Preface

The field of security has witnessed an explosive growth during the last years, as phenomenal advances in both research and applications have been made. Biometric and forensic imaging applications often involve photographs, videos and other image impressions that are fragile and include subtle details that are difficult to see. As a developer, one needs to be able to quickly develop sophisticated imaging applications that allow for an accurate extraction of precious information from image data for identification and recognition purposes. This is true for any type of biometric and forensic image data.

The applications covered in this book relate to Biometrics, Watermarking and Shoeprint recognition for forensic science. Image processing transforms using Discrete Fourier Transform, Discrete Wavelet Transforms Gabor Wavelets, Complex Wavelets, Scale Invariant Feature Transforms and Directional Filter banks are used in data modelling process for either feature extraction or data hiding tasks. The emphasis is on the methods and the analysis of data sets including comparative studies against existing and similar techniques. To make the underlying methods accessible to a wider audience, we have stated some of the key mathematical results given in a logical structure of the development.

For example, biometric based methods are emerging as the most reliable solutions for authentication and identification applications where traditional passwords (knowledge-based security) and ID cards (token-based security) have been used so far to access restricted systems. Automated biometrics deal with physiological or behavioural characteristics such as fingerprints, iris, voice and face that can be used to authenticate a person’s identity or establish an identity within a database. With rapid progress in electronic and Internet commerce, there is also a growing need to authenticate the identity of a person for secure transaction processing. Current biometric systems make use of fingerprints, hand geometry, iris, retina, face, facial thermograms, signature gait, and voiceprint to establish a person’s identity. While biometric systems have their limitations they have an edge over traditional security methods in that they cannot be easily stolen or shared. Besides bolstering security, biometric systems also enhance user convenience by alleviating the need to design and remember passwords.

Driven by the urgent need to protect digital media content that is being widely and wildly distributed and shared through the Internet by an ever-increasing number of users, the field of digital watermarking has witnessed an extremely fast-growing development since its inception almost a decade ago. The main purpose of digital watermarking, information embedding, and data hiding systems is to embed auxiliary information, usually called digital watermarks, inside a host signal (audio, image, and video) by introducing small and minor perturbations into the host signal. The quality of the host signal should not be degraded unacceptably and the introduced changes lie below the minimum perception threshold of the intended recipient. Watermark detection and extraction from the composite host signal should be possible in the presence of a variety of intentional and unintentional manipulations and attacks. It is obvious that these attacks and manipulations do not corrupt the composite host signal at an unacceptable level.

Watermarking systems are expected to play an important role in meeting at least two major challenges that resulted from the widespread use of Internet for the distribution and exchange of digital media: (i) error-free perfect copies of digital multimedia and (ii) availability of free and affordable tools for the manipulation and alteration of digital content. The first challenge was the driving force that led the combined efforts of academic and industrial research to produce first-generation watermarking algorithms. These algorithms were mainly concerned with the "*copyright protection*" of the digital content. For instance, illegal distribution and copying of digital music is causing the music industry massive gain losses. The second challenge has guided the research efforts to develop what are so-called "*tamper-proof*" or "*fragile*" watermarking algorithms. This class of watermarking schemes aims at detecting any "*intentional*" manipulation or corruption of the media.

Following the emergence and success of forensic science as a powerful and irrefutable tool for solving many enigmatic crime puzzles, images collected from crime scenes are abounding and, therefore, large image collections are being created. Shoeprint images are no exception and it has been indicated, recently, that shoeprint evidence, at crime scenes, is more frequently present than fingerprints. Very recently, it has been suggested that shoeprint evidence should be made comparable to that of fingerprint and DNA evidence. It is also true that shoeprint intelligence remains an untapped potential forensic source (usually overshadowed by the accepted fingerprint and DNA evidence). However, there is no practical technology to efficiently search shoeprint on large databases. Existing commercial systems still require manual involvement (manual annotation of both the impression under investigation and the primary database). The task of automated scenemark matching is a tedious one and researching the use of existing image processing and pattern recognition techniques is desired before an underpinning technology is developed.

One of the most distinctive features of the book is that it covers in detail a number of imaging applications and their deployment in security problems. In addition, the book appeals to both undergraduate and postgraduate students since each application problem includes a detailed description of the mathematical background and its implementation.

Most of the material of the book is derived from very recent research output generated by various researchers at doctoral level under the supervision of the author.

This brings some novelty of the topics through a thorough analysis of the results of the implementation. My indebtedness to those students, in particular W R Boukabou, M Gueham, M Laadjel, M Nabti, O Nibouche, I Thompson, H Su, K Zebbiche and A Baig of the Speech, Image and Vision Systems (SIVS) group at the School of Electronics, Electrical Engineering and Computer Science, Queen's University Belfast.

The book is organised as follows. Chapter 1 starts by defining the biometric technology including the characteristics required for a viable deployment using various operation modes such as verification, identification and watch-list. A number of currently used biometric modalities are also described with some emphasis of few emerging ones. Then the various steps of a typical biometric recognition system are discussed in detail. For example, data acquisition, image localisation, feature extraction and matching are all defined and the current methods employed for their implementation and deployment discussed and contrasted. The chapter concludes by briefly highlighting the need to use appropriate datasets for the evaluation of a biometric system.

