

Preface

This book would never have existed without the BioSecure Network of Excellence (NoE). This European project, launched in 2004 and that ended in 2007, was partly supported by the European Commission. It grouped 30 partners (all academic but one) from eight countries. Its main objective was to federate the biometric research conducted independently in different laboratories, as well as to give visibility to the European research in biometrics.

With the goal to continue to exploit the achievements of the BioSecure project, the “Association BioSecure” was created to handle the property rights and legal issues related to the distribution of biometric databases, as well as to assure the maintenance of the reference systems. The Association is also eager to organize further open evaluation campaigns in order to continue to exploit the biometric databases acquired during the BioSecure project.

When starting this project, it seemed obvious to us that one of the main obstacles to the progress of research in this domain was the lack of facilities for evaluation, considering the large number of modalities that can be encountered, without speaking of the emergence either of new modalities or of the interest in multimodality.

At that time the National Institute of Standards and Technologies (NIST) was conducting yearly speaker recognition evaluations, as well as the first face recognition competitions, putting databases, experimental protocols and baseline software at the disposal of researchers for comparative evaluations. The Fingerprint Verification Competitions (FVC) offered an independent evaluation for fingerprints every two years. But what about hand, iris, online handwritten signature or multimodality?

Our efforts were therefore focused on providing new evaluation tools for different modalities such as 2D and 3D face, iris, speaker, talking faces, hand, fingerprints, and online handwritten signature. Taking advantage of the multisite repartition of the Network, three large databases were gathered, including modalities recorded in different application conditions (mobility, access control and Internet communications). Open source reference systems were also produced for each modality, as well as assessment protocols for benchmarking.

During the First Residential Workshop organized in August 2005 within the BioSecure NoE¹, following the model of John's Hopkins University², we put the premises of the design of an evaluation framework, including publicly available databases, assessment protocols, and reference systems. They allowed a preliminary comparative evaluation of the algorithms developed by the BioSecure partners in their own laboratories.

During the 2005 Residential Workshop, the idea of this book was initialized, and it took us two more years to complete the drafted tasks, namely to complement and test the ten open source reference systems available at the companion URL site of this book³. In the meantime, the acquisition of the upper-mentioned databases was completed, and the BioSecure Multimodal Evaluation Campaign (BMEC'2007) took place in September 2007. Unfortunately, due to lack of time and data distribution obstacles, this evaluation was not open largely outside BioSecure.

Content This book is composed of eleven chapters. In Chap. 1, a short introduction about biometrics is provided. The proposed benchmarking methodology and its basic terminology are presented in Chap. 2. The next eight chapters (Chaps. 3–10), dedicated to iris, fingerprint, hand, online handwritten signature, speech, 2D and 3D face, and talking face modalities, follow a common structure. First, the state of the art and current issues and challenges are addressed. The existing databases and evaluation campaigns are next summarized. Then, the Biometric Evaluation Framework for the specific modality is introduced. Research systems are presented after, with experimental results according to the benchmarking protocols. Because for each modality all experiments presented follow the benchmarking protocol, the presented research results could be compared. Chapter 11 presents the experimental results from the mobile scenario of the BioSecure Multimodal Evaluation Campaign (BMEC'2007).

Intended audience This book, with its unique combination of state-of-the-art research on common benchmarking experimental protocols and practical evaluation tools, is intended for graduates, researchers and practitioners in the fields of Biometrics and Pattern Recognition.

Conclusions and Perspectives This book may not answer all the questions set forth in Chap. 1! At least some methodological suggestions are put forward to improve the performance and comparability of biometric systems:

- Open source reference software can be uploaded for a number of modalities.
- For each of the presented modalities, publicly available databases are used to define the benchmarking experimental protocols.
- The benchmarking results, obtained with the open source reference systems, benchmarking databases, and protocols are fully reproducible (How-to documents are also available on the companion URL.³)

¹ <http://www.biosecure.info>

² <http://www.clsp.jhu.edu/workshops/>

³ <http://share.int-evry.fr/svnview-eph/>

What is missing? What needs to be improved?

- Reference systems should be maintained and improved.
- Reference systems should be developed for emerging modalities, such as palm prints, hand vein, DNA, ear, teeth, etc. State-of-the-art classification and statistical modeling technique should be made compatible with the existing and new reference systems.
- Existing reference systems need to be improved and submitted to standardization organizations (such as ISO, CEN, W3C, etc.) to facilitate interoperability and comparability. A similar approach has proven quite successful for speech, audio and video coders. It should also be profitable for biometrics.
- More databases should be recorded in diverse conditions, with new sensors, over a long time span, with a huge number of subjects, etc.
- Evaluation protocols must be defined and published as soon as databases are available. Databases (and particularly multimodal data) should be made anonymous to protect privacy.
- Multimodal biometrics, revocability of biometric data, spoofing, privacy, and user acceptance are major issues that require further research and experimentation.
- Sequestered evaluation campaigns need to be organized regularly.

Acknowledgments

We would like first to thank all the authors of the different chapters for their hard work, cooperation, and for the time they spent to re-run their experiments with the benchmarking databases and protocols. Thanks are also due to several authors and members of the BioSecure Network who participated in the review process.

Special thanks to Aurélien Mayoue for his dedicated efforts to maintain, document, and test the reference systems.

The assistance of Danielle Paes de A. Camara for the $\text{\LaTeX}$ version is gratefully acknowledged.

Thanks to all the BioSecure partners and in particular to the participants to the BioSecure Residential Workshop and to the BMEC'2007 Evaluation Campaign.

Dijana Petrovska-Delacrétaz, Institut TELECOM, TELECOM SudParis
Gérard Chollet, Institut TELECOM, TELECOM ParisTech
Bernadette Dorizzi, Institut TELECOM, TELECOM SudParis
August 2008

<http://www.springer.com/978-1-84800-291-3>

Guide to Biometric Reference Systems and
Performance Evaluation

Petrovska-Delacrétaz, D.; Chollet, G.; Dorizzi, B. (Eds.)

2009, XXX, 382 p. 146 illus., 15 illus. in color.,

Hardcover

ISBN: 978-1-84800-291-3