# Handbook of Multibiometrics

# International Series on Biometrics

*Consulting Editors*

**Professor David D. Zhang**

*Department of Computer Science*
*Hong Kong Polytechnic University*
*Hung Hom, Kowloon, Hong Kong*

email: csdzhang@comp.polyu.edu.hk

**Professor Anil K. Jain**

*Dept. of Computer Science& Eng.*
*Michigan State University*
*3115 Engineering Bldg.*
*East Lansing, MI 48824-1226, U.S.A.*

Email: jain@cse.msu.edu

In our international and interconnected information society, there is an ever-growing need to authenticate and identify individuals. Biometrics-based authentication is emerging as the most reliable solution. Currently, there have been various biometric technologies and systems for authentication, which are either widely used or under development. The International Book Series on Biometrics will systematically introduce these relative technologies and systems, presented by biometric experts to summarize their successful experience, and explore how to design the corresponding systems with in-depth discussion.

In addition, this series aims to provide an international exchange for researchers, professionals, and industrial practitioners to share their knowledge of how to surf this tidal wave of information. The International Book Series on Biometrics will contain new material that describes, in a unified way, the basic concepts, theories and characteristic features of integrating and formulating the different facets of biometrics, together with its recent developments and significant applications. Different biometric experts, from the global community, are invited to write these books. Each volume will provide exhaustive information on the development in that respective area. The International Book Series on Biometrics will provide a balanced mixture of technology, systems and applications. A comprehensive bibliography on the related subjects will also be appended for the convenience of our readers.

*Additional titles in the series:*
**UNCONSTRAINED FACE RECOGNITION** *by Shaohua Kevin Zhou, Rama Chellappa, Wenyi Zhao;* ISBN: 0-387-26407-8
**HUMAN IDENTIFICATION BASED ON GAIT** *by Mark S. Nixon, Tieniu Tan and Rama Chellappa;* ISBN: 0-387-24424-7
**PALMPRINT AUTHENTICATION** *by David D. Zhang;* ISBN: 1-4020-8096-4
**HUMAN-COMPUTER INTERFACE** *by Antonio J. Colmenarez, Ziyou Xiong and Thomas S. Huang;* ISBN: 1-4020-7802-1
**FACIAL ANALYSIS FROM CONTINUOUS VIDEO WITH APPLICATIONS TO COMPUTATIONAL ALGORITHMS FOR FINGERPRINT RECOGNITION** *by Bir Bhanu and Xuejun Tan;* ISBN: 1-4020-7651-7

Additional information about this series can be obtained from our website:
springer.com

# Handbook of Multibiometrics

*by*

**Arun A. Ross**
*Lane Department of Computer Science and Electrical Engineering*
*West Virginia University, USA*

**Karthik Nandakumar**
*Department of Computer Science and Engineering*
*Michigan State University, USA*

**Anil K. Jain**
*Department of Computer Science and Engineering*
*Michigan State University, USA*

Springer

Arun A. Ross
West Virginia University
Dept. of Computer Science & Electrical Eng.
751 ESB
Morgantown WV 26506-6109
ross@csee.wwu.edu

Karthik Nandakumar
Michigan State Univ.
Dept. of Computer Science & Eng.
PRIP Lab
3208 Engineering Bldg.
East Lansing MI 48824
nandakum@cse.msu.edu

Anil K. Jain
Michigan State University
Dept. of Computer Science & Eng.
3115 Engineering Building
East Lansing MI 48824
jain@cse.msu.edu

Library of Congress Control Number: 2006923240

**Handbook of Multibiometrics**
by Arun A. Ross, Karthik Nandakumar and Anil K. Jain

ISBN-13: 978-0-387-22296-7
ISBN-10: 0-387-22296-0
e-ISBN-13: 978-0-387-33123-2
e-ISBN-10: 0-387-33123-9

Printed on acid-free paper.