Chapter 2 introduces the notion of data representation in the context of biometrics. The various stages of a typical biometric system are also enumerated and discussed and the most commonly deployed biometric modalities are stated. The chapter also examines various aspects related to image data representation and modelling for feature extraction and matching. Various methods are then briefly discussed and brought within the context of a biometric system. For example, image data formats, feature sets and system testing and performance evaluation metrics are detailed.

In Chapter 3 recent advances in enhancing the performance of face recognition using the concept of directional filter banks is discussed. In this context, the directional filter banks are investigated as pre-processing phase in order to improve the recognition rates of a number of different and existing algorithms. The chapter starts by reviewing the basic face recognition principles and enumerates the various steps of a face recognition system. Four algorithms representing both Component and Discriminant Analysis approaches, namely: PCA, ICA (FastICA), LDA and SDA are chosen for their proven popularity and efficiency to demonstrate the usefulness of the directional filter bank method. The mathematical models behind these approaches are also detailed. Then the proposed directional filter bank method is described and its implementation discussed. The results and their analysis are finally assessed using two well known face databases.

Chapter 4 is concerned with recent advances in iris recognition using a mutiscale approach. State of the art works in the area is first highlighted and discussed and a detailed review of the various steps of an automatic iris recognition system enumerated. Proposed developments are then detailed for both iris localisation and classification using an integrated multiscale wavelet approach. Extensive experimentation is carried out and a comparative analysis with some state of the art approaches given. The chapter concludes by giving some future directions to further enhance the results obtained.

In chapter 5, the use of complex wavelets for image and video watermarking is described. The theory of complex wavelets and their features are first highlighted.

The concept of spread transform watermarking is then given in detail and its combination with the complex wavelet transforms detailed. Information theoretic capacity analysis for watermarking with complex wavelets is then elucidated. The chapter concludes with some experiments and their analysis to demonstrate the improved levels of capacity that can be achieved through the superior feature representation offered by complex wavelet transforms.

Chapter 6 discusses the problem of one-bit watermark detection for protecting fingerprint images. Such a problem is theoretically formulated based on the maximum-likelihood scheme, which requires an accurate modeling of the host data. The watermarking is applied into the Discrete Wavelet Transform (DWT) due to the vavious advantages provided by this transform. First, a statistical study of DWT coefficients is carried out by investigating and comparing three distributions, namely, the generalized Gaussian, Laplacian and Cauchy models. Then, the performances of the detectors based on these models are assessed and evaluated through extensive experiments. The results show that the generalized Gaussian is the best model and its corresponding detector yields the best detection performance.

Chapter 7 is intended to introduce the emerging shoemark evidence for forensic use. It starts by giving a detailed background of the contribution of shoemark data to scene of crime officers including a discussion of the methods currently in use to collect shoeprint data. Methods for the collection of shoemarks will also be detailed and problems associated with each method highlighted. In addition, the chapter gives a detailed review of existing shoemark classification systems.

In Chapter 8, methods for automatically classifying shoeprints for use in forensic science are presented. In particular, we propose two correlation based approaches to classify low quality shoeprints: i) Phase-Only Correlation (POC) which can be considered as a matched filter, and ii) Advanced Correlation Filters (ACFs). These techniques offer two primary advantages: the ability to match low quality shoeprints and translation invariance. Experiments were conducted on a database of images of 100 different shoes available on the market. For the experimental evaluation, challenging test images including partial shoeprints with different distortions (such as noise addition, blurring and in-plane rotation) were generated. Results have shown that the proposed correlation based methods are very practical and provide high performance when processing low quality partial-prints.

Chapter 9 is concerned with the retrieval of scene-of-crime (or scene) shoeprint images from a reference database of shoeprint images by using a new local feature detector and an improved local feature descriptor. Similar to most other local feature representations, the proposed approach can also be divided into two stages: (i) a set of distinctive local features is selected by first detecting scale adaptive Harris corners where each corner is associated with a scale factor. This allows for the selection of the final features whose scale matches the scale of blob-like structures around them and (ii) for each feature, an improved Scale Invariant Feature Transform (SIFT) descriptor is computed to represent it. Our investigation has led to the development of two novel methods which are referred to as the Modified Harris-Laplace (MHL) detector and the Modified SIFT descriptor, respectively.

Contributions:

Chapter 2: "Data Representation and Analysis"
A. Baig and A. Bouridane

Chapter 3: "Improving Face Recognition Using Directional Faces"
W. R. Boukabou and A. Bouridane

Chapter 4: "Recent Advances in Iris Recognition: A Multiscale Approach"
M. Nabti and A. Bouridane

Chapter 5: "Spread Transform Watermarking Using Complex Wavelets"
I. Thompson and A. Bouridane

Chapter 6: "Protection of Fingerprint Data Using Watermarking"
K. Zebbiche and A. Bouridane

Chapter 7: "Shoemark Recognition for Forensic Science: An Emerging Technology"
H. Su and A. Bouridane

Chapter 8: "Techniques for Automatic Shoeprint Classification"
M. Gueham and A. Bouridane

Chapter 9: "Automatic Shoeprint Image Retrieval Using Local Features"
H. Su and A. Bouridane

Belfast, United Kingdom, 2008 Ahmed Bouridane

Springer

http://www.springer.com/978-0-387-09531-8

Imaging for Forensics and Security
From Theory to Practice
Bouridane, A.
2009, XVIII, 212 p. 60 illus., Hardcover
ISBN: 978-0-387-09531-8