded pairs shown in Fig. 5.3 based on a private key $S1$ which is stored on a smart card as illustrated later in Section 5.4.2.1. This key ($S1$) is used as an initial seed for the random number generators which will generate the four digits vector r within the range of 1 to 8. Hence, four new rows from the location array L shown in Table 5.1 will be chosen for each 8×8 block of the cover image based on the random numbers. For example, if $r = [2\ 3\ 5\ 8]$ this means that the $2^{nd}, 3^{rd}, 5^{th}$ and 8th rows from the location array L will be chosen and the corresponding pairs will be used for the embedding purpose. So, when the 8th row from the location array (L) is selected, this means that $p = 8$ and $DCT(L_{p,1})$ is (2,6) and $DCT(L_{p,2})$ is (3,6) which correspond to the values of 58 and 57 in Fig. 5.3, respectively.

Moreover, to improve the robustness of the watermarking algorithm, a watermark strength constant S is added such that $DCT_{u1,v1} - DCT_{u2,v2} > S$. If coefficients do not meet this criterion, a constant value will be added to satisfy the relation.

5.4.1.1 Embedding algorithm

Each 8×8 block of image will be used to hide one bit of watermark text. A binary text image (W) is taken as a watermarking object which can be interpreted as a $1D$ array of 1s and 0s. The watermark text image carries the person's bio-information such as name, ID

and date of birth. The steps of the embedding algorithm are shown in Algorithm 1 while the flow chart is depicted in Fig. 5.4.

Algorithm 1: Embedding algorithm.

Input: $s1, L, W, X$
    ($s1$: watermarking key, L: locations array, W: watermarking text, X: host image)
Output: Y
    (Y: watermarked image)
1: **for** $i = 1 \rightarrow size(W)$ **do**
2:    $X_{8 \times 8(i)} = X$;
    {subdivide the host image (X) into blocks of 8×8 pixel}
3:    $X_{DCT(i)} = 2D\text{-}DCT(X_{8 \times 8(i)})$
    {Compute the 2D-DCT of each 8×8 block of the host image}
4:    for each DCT block, generate 4 random numbers **r** within the range of $1 - 8$ based on the private key $s1$.
5:    **if** $W_{(i)} = 0$ **then**
6:      **for** $j = 1 \rightarrow 4$ **do**
7:        $p = \boldsymbol{r}(j)$ {select one of the random locations}
8:        exchange DCT coefficients to meet this condition
        $DCT(L_{p,1}) < DCT(L_{p,2})$
        {Now adjust the four values such that their difference becomes larger than the strenghth constant s, thus:}
9:        **if** $DCT(L_{p,1}) - DCT(L_{p,2}) < s$ **then**
10:          $DCT(L_{p,1}) = DCT(L_{p,1}) + s/2$
11:          $DCT(L_{p,2}) = DCT(L_{p,2}) - s/2$
12:        **end if**
13:      **end for**
14:    **else if** $W_{(i)} = 1$ **then**
15:      **for** $j = 1 \rightarrow 4$ **do**
16:        $p = \boldsymbol{r}(j)$ {select one of the random locations}
17:        exchange DCT coefficients to meet this condition
        $DCT(L_{p,1}) >= DCT(L_{p,2})$
        {Now adjust the three values such that their difference becomes larger than the strength constant s, thus:}
18:        **if** $DCT(L_{p,2}) - DCT(L_{p,1}) < s$ **then**
19:          $DCT(L_{p,2}) = DCT(L_{p,2}) + s/2$
20:          $DCT(L_{p,1}) = DCT(L_{p,1}) - s/2$
21:        **end if**
22:      **end for**
23:    **end if**
24:    Take inverse DCT to reconstruct Y
25: **end for**

The host image

Locations array (*L*)

1: {(1,4) ; (3,3)}
2: {(2,3) ; (4,1)}
3: {(1,6) ; (3,5)}
4: {(1,5) ; (3,4)}
5: {(3,4) ; (6,1)}
6: {(4,3) ; (5,2)}
7: {(4,2) ; (5,1)}
8: {(2,6) ; (3,6)}

Private key (*s1*)

Subdivide the host iris image into 8×8 block

Compute the 2D-DCT of each block

Watermark binary text

Name:
M. Abdula
ID: 1234
dd/mm/yy

For each bit in the monochrome watermark text *(W)*

For each DCT block, generate 4 numbers (*r*) between 1 and 8

W(i) = ?

W(i) = 0

W(i) = 1

$p=\textbf{\textit{r}}(j)$

$p=\textbf{\textit{r}}(j)$

Swap one pair such that:
DCT($L_{p,1}$) < DCT($L_{p,2}$)

Swap one pair such that:
DCT($L_{p,1}$) >= DCT($L_{p,2}$)

DCT($L_{p,1}$) - DCT($L_{p,2}$) <*s*?

DCT($L_{p,2}$) - DCT($L_{p,1}$) <*s*?

Yes Yes

No

Yes

No

Yes

DCT($L_{p,1}$)=DCT($L_{p,1}$)+*s*/2
DCT($L_{p,2}$)=DCT($L_{p,2}$)-*s*/2

DCT($L_{p,2}$)=DCT($L_{p,2}$)+*s*/2
DCT($L_{p,1}$)=DCT($L_{p,1}$)-*s*/2

j<=4

j<=4

No

No

Take the Inverse DCT

Reconstruct the watermarked image from the 8×8 blocks

The watermarked image

Figure 5.4: Block diagram of the proposed watermarking algorithm.

5.4.1.2 Strength of watermark

The robustness of the watermark has been increased by choosing an appropriate value of the strength constant S. Increasing S will degrade the image but it will reduce the chance of errors at the detection phase. Experimental results indicate that setting S equal to 15 is the most suitable value in terms of perceptibility versus robustness. Therefore, the experiments have been conducted by keeping $S = 15$.

5.4.1.3 Detection algorithm

Watermark extraction is the reverse procedure of the watermark embedding algorithm. The embedding location will be selected based on the private key ($S1$) which is either obtained from the smart card or generated from the stored template in the database ($share1$) with the help of a hash function as demonstrated later in Section 5.4.2.1. The steps of the detection algorithm are shown in Algorithm 2.

Algorithm 2: Detection algorithm.

    Input: $s1, L, Y$

        ($s1$: watermarking key, L: locations array, Y: watermarked image)

    Output: W

        (W: binary text)

  1: **for** $i = 1 \rightarrow size(W)$ **do**

  2:     for each DCT block, generate the same 4 random numbers **r** within the range of $1 - 8$ based on the private key $s1$.

  3:     $Y_{8 \times 8(i)} = Y$;

        {subdivide the cover image (Y) into blocks of 8×8 pixels}

  4:     $Y_{DCT(i)} = 2D\text{-}DCT(Y_{8 \times 8(i)})$

        {Compute the 2D-DCT of each 8×8 block of the cover image}

  5:     **for** $j = 1 \rightarrow 4$ **do**

  6:       $p = \boldsymbol{r}(j)$ {select one of the random locations}

  7:       **if** $DCT_{p,1} > DCT_{p,2}$ **then**

  8:         $W(i) = 1$

  9:       **else**

10:         $W(i) = 0$

11:       **end if**

12:     **end for**

13:     reconstruct the binary text image W from $W_{(i)}$

14: **end for**

5.4.2   Stage Two: Visual Cryptography

Attacks on the stored biometric template in a database are considered as one of the most destructive attacks because they lead to different vulnerabilities [122] such as gaining an unauthorized access to the system by creating a physical spoof from the template [91, 92]. In addition, they allow an unauthorized access to the system by the replication of the stolen template to the matcher. Moreover, the stored template could be replaced by an imposter. In this section, a novel template protection scheme in order to tackle the above problems is proposed. Furthermore, to protect the integrity of the template saved on the card or database, the SHA-2 hash function is used. SHA-2 is a set of one way hash functions designed by NSA [123] which generates a unique signature of a vector. Therefore, the hash function is implemented to generate a unique signature of the template as will be discussed in the next sub-section. The proposed template protection method consists of two modules namely: (A) Enrolment module and (B) Authentication module.

5.4.2.1   Enrolment module

In this module, the binary template (*IrisCode*) is extracted from the iris image using Daugman's encoding method [6]. Then, the binary template is decomposed into two shares using (2,2) VC and the original template is discarded. After that, two 256 bit signatures $S1$ and $S2$ are generated as signatures for $share1$ and $share2$ respectively using the SHA-256 hash function to maintain the integrity of the iris template. In the enrolment stage, one of the decomposed shares ($share1$) is stored in the database along with $S2$ (signature of $share2$) while $share2$ and $S1$ are given to the user on a smart card. $S1$ is also used as the private key which selects the watermarking embedding locations. The enrolment stage is shown in Fig. 5.5.

5.4.2.2   Authentication module

During the authentication process, the system sends a request to the database to fetch the corresponding share $share1$ based on the generated signature ($s2$) from $share2$. Then, the obtained share from the database is stacked together with the user's share from the smart card in order to reconstruct the original iris template. Moreover, to make sure that
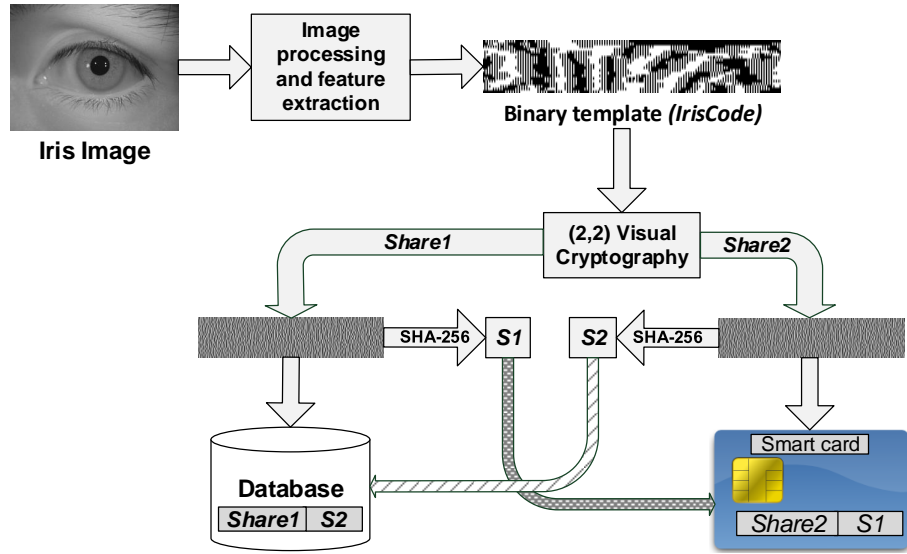
Figure 5.5: The enrolment module of the proposed method using VC.
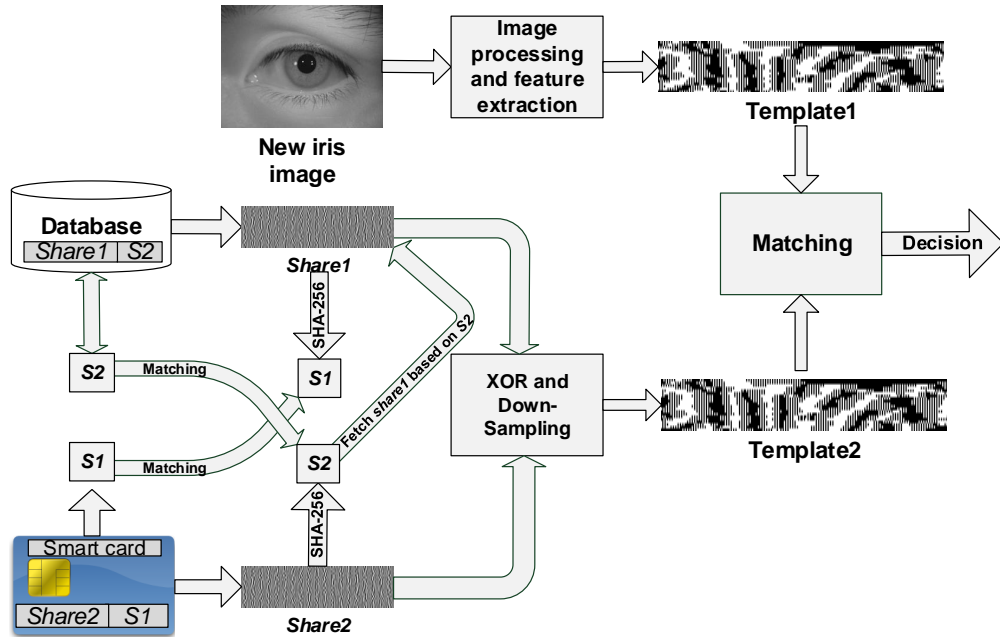
Figure 5.6: The authentication module of the proposed method using VC.

the template in the smart card or the database is not altered, the SHA-256 hash function is generated again and compared with the stored signatures $S1$ and $S2$. If the signatures do not match, authorization will not be granted. After that, the inbound user's iris template and the reconstructed iris template from the smart card and the database are compared together to authenticate the user. The authentication module is illustrated in Fig. 5.6.
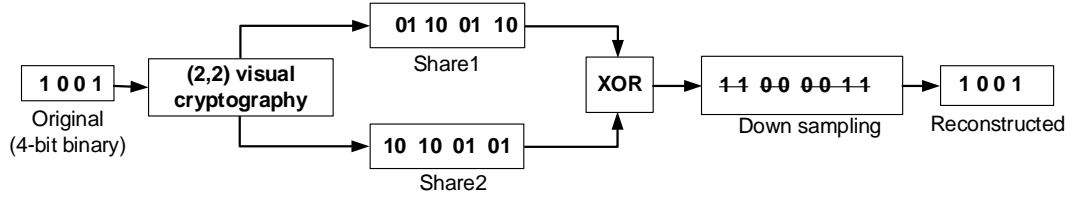
Figure 5.7: Down sampling to retrieve the original template size.

In order to restore the original template size after the expansion by VC, the reconstructed template is down sampled by selecting only one pixel from every 2×2 block as shown in Fig. 5.7. Thus, the generated image will have the same size as the original template and less storage and computational requirements.

5.5 Experimental Design and Results

The proposed method has been tested on the CASIA V4 and the UBIRIS V1 databases.

For the first stage, the iris images were watermarked with the 64×64 pixel text image shown in Fig. 5.8 (d) after converting it to a binary image. On the other hand, after feature extraction, the generated template is decomposed with (2,2) VC into two shares: one share is saved in the database and the other is saved on a smart card with the template on card architecture as proposed in the previous work [124]. In the next sub-sections an analysis is presented for each stage of the proposed scheme.

5.5.1 Stage one: watermarking

A good watermarking algorithm should meet different requirements such as perceptibility, robustness to various image manipulations and it should not degrade the matching performance of the biometric system significantly. In order to evaluate the proposed watermarking method, a set of different tests has been carried out as shown in the next sub-sections.
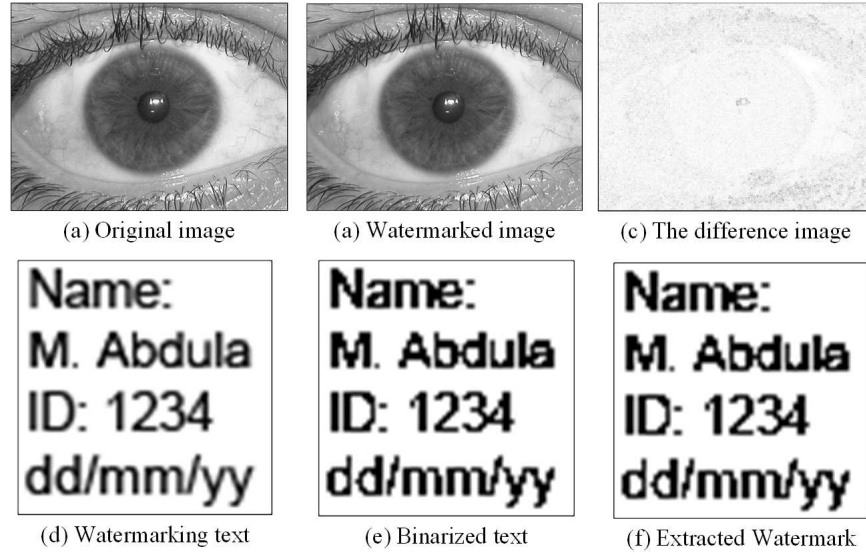
Figure 5.8: Perceptibility of the watermarked image; (a) original image, (b) watermarked image, (c) the difference image, (d) original watermark, (e) binarized text and (f) the extracted watermark.

5.5.1.1 Watermark Perceptibility

The similarity between the original and the watermarked image (perceptibility) indicates the impact of the watermarking algorithm on the cover image. Therefore, in a good watermarking algorithm, the watermarking effect should be imperceptible to the user. Fig. 5.8 (c) demonstrates that the difference between the original and the watermarked iris image is not noticeable to the naked eye without the help of the image processing techniques.

To evaluate quantitatively the performance of the watermarking algorithm, Peak Signal to Noise Ratio (PSNR) and Bit Error Rate (BER) are calculated. The average PSNR between the original iris and the watermarked iris is 38.47 and the average BER is 0.22% while the average PSNR and BER of the extracted watermarking text are 84.63 and 0.023%, respectively.

5.5.1.2 Effect on Matching Performance

To investigate the effect of the proposed watermarking algorithm on the iris recognition performance, the iris recognition system in [49] has been implemented with the segmentation algorithm proposed in the previous work [125], then the EER is calculated for the non-watermarked iris images. After that, the proposed watermarking algorithm is applied

on the same iris images and the EER is calculated again. Fig. 5.9 illustrates the effect of the proposed watermarking algorithm on iris recognition performance in terms of the ROC curve and EER. According to Fig. 5.9, the proposed watermarking algorithm barely disturbs the EER across both UBIRIS V1 and CASIA V4 databases. Consequently, the proposed watermarking algorithm does not involve noticeable effect on the iris recognition performance.