© 2006 Springer Science+Business Media, LLC
All rights reserved. This work may not be translated or copied in whole or in part without the written permission of the publisher (Springer Science+Business Media, LLC, 233 Spring Street, New York, NY 10013, USA), except for brief excerpts in connection with reviews or scholarly analysis. Use in connection with any form of information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now know or hereafter developed is forbidden.
The use in this publication of trade names, trademarks, service marks and similar terms, even if the are not identified as such, is not to be taken as an expression of opinion as to whether or not they are subject to proprietary rights.

Printed in the United States of America.

9 8 7 6 5 4 3 2 1

springer.com

# Contents

List of Figures vii
List of Tables xvii
Preface xix

1. BIOMETRICS: WHEN IDENTITY MATTERS 1
   1.1 Introduction 1
   1.2 Operation of a biometric system 5
   1.3 Verification versus identification 8
   1.4 Performance of a biometric system 10
   1.5 Applications of biometrics 17
   1.6 Biometric characteristics 19
   1.7 Limitations of biometric systems 24
   1.8 Biometric standards 29
   1.9 Multibiometric systems 31
   1.10Summary 32

2. INFORMATION FUSION IN BIOMETRICS 37
   2.1 Introduction 37
   2.2 Fusion in biometrics 40
   2.3 Issues in designing a multibiometric system 42
   2.4 Sources of multiple evidence 44
   2.5 Acquisition and processing architecture 51
   2.6 Levels of fusion 55
   2.7 Summary 57

3. LEVELS OF FUSION IN BIOMETRICS 59
3.1 Introduction 59
3.2 Sensor level fusion 60
3.3 Feature level fusion 64
3.4 Rank level fusion 70
3.5 Decision level fusion 73
3.6 Summary 82

4. SCORE LEVEL FUSION 91
4.1 Introduction 91
4.2 Classifier combination rules 93
4.3 Score fusion techniques 98
4.4 Density-based score fusion 99
4.5 Transformation-based score fusion 111
4.6 Classifier-based score fusion 124
4.7 Comparison of score fusion techniques 128
4.8 User-specific score fusion 131
4.9 Summary 141

5. FUSION INCORPORATING ANCILLARY INFORMATION 143
5.1 Introduction 143
5.2 Quality-based fusion 143
5.3 Soft biometrics 159
5.4 Summary 172

Appendices 173
A Evaluation of multibiometric systems 173
A.1 Biometric system evaluation 173
A.2 Issues in multibiometric system evaluation 174
A.3 Multimodal biometric databases 176

References 179

Index 195

# List of Figures

1.1 Authentication schemes. (a) Traditional schemes use ID cards, passwords and keys to validate individuals and ensure that system resources are accessed by a legitimately enrolled individual. (b) With the advent of biometrics, it is now possible to establish an identity based on "who you are" rather than by "what you possess" or "what you remember". 2

1.2 Examples of biometric traits that can be used for authenticating an individual. Physical traits include fingerprint, iris, face and hand geometry while behavioral traits include signature, keystroke dynamics and gait. 4

1.3 The Bertillonage system, so named after its inventor Alphonse Bertillon, relied on the precise measurement of various attributes of the body for identifying recidivists. These measurements included the height of the individual, the length of the arm, geometry of the head and the length of the foot. The process was tedious to administer and did not guarantee uniqueness across individuals. 5

1.4 A variety of fingerprint sensors with different specifications (e.g., sensing technology, image size, image resolution, image quality, etc.) are now available. These rather compact sensors may be embedded in computer peripherals and other devices to facilitate user authentication. 6

1.5 Enrollment and recognition (verification and identification) stages of a biometric system. The quality assessment module determines if the sensed data can be effectively used by the feature extractor. Note that the process of quality assessment in itself may entail the extraction of some features from the sensed data. 9

1.6 Multiple feature sets of the same biometric trait seldom result in an exact match. Here, three fingerprint impressions of a person's finger (left) and the corresponding minutia points (right) are shown. Due to variations in finger placement, elasticity of the skin and finger pressure, the minutiae distributions of the three impressions are observed to be quite different. A perfect match between two samples of the same finger is almost impossible to achieve. 11

