Preface

Biometric authentication refers to identifying an individual based on his or her distinguishing physiological and/or behavioral characteristics. It associates an individual with a previously determined identity based on that individual's appearance or behavior. Because many physiological or behavioral characteristics (biometric indicators) are distinctive to each person, biometric identifiers are inherently more reliable and more capable than knowledge-based (e.g., password) and token-based (e.g., a key) techniques in differentiating between an authorized person and a fraudulent impostor. For this reason, more and more organizations are looking to automated identity authentication systems to improve customer satisfaction, security, and operating efficiency as well as to save critical resources.

Biometric authentication is a challenging pattern recognition problem; it involves more than just template matching. The intrinsic nature of biometric data must be carefully studied, analyzed, and its properties taken into account in developing suitable representation and matching algorithms. The intrinsic variability of data with time and environmental conditions, the social acceptability and invasiveness of acquisition devices, and the facility with which the data can be counterfeited must be considered in the choice of a biometric indicator for a given application. In order to deploy a biometric authentication system, one must consider its reliability, accuracy, applicability, and efficiency. Eventually, it may be necessary to combine several biometric indicators (multimodal-biometrics) to cope with the drawbacks of the individual biometric indicators.

One of the most important aspects of a biometric authentication system is benchmarking. A biometric authentication system is likely to make some errors. Understanding the inherent limitations of a biometric system and evaluating competing systems are the most difficult, but necessary tasks. The reason is that, quite often, the test data used is not truly representative of the population and the operating environment; the performance evaluation tests only take a snapshot of all the possible behaviors of the system, ignoring the variability due to the differences in the population of all real users as well as the variability due to environment.

We hope that this workshop will help many people working in biometrics to attain a broader vision of the open problems and their solutions. A couple of papers at this workshop deal with the psychological aspects of biometrics, which is a rather unexplored aspect of this discipline. Even though the papers included in this volume do not cover all facets of this emerging and promising discipline and technology, we would be satisfied if this book led to some new insights in developing the next generation of biometric authentication systems.

April 2002

Massimo Tistarelli
Josef Bigun
Anil K. Jain

Program Committee Members

Massimo Tistarelli
Computer Vision Laboratory
DIST-Universtity of Genova, Italy

Josef Bigun
Department of Computer Science
Halmstad University, Sweden

Anil Jain
Computer Science and Engineering
Michigan State University, East Lansing, MI - USA

Bir Bhanu
University of California at Riverside, CA, USA

Roberto Brunelli
IRST, Trento, Italy

Jean-Christophe Fondeur
AFIS Technology – SAGEM, France

Robert Frisholtz
BioId – Dialog Communication Systems AG, Erlangen, Germany

Enrico Grosso
Computer Vision Laboratory
DIST-Universtity of Genova, Italy

Kenneth Jonsson
Fingerprint cards AB, Sweden

Helmut Kristen
Precise Biometrics AB, Lund, Sweden

Josef Kittler
Signal Processing Laboratory
University of Surrey, UK

Davide Maltoni
University of Bologna, Italy

K.V. Prasad
Ford Motor Company, Dearborn, MI (USA)