5.5.1.3 Performance against compression and noise

Other factors that may degrade the images were tested here such as compression and noising. In fact, the compression of large images become inevitable when transmitting such images over low bandwidth channels. On the other hand, there is an increased susceptibility to image degradation due to the noise in such channels.

To simulate these factors, the image compression algorithm, JPEG has been applied with different quality factors (Q) on the watermarked iris images. In addition, additive zero mean white Gaussian noise (AWGN) is applied to the watermarked iris images with zero mean and variance equal to 10^{-3}. Table 5.2 clearly indicates that the extracted text is still discernible even after adding Gaussian noise or applying JPEG compression with different quality factors.

Table 5.2: BER and PSNR of the extracted watermark after different manipulations using different watermarking algorithms.

Manipulation type	DWT-PN [127]		LSB		CDMA		Proposed	
	PSNR	BER	PSNR	BER	PSNR	BER	PSNR	BER
JPEG (Q=70)	70.14	0.54%	D	D	65.1	2.3%	84.25	0.024%
JPEG (Q=60)	60.23	4.15%	D	D	63.89	3.7%	83.25	0.044%
Median 3×3	21.25	39.56%	D	D	55.88	6.6%	69.88	1.2%
Histogram equalization	D*	D	D	D	D	D	76.47	0.15%
Gaussian white noise,($v = 10^{-3}$)	D	D	19	40.2%	26.4	28.5%	79.21	0.076%
Salt & pepper,(noise density=0.005)	30.15	10.18%	61.36	2.29%	32.15	9.18%	70.63	0.56%
Cropping (33%)	45.21	7.84%	47.15	5.05%	41.21	6.84%	79.48	0.074%
*D: means that the watermarking text is destroyed.								

5.5.1.4 Performance against image manipulations and attacks

The proposed watermarking algorithm was tested against various number of image manipulations such as median filtering, histogram equalization, compression, cropping and
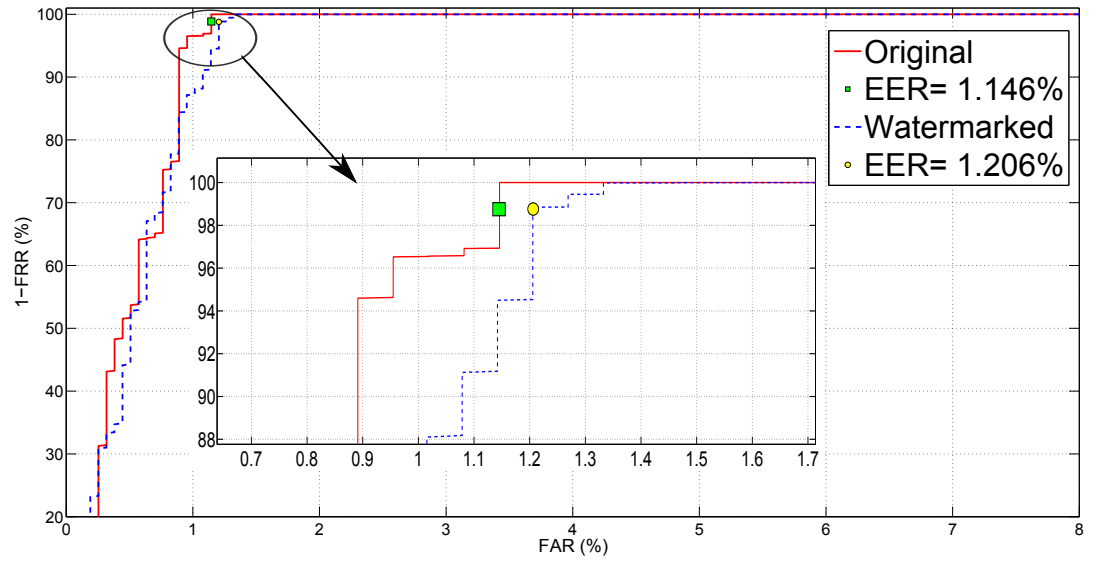
(a)
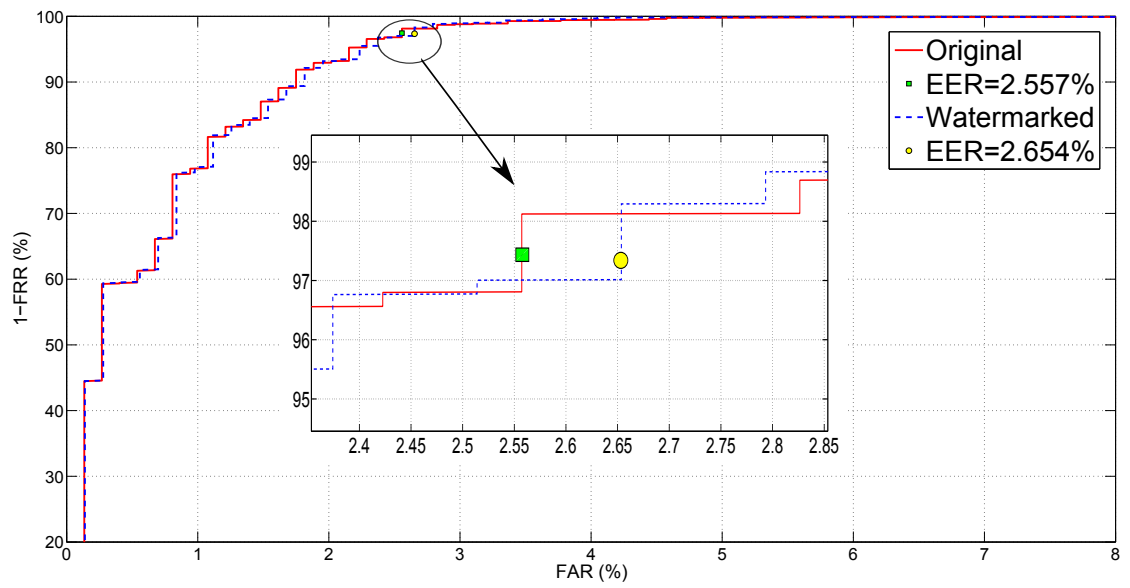
(b)

Figure 5.9: Effect of the proposed watermarking algorithm on the iris recognition performance: (a) UBIRIS V1 and (b) CASIA V4.

noising. In addition, the BER and PSNR of the extracted text were calculated for each type of manipulation as shown in Table 5.2.

Moreover, the recognition performances of the watermarked iris images are compared with the manipulated iris images in terms of ROC curves and EER as shown in Fig. 5.10. The slight degradation in the recognition performance in these cases is due to the added noise factors and not due to the watermarking algorithm.

5.5.1.5   Comparison with other watermarking methods

In order to appreciate the efficiency of the proposed method, different image watermarking methods such as LSB [114], Code Division Multiple Access (CDMA) [126] and DWT with Pseudo Noise (DWT-PN) [127] are implemented and compared with the proposed method and the same manipulations are applied to the watermarked iris images. Moreover, the proposed watermarking scheme is implemented with different strength constants as shown in Fig. 5.11 which depicts the extracted watermark after various manipulations using different watermarking methods.

As expected the LSB technique could not tolerate most of the attacks and the watermarked image is destroyed; whereas, CDMA and DWT-PN performs slightly better than LSB by tolerating JPEG compression however they failed to withstand several types of manipulation. On the other hand, exchanging only one pair of DCT coefficients failed to withstand all attacks because the coefficient can be easily destroyed by noise. It is noticed that there is a prominent improvement in the performance of the watermarking algorithm after adding the proposed strength constant but it is still vulnerable to median filtering and compression. On the contrary, the proposed algorithm which randomly exchanges four pairs with a strength constant ($S = 15$) sustained all the above image manipulations and demonstrated that the watermarking scheme is resistant to different types of attacks.

5.5.2   Stage two: visual cryptography

The proposed scheme achieves the template protection requirements namely: revocability, diversity, security and performance maintenance[122]. Firstly, in terms of revocability, whenever the iris template stored in the smart card/database is compromised, a new iris
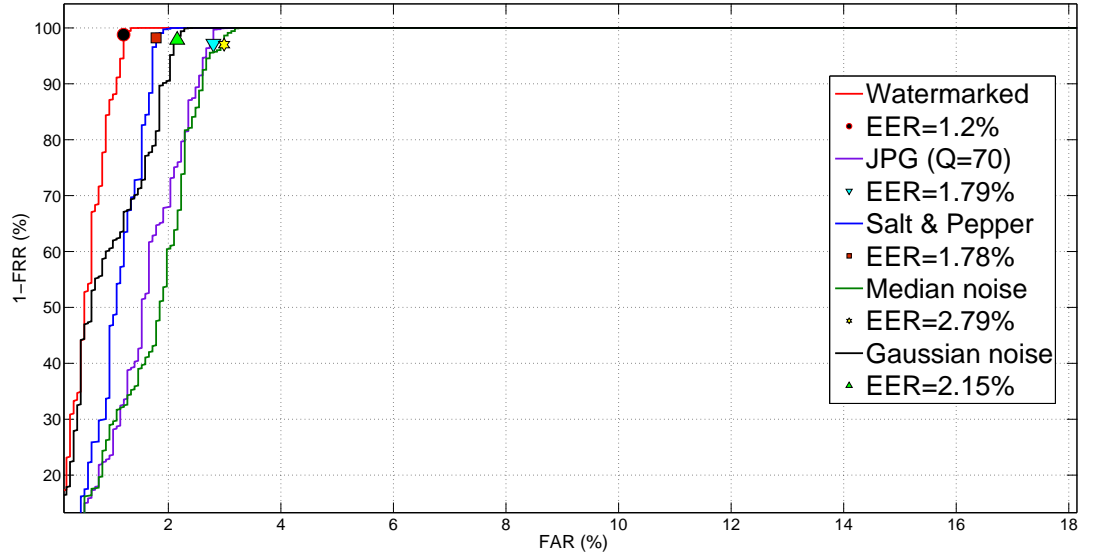
(a)
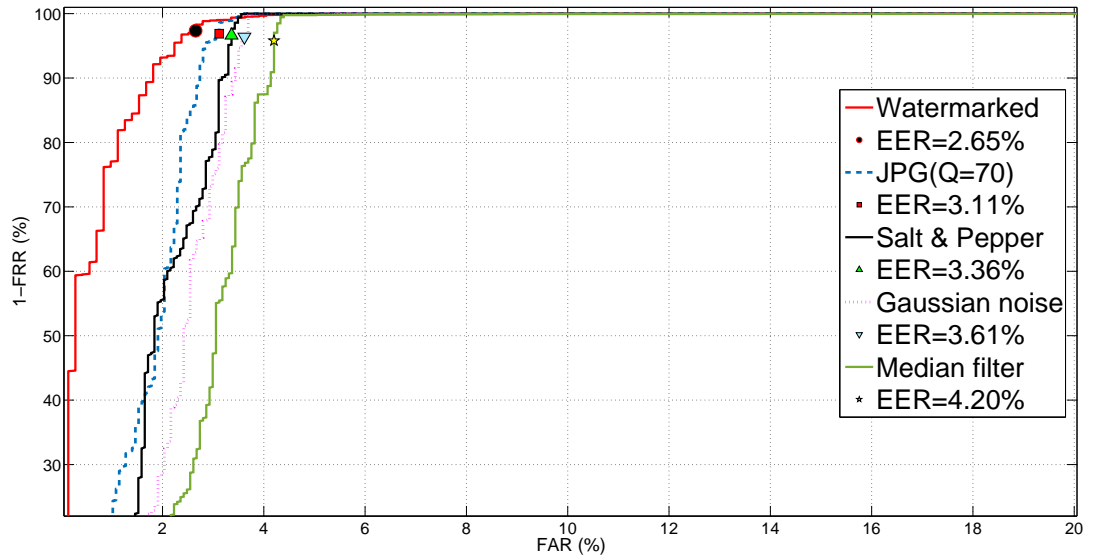
(b)

Figure 5.10: Effect of different manipulations on the iris recognition performance: (a) UBIRIS V1 and (b) CASIA V4.

template can be generated and decomposed into new shares. Nevertheless, to boost the security, this operation is recommended to be carried out at regular intervals. Secondly, as for diversity, the shares appear as random noise so it is hard to match them across the database as demonstrated later in Section 5.5.2.3. Thirdly, the iris template is secured after the VC because the iris template can only be generated if both shares are available

Attacks	LSB	Wavelet-PN	CDMA	Proposed 1 pair, $S=1$	Proposed 1 pair, $S=15$	Proposed 4 pairs, $S=15$
Histogram Eq.					Name: M. Abdula ID: 1234 dd/mm/yy	Name: M. Abdula ID: 1234 dd/mm/yy
Salt & pepper	Name: M. Abdula ID: 1234 dd/mm/yy	Name: M. Abdula ID: 1234 dd/mm/yy	Name: M. Abdula ID: 1234 dd/mm/yy	Name: M. Abdula ID: 1234 dd/mm/yy	Name: M. Abdula ID: 1234 dd/mm/yy	Name: M. Abdula ID: 1234 dd/mm/yy
Gaussian noise $v=10^{-3}$	Name: M. Abdula		Name: M. Abdula ID: 1234 dd/mm/yy		Name: M. Abdula ID: 1234 dd/mm/yy	Name: M. Abdula ID: 1234 dd/mm/yy
Median Filter 3×3		Name: M. Abdula ID: 1234 dd/mm/yy	Name: M. Abdula ID: 1234 dd/mm/yy		Name: M. Abdula ID: 1234 dd/mm/yy	Name: M. Abdula ID: 1234 dd/mm/yy
JPG (Q=70)		Name: M. Abdula ID: 1234 dd/mm/yy	Name: M. Abdula ID: 1234 dd/mm/yy			Name: M. Abdula ID: 1234 dd/mm/yy
JPG (Q=60)		Name: M. Abdula ID: 1234 dd/mm/yy	Name: M. Abdula ID: 1234 dd/mm/yy			Name: M. Abdula ID: 1234 dd/mm/yy

Figure 5.11: Effects of various attacks on the extracted watermark using different water-marking algorithms.

simultaneously. Therefore, even if the smart card is lost or stolen, the attacker will not be able to generate the iris template. Fourthly, the performance of the biometric system is not affected by the proposed scheme as using the original template or the generated template from VC gave the same EER in both cases.

In the next sub-sections, different statistical tests are carried out in order to check for randomness in the encrypted template and check its ability to confront statistical attacks.

5.5.2.1 Adjacent pixels correlation

To test the randomness of the generated shares after VC, the correlation coefficient [128] of the adjacent pixels is tested. In a random image, the adjacent pixels should have little correlation amongst them.

Table 5.3 lists the averages of the horizontal, vertical and diagonal correlation coefficients of the adjacent pixels for the template, $share1$ and $share2$ respectively. It can be seen from Table 5.3 that there is a very little correlation among the pixels of the shares while the original template pixels have high correlation.

Table 5.3: Adjacent pixel correlation coefficient.

	Horizontal	Vertical	Diagonal
Template	-0.0724	0.5397	0.0452
$Share1$	-0.5014	0.0037	-0.0078
$Share2$	-0.4942	-0.0035	0.0078

5.5.2.2 Pixel distribution test

This test is used to check the distribution of the pixels in the resulting share. A random vector should have almost a uniform distribution of zeros and ones. To check the distribution, the number of pixels in each row of the original templates is counted and plotted then compared with the encrypted shares before down-sampling. Fig. 5.12 shows that the pixels of the encrypted share are uniformly distributed across all the columns which confirms the random nature of the resultant shares.

5.5.2.3 Share to template matching

In this test, the possibility of share matching against a template is investigated. The procedure consists of matching a probe against the whole gallery in the database. The shares are used after down sampling as probes and the original templates are used as a gallery. The result in terms of EER equals to 47% which clearly indicates that it is not possible to authorize a person with either of the shares. On other hand, using the original template or the generated template from VC gave the same EER in both cases. These results clearly indicate that the iris recognition performance is not affected when using the proposed VC scheme.

