Preface

In the last decade biometrics has emerged as a valuable means to automatically recognize people, on the base is of their either physiological or behavioral characteristics, due to several inherent advantages they offer over conventional methods. In fact biometrics-based recognition relies on who a person is or what a person does in contrast with traditional authentication approaches, based on what a person knows, e.g. a password, or what a person has, e.g., ID card, token, etc. Therefore, biometrics-based recognition systems, being based on personal traits, either biological or behavioral, it is much harder for biometric data to be lost, forgotten, stolen, copied or forged than traditional identifiers. The recent technological developments have made possible the deployment of biometrics-based systems deploying mature biometrics, like face, iris, and fingerprints, in a wide range of applications ranging from criminal investigation to civilian registration, border control, national identity document verification, e-commerce, e-banking, on-line payment, physical and logical access control.

In the design of a biometrics-based authentication system, different issues, strictly related to the specific application under analysis, must be taken into account. As established in literature, from an ideal point of view, biometrics should be universal, unique, permanent, collectable, and acceptable. Moreover, besides the choice of the biometrics to employ, many other issues must be considered in the design stage. Specifically, the system accuracy, the computational speed and cost are also important design parameter, especially for those systems intended for large populations.

Biometrics-based people recognition poses new challenges related to personal data protection, not raised by traditional recognition methods. If biometric data are captured or stolen by an attacker, they may be replicated and misused. Users' biometrics cannot be changed if compromised, different from a PIN or a password which can be reissued if needed. Moreover, the use of biometrics poses additional privacy concerns since biometric data may reveal sensitive information about a person's personality and health, which can be stored, processed, and distributed without the users' authorization. This information can be used to discriminate against people for instance by denying insurance to people with latent health problems. Moreover

the uniqueness of biometrics across individuals allows cross-matching to biometric databases thus performing unauthorized tracking of the subjects' activities. Also, in a scenario where either governmental agencies or private companies can collect huge databases of citizens' biometrics, some risks for the person's privacy and human dignity could be foreseen. In fact, in the aforementioned scenario, *function creep*, that is a situation where the data, collected for some specific purposes, are used for different ones, is likely to happen in the long run. All this would lead to users' privacy loss.

Therefore the need to protect both privacy and security from a procedural, legal, and a technological point of view arises. This book examines the up to date solutions for protecting both security and privacy in a holistic way tackling also ethical, legal, and procedural aspects. Specifically, this book deals with both theoretical and practical implementations of secure and privacy compliant solutions to the problem of automatic people recognition. It focuses on new approaches and new architectures for unimodal and multimodal template protection, signal processing techniques in the encrypted domain, security and privacy leakage assessment, and standardization aspects. Some practical applications of secure and privacy compliant systems are also presented with specific focus on biometrics-based electronic documents, face and fingerprint based automatic user recognition, and biometric systems employing smart cards for enhancing security and privacy. Moreover, the ethical implications of a spread use of biometrics in everyday life and its effect on human dignity are addressed. Best practices for the processing of biometric data are indicated and a legal framework is eventually given.

The book is organized as follows. In Chap. 1 a general introduction to both the privacy and security issues affecting biometric systems are given along with some state of the art mitigation approaches. Chapter 2 introduces the main security requirements for the biometric processing pipeline and summarizes general design principles and approaches. General security principles in information technology and selected paradigms such as template protection by biometric hashing and biometric cryptosystems are reviewed. Moreover a brief introduction on the design principles of biometric matching algorithms operating in the encrypted domain is given. In Chap. 3 the limitations of public key infrastructure (PKI) for key management are pointed out and a novel paradigm making use of biometrics for mitigating the PKI related trust problems at both the user and certificate authority level is proposed. An innovative infrastructure, namely biocryptographic key infrastructure (BKI), able to guarantee a high level of privacy while establishing trust, is thus proposed. Chapter 4 deals with the issue of biometric template protection and a categorization of the state of the art approaches is given. A theoretical analysis is provided and practical implementations for real world biometrics are discussed. In Chap. 5, privacy and secrecy aspects of biometric key-binding systems are analyzed within an information theoretic framework. Specifically, the fundamental trade-off between secret-key rate and privacy-leakage rate is determined for independent and identically distributed Gaussian biometric sources. The effect of code selection and binary quantization in the fuzzy commitment cryptographic protocol is also reported. In Chap. 6 the issue of template protection for multi-biometric systems is