1.7 The genuine and impostor distributions corresponding to the Face-G matcher in the NIST BSSR1 database. The threshold, $\eta$, determines the FAR and FRR of the system. Note that given these two distributions, the FAR and the FRR cannot be reduced *simultaneously* by adjusting the threshold. 13

1.8 The performance of a biometric system can be summarized using DET and ROC curves. In this example, the performance curves are computed using the match scores of the Face-G matcher from the NIST BSSR1 database. The graph in (a) shows a DET curve that plots FRR against FAR in the normal deviate scale. In (b) a ROC curve plots FRR against FAR in the linear scale, while in (c) a ROC curve plots GAR against FAR in a semi-logarithmic scale. 14

1.9 Biometric systems are being deployed in various applications. (a) The Schiphol Privium program at the Amsterdam airport uses iris scans to validate the identity of a traveler (www.airport-technology.com). (b) The Ben Gurion airport in Tel Aviv uses Express Card entry kiosks fitted with hand geometry systems for security and immigration (www.airportnet.org). (c) A few Kroger stores in Texas use fingerprint verification systems that enable customers to render payment at the check-out counter. The fingerprint information of a customer is linked with her credit or debit card (www.detnews.com). (d) Finger geometry information is used in Disney World, Orlando to ensure that a single season pass is not fraudulently used by multiple visitors. (e) A cell-phone that validates authorized users using fingerprints and allows them access to the phone's special functionalities such as mobile-banking (www.mobileburn.com). (f) The US-VISIT program currently employs two-print information to validate the travel documents of visitors to the United States (www.dhs.gov). 20

1.10 Intra-class variation associated with an individual's face image. Due to change in pose, an appearance-based face recognition system is unlikely to match these three images successfully, although they belong to the same individual (Hsu, 2002). 26

1.11 Non-universality of fingerprints. The four impressions of a user's fingerprint shown here cannot be enrolled by most fingerprint systems due to the poor image quality of the ridges. Consequently, alternate methods must be adopted in order to include this user in the biometric authentication system. 28

1.12 A biometric system is vulnerable to a variety of attacks (adapted from Ratha et al., 2001). For functional integrity, there should be protocols in place that deflect, detect and rectify the consequences of these attacks. 29

2.1 Two general approaches to solving a pattern recognition problem. Each cell in this diagram indicates the application of a particular classifier, $C_i$, to a specific pattern representation (i.e., feature set), $F_j$. The approach in (a) is to determine the best set of features and the best classifier, while in (b) the goal is to determine the best set of classifiers and an optimal fusion algorithm to integrate these classifiers. The feature sets $F_1, F_2, \ldots, F_N$ do not have to be mutually exclusive. 39

2.2 A multimodal interface to acquire face, fingerprint and hand geometry images of a person. A well designed interface can enhance user convenience and ensure that multiple sources of evidence are reliably acquired. In this example, integrating the hand and fingerprint input devices into a single unit may be beneficial as it would reduce the burden on the individual to explicitly interact with two spatially separated devices. 43

2.3 Multimodal biometric systems utilize different body traits to establish identity. In principle, a large number of traits can be used to improve the identification accuracy. In practice, factors such as cost of deployment, finite training sample size, throughput time and user training will limit the number of traits used in a particular application. 44

2.4 The various sources of information in a multibiometric system: multi-sensor, multi-algorithm, multi-instance, multi-sample and multimodal. In the first four scenarios, a single biometric trait provides multiple sources of evidence. In the fifth scenario, different biometric traits are used to obtain evidence. 45

2.5 The multi-algorithm fingerprint matcher designed by Ross et al., 2003. The system utilizes both minutiae and texture information to represent and match two fingerprint images (query and template). The minutiae matching module provides the transformation parameters necessary to align the query image with the template before extracting the texture information from the former. The texture information is represented using ridge feature maps. 47