5.5.2.4 Unlinkability of protected shares

Unlinkability means that protected templates should not allow cross-matching so that protected templates generated from a single object should differ from each other (diversity) [110]. The unlinkability of the shares is tested by matching a probe against the whole gallery in the database. The shares are used as a gallery and each share is used as a probe to perform cross-matching. This resulted in EER equal to 48.5% which clearly indicates the unlinkability of the shares.
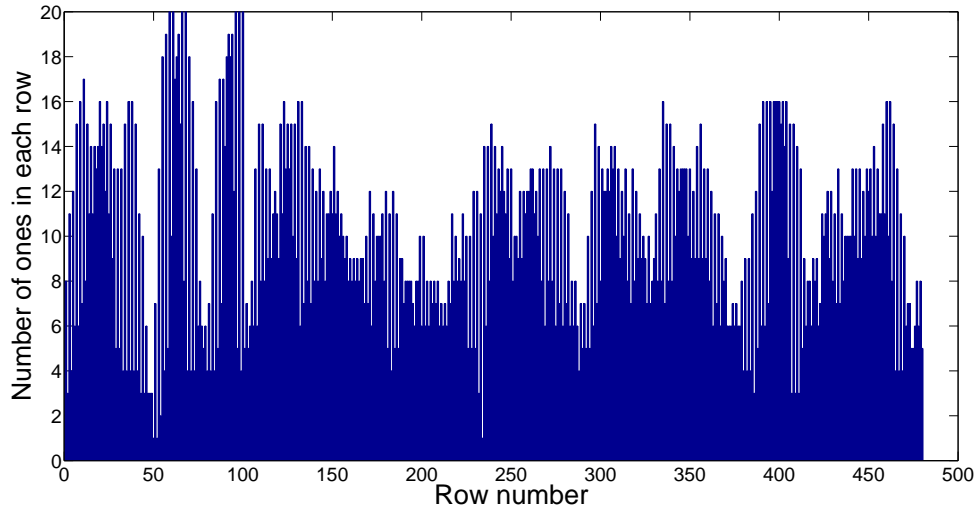
(a)
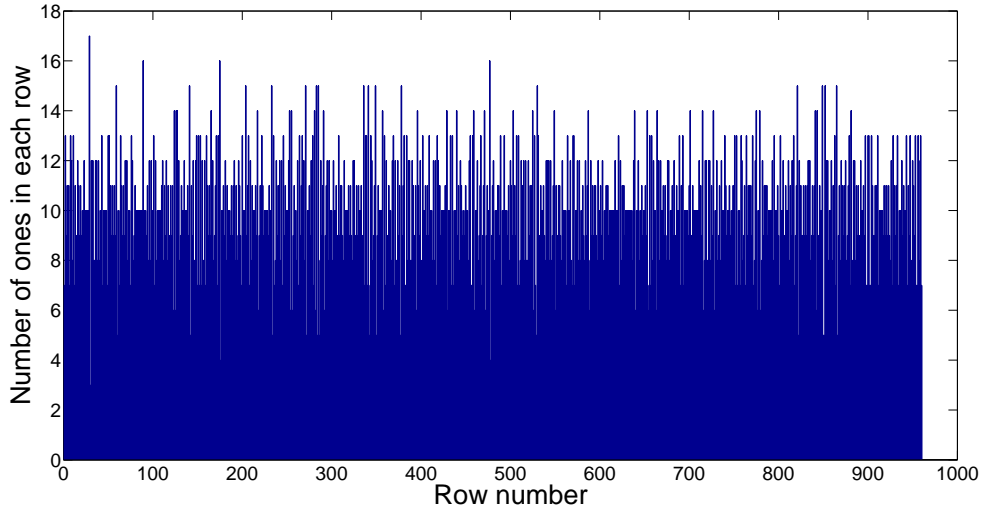
(b)

Figure 5.12: Pixels distribution: (a) the original iris template and (b) the encrypted share.

5.5.3 Computation Time

All experiments were conducted on a 3.2 GHz core i5 PC with 8 GB of RAM under the Matlab environment. The proposed method can be divided into two stages namely: watermarking and VC.

The proposed watermarking algorithm is based on the DCT which is widely used in real time devices. This is because the DCT can be implemented easily as it is based on real cosine basis functions that are easy to compute and implement [129]. Although the direct application of these formulas would require $O(N^2)$ operations, the same formula

can be implemented with only $O(NlogN)$ complexity by factorizing the computation with a similar approach to the fast Fourier transform. On the other hand, the VC scheme proposed in this chapter utilizes the logical XOR operator which is mapped to a single-cycle operation on modern processors. Therefore, the overall complexity of the proposed approach can be approximated to $[O(NlogN) + O(N)]$ which can be approximated to $O(NlogN)$ for large values of N.

Table 5.4: The average computation times (in sec) of each stage in the proposed algorithm.

	CASIA V4	UBIRIS V1
Watermarking	0.42	0.53
VC	0.1	0.1
Total	0.52	0.63

Table 5.4 shows the average computation time for each stage of the proposed method in each database. The variations in the computation times among databases in the watermarking stage are due to the different images size. The proposed method takes less than a second to be executed which implies that it is suitable for real time operation and is practical in many applications. Although the reported computational time of the proposed scheme is short, this time can be drastically reduced with code optimization and porting to a compiled language since there are no involved computations.

5.5.4 Comparisons with state-of-the-art methods

In order to achieve a fair comparison, each protection layer in the proposed protection scheme is considered individually. In terms of watermarking, comparison with the same scenario is difficult because most of the papers in the literature focus on protecting the biometric data with watermarking by embedding such data in a cover signal [102, 103, 93]. However, a few focus on protecting the biometric image itself [104]. Table 5.5 lists the few available state-of-the-art biometric watermarking methods. The work of [102] adopted the DWT and SVD to embed the iris feature inside an arbitrary cover image. However, the watermarked image and a key are required during the watermarking extraction stage [102]. Similarly, the work of [93] exploited the DWT and SVD to embed the fingerprint feature inside a face image. However, this method requires a shuffling key to

encrypt the watermarked image and the performance of this method is affected by noise [93]. In addition, the aforementioned methods used the SVD which has a complexity of $O(N^2)$ in its best implementation [130]. In the work of [103], a watermarking algorithm is proposed to embed the fingerprint and iris feature in the low frequency coefficients of the DCT blocks of a cover image. The cover image is then divided into smooth and edge blocks where the latter are eliminated. Unfortunately, embedding the watermark in the low frequency AC coefficients is vulnerable to attacks [117]. In addition, removing the edge blocks will degrade the watermarked image. This is going to affect the biometric system performance significantly when the watermarked image is a biometric image. In the previous work [104], it was proposed to protect the iris images based on interchanging fixed locations of the DCT middle band coefficients. However, there is a possibility that an attacker can predict these fixed locations and destroy the watermark information or embed false watermark data.

As for template protection, as mentioned before, few papers address biometric template protection with VC. Since the same scenario is not available, the proposed VC method is compared with similar template protection scenarios proposed in [107, 109, 131] as shown in Table 5.6. A method is proposed in [107] for preserving the privacy of the iris template. This method involves some performance degradation as well as complex operations to generate the BioCapsul and requires keys to be extracted from the user's signal. In addition, this method is designed to protect the templates resulting from the Gabor filter and hence it is limited to the application of biometric systems that adopt the Gabor filter for feature extraction [107].

Table 5.5: Comparisons with state-of-the-art biometric watermarking methods.

Watermarking method	Type	Approach	Remarks	Complexity
Majumder et al. [102]	Embed iris feature inside an arbitrary cover image.	DWT and SVD.	-Requires the watermarked image and a key during the watermark extraction stage.	$O(N^2)$
Paunwala et al. [103]	Embed fingerprint and iris feature inside an arbitrary cover image.	Embeds watermark in low frequency AC coefficients of selected DCT blocks.	-Embedding the watermark in low frequency AC coefficients makes it vulnerable to attacks. -Removing the edge blocks degrades the watermarked image.	$O(NlogN)$
Nafea et al. [93]	Embed fingerprint features inside a face image.	DWT and SVD.	-The performance of proposed approach is degraded with the presence of noise.	$O(N^2)$
Abdullah et al. [104]	embed text data as a contextual watermark in the biometric image.	Exchanging fixed locations of the DCT middle band coefficients.	-The embedded data could be corrupted if the fixed locations are divulged.	$O(NlogN)$
Proposed		Randomly exchanging four middle band coefficients of the DCT blocks.	-Applicable to multiple biometrics.	$O(NlogN)$

Table 5.6: Comparisons with state-of-the-art iris template protection methods.

Template protection method	Remarks	Complexity
BioCapsule [107]	-Involves performance degradation. -Limited to the biometrics traits that adopt Gabor filter for feature extraction. [107].	$O(N^2)$
Bloom filters [109]	-Vulnerable to reversibility and cross shares matching [110].	$O(N)$
Cancelable biometrics [131]	-Vulnerable to reversibility, spoofing and coalition attacks [132].	$O(N)$
Proposed (VC)	-No performance degradation.	$O(N)$

Next, an alternative method is proposed in [109] to protect the binary iris template based on Bloom filters. However, Hermans et al. [110] demonstrate that the work of [109] is vulnerable to cross-shares matching and the reversibility is possible for a nonuniform randomly generated template. On the other hand, the cancelable biometric approach is proposed for iris template protection in [131]. Yet, the works of [132] demonstrated that there are several drawbacks of using the cancelable biometrics such as reversibility and venerability to spoofing and coalition attacks.

In this chapter all the previous drawbacks have been addressed since the proposed watermarking approach is robust against noise and considered as a "blind watermarking technique" as it does not require the original image for extracting the embedded watermark. In addition, the proposed watermarking method makes no restrictive hypothesis on the biometric image and hence it is applicable to multiple biometrics traits. On the other hand, the proposed VC scheme does not involve any effect on the iris recognition performance and does not require any key for the decryption. Moreover, integrating the hash function with the smart card will maintain the integrity of the stored data and offers robustness against data modification attempts in either the smart card or the database.

5.5.5   Applicability and Limitations

The proposed scheme is designed to effectively protect the image and template of the iris biometric. One of the main advantages of the proposed watermarking scheme is that it can be readily applied to any type of images other than the iris images. Yet, the type of the embedded data should be binary data such as a binary image or an ASCII code. Since one bit can be hidden in each image block, the maximum size of the embedded data is equal to $(height \times width)/blocksize$. For example, for a block size of 8×8, if an image resolution is 800×600, the maximum watermark size will be 7500 bits.

On the other hand, the proposed VC scheme is capable of working with binary template or data. This type of biometric template is widely used in feature representation of various biometric traits such as iris, face and fingerprint [7, 133, 134].

The stored template in the database has almost the same size as the conventional *IrisCode* with only 256 additional bits for the hash function. In addition, the watermarked iris image has a similar size to the original iris image. This makes it analogous to available

iris recognition systems in terms of database handling.

5.6 Summary

The work proposed in this chapter aimed to bring insight into the problem of biometric security. Novel schemes were proposed for iris image and template protection which consist of two security layers. The first layer is a robust watermarking algorithm which was implemented to protect the integrity of the biometric image. In particular, a binary text image that accommodates the bio-data of the person to be authenticated was embedded in the iris image by randomly interchanging four pairs of the DCT middle band coefficients. The embedding locations were randomly selected based on a private key. Moreover, the proposed strength constant S was included to add more robustness to the watermarking algorithm.

The second layer involved using the VC to protect the iris template by decomposing the original iris template into two shares using (2,2) VC where one share is given to the user on a smart card while the other is stored in a database. The proposed VC scheme allows the iris template to be perfectly restored with the same quality and size when the shares are available, and therefore it does not hinder the iris recognition performance. To this end, an extra layer of security is provided to the iris template because even if either of the shares in the database or the smart card is compromised, the original template cannot be retrieved. Further, the integrity of the iris templates, in both the smart card and the database, is also guaranteed with the use of the hash signatures. The generated signature from the hash function is not only beneficial to maintain the integrity of the smart card but also it has been used to select the embedding locations for the watermarking algorithm.

The experimental results and comparison with state-of-the-art methods revealed that the proposed scheme was robust in terms of iris image and templates protection and capable of withstanding attacks while it did not involve degradation to iris recognition performance.

The next chapter presents the proposed framework for cross-spectral iris matching. In addition, this chapter highlights the applications and benefits of using multi-spectral iris information in iris recognition systems.

Chapter 6

Cross-spectral Iris Matching

6.1 Introduction

Nearly all currently deployed iris recognition systems operate predominately in the NIR spectrum capturing images at 800-900nm wavelength. This is because there are fewer reflections coming from the cornea and the dark pigmented irides look clearer under NIR light. In addition, external factors such as shadows and diffuse reflections become less prominent under NIR light [6, 39].

Research in VL iris recognition has been gaining more attention in recent years due to the interest in iris recognition at a distance [37]. In addition, competitions such as the noisy iris challenge evaluation [135] and the mobile iris challenge evaluation [65] focus on the processing of VL iris images. This attention to visible wavelength-based iris recognition is boosted by several factors such as: (1) visible range cameras can acquire images from long distance and they are cheaper than NIR cameras; (2) surveillance systems work in the visible range by capturing images of the body, face and iris which could be used later for authentication [136].

Since both VL and NIR iris recognition systems are now widely deployed, cross-spectral matching is paramount due to its use in several security applications such as surveillance at-a-distance and automated watch-list identification. Typically, a person's iris images are captured under NIR but most security cameras operate in the VL spectrum. Hence, NIR vs. VL matching is desired. In addition, studying the performance difference of iris recognition systems exploiting NIR and VL images is important because it gives insight into the essential features in each wavelength which in turn helps to develop a robust automatic identification system.

Cross-domain matching can be divided into two main categories: cross-sensor matching and cross-spectral matching. Cross-sensor matching represents the case when the iris images acquired from one iris sensor must be matched against those from another sensor. This cross-sensor matching is believed to degrade recognition performance due to several factors such as the variations in lenses, sensor sensitivity and the difference in NIR illumination [38]. On the other hand, cross-spectral matching represents the case of matching iris images taken under different illumination conditions i.e. NIR vs. VL. Cross-spectral matching is a challenging task because there are considerable differences among images

pertaining to different wavelength bands. As the topic of this chapter is surveillance and security applications, the focus will be on the second type (cross-spectral matching).

In this chapter, two methods are proposed for the problem of VL to NIR iris matching (and vice versa) dealing with unregistered and registered iris images belonging to the same subject. In addition, the difference in iris recognition performance has been investigated with NIR and VL imaging. In particular, iris performance in each channel (red, green, blue and NIR) and the feasibility of cross-channel authentication (i.e. NIR vs. VL) have been explored. Furthermore, enhancing the iris recognition performance with multi-channel fusion is attained.

The rest of this chapter is organized as follows: related works and properties of the iris are given in Section 6.2 and Section 6.3, respectively. The proposed framework for cross-spectral iris matching is explained in Section 6.4. Section 6.5 presents the experimental results and the discussion while Section 6.6 summarizes this chapter.

6.2 Related Work

Iris recognition technology has witnessed a rapid development over the last decade driven by its wide applications across the globe. At the outset, Daugman [7] proposed the first working iris recognition system which has been adopted later by several commercial companies such as IBM, Irdian and Oki. Several works followed after that, but almost all of them assessed iris recognition performance under NIR.

The demand for more accurate and robust biometric systems has increased with the expanded deployment of large-scale national identity programs. Hence, researchers have investigated iris recognition performance under different wavelengths; or the possibility of fusing NIR and VL iris images to enhance recognition performance. Nevertheless, inspecting the correlation between NIR and VL iris images has been understudied and the problem of cross-spectral iris recognition is still unsolved.

In this context, Boyce et al. [137] explored iris recognition performance under different wavelengths on a small multi-spectral iris databases consisting of 120 images from 24 subjects. According to the authors, higher accuracy was achieved for the red channel compared to green and blue channels. The study also suggested that cross-channel match-

ing is feasible. The iris images were fully registered and captured under ideal conditions. In [138] the authors employed the feature fusion approach to enhance the recognition performance of iris images captured under both VL and NIR. The wavelet transform and discrete cosine transform were used for feature extraction while the features were augmented with the ordered weighted average method to enhance the performance.

In Ngo et al. [139] a multi-spectral iris recognition system was implemented which employed eight wavelengths ranges from 405nm-1550nm. The results on a database of 392 iris images showed that the best performance was achieved with a wavelength of 800nm. Cross-spectral experimental results demonstrated that the performance degraded with larger wavelength difference. Ross et al. [140] explored the performance of iris recognition in wavelengths beyond 900nm. In their experiments, they investigated the possibility of observing different iris structures under different wavelengths and the potential of performing multi-spectral fusion for enhancing iris recognition performance. Similarly, Ives et al. [141] examined the performance of iris recognition under a wide range of wavelengths between 405nm-1070nm. The study suggests that illumination wavelength has a significant effect on iris recognition performance. Hosseini et al. [39] proposed a feature extraction method for iris images taken under VL using a shape analysis method. Potential improvement in recognition performance was reported when combining features from both NIR and VL iris images taken from the same subject.

Recently, a method has been proposed in [142] for cross-spectral periocular verification using an Artificial Neural Network (ANN). Experiments were conducted on a database consisting of eye images captured under VL, night vision and NIR. Alonso-Fernandez et al. [143] conducted comparisons on the iris and periocular modalities and their fusion under NIR and VL imaging. However, the images were not taken from the same subjects as the experiments were carried out on different databases (three databases contained close-up NIR images, and two others contained VL images). Unfortunately, this may not give an accurate indication about the iris performance as the images do not belong to the same subject. In [144] the authors suggested enhancing iris recognition performance in non-frontal images through multi-spectral fusion of the iris pattern and scleral texture. Since the scleral texture is better seen in VL and the iris pattern is observed in NIR, multi-spectral fusion could improve the overall performance.

In terms of cross-spectral iris matching, the authors in [136] proposed an adaptive method to predict the NIR channel image from VL iris images using an ANN. Similarly, Burge and Monac [145, 146] proposed a model to predict NIR iris images using features derived from the color and structure of the VL iris images. In [147], the authors explored the differences in iris recognition performance across the VL and NIR spectra. In addition, the possibility of cross-channel matching between the VL and NIR imaging was investigated. The cross-spectral matching turns out to be challenging with an EER larger than 27% in the UTIRIS database.

Lately, Ramaiah and Kumar [148] emphasized the need for cross-spectral iris recognition and introduced a database of registered iris images and conducted experiments on iris recognition performance under both NIR and VL. The results of cross-spectral matching achieved an EER larger than 34% which confirms the challenge of cross-spectral matching. The authors concluded their paper with the comment: "it is reasonable to argue that cross-spectral iris matching seriously degrades the iris matching accuracy". More recently, Ramaiah and Kumar [38] introduced a new iris database containing NIR and VL iris images acquired simultaneously and performed experiments to improve the cross-sensor and cross-spectral iris matching. In the previous work [149], the authors proposed a framework for cross-spectral iris matching capable of working with unregistered iris images pertaining to the same subject. Experiments on the UTIRIS database showed that the proposed framework notably improved the cross-spectral matching performance.

6.3   Iris Pigmentation

The color of the irides is governed by the congruity of two molecules: eumelanin (black/ brown) and pheomelanin (red/yellow). The iris color varies from brown, green, blue, hazel to gray depending on not only the pigmentation but also other factors such as blood vessel and fibrous tissue inside the iris texture. However, occasionally the lack of pigmentation results in a white-pinkish color which is known as oculo-cutaneous albinism as shown in Fig. 6.1 [150].