addressed. Specifically, a multi-biometric cryptosystem based on the fuzzy commitment scheme, in which a crypto-biometric key is derived from multi-biometric data is presented. The scheme, in principle applicable to different modalities, is detailed for a multi-unit system based on the use of two-irises and for a multi-modal system using a combination of iris and face. It is shown that in addition to generation of strong keys, the proposed systems address the issues of revocability, template diversity, and protection of user's privacy. In Chap. 7 some approaches to process the biometric data in encrypted form stemming from the "Secure Two Party Computation" theory are described. Specifically, homomorphic encryption and garbled circuits are discussed and the ways such techniques can be used to develop a full biometric matching protocol are detailed. The significant advantage of the illustrated techniques is that any risk that private biometric information is leaked during an identification process is eliminated whereas they surely require a better efficiency to be deployed in real life applications. Chapter 8 deals with a practical application of template protection techniques to recognition systems relying on fingerprints. Specifically, practical challenges related to the use of fingerprints, like the need of registration without any information leakage about the deployed features, and the extraction of highly characterizing yet stable features are addressed. An analysis of how the design choices affect the trade-off between the security and matching accuracy is also provided. In Chap. 9 biometric cryptosystems are used as a Privacy-Enhancing Technology in a face biometrics-based watch list scenario that has been successfully employed in the Ontario Lottery and Gaming Corporation's self-exclusion program. The proposed architecture treats the biometric cryptosystem module as an important component in a multi-layered approach to privacy and security of the overall system. Chapter 10 shows how smart card technology can be beneficial to biometric systems. Special emphasis is given to the security mechanisms included in most smart cards and how these mechanisms can be employed to protect biometric data and processes. Different architectures for the integration of biometrics and smart cards are presented and two major deployments making joint use of smart cards and biometrics, specifically the ePassports and the Electronic Spanish National ID Card, are described. In Chap. 11, two secure and privacy compliant systems, one devoted to local access control and the other one to remote identification, to be deployed in real life applications are described. A synergic use of biometric cryptosystems, match on card, and advanced cryptographic protocols is made in order to guarantee security, performance, and accuracy. Chapter 12 discusses biometric data protection from the standardization perspective. It covers technical standards developed at ISO (e.g., SC27, SC37, and TC68) and at other standards development organizations as well as technical reports developed by these groups. In addition to those that address the confidentiality and integrity of biometric/identity data directly, other standards covering security of biometric systems in general are discussed. Chapter 13 considers the impact on and ethical implications for society of widening biometric applications to daily life. Moreover it explores the contradictions between the claims that biometrics will boost security and prevent identity theft, and the growing evidence of increased, with introduction of more biometric documents, e-crime that threatens personal identity and security,

and collective security in the cyber space and in the personal life. Chapter 14 discusses best practices which can be put in place for the processing of biometric data, taking privacy and data protection into account, particularly for the private sector. More specifically, it is pointed out that the revocability, irreversibility, and unlinkability of biometric identities, obtained by specific methods and technologies, are essential for the use of biometric data in the private sector from a privacy and data protection point of view. In Chap. 15 a comprehensive analysis of the legal principles governing personal data are given and the European data protection framework for biometrics is detailed. A deep understanding of the privacy and data protection challenges brought by the use of biometric data is gained. The impact of the choices like the use of different system architectures, voluntary or compulsory enrolment, raw data or templates, and the use of different kinds of biometrics is analyzed in a holistic way from the legal perspective and eventually some recommendations are given. In Chap. 16, based on two cases of biometric application, which have been assessed by the Danish Data Protecting Agency, a set of recommendations is presented to legislators, regulators, corporations, and individuals on the appropriate use of biometric technologies put forward by the Danish Board of Technology. The recommendations are discussed and compared to the similar proposal put forward by the European Article 29 Data Protection Working Party.

June 2013 Patrizio Campisi

http://www.springer.com/978-1-4471-5229-3

Security and Privacy in Biometrics
Campisi, P. (Ed.)
2013, X, 438 p., Hardcover
ISBN: 978-1-4471-5229-3