Patrizio Campisi *Editor*

Security and Privacy in Biometrics

Springer

Security and Privacy in Biometrics

Patrizio Campisi
Editor

Security and Privacy in Biometrics

Springer

Editor
Patrizio Campisi
Section of Applied Electronics
Department of Engineering
University of Roma Tre
Rome, Italy

ISBN 978-1-4471-5229-3 ISBN 978-1-4471-5230-9 (eBook)
DOI 10.1007/978-1-4471-5230-9
Springer London Heidelberg New York Dordrecht

Library of Congress Control Number: 2013942399

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

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

Contents

Chapter 1
Security and Privacy in Biometrics: Towards a Holistic Approach

Patrizio Campisi

Abstract Security and privacy in biometric systems have been traditionally seen as two requirements hindering each other. Only in the recent past researchers have started investigating it as a joint optimization problem which needs to be tackled from both a legal, procedural, and a technological point of view. Therefore in this chapter we take a holistic approach and we introduce some basics about the privacy and the security issues which can affect a biometric system and some possible mitigation approaches, both procedural and technological, that can help in designing secure and privacy compliant biometric based recognition systems.

1.1 Foreword

In the last few years biometric technologies have been employed for automatic people recognition at an increasing rate due to several inherent advantages they offer over conventional methods. In fact biometrics-based recognition systems rely on who a person is or what a person does, in contrast with traditional authentication approaches, based on what a person knows (password) or what a person has (e.g., ID card, token). Being based on personal, either physiological or behavioral traits, it is much harder for biometric data to be lost, forgotten, stolen, copied or forged than traditional identifiers. Loosely speaking, biometric systems are essentially pattern-recognition-based systems, performing verification or identification using features derived from either physiological biometric data like fingerprint, face, iris, retina, hand geometry, thermogram, vein patterns, ear shape, body odor, or behavioral traits like voice, signature, handwriting, key stroke, gait, to cite a few.

In the design of a biometrics-based recognition system, different issues, strictly related to the specific application under analysis, must be taken into account. As well established in literature, from an ideal point of view, the employed biometrics should be universal, unique, permanent, collectable, robust to attacks, and acceptable. Moreover, besides the choice of the biometrics to employ, other issues must

P. Campisi (✉)
Section of Applied Electronics, Department of Engineering, University of Roma Tre, Via Vito Volterra 62, 00146 Rome, Italy
e-mail: patrizio.campisi@uniroma3.it

P. Campisi (ed.), *Security and Privacy in Biometrics*,
DOI 10.1007/978-1-4471-5230-9_1,

be considered in the design stage. Specifically, the system accuracy, the computational speed, the cost of the systems and its maintenance are also important design parameters, especially for those systems intended for large populations.

Besides all the aforementioned requirements, the use of biometric data raises many security issues which are peculiar of biometrics-based recognition systems not affecting other approaches employed for automatic people recognition. In fact, some biometrics such as voice, face, fingerprints, and many others are exposed traits, they are not secret and therefore they can be covertly acquired or stolen by an attacker and misused. This can lead for example to identity theft. Moreover, raw biometrics cannot be revoked, canceled, or reissued if compromised, since they are user's intrinsic characteristics and they are in limited number. Therefore, if a biometrics is compromised, all the applications making use of that biometrics are compromised, and since biometric identifiers are permanent an issue is raised when it is needed to change them. The use of biometrics poses also many privacy concerns, in fact, when an individual gives out his biometrics, either willingly or unwillingly, he discloses unique information about himself. It has also been demonstrated that biometric data can contain relevant information regarding people health. This information can be used, for example, to discriminate people for hiring or to deny insurance to those with latent health problems. The use of biometrics can also raise cultural, religious as well as ethnicity related concerns. To some extent, the loss of anonymity can be directly perceived by users as a loss of autonomy.

Therefore the need to protect both privacy and security from both a legal, procedural, and a technological point of view arises.