During the first three years of life the color of the iris can change due to light exposure. Following the age of three, the melanin content becomes stable to form the natural color

Figure 6.1: Oculo-cutaneous albinism resulting from the lack of melanin pigment.

of the iris. Nevertheless, some changes may occur to the iris color as exposure to sun light increases the melanin in a similar manner to the skin color [151].

Dark pigmented irides have high concentration of eumelanin. As the latter deeply absorbs VL, stromal features of the iris are only revealed under NIR and they become hidden in VL so the information related to the texture is revealed rather than the pigmentation. On the other hand, pheomelanin is dominant in light pigmented irides. Capturing such irides under NIR light eliminates most of the rich pheomelanin information because the chromophore of the human iris is only visible under VL [39, 152]. Consequently, capturing iris images under different light conditions reveals different textural information.

6.4   Proposed Cross-Spectral Iris Matching Framework

Matching across iris images captured in VL and NIR is a challenging task because there are considerable differences among such images pertaining to different wavelength bands. Although the appearance of iris images under different spectra is not constant, the structure is the same as they belong to the same person. Generally speaking, to alleviate the perceptual differences, two approaches can be adopted: a training-based approach and a photometric/descriptor-based approach. The training-based approach is known to achieve outstanding performance for cross-spectral matching of registered images [142, 38] but the training-based approach tends to fail due to the lack of pixel correspondence among unregistered images.

In this section, two methods are proposed for cross-spectral iris matching. The first is designed to work with registered iris images in the verification mode. The key idea is to synthesize the corresponding NIR images from the VL images using the ANN techniques.

After that, the predicted NIR images can be matched against the VL images to perform cross-spectral matching. The second method is capable of working with unregistered iris images in the identification mode based on integrating the Gabor filter with different photometric normalization models and descriptors along with decision level fusion. Details of these methods are described in the next sections.

6.4.1 Matching of Registered Images

The problem of training a predictive model is considered to be a non-linear multivariate regression problem. As cross-spectral matching can be stated to be non-linear matching, the predictive model is estimated using the ANN technique due to its ability in establishing a non-linear mapping between inputs and targets. Accordingly, after estimating the mapping, the target parameters (NIR pixels) are predicted from the input parameters (gray-scale pixels of a query image).

A Feed Forward Neural Network (FFNN) is used to build the predictive model for cross-spectral matching. It is trained on the gray-scale pixels of the color iris images and the target is set to be the corresponding NIR pixels. The training data set which consists of 30 classes, is randomly divided into two subsets. The learning subset consists of 60% of the training data while the testing subset is composed of the remaining 40%. In the experiments, the FFNN is composed of two hidden-layers. The number of layers and neurons is chosen as a trade-off between complexity and network performance. The iris images are segmented and normalized as proposed in [125] to ensure only iris pixels are fed to the network.

In the training phase, training is performed using the scaled conjugate gradient back-propagation approach with a tangent sigmoid non-linearity in the hidden layer and a linear activation function in the output layer; then the final weights are stored for each subject. The training process stops when the mean square error equals to 10^{-5}, a value which has been determined empirically. During the testing phase, these weights are used to generate the predicted NIR iris image. The block diagrams of the training and testing phase are illustrated in Fig 6.2.
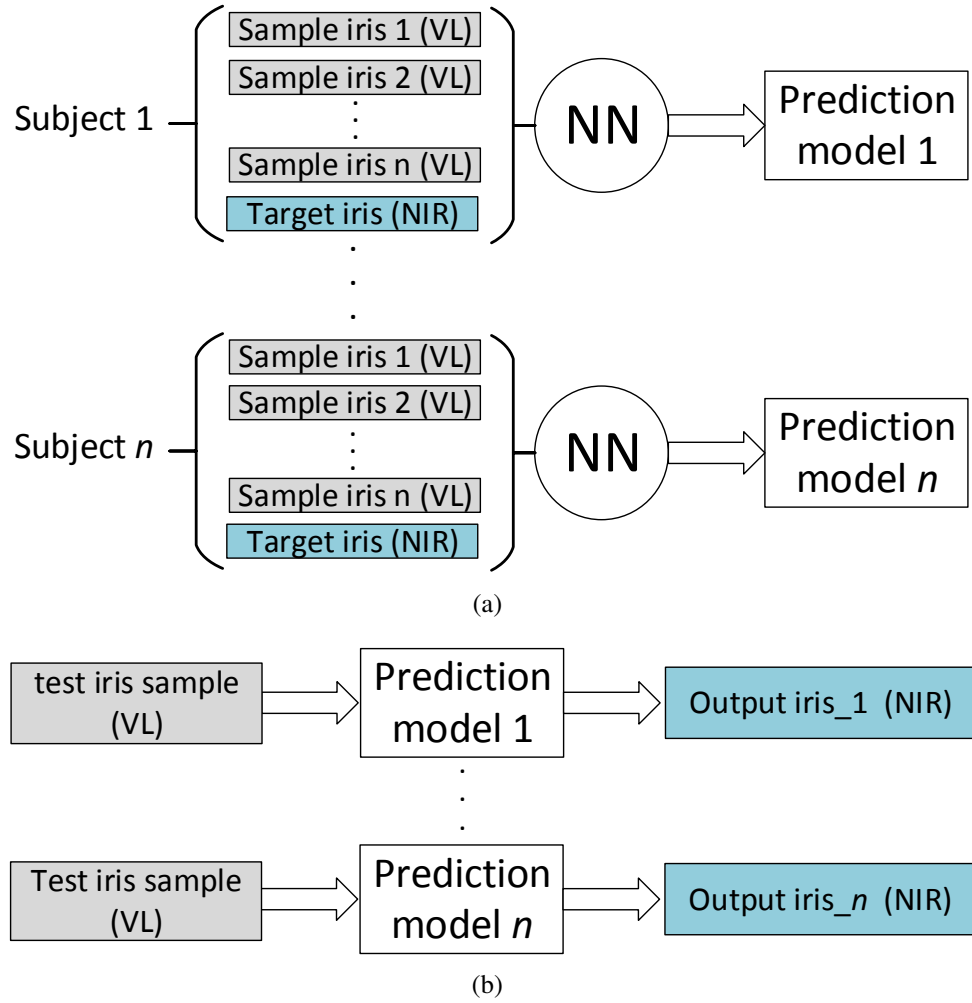
Figure 6.2: Block diagram of the prediction model: (a) training phase (b) testing phase.

6.4.2 Matching of Unregistered Images

Cross-spectral matching of unregistered images is more challenging due to the lack of pixel correspondence in the unregistered images. Therefore, more sophisticated methods are needed to address the spectral bands difference and illumination variations.

Different photometric normalization techniques and descriptors have been investigated to alleviate these differences. In this context, the Binarized Statistical Image Features (BSIF) descriptor [153] and Difference-of-Gaussian (DoG) filtering have been employed in addition to a collection of photometrice normalization techniques available from the INface Toolbox[1] [154, 155]: adaptive single scale retinex, non-local means, wavelet based normalization, homomorphic filtering, multi-scale quotient, Tan and Triggs nor-

---
[1]http://luks.fe.uni-lj.si/sl/osebje/vitomir/face_tools/INFace/

malization and Multi Scale Weberface (MSW).

Among these illumination techniques and descriptors, the DoG, BSIF and MSW are found to reduce the iris cross-spectral variations. These models are described in the next subsections.

6.4.2.1 Difference of Gaussian (DoG)

The DoG is a feature enhancement technique which depends on the difference of Gaussian filters to generate a normalized image by acting as a bandpass filter. This is achieved by subtracting two blurred version of the original images from each other [156]. The blurred versions $G(x, y)$ are obtained by convolving the original image $I(x, y)$ with two Gaussian kernels having different standard deviations as shown in equation 6.1:

$$D(x, y | \sigma_0, \sigma_1) = [G(x, y | \sigma_0) - G(x, y | \sigma_1)] * I(x, y), \tag{6.1}$$

where * is the two-dimensional convolution operator and $G(x, y | \sigma)$ represents the Gaussian kernel function which is defined as:

$$G(x, y | \sigma) = \frac{1}{\sqrt{2\pi\sigma^2}} e^{-(x^2 + y^2)/2\sigma^2}. \tag{6.2}$$

Here $\sigma_0 < \sigma_1$ is used to construct a bandpass filter. The values of σ_0 and σ_1 are empirically set to 1 and 2, respectively. The DoG filter has a low computation complexity and is able to alleviate the illumination variation and aliasing. As there are variations in the frequency between VL and NIR images, the DoG filter is efficient because it suppresses these variations and alleviates noise and aliasing which paves the way for better cross-spectral matching [156].

6.4.3 Binarized Statistical Image Features (BSIF)

The Binarized Statistical Image Features (BSIF) [153] have been employed due to their ability to tolerate image degradation such as rotation and blurring [153]. Generally speaking, feature extraction methods usually filter the images with a set of linear filters then quantize the response of such filters. In this context, BSIF filters are learned by exploiting

the statistics of natural images rather than using manually built filters. This has resulted in promising results for classifying the texture in different biometric traits [157, 158].

For an image patch X of size $l \times l$ pixels and a linear filter W_i of the same size, the filter response s_i is obtained by:

$$s_i = \sum W_i(u,v)X(u,v) = w_i^T x. \tag{6.3}$$

The binarized feature b_i is obtained based on the response values by setting $b_i = 1$ if $s_i > 0$ and $b_i = 0$ otherwise. The filters are learned from natural images using independent component analysis by maximizing the statistical independence of s_i. Two parameters control the BSIF descriptor: the number of filters (length n of the bit string) and the size of the filter l. In this approach the default set of filters[1] was used which were learned from 5000 patches. Empirical results demonstrated that a filter size of 7×7 with 8 bits gives the best results.

6.4.4 Multi-Scale Weberfaces (MSW)

Inspired by Weber's law which states that the ratio of the increment threshold to the background intensity is a constant [159], the authors in [160] showed that the ratio between local intensity of a pixel and its surrounding variations is constant. Hence, in [160] the face image is represented by its reflectance and the illumination factor is normalized and removed using the Weberface model. Following this the Weberface model is applied to the iris images to remove the illumination variations that result from the differences between the VL and NIR imaging. Thus making the iris images illumination invariant.

Following the works of [154, 155], the Weberface algorithm has been applied with three scales using the following values: $\sigma = [1\ 0.75\ 0.5]$, $Neighbor = [9\ 25\ 49]$ and $alfa = [2\ 0.2\ 0.02]$. The steps of the Weberface algorithm are listed in Algorithm 3.

6.4.5 Proposed Scheme

Extensive experiments demonstrated that using one of the aforementioned methods alone is not sufficient to achieve an acceptable iris recognition performance for unregistered iris

---

[1] http://www.ee.oulu.fi/~jkannala/bsif/bsif.html

Algorithm 3: Weberface normalization.

   Input: Iris image I
   Output: Weber iris image W
  1: Smooth the image using a Gaussian filter
  2: $I = I * G(X, Y, \sigma)$
  3: For each pixel in the image
     $sum = \sum(PixelIntensity - NeighborValues)/PixelIntensity$;
     $W_i = arctan(alfa \times sum)$;
  4: Assign W_i to the pixel in the Weber iris image.
---

images with EER > 17% as shown later in Table 6.4. Therefore, integrating the Gabor filter with these methods is proposed in addition to decision level fusion to achieve a robust cross-spectral iris recognition. Also, using the phase information of the Gabor filter rather than amplitude is known to result in robustness to different variations such as: illumination variations, imaging contrast and camera gain [6].

Hence, integrating the 1D log-Gabor filter [49] with DoG, BSIF and MSW to produce the G-DoG, G-BSIF and G-MSW (where G stands for Gabor) is proposed in addition to decision level fusion to achieve a robust cross-spectral iris recognition. The block diagram of the proposed framework is depicted in Fig. 6.3.

6.5 Results and Discussion

The aim of this work is to ascertain true cross-spectral iris matching using images taken from the same subject under the VL and NIR spectra. In addition, iris biometric performance under different imaging conditions is investigated and the fusion of VL+NIR images is employed to boost the recognition performance. The cross-spectral experiments are conducted using two publicly available cross-spectral iris databases, the PolyU bi-spectral iris database [38] and the UTIRIS database [39]. The recognition performance is measured with the EER and ROC curves.

6.5.1 Pre-processing and Feature Extraction

Typically, an iris recognition system operates by extracting and comparing the pattern of the iris in the eye image. These operations involve four main steps namely: image
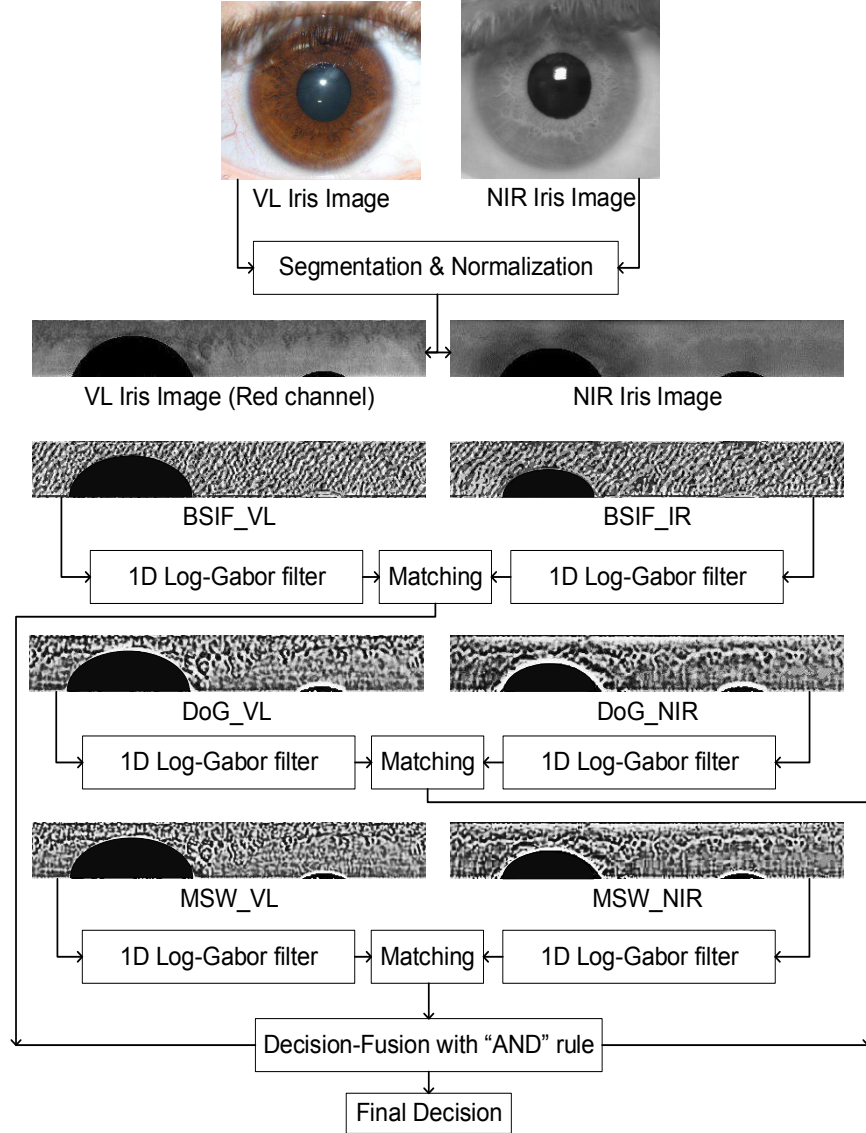
Figure 6.3: Block diagram of the proposed cross-spectral matching framework.

acquisition, iris segmentation, normalization, feature extraction and matching [7].