2.6 The scenario envisioned by Beattie et al., 2005 in which biometric sensors are installed at various locations within a building that is partitioned into various zones. The authentication decision rendered at a particular location for a specific user, is a function of the decisions generated at other locations previously visited by the same user. Thus, there is an integration of evidence across space and time. Moreover, the fusion rule employed at a particular site can vary depending upon the security level of the associated zone. For example, in the above illustration, a user entering site **B** has to be verified using two biometric sensors whose decisions may be combined using the AND decision rule. 50

2.7 In the cascade (or serial) mode of operation, evidence is incrementally processed in order to establish identity. This scheme is also known as sequential pattern recognition. It enhances user convenience while reducing the average processing time since a decision can be made without having to acquire all the biometric traits. 53

2.8 In the parallel mode of operation, the evidence acquired from multiple sources is simultaneously processed in order to establish identity. Note that the evidence pertaining to the multiple sources may be acquired in a sequential fashion. 54

2.9 The cascade mode of processing permits database indexing where one modality can be used to retrieve a subset of identities while the second modality determines the best match. In this example, the face system is employed to recover the top $n$ matches while the fingerprint system decides the identity of the user based on the $n$ retrieved matches. 54

2.10 Fusion can be accomplished at various levels in a biometric system. Most multibiometric systems fuse information at the match score level or the decision level. More recently researchers have begun to fuse information at the sensor and feature levels. In biometric systems operating in the identification mode, fusion can be done at the rank level (not shown here). FE: feature extraction module; MM: matching module; DM: decision-making module; FM: fusion module. 56

3.1 The amount of information available for fusion gets compressed as one progresses along the various processing modules of a biometric system. The raw data represents the richest source of information, while the final decision (in a verification scenario) contains just a single bit of information. However, the raw data is corrupted by noise and may have large intra-class variability which is expected to be reduced in the subsequent modules of the system. 60

3.2 Constructing a fingerprint mosaic from multiple dab prints using the technique proposed by Jain and Ross, 2002a. (a) and (b) are dab impressions obtained after image segmentation and histogram normalization. The result of mosaicing is shown in (c). The minutiae points extracted from the composite print can be seen in (d). Typically, a larger number of minutiae and more ridge details are available in the composite print (compared to individual dab prints) thus enhancing the accuracy of a fingerprint matcher. 62

3.3 Constructing a 3D face texture by combining the evidence presented by a 2D texture image and a 3D range image. (a) The 2D face texture of a person. (b) The corresponding 3D range (depth) image. (c) The 3D surface after mapping the 2D texture information from (a). (d) The local texture information available in the triangular meshes along with the high curvature points that define the shape of the face can be used for comparing two such face surfaces. 64

3.4 A template update procedure may be viewed as a feature fusion scheme. In this example, the nine-dimensional feature set of a user ('Feature Set 1') is updated based on the evidence presented by the current feature set ('Feature Set 2'), via the averaging scheme. 65

3.5 The procedure adopted by Ross and Govindarajan, 2005 to perform feature level fusion. 70

3.6 The flow of information when data from the feature level and match score level are combined in a multibiometric system ( Ross and Govindarajan, 2005). 71

3.7 An illustration of rank level fusion as performed by the highest rank method, Borda count and logistic regression. In this example, the three schemes assign different consensus ranks to the individual identities. 73

3.8 Flow of information when decisions provided by multiple biometric matchers are combined using the majority vote fusion scheme. Here "ID" and "Ver" represent the identification and verification modes of operation, respectively. For the verification mode, the claimed identity is Bob. 76

4.1 Flow of information in a match score level fusion scheme. In this example, the match scores have been combined using the sum of scores fusion rule after min-max normalization of each matcher's output. Note that the match scores generated by the face and fingerprint matchers are similarity measures. The range of match scores is assumed to be $[-1, +1]$ and $[0, 100]$ for the face and fingerprint matchers, respectively. 92

4.2 Histograms of match scores and the corresponding Gaussian density estimates for the Face-G matcher in the NIST BSSR1 database. (a) Genuine and (b) Impostor. Note that the Gaussian density does not account well for the tail in the genuine score distribution and the multiple modes in the impostor score distribution. 101

4.3 Histograms of match scores and corresponding generalized density estimates for MSU-Multimodal database. First Row: Histograms of match scores for face modality (a) genuine and (b) impostor. Second Row: Histograms of match scores for fingerprint modality (c) genuine and (d) impostor. Third Row: Histograms of match scores for hand geometry modality (e) genuine and (f) impostor. The solid line is the estimated density using the kernel density estimator, and the spikes in (d) and (e) correspond to the detected discrete components. Note that no score normalization needs to be performed before density estimation. 107

4.4 Performance of product and copula fusion on the MSU-Multimodal database based on (a) continuous and (b) generalized density estimates. 112

4.5 Performance of product and copula fusion on the NIST BSSR1 database. 113

4.6 Double sigmoid normalization with $\tau = 200$, $\alpha_1 = 20$, and $\alpha_2 = 30$. 117

4.7 Hampel influence function with $a = 0.7$, $b = 0.85$, and $c = 0.95$.118

4.8 ROC curves for the individual modalities in the MSU-Multimodal database. 120

4.9 ROC curves for sum of scores fusion method under different normalization schemes on the MSU-Multimodal database. 122

4.10 Robustness analysis of min-max normalization. Note that TrueMax represents the maximum fingerprint match score in the training set. The different ROC curves are obtained by replacing the maximum fingerprint score in the training set with an outlier score whose value is 75%, 125%, 150%, 175% or 200% of TrueMax. 123

4.11 Robustness analysis of z-score normalization. Note that TrueStd represents the standard deviation of the fingerprint match scores in the training set. The different ROC curves are obtained by introducing outlier scores in the training set so that the standard deviation of the fingerprint match scores is changed to 75%, 125%, 150%, 175% or 200% of TrueStd. 125

4.12 Robustness analysis of tanh normalization. Note that TrueStd represents the standard deviation of the fingerprint match scores in the training set. The different ROC curves are obtained by introducing outlier scores in the training set so that the standard deviation of the fingerprint match scores is changed to 75%, 125%, 150%, 175% or 200% of TrueStd. 126

4.13 Example of a linear decision boundary learned by a classifier in a 2-dimensional ($R = 2$) feature space. During verification, any match score vector that falls in the region marked as 'Genuine' (to the right of the decision boundary) is classified as "genuine user". On the other hand, any match score vector that falls in the region marked as 'Impostor' (to the left of the decision boundary) is classified as "impostor". 127

4.14 Comparison of recognition performance of the classifier combination rules proposed by Kittler et al., 1998 on the NIST BSSR1 database. In this experiment, the match scores are converted into probabilities using a non-parametric density estimation technique. 130

4.15 ROC curves for sum of scores fusion method under different normalization schemes on NIST BSSR1 dataset. 131

4.16 Comparison of recognition performance of the density-based, transformation-based and classifier-based score fusion approaches on the NIST BSSR1 database. 132

4.17 The impostor distributions of the face biometric of three different users. (a), (c) and (e) are the histograms of impostor scores associated with the three users. (b), (d) and (f) are the corresponding cumulative histograms. For $\gamma = 0.3$, it is observed that the thresholds for each of the three users are different. 135

4.18 ROC curves exhibiting performance improvement when user-specific thresholds are utilized to verify a claimed identity. (a) Fingerprint and (b) Face. 136

4.19 ROC curves when using (a) equal weights for the three traits and a user-specific matching threshold; and (b) user-specific weights for all the three traits and a common matching threshold (Jain and Ross, 2002b). 138