All iris images were segmented and normalized using the robust iris segmentation algorithm from the previous work [125]. For the PolyU database, the NIR images were segmented first and the same parameters were used to segment the corresponding VL images because the images are registered. On the other hand, for the UTIRIS database, it is noticed that the red channel gives the best segmentation results because the pupil region in this channel contains the smallest amount of reflection as shown in Fig. 6.4 and Fig. 6.5. The images in the VL session were down-sampled by two in each dimension to obtain the same size as the images in the NIR session.
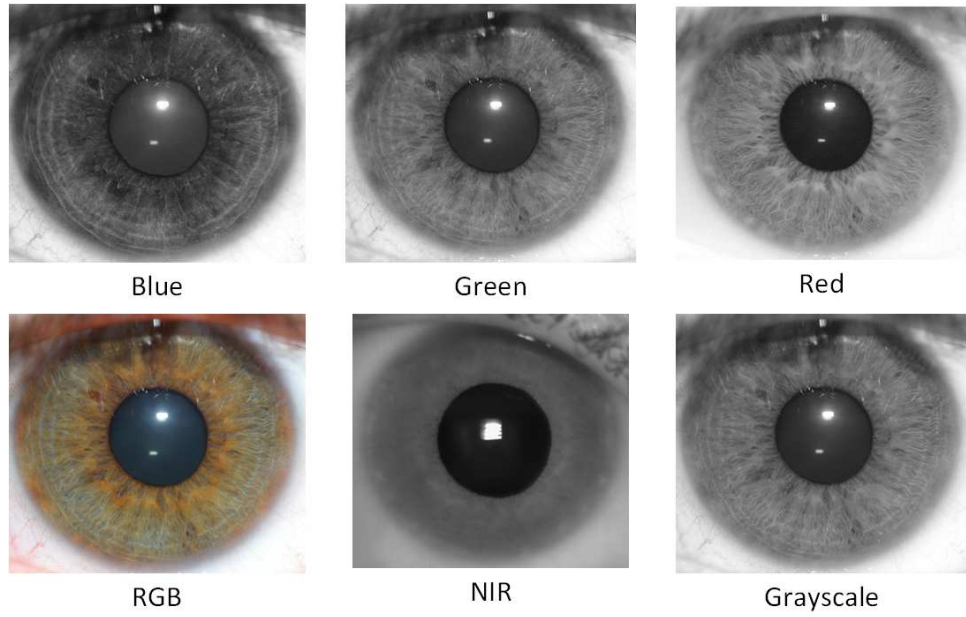
Figure 6.4: Green-yellow iris image decomposed into red, green, blue and grayscale with the NIR counterpart.
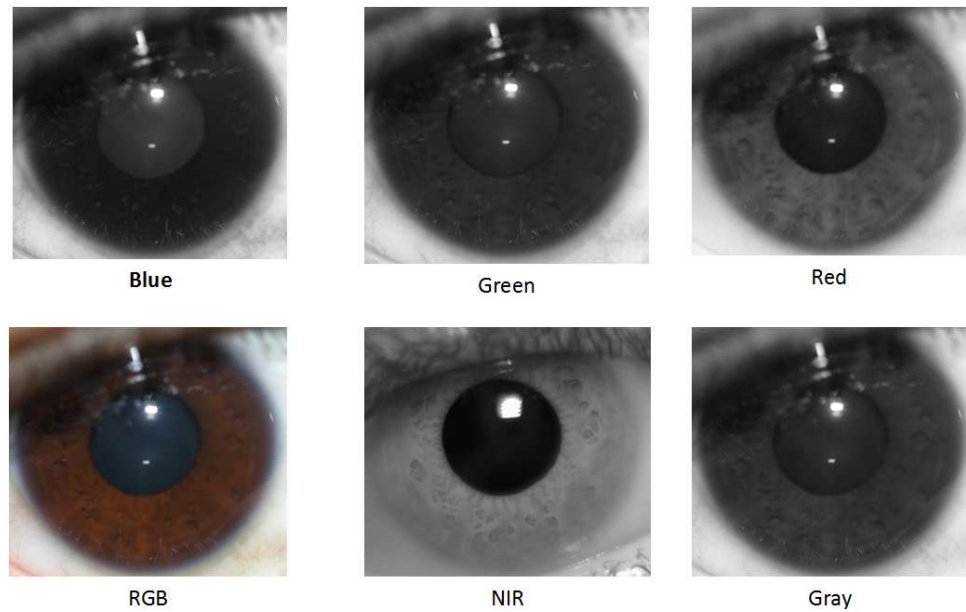
Figure 6.5: Brown iris image decomposed into red, green, blue and grayscale with the NIR counterpart.

For feature extraction, the normalized iris image is convolved with the 1D log-Gabor filter to extract the features where the output of the filter is phase quantized to four levels to form the binary iris vector [49]. After that, the Hamming distance is used to find the similarity between two IrisCodes in order to decide if the vectors belong to the same

person or not. Then, the ROC curves and the EER are used to judge the iris recognition performance for the images in each channel as illustrated in the next subsections.

6.5.2   Light-Eyed vs. Dark-Eyed

As mentioned before, capturing iris images under NIR light eliminates most of the rich melanin information because the chromophore of the human iris is only visible under VL [39, 152]. Therefore, light pigmented irides exhibit more information under visible light. Fig. 6.4 shows a green-yellow iris image captured under NIR and VL. It can be seen that the red channel reveals more information than the NIR image. So, intuitively the recognition performance would be better for such images in the VL rather than the NIR spectrum.

On the contrary, with dark pigmented irides, stromal features of the iris are only revealed under NIR and they become hidden in VL so the information related to the texture is revealed rather than the pigmentation as shown in Fig. 6.5. Therefore, the recognition performance for the dark pigmented irides would give better results if the images were captured under NIR spectrum.

6.5.3   NIR vs. VL Performance

Different experiments have been carried out on each channel (i.e. NIR, red, green and blue) and the performance has been measured using ROC and EER.

For the UTIRIS database, it can be seen from Fig. 6.6 that the best performance is achieved under the red channel with EER = 2.92% followed by the green channel with EER = 3.50% while the blue channel achieved worse results with EER = 6.33%. It is also noticed that NIR images did not give the best performance for this database (EER = 3.45%). This is because most of the iris images in the UTIRIS database are light pigmented. This is in agreement with the obtained results where the red channel images achieved better results than the NIR images as most of the iris images in the UTIRIS database are light pigmented. Fig. 6.7 shows the distribution of the irides color in the UTIRIS database.

On the contrary, as most of the images in the PolyU iris database are dark pigmented,
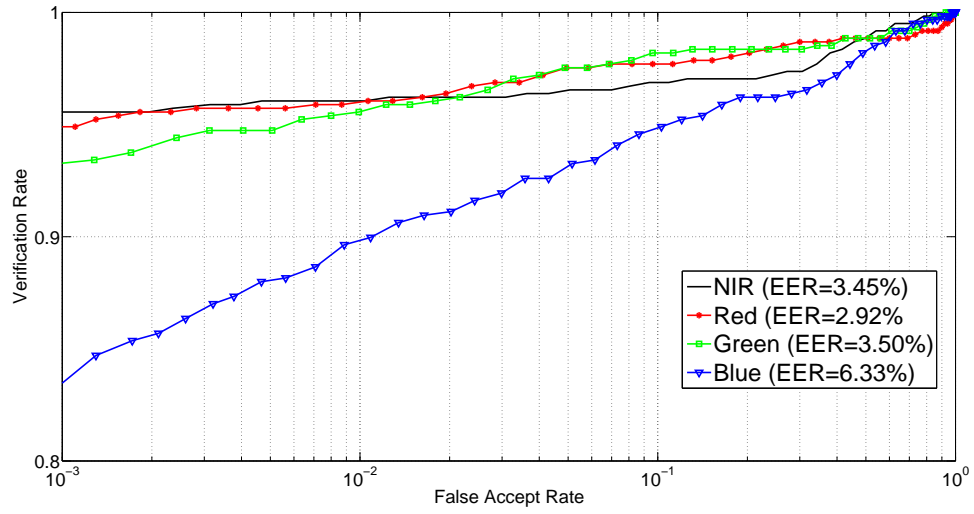
Figure 6.6: The performance of the iris recognition under red, green, blue and NIR spectra.
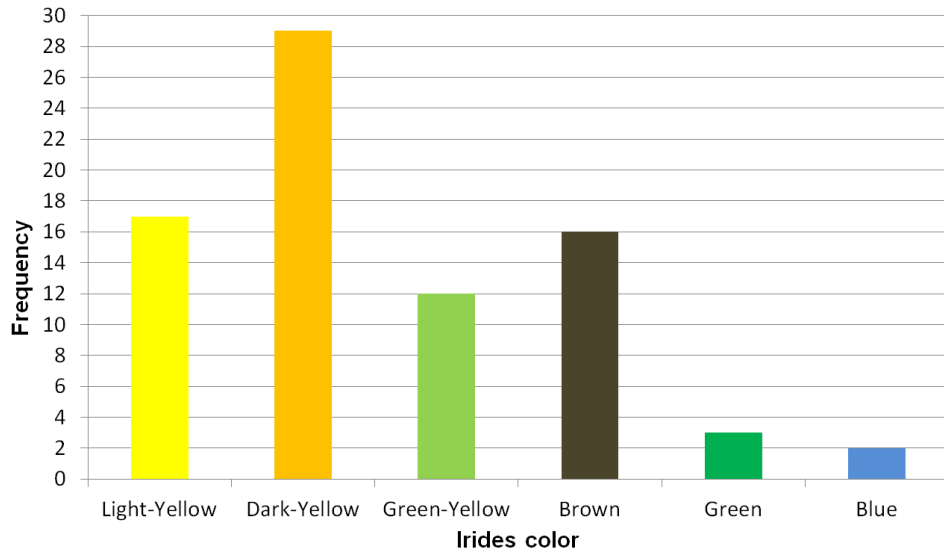
Figure 6.7: The color distributions of the irides of the 79 subjects in the UTIRIS database.

the NIR images achieved the best results as shown in Fig. 6.8 with EER = 2.71% while the red channel achieved a worse EER of 7.49% followed by the green and blue channels with EER of 9.09% and 16.02%, respectively.

6.5.4 Cross-spectral Experiments

Cross-spectral study is important because it shows the feasibility of performing iris recognition in several security applications such as information forensics, security surveillance
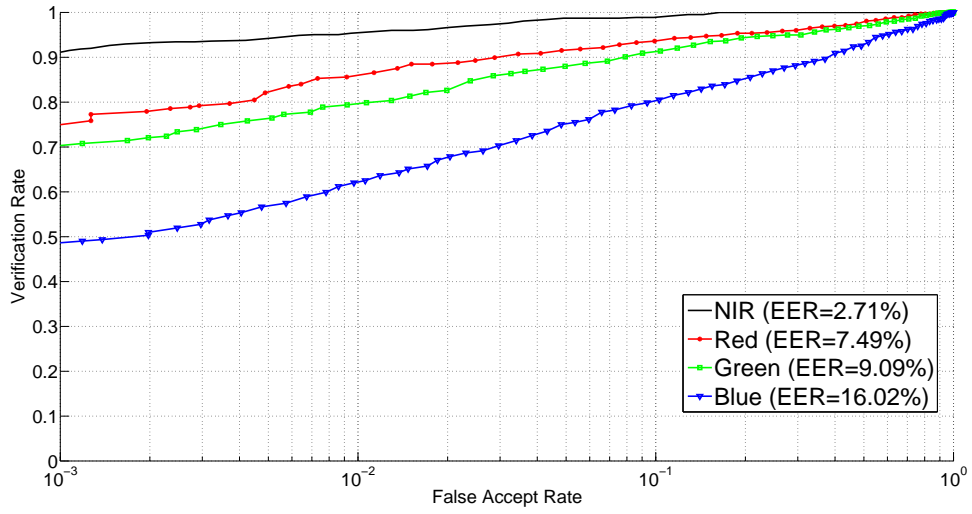
Figure 6.8: The performance of the iris recognition under red, green, blue and NIR spectra for the PolyU database.

Table 6.1: EER (%) of different channels comparison on the UTIRIS database

	NIR	Red	Green	Blue
NIR	3.45	27.53	38.81	40.31
Red	-	2.92	3.64	15.34
Green	-	-	3.50	6.45
Blue	-	-	-	6.33

and hazard assessment. Typically, a person's iris images are captured under NIR but most of the security cameras operate in the VL spectrum. Hence, NIR vs. VL matching is desired.

In this context, these comparisons are carried out using the traditional 1D Log-Gabor filter: NIR vs. red, NIR vs. green and NIR vs. blue on the UTIRIS and PolyU databases. Fig. 6.10 and Fig 6.11 depict the ROC curves of these comparisons for the UTIRIS database and the PolyU database, respectively. Accordingly, the green and blue channels resulted in bad performance due to the big gap in the electromagnetic spectrum between these channels and the NIR spectrum.

On the contrary, the red channel gave the best performance compared to the green and blue channels. This can be attributed to the small gap in the wavelength of the red channel (780nm) compared to the NIR (850nm). Therefore, the comparisons of Red vs NIR are considered as the baseline for cross-spectral matching. Table 6.1 and Table 6.2 show the EERs of cross-channel matching experiments for both the UTIRIS and PolyU databases,

Table 6.2: EER (%) of different channels comparison on the PolyU database

	NIR	Red	Green	Blue
NIR	**2.71**	17.16	22.74	36.17
Red	-	7.49	10.37	14.34
Green	-	-	9.09	13.48
Blue	-	-	-	16.02

respectively.

For all cross-spectral experiments, the leave-one-out approach has been adopted to obtain the comparison results [161]. Hence, for each subject with (m) iris samples, one sample is set as a probe and the comparison is repeated iteratively by swapping the probe with the remaining $(m-1)$ samples. The experiments for each subject are repeated $(m(m-1)/2)$ times and the final performance is measured in terms of EER by taking the minimum of the obtained comparison scores of each subject.

6.5.4.1 Cross-spectral Matching of Registered Images

A training based approach is adopted for the iris images in the PolyU database as these images have the same pixel correspondence. An FFNN is built for each subject and the unwrapped iris images of the same subject were converted to the gray-scale and used as an input to the ANN.

The target of the ANN is set to be one of the corresponding NIR images of the same subject. In the testing phase, the output image (NIR pixels) is predicted from the input VL image and the verification is performed. Fig. 6.9 shows the input VL image and the predicted NIR image while Table 6.3 shows the cross-spectral recognition performance.

Table 6.3: The results of the cross-spectral verification using the FFNN on the PolyU database.

Matching	EER
NIR vs. NIR	2.71
NIR vs. NIR_Predicted	2.75
NIR vs. Red	17.16

(a)

(b)

(c)
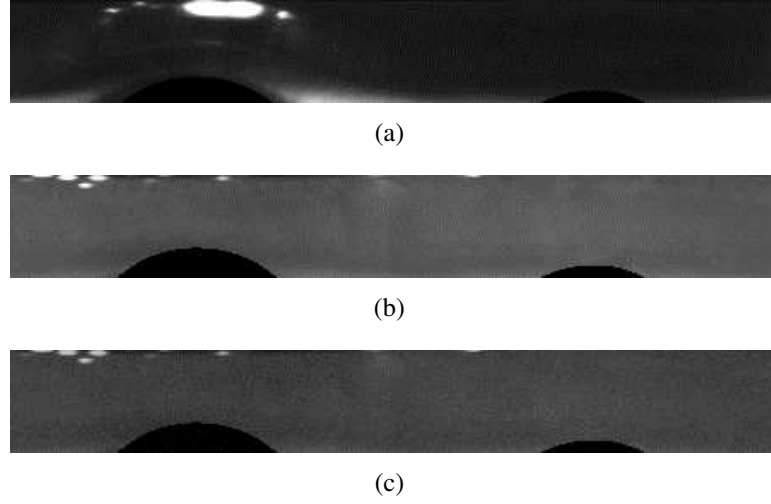
Figure 6.9: Unwrapped iris images: (a) R channel, (b) NIR image and (c) the predicted NIR image.

Table 6.4: Experiments on different descriptors for cross-spectral matching on the UTIRIS database.

Method	EER (%)
Baseline	27.53
LBP (different combinations) [162]	>28
Adaptive single scale retinex	25.56
Non-local means normalization	27.49
Wavelet based normalization	28.65
Homomorphic filtering	29.07
Multi scale self quotient	26.99
Tan and Triggs normalization	23.43
DoG	**19.51**
MSW	**18.91**
BSIF	**20.64**

6.5.4.2 Cross-spectral Matching of Unregistered Images

Cross-spectral matching is more challenging for unregistered images as is the case in the UTIRIS database and a training based approach tends to fail on such images due to the lack in pixel correspondence. Therefore, to alleviate the cross-spectrum differences, different descriptors and feature enhancement techniques are employed, out of which the DoG, MWS and BSIF recorded the best results as shown in Table 6.4. Hence, the proposed framework, which is depicted in Fig. 6.3, is based on these descriptors.

To further enhance the performance of cross-spectral matching, the fusion of the G-DoG, G-BSIF and G-MSW is considered. Different fusion methods are investigated with

the UTIRIS database namely: feature fusion, score fusion and decision fusion; out of which the decision fusion is observed to be the most effective.

Table 6.5 shows the performance of different fusion strategies for cross-spectral matching in terms of EER. Feature fusion resulted in poor results where the EER varied from 14-18%. Score level fusion with minimum rule achieved better results. On the other hand, the AND rule decision level fusion achieved the best results with EER = 6.81% as shown in Fig. 6.10.

A low FAR is preferred to achieve a secure biometric system. To further enhance the performance and reduce the FAR, a fusion at the decision level is performed. Therefore, the conjunction "AND" rule is used to combine the decisions from the G-DoG, G-BSIF and G-MSW. This means a false accept can only happen when all the previous descriptors produce a false accept [163].