4.20 Examples of users with varying weights for the different modalities. (a) and (b) Fingerprint images of user number 4 whose ridge details are not very clear ($w_1$ = 0.2). (c), (d) and (e) Varying face poses of user number 3 ($w_2$ = 0.1). (f) and (g) Incorrect placement of hand and the curved finger of user number 2 ($w_3$ = 0.2). 140

5.1 Minutiae extraction results for fingerprint images of varying quality. (a) A good quality fingerprint image. (b) A noisy fingerprint image (due to smearing, residual deposits, etc.). (c) Minutia points detected in the good quality fingerprint image by an automatic minutiae extraction algorithm (Jain et al., 1997a). (d) Minutia points detected in the noisy fingerprint image by the same automatic minutiae extraction algorithm (Jain et al., 1997a). The circles represent true minutia points while the squares represent false (spurious) minutiae. Note that the classification of minutia points into true and false minutiae is performed by a human expert. While no spurious minutia is detected in the good quality fingerprint image, several false minutia points are detected when the fingerprint image quality is poor. 145

5.2 Improvement in the performance of a minutiae-based fingerprint matcher when poor quality fingerprint images are successively pruned from the database. 146

5.3 Feature extraction results for iris images of varying quality. (a) A good quality iris image. (b) A poor quality iris image (due to occlusion, motion blur and non-uniform illumination). (c) Normalized iris pattern of the good quality iris image extracted using the algorithm proposed by Daugman, 1999. (d) Normalized iris pattern of the poor quality iris image extracted using the algorithm proposed by Daugman, 1999. The iris pattern shown in (c) contains rich texture information. On the other hand, the left side of the iris pattern in (d) is occluded by the upper eyelid and the right side of the pattern is blurred. 147

5.4 Performance of a iris matcher on iris images of varying quality. 148

5.5 A fingerprint image showing two regions where the ridges have a fixed dominant orientation, and the core and delta regions where the orientation of the ridge changes abruptly. 149

5.6 Computation of the global quality index of a fingerprint image in the frequency domain. (a) A good quality fingerprint image. (b) A poor quality fingerprint image. (c) Power spectrum of the good quality fingerprint image showing a distinct dominant frequency band. (d) Power spectrum of the poor quality fingerprint image. (e) Energy distribution of the good quality fingerprint image across concentric rings in the spatial frequency domain. (f) Energy distribution of the poor quality fingerprint image. It can be observed that the energy distribution is more peaked for the good quality fingerprint image. The resulting global quality measures for the fingerprint images in (a) and (b) are 0.92 and 0.05, respectively. 152

5.7 Poor quality of iris images caused by (a) occlusion, (b) poor focus and eye motion, (c) non-uniform illumination, and (d) large pupil area. 153

5.8 Quality estimation for two iris images. (a) and (b) Detected iris boundaries and eyelids. (c) and (d) Extracted iris patterns after eyelash removal. (e) and (f) Local quality measures based on the energy concentration in the individual windows. The quality score for the good quality iris image on the left is 0.89, while the quality score for the poor quality iris image on the right is 0.58. 155

5.9 DET plot demonstrating the improvement in the verification performance due to the quality-weighted sum rule. 160

5.10 A scenario where the primary biometric identifier (face) and the soft biometric attributes (gender, ethnicity, eye color and height) are automatically extracted and utilized to verify a person's identity. 160

5.11 A sample FBI fingerprint card (`http://www.highered.nysed.gov/tcert/ospra/samplefpcard.html`). Information on the gender, ethnicity, height, weight, eye color and hair color of the person is included in the encircled region. 161

5.12 Examples of soft biometric traits. 164

5.13 Framework for fusion of primary and soft biometric information. Here $x$ is the primary (fingerprint) feature vector and $y$ is the soft biometric feature vector. 167

5.14 Improvement in the performance of a multimodal (face and fingerprint) system after addition of soft biometric traits. (a) Identification and (b) Verification mode. 171

A.1 ROC curves of the multimodal (face and fingerprint) biometric system for the $1,000$ virtual user sets randomly created by Indovina et al., 2003. The variation in matching performance among these virtual user sets is not significant which seems to validate the use of virtual users. 175

# List of Tables

1.1 Authentication solutions employing biometrics can be used in a variety of applications which depend on reliable user authentication mechanisms. 17

1.2 The false accept and false reject error rates associated with the fingerprint, face, voice and iris modalities. The accuracy estimates of biometric systems depend on a number of test conditions including the sensor employed, acquisition protocol used, subject disposition, number of subjects, number of biometric samples per subject, demographic profile of test subjects, subject habituation, time lapse between data acquisition, etc. 27

3.1 A sample behavior knowledge space lookup table. Here, two face recognition algorithms are used for identifying three users. 100 face images from each user are used for constructing the BKS lookup table. 82

3.2 Examples of multi-sensor systems. 84

3.3 Examples of multi-algorithm systems. 85

3.4 Examples of multi-sample and multi-instance systems. 87

3.5 Examples of multimodal systems. 88

4.1 Summary of score normalization techniques. 119

4.2 Genuine Accept Rate (GAR) (%) of different normalization and fusion techniques at the 0.1% False Accept Rate (FAR) for the MSU-Multimodal database. At 0.1% FAR, the GAR of the unimodal systems are 83.6%, 67.7% and 46.8% for the fingerprint, face and hand geometry modalities, respectively. Note that the values in the table represent average GAR, and the values indicated in parentheses correspond to the standard deviation of GAR computed over the 40 trials of randomly splitting the available data into training and test sets. 121

4.3 User-specific thresholds for the biometric traits of 10 users at a FAR of 1%. 134

4.4 Weights of different biometric modalities for 10 users (Jain and Ross, 2002b). 139

# Preface

The pronounced need for reliably determining or verifying the identity of a person has spurred active research in the field of biometric authentication. Biometric authentication, or simply biometrics, is the science of establishing an identity based on the physical or behavioral attributes of an individual, including fingerprint, face, voice, gait, iris, signature, hand geometry and ear. It is becoming increasingly apparent that a single biometric trait (used in a unibiometric system) is not sufficient to meet a number of system requirements - including matching performance - imposed by several large-scale authentication applications. Multibiometric systems seek to alleviate some of the drawbacks encountered by unibiometric systems by consolidating the evidence presented by multiple biometric sources. These systems can significantly improve the recognition performance of a biometric system besides improving population coverage, deterring spoof attacks, and reducing the failure-to-enroll rate. Although the storage requirements, processing time and the computational demands of a multibiometric system can be significantly higher (than a unibiometric system), the above mentioned advantages present a compelling case for deploying multibiometric systems in large-scale authentication systems (e.g., border crossing) and systems requiring very high accuracies (e.g., access to a secure military base).

The field of multibiometrics has made rapid advances over the past few years. These developments have been fueled in part by recent government mandates stipulating the use of biometrics for delivering crucial societal functions. The US-VISIT program (United States Visitor and Immigration Status Indicator Technology) is a border security system that validates the travel documents of foreign visitors to the United States. Currently, fingerprint images of left- and right-index fingers of a person are being used to associate a visa with an individual entering the United States; in the future, all ten fingers may be used thereby necessitating the development of efficient data capture as well as fusion algorithms. The International Civil Aviation Organization (ICAO) has unanimously recommended that its member States use Machine Readable Travel Documents (MRTDs) that incorporate at least the face biometric (some combination of face, fingerprint and iris can also be used) for purposes of establishing the identity of a passport holder. Thus, research in multibiometrics has the potential to impact several large-scale civilian and commercial applications.

From an academic perspective, research in multibiometrics has several different facets: identifying the sources of multiple biometric information; determining the type of information to be fused; designing optimal fusion methodologies; evaluating and comparing different fusion methodologies; and building robust multimodal interfaces that facilitate the efficient acquisition of multibiometric data. One of the goals of this book is to lend structure to the amorphous body of research work that has been conducted in the field of multibiometrics. To this end, we have attempted to assemble a framework that can be effectively used to understand the issues and progress being made in multibiometrics while identifying the challenges and potential research directions in this field.