Let $PD(FA)$, $PS(FA)$ and $PM(FA)$ represent the probability of a false accept using G-DoG, G-BSIF and G-MSW respectively. Similarly, $PD(FR)$, $PS(FR)$ and $PM(FR)$ represent the probability of a false reject. Therefore, the combined probability of a false accept $PC(FA)$ is the product of the three probabilities of the descriptors:

$$PC(FA) = PD(FA).PS(FA).PM(FA). \tag{6.4}$$

On the other hand, the combined probability of a false reject $PC(FR)$ can be expressed as the complement of the probability that none of the descriptors produce a false

Table 6.5: Experiments on different fusion strategies for cross-spectral matching on the UTIRIS database.

| Method	EER (%)		
	Feature fusion	Score fusion (min)	Decision fusion (AND)
DoG+MSW	16.56	14.21	8.08
DoG+BSIF	17.56	15.42	8.77
BSIF+MSW	18.12	16.34	8.33
DoG+BSIF+MSW	14.59	12.83	**6.81**
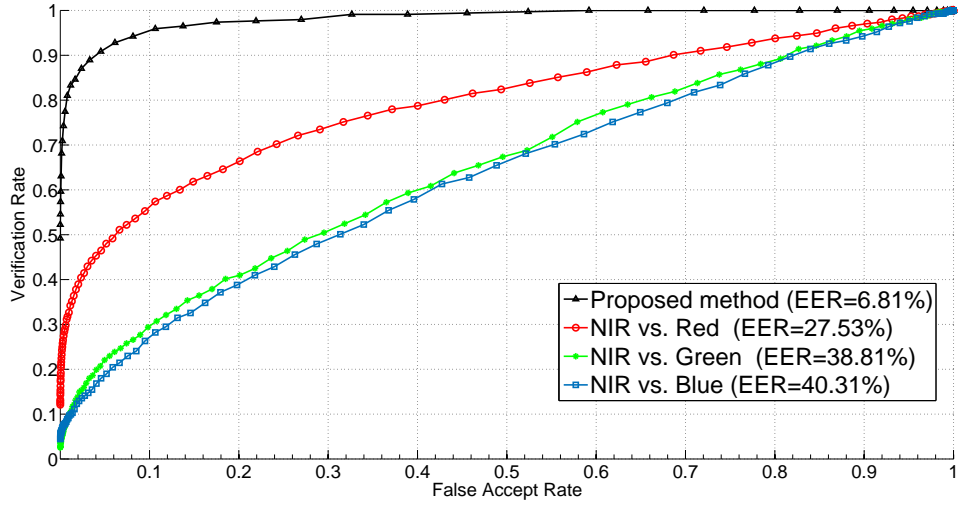
Figure 6.10: Cross-channel matching of the UTIRIS database.
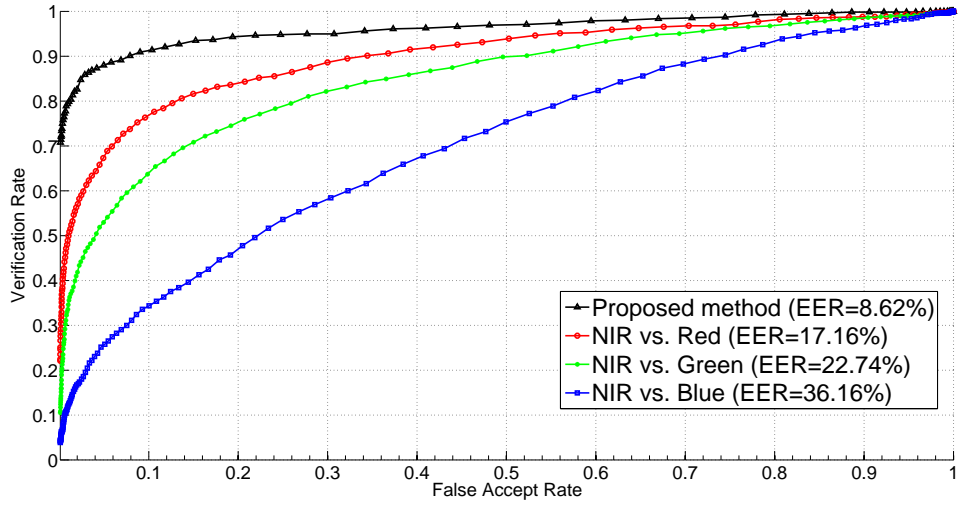
Figure 6.11: Cross-channel matching of the PolyU database.

reject:

$$PC(FR) = (PD(FR)'.PS(FR)'.PM(FR)')',$$
$$= (1 - (1 - PD(FR))(1 - PS(FR))(1 - PM(FR))),$$
$$= PD(FR) + PS(FR) + PM(FR)+$$
$$PD(FR).PS(FR) + PD(FR).PM(FR)+$$
$$PS(FR).PM(FR) + PD(FR).PS(FR).PM(FR). \quad (5)$$

127

It can be seen from the previous equations that the joint probability of false rejection increases while the joint probability of false acceptance decreases when using the AND conjunction rule.

The proposed framework for cross-spectral matching has also been applied on the PolyU iris database and an enhancement in the cross-spectral matching is recorded as shown in Fig 6.11. However, this improvement is not as good as the performance improvement of the UTIRIS database as the images in the PolyU database are registered. The training based approach achieves better results however it might be difficult to acquire registered images in the real life situations.

6.5.5 Multi-spectral Iris Recognition

The cross-channel comparisons demonstrated that red and NIR channels are the most suitable candidates for fusion as they gave the lowest EER compared to other channels as shown in Fig. 6.10 and Fig. 6.11 so it is common sense to fuse them in order to boost the recognition performance. Score level fusion is adopted for this purpose due to its efficiency and low complexity [164]. Hence, the matching scores (Hamming distances) are combined from both the red and NIR images using sum rule based fusion with equal weights to generate a single matching score. After that the recognition performance is evaluated again with the ROC curves and EER.

The VL and NIR images in the UTIRIB database are not registered. Therefore, they provide different iris texture information. It is evident from Fig. 6.12 that such fusion is useful to the iris biometric as there is a significant improvement in the recognition performance after the fusion with EER of only 0.54% compared to 2.92% and 3.45% before the fusion.

On the other hand, the fusion of the VL and NIR images in the PolyU database barely improved the recognition performance as shown in Fig. 6.13. This is because the iris images in the PolyU database are registered and hence they do not provide much different information as the iris texture is similar.
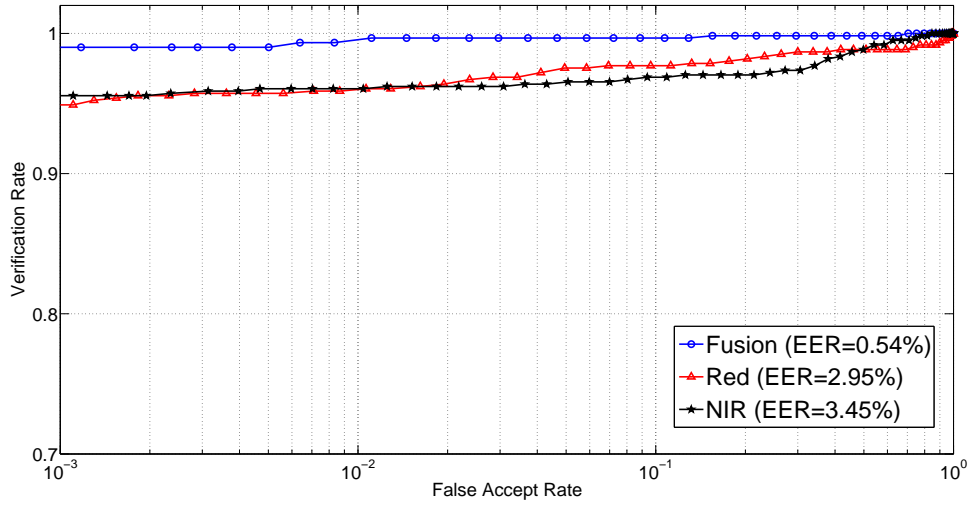
Figure 6.12: ROC curves showing the iris recognition performance before and after fusing the information of the red and NIR channels for the UTIRIS database.
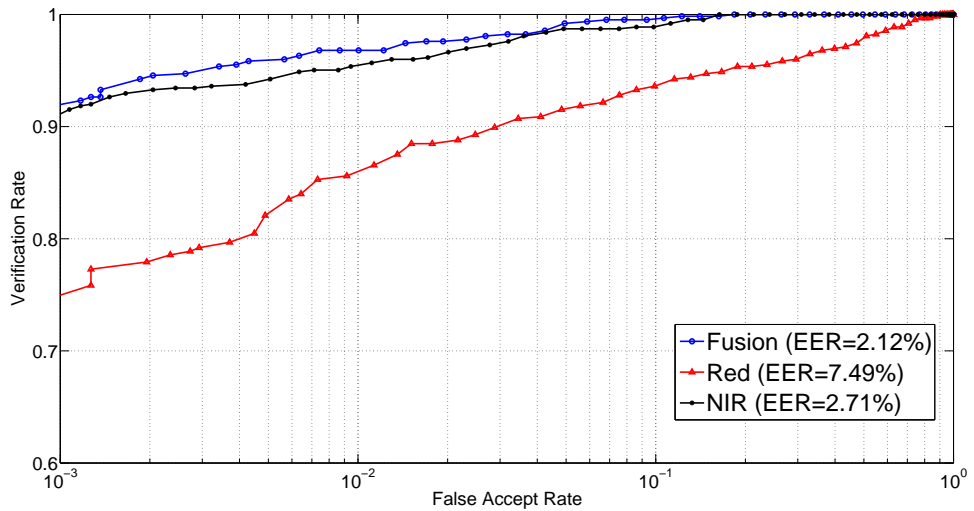
Figure 6.13: ROC curves showing the iris recognition performance before and after fusing the information of the red and NIR channels for the PolyU database.

6.5.6 Comparisons with Related Work

As mentioned earlier, the previous works have either adopted training models [136] to predict the corresponding iris images or descriptor models to alleviate the difference among iris images captured under different lighting conditions [149].

In [136] the authors adopted a training based approach using the FFNN to predict the NIR from the VL images. Although good results were reported, the main drawback

129

is adopting a sequential process to train the ANN. The problems of using this style are: long time in the training phase, high error values in the training and testing phases; and increasing the possibility of the local minima. On the contrary, constructing the output (NIR images) in one burst output will generally overcome the aforementioned drawbacks. It can be argued that this style would increase the memory requirements, but this issue can be overlooked taking in mind the memory capacity of current computers.

In the works of [147] and [165], the results of cross-spectral matching on unregistered iris images were reported. However, no models were proposed to enhance the cross-spectral iris matching. Table 6.6 shows the comparison results of the aforementioned works compared to this method.

Table 6.6: Cross-spectral matching comparison with different methods.

Method	Database	EER (%)
Wild et al. [165]	UTIRIS	33-55
Ramaiah & Kumar [148]	Private	34.01
Abdullah et al. [147]	UTIRIS	27.46
Proposed	UTIRIS	6.81
Proposed	PolyU	2.75

6.5.7 Processing Time

All experiments were conducted on a 3.2 GHz core i5 PC with 8 GB of RAM under the Matlab environment. The average training time for the FFNN is 7.5 minutes while the testing time was less than two seconds.

On the other hand, the proposed framework for cross-spectral matching of unregistered images consists of four main descriptors namely: BSIF, DoG, MSW and 1D log-Gabor filter. The processing times of the 1D log-Gabor filter, BSIF and DoG descriptors are 10, 20 and 70 ms, respectively while the MSW processing times is 330 ms. Therefore, the total computations time of the proposed method is less than half a second which implies its suitability for real time applications.

6.6 Summary

In this chapter, a framework for cross-spectral iris matching was proposed. In addition, the applications and benefits of using multi-spectral iris information in iris recognition systems were highlighted. Iris recognition performance has been investigated under different imaging channels: red, green, blue and NIR. The experiments were carried out on the UTIRIS and the PolyU databases and the performance of the iris biometric was measured.

Two methods were proposed for cross-spectral iris matching. The first method was designed to work with registered iris images which adopted an FFNN to synthesize the corresponding NIR images from the VL images to perform the verification. The second method is capable of working with unregistered iris images based on integrating the Gabor filter with different photometric normalization models and descriptors along with decision level fusion to achieve the cross-spectral matching.

The following conclusions can be drawn from the results. According to Table 6.4, among a variety of descriptors, the DoG, BSIF and MSW were found to give good cross-spectral performance for unregistered iris images after integrating them with the 1D log-Gabor filter. Table 6.6 and Fig. 6.10 showed a significant improvement in the cross-spectral matching performance of the UTIRIS database using the proposed framework.

In terms of multi-spectral iris performance, Fig. 6.6 showed that the red channel of iris images in the UTIRIS database achieved better performance compared to other channels or the NIR imaging. This can be attributed to the large number of the light pigmented irides in this database. However, the NIR images in the PolyU database achieved the best performance among other channels due to the dominance of the brown irides in the PolyU database.

It was also noticed from Fig. 6.10 and Fig. 6.11 that the performance of the iris recognition varied as a function of the difference in wavelength among the image channels. Fusion of the iris images from the red and NIR channels improved the recognition performance in the UTIRIS database. The results implied that both VL and NIR imaging were important to form a robust iris recognition system as they provided complementary features for the iris pattern. The next chapter draws the overall conclusions and provides directions for future work.

Chapter 7

Conclusions and Future Work

Conclusions

Among the various traits used for human identification, the iris pattern has gained an increasing amount of attention for its accuracy, reliability, and noninvasive characteristics. Iris recognition is an active research area with several unsolved problems. In this work, the most important open issues in exploiting the iris biometric were presented and novel methods to address these problems were proposed.

In Chapter 1, a general introduction to biometrics has been presented along with the commonly used biometric traits and their characteristics. In addition, the aims and contributions of this work were given. All of the aims and objectives set out in Chapter 1 have been fulfilled in this thesis.

In Chapter 2, a brief history of iris recognition was presented showing the main milestones in iris recognition development. In addition, the anatomy and properties of the human iris were presented from image acquisition to feature matching. After that, the main stages in iris recognition namely: segmentation, normalization, feature extraction and matching were presented and their corresponding algorithms were explained.

In Chapter 3, a brief introduction to biometric systems performance evaluation was given along with the performance graphs. In addition, the potential of the iris biometric was illustrated by the current national scale public deployment of iris based recognition systems. Moreover, a survey of the available public iris databases was given.

In Chapter 4, a novel method for iris segmentation has been proposed. A new pressure force was designed and integrated within the GVF active contour to allow the contour to expand or shrink, which in turn helps to achieve robust iris and image segmentation. The proposed iris segmentation process consisted of two models: pupil segmentation and

iris segmentation. For pupil segmentation, two schemes were proposed to determine the approximate parameters of the pupil in the iris images which are captured under visible and near infrared light. These parameters were then used to set the initial mask for the active contour. On the other hand, for iris segmentation, the Hough line transform was employed for eyelid detection. Hence, if the eyelid is closed or covering the pupil, the contour will shrink from the initial mask which is set to be larger than the iris. In contrast, if the eyelid is not close to the pupil, the contour will expand from the initial mask which is set outside the pupil boundary. The proposed scheme is robust in finding the exact iris boundary and isolating the eyelids of the iris images.

The experimental results on the CASIA V4, MMU2, UBIRIS V1 and UBIRIS V2 databases showed that the proposed scheme achieved state-of-the-art results in terms of segmentation accuracy and recognition performance while being computationally more efficient for both iris images captured under NIR and VL. In this context, improvements of 60.5%, 42% and 48.7% were achieved in segmentation accuracy for the CASIA V4, MMU2 and UBIRIS V1 databases, respectively, compared to the nearest best results as shown in Table 4.2. As for the UBIRIS V2 database, a superior time reduction was reported (85.7%) compared to the nearest best result as shown in Table 4.3 while maintaining a similar accuracy. Similarly, considerable time improvements of 63.8%, 56.6% and 29.3% were achieved for CASIA V4, MMU2 and UBIRIS V1 database, respectively, as shown in Table 4.5.

Chapter 5 brought insight into the problem of biometric security. Novel schemes were proposed for iris biometric protection which consisted of two security layers. The first layer exploited a robust watermarking algorithm which was implemented to protect the

integrity of the biometric image. In particular, a binary text image that accommodates the bio-data of the person to be authenticated was embedded in the iris image by randomly interchanging four pairs of the DCT middle band coefficients. The embedding locations were randomly selected based on a private key. Moreover, the proposed strength constant S was included to add more robustness to the watermarking algorithm. The second layer involved using VC to protect the iris template by decomposing the original iris template into two shares where one share is given to the user on a smart card while the other is stored in a database. The proposed VC scheme allows the iris template to be perfectly restored with the same quality and size when the shares are available, and therefore it does not hinder the iris recognition performance. Furthermore, the integrity of the iris templates, in both the smart card and the database, was also guaranteed with the use of hash signatures.

The experimental results and comparison with state-of-the-art methods revealed that the proposed scheme was robust in terms of iris image and templates protection and capable of withstanding attacks, while it did not involve significant degradation to iris recognition performance. The proposed method has a minimal effect on the iris recognition performance of only 3.6% and 4.9% for the CASIA V4 and UBIRIS V1 databases, respectively, as shown in Table 5.9. This can be overlooked by the obtained benefits of protecting the integrity of the iris image. The proposed method also outperformed similar watermarking methods by withstanding different attacks, for example PSNR improvements of 69.5% and 27.6% were achieved for median filter attack and JPEG compression compared to the nearest best method as shown in Table 5.2. In addition, the VC scheme is designed to be readily applied to protect any biometrics binary template without degrad-

ing the recognition performance with a complexity of only $O(N)$.

In Chapter 6, a novel framework for cross-spectral iris matching was proposed. In addition, this work highlights the applications and benefits of using multi-spectral iris information in iris recognition systems. Two methods were proposed for cross-spectral iris matching. The first method was designed to work with registered iris images which adopted a FFNN to synthesize the corresponding NIR images from the VL images to perform the verification. The second method is capable of working with unregistered iris images based on integrating the Gabor filter with different photometric normalization models and descriptors along with decision level fusion to achieve robust cross-spectral matching. Among a variety of descriptors, the DoG, BSIF and MSW were found to give a good cross-spectral performance for unregistered iris images after integrating them with the 1D log-Gabor filter. In terms of multi-spectral iris performance, the red channel of iris images in the UTIRIS database achieved better performance compared to other channels or NIR imaging. This can be attributed to the large number of light pigmented irides in this database. On the other hand, the best performance among other channels was achieved with the NIR images in the PolyU database due to the dominance of the brown irides in the PolyU database. It was also noticed that the performance of the iris recognition varied as a function of the difference in wavelength among the image channels. Fusion of the iris images from the red and NIR channels improved the recognition performance in the UTIRIS database. The results implied that both VL and NIR imaging were important to form a robust iris recognition system as they provided complementary features for the iris pattern.

The proposed methods attained a significant improvement in cross-spectral matching

results. This can be clearly seen from Table 6.6 where an improvement of 79.3% was attained in the cross-spectral matching for the UTIRIS database compared to the best available result. As for the PolyU database, the proposed verification method achieved an improvement of 83.9% in terms of NIR vs Red channel matching as shown in Table 6.3.

Future Work

Widespread deployments of iris recognition systems confirm that iris biometrics perform well in relatively constrained environments. Nevertheless, there are still open gaps regarding the use of iris biometric in unconstrained environments. In addition, the growing number of employed iris recognition systems across the globe flags the issue of the security of raw data and iris template protection. Needless to say, the increased number of security incidents has highlighted the interest in cross-spectral iris matching in forensics applications.