The book is organized as follows. Chapter 2 introduces the notion of information fusion in the context of biometrics and enumerates the advantages imparted by multibiometric systems. The various sources of biometric information that can be integrated in a multibiometric framework, such as multiple sensors, multiple algorithms and multiple samples, are then discussed with examples from the literature. This chapter also examines different types of acquisition and processing schemes that are relevant to multibiometric systems. Finally, the types of information (also known as the levels of fusion) that can be accommodated in a fusion architecture are briefly visited. In Chapter 3, the sensor-level, feature-level, rank-level and decision-level fusion schemes are explored in detail along with examples highlighting the pros and cons of each fusion level. Integration strategies for each of these fusion levels are presented, both from the multibiometric as well as the multiple classifier system literature. The chapter concludes by categorizing some of the representative publications in multibiometrics on the basis of the sources of biometric information used and the level of fusion adopted. Chapter 4 is entirely dedicated to score-level fusion, since fusion at this level has been elaborately studied in the literature. The integration strategies pertinent to this level are presented under three distinct categories: (i) density-based score fusion, (ii) transformation-based score fusion, and (iii) classifier-based score fusion. This chapter discusses examples embodying each of these categories; a mathematical framework is adopted in order to assist the reader in understanding the differences between the three categories. The chapter concludes by indicating how the performance of a score fusion system can be further enhanced by utilizing user-specific parameters. In Chapter 5, the possibility of incorporating ancillary information, such as the quality of the biometric data and the soft biometrics of individuals, in a biometric fusion framework is discussed. Soft biometric traits include characteristics such as gender, height, weight, eye color, etc. that provide added information about an individual, but lack the distinctiveness and permanence to sufficiently differentiate between multiple individuals. The chapter presents an information fusion framework to include soft biometric traits in the authentication process. The final contribution of this book is an Appendix that lists some of the databases that have been used for evaluating the performance of various multibiometric algorithms.

We are grateful to a number of individuals who lent their generous support to this project. Julian Fierrez-Aguilar, Universidad Autonoma de Madrid, Patrick Flynn, University of Notre Dame, Lawrence Hornak, West Virginia University, Richard Lazarick, Computer Sciences Corporation, Norman Poh, IDIAP, Salil Prabhakar, Digital Persona, Inc., Choonwoo Ryu, INHA University, Marios Savvides, Carnegie Mellon University, Yunhong Wang, Beihang University and James Wayman, San Jose State University reviewed and provided valuable comments on preliminary drafts of this book. We had a number of useful discussions with Josef Bigun, Halmstad University, Sarat Dass, Michigan State University, Josef Kittler, University of Surrey, Sharath Pankanti, IBM T. J. Watson Research Center and David Zhang, Hong Kong Polytechnic University. Arun George, West Virginia University and Yi Chen, Michigan State University designed several of the illustrations in this book. Thanks to Samir Shah and Rohan Nadgir, West Virginia University and Umut Uludag, Michigan State University for proofreading the manuscript. We would also like to thank the Center for Identification Technology Research (CITeR), West Virginia University, the National Science Foundation (NSF) and the Department of Homeland Security (DHS) for supporting our research in multibiometrics.

This book has been written for researchers, engineers, students and biometric system integrators who are keen on exploring the fundamentals of multibiometrics. It can be used as a reference guide for a graduate course in biometrics. Some of the concepts presented in this book are applicable to the general domain of information fusion and, hence, students of this field will also benefit from the book. We hope that the concepts and ideas presented in the following pages will stimulate the reader's curiosity and help develop an appreciation for this rapidly evolving field, called Multibiometrics.

ARUN ROSS, MORGANTOWN, WV
KARTHIK NANDAKUMAR, EAST LANSING, MI
ANIL K. JAIN, EAST LANSING, MI