It is difficult to cover all the aspects of this system and address all of its challenges in one thesis. The following are some of the proposed ideas to be considered in future work which can be divided into several categories.

Firstly, in terms of segmentation and recognition performance, the following points are still not fully addressed:

- Designing new methods which are capable of segmenting the iris from real-time videos in real life applications.

- Improving the ability of the current system in discarding bad quality images.

- Enhancing the performance of at-a-distance and on-the-move iris recognition.

- Investigating the surveillance-based recognition performance of the iris biometric.

Secondly, regarding the stability of the iris texture and its ability to withstand variations, the following issues can be summarized:

- Long-term (10 years) iris image collection to investigate the effects of aging and stability.

138

- The effect of eye surgery on iris recognition performance is not properly considered. The number of studies and data available on this subject are limited.

- Studying the effects of varying pupil dilation on iris recognition and designing methods to counteract the deformation caused by this effect.

On the other hand, the use of iris biometrics in forensics is an emerging topic which is still understudied. There is plenty of room for research in the following points:

- Inspecting human-aided iris recognition for use in court along with face and finger biometrics needs further study.

- Designing new methods to detect counterfeit iris images.

- Postmortem iris recognition is still an understudied topic, therefore, more work needs to be carried out to investigate iris recognition performance for such images.

Finally, new topics such as cross-spectral matching and deep learning for iris biometrics need to be further studied with respect to the following points:

- Experiments in cross-spectral matching need to be generalized on large scale databases to accurately judge the performance.

- Utilizing deep learning for iris biometrics is still understudied. Deep learning is achieving promising results in various contexts and iris biometrics should not be an exception.

- Developing new methods for "eye print" recognition that utilize all the available biometric modalities in this area namely, iris, ocular and sclera traits.

References

[1] A. K. Jain, A. A. Ross, and K. Nandakumar, *Introduction to Biometrics*. Springer, US, 2011.

[2] A. Jain, P. Flynn, and A. A. Ross, *Handbook of Biometrics*. Springer US, 2008.

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

[4] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, *Handbook of Fingerprint Recognition*. Springer, 2009.

[5] S. Z. Li and A. K. Jain, *Handbook of Face Recognition*. Springer, 2011.

[6] J. Daugman, "How iris recognition works," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 14, no. 1, pp. 21–30, 2004.

[7] J. Daugman, "High confidence visual recognition of persons by a test of statistical independence," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 15, no. 11, pp. 1148–1161, 1993.

[8] A. K. Jain, K. Nandakumar, and A. Ross, "50 years of biometric research: Accomplishments, challenges, and opportunities," *Pattern Recognition Letters*, vol. 79, pp. 80–105, 2016.

[9] U. Park, R. R. Jillela, A. Ross, and A. K. Jain, "Periocular biometrics in the visible spectrum," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 1, pp. 96–106, 2011.

[10] S. Alkassar, W. L. Woo, S. S. Dlay, and J. A. Chambers, "Robust sclera recognition system with novel sclera segmentation and validation techniques," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 43, no. 3, pp. 474–486, 2017.

[11] Z. Zhou, E. Y. Du, C. Belcher, N. L. Thomas, and E. J. Delp, "Quality fusion based multimodal eye recognition," in *2012 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, pp. 1297–1302.

[12] M. S. Nixon, T. Tan, and R. Chellappa, *Human Identification Based on Gait*. Springer US, 2006.

[13] D. Cunado, M. S. Nixon, and J. N. Carter, "Automatic extraction and description of human gait models for recognition purposes," *Computer Vision and Image Understanding*, vol. 90, no. 1, pp. 1 – 41, 2003.

[14] M. J. Burge and K. W. Bowyer, *Handbook of Iris Recognition*. Springer, 2013.

[15] C. Newman, "A life revealed," *National Geographic*, 2002. [Online]. Available: http://www.nationalgeographic.com/magazine/2002/04/afghan-girl-revealed/

[16] J. Daugman, "How the Afghan girl was identified by her iris patterns," 2002. [Online]. Available: http://www.cl.cam.ac.uk/~jgd1000/afghan.html

[17] J. Wayman, N. Orlans, Q. Hu, F. Goodman, A. Ulrich, and V. Valencia, "Technology assessment for the state of the art biometrics excellence roadmap," MITRE Corporation, Tech. Report: US Gov Contr. J-FBI-07-164, 2009.

[18] R. P. Wildes, "Iris recognition: an emerging biometric technology," *Proceedings of the IEEE*, vol. 85, no. 9, pp. 1348–1363, 1997.

[19] C. Hollitt, "Reduction of computational complexity of Hough transforms using a convolution approach," in *24th International Conference on Image and Vision Computing*, 2009, pp. 373–378.

[20] M. Haidekker, *Deformable Models and Active Contours*. Wiley-IEEE Press, 2011, pp. 173–210.

[21] C. Xu and P. J. L., "Snakes, shapes, and gradient vector flow," *IEEE Transactions on Image Processing*, vol. 7, no. 3, pp. 359–369, 1998.

[22] J. Ryan, D. Woodard, A. Duchowski, and S. Birchfield, "Adapting starburst for elliptical iris segmentation," in *2nd IEEE International Conference on Biometrics: Theory, Applications and Systems, (BTAS2008)*, 2008, pp. 1–7.

[23] S. A. Sahmoud and I. S. Abuhaiba, "Efficient iris segmentation method in unconstrained environments," *Pattern Recognition*, vol. 46, no. 12, pp. 3174–3185, 2013.

[24] C. Rathgeb, A. Uhl, and P. Wild, *Iris Biometrics From Segmentation to Template Security*. Springer Verlag, 2013.

[25] W. W. Boles and B. Boashash, "A human identification technique using images of the iris and wavelet transform," *IEEE Transactions on Signal Processing*, vol. 46, no. 4, pp. 1185–1188, 1998.

[26] H. G. Feichtinger and T. Strohmer, *Gabor Analysis and Algorithms: Theory and Applications*.   Springer, New York, 1998.

[27] A. V. Oppenheim and J. S. Lim, "The importance of phase in signals," *Proceedings of the IEEE*, vol. 69, no. 5, pp. 529–541, 1981.

[28] D. J. Field, "Relations between the statistics of natural images and the response properties of cortical cells," *Journal of the Optical Society of America*, vol. 4, no. 12, pp. 2379–2393, 1987.

[29] Z. Yong, T. Tieniu, and W. Yunhong, "Biometric personal identification based on iris patterns," in *15th International Conference on Pattern Recognition*, vol. 2, 2000, pp. 801–804 vol.2.

[30] T. Dunstone and N. Yager, *Biometric System and Data Analysis: Design, Evaluation, and Data Mining*.   New York, USA: Springer, 2008.

[31] J. Daugman, "Probing the uniqueness and randomness of iriscodes: Results from 200 billion iris pair comparisons," *Proceedings of the IEEE*, vol. 94, no. 11, pp. 1927–1935, 2006.

[32] P. J. Grother, G. W. Quinn, J. R. Matey, M. L. Ngan, W. J. Salamon, G. P. Fiumara, and C. I. Watson, "IREX III: Performance of iris identification algorithms," National Institute of Standards and Technology, USA, Report, 2012.

[33] J. Daugman, "Evolving methods in iris recognition," in *IEEE International Conference on Biometrics: Theory, Applications, and Systems, (BTAS07)*, 2007. [Online]. Available: http://www.cse.nd.edu/BTAS_07/John_Daugman_BTAS.pdf

[34] Chinese Academy of Sciences Institute of Automation, "CASIA Iris Image Database." [Online]. Available: http://biometrics.idealtest.org/dbDetailForUser.do?id=4

[35] Malaysian Multimedia University, "Multimedia university version 2 iris database," 2010. [Online]. Available: http://pesona.mmu.edu.my/~ccteo/

[36] H. Proena and L. A. Alexandre, "UBIRIS: A noisy iris image database," in *13th International Conference on Image Analysis and Processing (ICIAP2005)*, vol. 3617. Springer, 2005, pp. 970–977.

[37] H. Proenca, S. Filipe, R. Santos, J. Oliveira, and L. A. Alexandre, "The UBIRIS.v2: A Database of Visible Wavelength Iris Images Captured On-the-Move and At-a-Distance," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 32, no. 8, pp. 1529–1535, 2010.

[38] P. R. Nalla and A. Kumar, "Toward more accurate iris recognition using cross-spectral matching," *IEEE Transactions on Image Processing*, vol. 26, no. 1, pp. 208–221, Jan 2017.

[39] M. S. Hosseini, B. N. Araabi, and H. Soltanian-Zadeh, "Pigment melanin: Pattern for iris recognition," *IEEE Transactions on Instrumentation and Measurement*, vol. 59, no. 4, pp. 792–804, 2010.

[40] M. Dobes and L. Machala, "UPOL iris image database," 2004. [Online]. Available: http://www.upol.cz

[41] S. E. Baker, A. Hentz, K. W. Bowyer, and P. J. Flynn, "Degradation of iris recognition performance due to non-cosmetic prescription contact lenses," *Computer Vision and Image Understanding*, vol. 114, no. 9, pp. 1030 – 1044, 2010.

[42] S. P. Fenker and K. W. Bowyer, "Analysis of template aging in iris biometrics," in *2012 IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops*, 2012, pp. 45–51.

[43] J. Galbally, J. Ortiz-Lopez, J. Fierrez, and J. Ortega-Garcia, "Iris liveness detection based on quality related features," in *2012 5th IAPR International Conference on Biometrics (ICB)*, 2012, pp. 271–276.

[44] J. Huang, X. You, Y. Tang, L. Du, and Y. Yuan, "A novel iris segmentation using radial-suppression edge detection," *Signal Processing*, vol. 89, no. 12, pp. 2630–2643, 2009.

[45] H. Proenca and L. A. Alexandre, "A method for the identification of inaccuracies in pupil segmentation," in *The First International Conference on Availability, Reliability and Security. (ARES2006)*, 2006, pp. 1–5.

[46] R. Jillela and A. Ross, *Methods for Iris Segmentation*. Springer London, 2016, pp. 137–184.

[47] M. Kass, A. Witkin, and D. Terzopoulos, "Snakes: Active contour models," *International Journal of Computer Vision*, vol. 1, no. 4, pp. 321–331, 1988.

[48] L. D. Cohen and I. Cohen, "Finite-element methods for active contour models and balloons for 2-D and 3-D images," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 15, no. 11, pp. 1131–1147, 1993.

[49] L. Masek and P. Kovesi, "Matlab source code for a biometric identification system based on iris patterns," The School of Computer Science and Software Engineering, The University of Western Australia, 2003.

[50] M. Li, T. Tieniu, W. Yunhong, and Z. Dexin, "Efficient iris recognition by characterizing key local variations," *IEEE Transactions on Image Processing*, vol. 13, no. 6, pp. 739–750, 2004.

[51] X. Liu, K. Bowyer, and P. Flynn, "Experiments with an improved iris segmentation algorithm," in *Fourth IEEE Workshop on Automatic Identification Advanced Technologies*, 2005, pp. 118–123.

[52] T. Tan, Z. He, and Z. Sun, "Efficient and robust segmentation of noisy iris images for non-cooperative iris recognition," *Image and Vision Computing*, vol. 28, no. 2, pp. 223–230, 2010.

[53] A. Radman, K. Jumari, and N. Zainal, "Fast and reliable iris segmentation algorithm," *Image Processing, IET*, vol. 7, no. 1, pp. 42–49, 2013.

[54] W. Hong-Lin, L. Zhi-Cheng, Q. Jian-Ping, and L. Bao-Sheng, "Non-ideal iris segmentation using anisotropic diffusion," *Image Processing, IET*, vol. 7, no. 2, pp. 111–120, 2013.

[55] H. Zhaofeng, T. Tieniu, S. Zhenan, and Q. Xianchao, "Toward accurate and fast iris segmentation for iris biometrics," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 31, no. 9, pp. 1670–1684, 2009.

[56] F. Jan and I. Usman, "Iris segmentation for visible wavelength and near infrared eye images," *Optik - International Journal for Light and Electron Optics*, vol. 125, no. 16, pp. 4274–4282, 2014.

[57] M. Frucci, M. Nappi, D. Riccio, and G. Sanniti di Baja, "Wire: Watershed based iris recognition," *Pattern Recognition*, vol. 52, pp. 148–159, 2016.

[58] H. Ghodrati, M. Dehghani, M. Helfroush, and K. Kazemi, "Localization of non-circular iris boundaries using morphology and arched Hough transform," in *Second International Conference on Image Processing Theory Tools and Applications, (IPTA10)*, 2010, pp. 458–463.

[59] J. Daugman, "New methods in iris recognition," *IEEE Transactions on System, Man and, Cybernetics, Part B*, vol. 37, no. 5, pp. 1167–1175, 2007.

[60] M. Vatsa, R. Singh, and A. Noore, "Improving iris recognition performance using segmentation, quality enhancement, match score fusion, and indexing," *IEEE Transactions on System, Man and, Cybernetics, Part B*, vol. 38, no. 4, pp. 1021–1035, 2008.

[61] S. Shah and A. Ross, "Iris segmentation using geodesic active contours," *IEEE Transactions on Information, Forensic and Security*, vol. 4, no. 4, pp. 824–836, 2009.

[62] S. M. Talebi, A. Ayatollahi, and S. M. S. Moosavi, "A novel iris segmentation method based on balloon active contour," in *6th Iranian Machine Vision and Image Processing*, 2010, pp. 1–5.

[63] K. Roy, P. Bhattacharya, and C. Suen, *Unideal Iris Segmentation Using Region-Based Active Contour Model*. Springer Berlin Heidelberg, 2010, vol. 6112, book section 26, pp. 256–265.

[64] L. Hilal, B. Daya, and P. Beauseroy, "Hough transform and active contour for enhanced iris segmentation," *IJCSI International Journal of Computer Science Issues*, vol. 9, no. 6, pp. 1–10, 2012.

[65] M. De Marsico, M. Nappi, D. Riccio, and H. Wechsler, "Mobile Iris Challenge Evaluation (MICHE)-I, biometric iris dataset and protocols," *Pattern Recognition Letters*, vol. 57, no. 0, pp. 17–23, 2015.

[66] H. Hofbauer, F. Alonso-Fernandez, P. Wild, J. Bigun, and A. Uhl, "A ground truth for iris segmentation," in *22nd International Conference on Pattern Recognition*, 2014, pp. 527–532.

[67] R. R. Jillela and A. Ross, "Segmenting iris images in the visible spectrum with applications in mobile biometrics," *Pattern Recognition Letters*, vol. 57, pp. 4–16, 2015.

[68] V. Caselles, R. Kimmel, and G. Sapiro, "Geodesic active contours," in *Fifth International Conference on Computer Vision*, 1995, pp. 694–699.

[69] T. F. Chan and L. A. Vese, "Active contours without edges," *IEEE Transactions on Image Processing*, vol. 10, no. 2, pp. 266–277, 2001.

[70] W. P. Choi, K. M. Lam, and W. C. Siu, "An adaptive active contour model for highly irregular boundaries," *Pattern Recognition*, vol. 34, no. 2, pp. 323–331, 2001.

[71] M. A. M. Abdullah, S. S. Dlay, and W. L. Woo, "Fast and accurate pupil isolation based on morphology and active contour," in *the 4th International Conference on Signal, Image Processing and Applications*. IACSIT, 2014, pp. 418–420.

[72] D. Comaniciu and P. Meer, "Mean shift: a robust approach toward feature space analysis," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 24, no. 5, pp. 603–619, 2002.

[73] N. Otsu, "A threshold selection method from gray-level histograms," *IEEE Transactions on System, Man and Cybernetics*, vol. 9, no. 1, pp. 62–66, 1979.

[74] H. Proenca, "Iris recognition: On the segmentation of degraded images acquired in the visible wavelength," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 32, no. 8, pp. 1502–1516, 2010.

[75] L. Sigal, S. Sclaroff, and V. Athitsos, "Skin color-based video segmentation under time-varying illumination," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 26, no. 7, pp. 862–877, 2004.

[76] C. O. Conaire, N. E. O'Connor, and A. F. Smeaton, "Detector adaptation by maximising agreement between independent data sources," in *IEEE Conference on Computer Vision and Pattern Recognition, 2007*, pp. 1–6.

[77] P. Li, X. Liu, L. Xiao, and Q. Song, "Robust and accurate iris segmentation in very noisy iris images," *Image and Vision Computing*, vol. 28, no. 2, pp. 246–253, 2010.

[78] E. M. Arvacheh, "A study of segmentation and normalization for iris recognition systems," University of Waterloo, Master desertation, 2006.

[79] H. Proenca and L. A. Alexandre, "The NICE.I: Noisy Iris Challenge Evaluation - Part I," in *First IEEE International Conference on Biometrics: Theory, Applications, and Systems*, 2007, pp. 1–4.

[80] M. A. Luengo-Oroz, E. Faure, and J. Angulo, "Robust iris segmentation on uncalibrated noisy images using mathematical morphology," *Image and Vision Computing*, vol. 28, no. 2, pp. 278–284, 2010.

[81] Y. Chen, M. Adjouadi, C. Han, J. Wang, A. Barreto, N. Rishe, and J. Andrian, "A highly accurate and computationally efficient approach for unconstrained iris segmentation," *Image and Vision Computing*, vol. 28, no. 2, pp. 261–269, 2010.

[82] R. Donida Labati and F. Scotti, "Noisy iris segmentation with boundary regularization and reflections removal," *Image and Vision Computing*, vol. 28, no. 2, pp. 270–277, 2010.

[83] C.-W. Tan and A. Kumar, "Unified framework for automated iris segmentation using distantly acquired face images," *IEEE Transactions on Image Processing*, vol. 21, no. 9, pp. 4068–4079, 2012.

[84] M. A. M. Abdullah, S. S. Dlay, and W. L. Woo, "Fast and accurate method for complete iris segmentation with active contour and morphology," in *2014 IEEE*

International Conference on Imaging Systems and Techniques (IST2014), 2014, pp. 123–128.

[85] M. Nabti and A. Bouridane, "New active contours approach and phase wavelet maxima to improve iris recognition system," in *4th European Workshop on Visual Information Processing, (EUVIP)*, 2013, pp. 238–244.

[86] C. W. Tan and A. Kumar, "Accurate iris recognition at a distance using stabilized iris encoding and zernike moments phase features," *IEEE Transactions on Image Processing*, vol. 23, no. 9, pp. 3962–3974, Sept 2014.

[87] P. Stavroulakis and M. Stamp, *Handbook of Information and Communication Security*. Springer, 2010.

[88] N. Ratha, J. Connell, and R. Bolle, *An Analysis of Minutiae Matching Strength*. Springer Berlin Heidelberg, 2001, vol. 2091, book section 32, pp. 223–228.

[89] K. Martin, L. Haiping, F. M. Bui, K. N. Plataniotis, and D. Hatzinakos, "A biometric encryption system for the self-exclusion scenario of face recognition," *IEEE Systems Journal*, vol. 3, no. 4, pp. 440–450, 2009.

[90] A. Jain, A. Ross, and U. Uludag, "Biometric template security: Challenges and solutions," in *13th European Signal Processing Conference, EUSIPCO*, 2005.

[91] S. Venugopalan and M. Savvides, "How to generate spoofed irises from an iris code template," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 2, pp. 385–395, 2011.

[92] J. Galbally, A. Ross, M. Gomez-Barrero, J. Fierrez, and J. Ortega-Garcia, "Iris image reconstruction from binary templates: An efficient probabilistic approach based on genetic algorithms," *Computer Vision and Image Understanding*, vol. 117, no. 10, pp. 1512–1525, 2013.

[93] O. Nafea, S. Ghouzali, W. Abdul, and E.-u.-H. Qazi, "Hybrid multi-biometric template protection using watermarking," *The Computer Journal*, vol. 59, no. 2, 2015.

[94] G. Bhatnagar, Q. M. Wu, and B. Raman, "Biometric template security based on watermarking," *Procedia Computer Science*, vol. 2, pp. 227–235, 2010.

[95] A. K. Jain, U. Uludag, and H. Rein-Lien, "Hiding a face in a fingerprint image," in *16th International Conference on Pattern Recognition*, vol. 3, 2002, pp. 756–759.

[96] M. Islam, M. Sayeed, and A. Samraj, "Biometric template protection using watermarking with hidden password encryption," in *International Symposium on Information Technology, ITSim2008.*, vol. 1, 2008, pp. 1–8.

[97] M. R. Isa and S. Aljareh, "Biometric image protection based on Discrete Cosine Transform watermarking technique," in *International Conference on Engineering and Technology (ICET2012)*, 2012, pp. 1–5.

[98] I. J. Cox, J. Kilian, F. T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," *IEEE Transactions on Image Processing*, vol. 6, no. 12, pp. 1673–1687, 1997.

[99] K. Park, D. Jeong, B. Kang, and E. Lee, *A Study on Iris Feature Watermarking on Face Data*. Springer Berlin Heidelberg, 2007, vol. 4432, book section 47, pp. 415–423.

[100] N. Bartlow, N. Kalka, B. Cukic, and A. Ross, "Protecting iris images through asymmetric digital watermarking," in *2007 IEEE Workshop on Automatic Identification Advanced Technologies*, 2007, pp. 192–197.

[101] A. Hassanien, A. Abraham, and C. Grosan, "Spiking neural network and wavelets for hiding iris data in digital images," *Soft Computing*, vol. 13, no. 4, pp. 401–416, 2009.

[102] S. Majumder, K. J. Devi, and S. K. Sarkar, "Singular value decomposition and wavelet-based iris biometric watermarking," *Biometrics, IET*, vol. 2, no. 1, pp. 21–27, 2013.

[103] M. Paunwala and S. Patnaik, "Biometric template protection with DCT-based watermarking," *Machine Vision and Applications*, vol. 25, no. 1, pp. 263–275, 2014.

[104] M. A. M. Abdullah, S. S. Dlay, and W. L. Woo, "Securing iris images with a robust watermarking algorithm based on Discrete Cosine Transform," in *Proceedings of the 10th International Conference on Computer Vision Theory and Applications*, vol. 3, 2015, pp. 108–114.

[105] F. Hao, R. Anderson, and J. Daugman, "Combining crypto with biometrics effectively," *IEEE Transactions on Computers*, vol. 55, no. 9, pp. 1081–1088, 2006.

[106] J. Bringer, H. Chabanne, G. Cohen, B. Kindarji, and G. Zemor, "Theoretical and practical boundaries of binary secure sketches," *IEEE Transactions on Information Forensics and Security*, vol. 3, no. 4, pp. 673–683, 2008.

[107] S. Yan, Z. Xukai, E. Y. Du, and L. Feng, "Design and analysis of a highly user-friendly, secure, privacy-preserving, and revocable authentication method," *IEEE Transactions on Computers*, vol. 63, no. 4, pp. 902–916, 2014.

[108] S. Cimato, M. Gamassi, V. Piuri, R. Sassi, and F. Scotti, *A Multi-biometric Verification System for the Privacy Protection of Iris Templates*. Springer Berlin Heidelberg, 2009, vol. 53, book section 29, pp. 227–234.

[109] C. Rathgeb, F. Breitinger, C. Busch, and H. Baier, "On application of bloom filters to iris biometrics," *Biometrics, IET*, vol. 3, no. 4, pp. 207–218, 2014.

[110] J. Hermans, B. Mennink, and R. Peeters, "When a bloom filter is a doom filter: Security assessment of a novel iris biometric template protection system," in *International Conference of the Biometrics Special Interest Group (BIOSIG)*, 2014, pp. 1–6.

[111] D. Aeloor and A. Manjrekar, *Securing Biometric Data with Visual Cryptography and Steganography*. Springer Berlin Heidelberg, 2013, vol. 377, book section 33, pp. 330–340.

[112] K. Anusree and G. S. Binu, "Biometric privacy using visual cryptography, halftoning and watermarking for multiple secrets," in *National Conference on Communication, Signal Processing and Networking*, 2014, pp. 1–5.

[113] W. Yiwei, J. F. Doherty, and R. E. Van, "A wavelet-based watermarking algorithm for ownership verification of digital images," *IEEE Transactions on Image Processing*, vol. 11, no. 2, pp. 77–88, 2002.

[114] C.-K. Chan and L. M. Cheng, "Hiding data in images by simple LSB substitution," *Pattern Recognition*, vol. 37, no. 3, pp. 469–474, 2004.

[115] R. M. Thanki, R. K. Kher, and D. Vyas, "Robustness of correlation based watermarking techniques using WGN against different order statistics filters," *International Journal of Computer Science and Telecommunications*, vol. 2, no. 4, pp. 45–49, 2011.

[116] P. Dabas and K. Khanna, "A study on spatial and transform domain watermarking techniques," *International Journal of Computer Applications*, vol. 71, no. 14, pp. 38–41, 2013.

[117] G. C. Langelaar, I. Setyawan, and R. L. Lagendijk, "Watermarking digital image and video data. a state-of-the-art overview," *IEEE Signal Processing Magazine*, vol. 17, no. 5, pp. 20–46, 2000.

[118] M. Naor and A. Shamir, "Visual cryptography," in *Advances in Cryptology-EUROCRYPT'94*. Springer Berlin Heidelberg, 1995, vol. 950, pp. 1–12.

[119] F. Liu and W. Yan, "Various problems in visual cryptography," in *Visual Cryptography for Image Processing and Security*. Springer International Publishing, 2014, pp. 23–61.

[120] J. R. Hernandez, M. Amado, and F. Perez-Gonzalez, "DCT-domain watermarking techniques for still images: detector performance analysis and a new structure," *IEEE Transactions on Image Processing*, vol. 9, no. 1, pp. 55–68, 2000.

[121] N. F. Johnson and S. Katzenbeisser, *A Survey of Steganographic Techniques*. Artech House Books, 2000, pp. 1–17.

[122] A. K. Jain, K. Nandakumar, and A. Nagar, "Biometric template security," *EURASIP Journal on Advances in Signal Processing*, vol. 2008, no. 113, 2008.

[123] U.S. Department of Commerce, "Secure Hash Standard (SHS)," 2008.

[124] M. A. M. Abdullah, F. Al-Dulaimi, W. Al-Nuaimy, and A. Al-Ataby, "Smart card with iris recognition for high security access environment," in *2011 1st Middle East Conference on Biomedical Engineering (MECBME)*, 2011, pp. 382–385.

[125] M. A. M. Abdullah, S. S. Dlay, W. L. Woo, and J. A. Chambers, "Robust iris segmentation method based on a new active contour force with a noncircular normalization," *IEEE Transactions on Systems, Man and Cybernetics: Systems*, vol. In press, no. 1, p. 11, 2016.

[126] F. Zhang, G. Yang, X. Liu, and X. Zhang, *Image Watermarking Algorithm Based on the Code Division Multiple Access Technique*, ser. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2006, vol. 4252, book section 26, pp. 204–211.

[127] W. Yu-Pin, C. Mei-Juan, and C. Po-Yuen, "Robust image watermark with wavelet transform and spread spectrum techniques," in *34th Conference on Signals, Systems and Computers*, vol. 2, 2000, pp. 1846–1850.

[128] G. Chen, Y. Mao, and C. K. Chui, "A symmetric image encryption scheme based on 3D chaotic cat maps," *Chaos, Solitons and Fractals*, vol. 21, no. 3, pp. 749–761, 2004.

[129] M. Narasimha and A. Peterson, "On the computation of the discrete cosine transform," *IEEE Trans. Commun.*, vol. 26, no. 6, pp. 934–936, 1978.

[130] B. Groer and B. Lang, "An $O(n^2)$ algorithm for the bidiagonal SVD," *Linear Algebra and its Applications*, vol. 358, no. 13, pp. 45–70, 2003.

[131] C. Rathgeb, A. Uhl, and P. Wild, *Cancelable Iris Biometrics*.   Springer New York, 2013, vol. 59, book section 12, pp. 223–231.

[132] J. Bringer, H. Chabanne, and C. Morel, "Shuffling is not sufficient: Security analysis of cancelable iriscodes based on a secret permutation," in *2014 IEEE International Joint Conference on Biometrics (IJCB)*, 2014, pp. 1–8.

[133] A. Jain, K. Nandakumar, and A. Nagar, "Fingerprint template protection: From theory to practice," in *Security and Privacy in Biometrics*.   Springer London, 2013, pp. 187–214.

[134] Y. Feng and P. Yuen, "Binary discriminant analysis for generating binary face template," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 2, pp. 613–624, 2012.

[135] K. W. Bowyer, "The results of the NICE.II Iris biometrics competition," *Pattern Recognition Letters*, vol. 33, no. 8, pp. 965–969, 2012.

[136] Z. Jinyu, F. Nicolo, and N. A. Schmid, "Cross spectral iris matching based on predictive image mapping," in *Fourth IEEE International Conference on Biometrics: Theory Applications and Systems (BTAS'10)*, 2010, pp. 1–5.

[137] C. Boyce, A. Ross, M. Monaco, L. Hornak, and L. Xin, "Multispectral iris analysis: A preliminary study," in *Computer Vision and Pattern Recognition Workshop*, 2006, pp. 51–51.

[138] N. Tajbakhsh, B. N. Araabi, and H. Soltanianzadeh, "Feature fusion as a practical solution toward noncooperative iris recognition," in *11th International Conference on Information Fusion*, 2008, pp. 1–7.

[139] H. T. Ngo, R. W. Ives, J. R. Matey, J. Dormo, M. Rhoads, and D. Choi, "Design and implementation of a multispectral iris capture system," in *Asilomar Conference on Signals, Systems and Computers*, 2009, pp. 380–384.

[140] A. Ross, R. Pasula, and L. Hornak, "Exploring multispectral iris recognition beyond 900nm," in *IEEE 3rd International Conference on Biometrics: Theory, Applications, and Systems. (BTAS'09)*, 2009, pp. 1–8.

[141] R. W. Ives, H. T. Ngo, S. D. Winchell, and J. R. Matey, "Preliminary evaluation of multispectral iris imagery," in *IET Conference on Image Processing (IPR 2012)*, 2012, pp. 1–5.

[142] A. Sharma, S. Verma, M. Vatsa, and R. Singh, "On cross spectral periocular recognition," in *IEEE International Conference on Image Processing (ICIP)*, 2014, pp. 5007–5011.

[143] F. Alonso-Fernandez, A. Mikaelyan, and J. Bigun, "Comparison and fusion of multiple iris and periocular matchers using near-infrared and visible images," in *2015 International Workshop on Biometrics and Forensics (IWBF)*, 2015, pp. 1–6.

[144] S. G. Crihalmeanu and A. A. Ross, *Multispectral Ocular Biometrics*. Springer International Publishing, 2016, pp. 355–380.

[145] M. J. Burge and M. K. Monaco, "Multispectral iris fusion for enhancement, interoperability, and cross wavelength matching," *Proceedings of the SPIE 7334, Algorithms and Technologies for Multispectral, Hyperspectral, and Ultraspectral Imagery XV*, vol. 7334, pp. 73 341D–1–73 341D–8, 2009.

[146] M. Burge and M. Monaco, *Multispectral Iris Fusion and Cross-Spectrum Matching*, ser. Advances in Computer Vision and Pattern Recognition. Springer London, 2013, book section 9, pp. 171–181.

[147] M. A. M. Abdullah, S. S. Dlay, W. L. Woo, and J. A. Chambers, "Iris biometric: Is the near-infrared spectrum always the best?" in *3rd Asian Conference on Pattern Recognition (ACPR2015)*, 2015.

[148] N. P. Ramaiah and A. Kumar, *Advancing Cross-Spectral Iris Recognition Research Using Bi- Spectral Imaging*, ser. Advances in Intelligent Systems and Computing. Springer, 2016, vol. 390, book section 1, pp. 1–10.

[149] M. A. M. Abdullah, S. S. Dlay, W. L. Woo, and J. A. Chambers, "A novel framework for cross-spectral iris matching," *IPSJ Transactions on Computer Vision and Applications*, vol. 8, no. 9, pp. 1–11, 2016.

[150] S. M. Carden, R. E. Boissy, P. J. Schoettker, and W. V. Good, "Albinism: Modern molecular diagnosis," *British Journal of Opthamology*, vol. 82, no. 2, pp. 189–195, 1998.

[151] J. C. Khan, H. Shahid, D. A. Thurlby, M. Bradley, D. G. Clayton, A. T. Moore, A. C. Bird, and J. R. W. Yates, "Age related macular degeneration and sun exposure, iris colour, and skin sensitivity to sunlight," *British Journal of Ophthalmology*, vol. 90, no. 1, pp. 29–32, 2006.

[152] P. Meredith and T. Sarna, "The physical and chemical properties of eumelanin," *Pigment Cell Res.*, vol. 19, no. 6, pp. 572–594, 2006.

[153] J. Kannala and E. Rahtu, "Bsif: Binarized statistical image features," in *21st International Conference on Pattern Recognition (ICPR)*, 2012, pp. 1363–1366.

[154] V. Struc and N. Pavesic, "Gabor-based kernel partial-least-squares discrimination features for face recognition," *Informatica*, vol. 20, no. 1, pp. 115–138, 2009.

[155] V. Struc and N. Pavesic, *Photometric Normalization Techniques for Illumination Invariance*.   Hershey, PA, USA: IGI Global, 2011, pp. 279–300.

[156] X. Tan and B. Triggs, "Enhanced local texture feature sets for face recognition under difficult lighting conditions," *IEEE Transactions on Image Processing*, vol. 19, no. 6, pp. 1635–1650, June 2010.

[157] S. R. Arashloo and J. Kittler, "Class-specific kernel fusion of multiple descriptors for face verification using multiscale binarised statistical image features," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 12, pp. 2100–2109, 2014.

[158] X. Li, W. Bu, and X. Wu, *Palmprint Liveness Detection by Combining Binarized Statistical Image Features and Image Quality Assessment.* Springer International Publishing, 2015, pp. 275–283.

[159] A. K. Jain, *Fundamentals of Digital Image Processing.* Upper Saddle River, NJ, USA: Prentice-Hall, Inc., 1989.

[160] B. Wang, W. Li, W. Yang, and Q. Liao, "Illumination normalization based on weber's law with application to face recognition," *IEEE Signal Processing Letters*, vol. 18, no. 8, pp. 462–465, 2011.

[161] K. B. Raja, R. Raghavendra, V. K. Vemuri, and C. Busch, "Smartphone based visible iris recognition using deep sparse filtering," *Pattern Recogonition Letters*, vol. 57, no. C, pp. 33–42, May 2015.

[162] T. Ojala, M. Pietikainen, and T. Maenpaa, "Multiresolution gray-scale and rotation invariant texture classification with local binary patterns," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 24, no. 7, pp. 971–987, 2002.

[163] D. Maltoni, D. Maio, A. Jain, and S. Prabhakar, *Multimodal Biometric Systems.* New York, NY: Springer New York, 2003, pp. 233–255.

[164] M. He, S.-J. Horng, P. Fan, R.-S. Run, R.-J. Chen, J.-L. Lai, M. K. Khan, and K. O. Sentosa, "Performance evaluation of score level fusion in multimodal biometric systems," *Pattern Recognition*, vol. 43, no. 5, pp. 1789–1800, 2010.

[165] P. Wild, P. Radu, and J. Ferryman, "On fusion for multispectral iris recognition," in *2015 International Conference on Biometrics (ICB)*, 2015, pp. 31–37.