In the following we provide some basic notions about the privacy and security issues which can affect a biometric system and the possible mitigation approaches that can help in designing secure and privacy compliant biometrics-based recognition systems. Specifically the privacy and security issues affecting a biometric system are introduced in Sects. 1.2 and 1.3 respectively, whereas the relationship between privacy and security within the biometric scenario is briefly addressed in Sect. 1.4. An historical perspective of the privacy enhancing technologies is given in Sect. 1.5. The major international projects related to privacy and security are briefly sketched in Sect. 1.6. Eventually, some possible research directions are highlighted in Sect. 1.7.

1.2 Privacy in Biometric Systems

In this Section the different connotations of the term "privacy" are illustrated as long as with some basic principles and procedures that can provide directions towards the development of privacy compliant applications. Moreover the specific privacy risks related to the use of biometric data are illustrated.

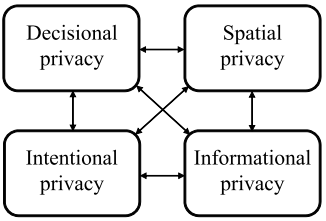

Fig. 1.1 Privacy connotations

1.2.1 Privacy Conceptualization

The word privacy is a general term which encompasses both different areas of study and real life situations. It is commonly accepted [1, 2] that the general term privacy can assume slightly different connotations as depicted in Fig. 1.1 and specified in the following. In detail, we talk about:

- *decisional privacy* when we refer to the right of the individual to make decisions regarding his life without any undue interference;
- *spatial privacy* when we refer to the right of the individual to have his own personal physical spaces which cannot be violated without his explicit consent;
- *intentional privacy* when we refer to the right of the individual to forbid/prevent further communication of observable events (e.g., conversations held in public) or exposed features (e.g., publishing photos);
- *informational privacy* when we refer to the right of the individual to limit access to personal information which represents any information that could be used in any way to identify an individual. It is worth pointing out that some data which do not appear to be personal information could be used in the future to identify an individual.

Of course there are no clear boundaries among the given connotations as sketched in Fig. 1.1. According to the application, a particular privacy conceptualization may be chosen as prevalent, the other aspects still being worth of consideration in the privacy assessment. However, because of the dramatic advances of information technology in the last decades, informational privacy has gained a predominant role within the considered scenario.

1.2.2 Fair Information Practices

In 1980, a formalization of the guidelines governing the protection of privacy and transnational flow of personal data, which represents a milestone for privacy, was introduced by the Organisation for Economic Co-operation and Development (OECD) in [3]. The OECD privacy guideline relies on a set of eight principles, often referred to as Fair Information Practices, namely:

- *Purpose specification principle*: the purpose for which the data are collected should be specified when the data are collected. Moreover, the data usage should be limited to the fulfillment of the specified purposes and should not be changed.
- *Openness principle*: the objectives of research, the main purposes of the use of personal data and the policies and practices related to their protection, and the identity of the data controller should be open to the public.
- *Collection limitation principle*: the collection of personal data should be obtained by lawful and fair means and, whenever applicable, with the knowledge and consent of the individual.
- *Data quality principle*: personal data should be relevant, accurate, complete, and up to date for the intended purposes.
- *Accountability principle*: a data controller should be accountable for complying with measures which give effect to the stated principles.
- *Use limitation principle*: personal data should be not be made available for other purposes than the ones agreed with the individual in the Purpose Specification Principle except with the consent of the data subject or by the authority of the law.
- *Individual participation principle*: the individual should have the right to:
  - know from the data controller if some data regarding him are stored;
  - to have communicated to him, if there are data relating to him, within a reasonable time, at a charge, if any, that is not excessive, in a reasonable manner, and in a form that it is intelligible to him;
  - to be given reasons if a request made under this principle is denied, and to be able to challenge such denial;
  - to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.
- *Security safeguards principle*: personal data should be protected against security risks like unauthorized disclosure, use, modification, destruction, and loss.

These are the basic principles which need to be translated into procedures and legislation to prevent violations of privacy.

1.2.3 Privacy Compliance Lifecycle

A privacy compliance lifecycle [4] is aimed at integrating privacy protection into systems which collect, process, or produce personal information. It has to be performed at the earliest stages of the system design in order to embed into the system the answers to the privacy concerns which have been identified and to limit the potential costs resulting from negligent information management. It is worth pointing out that the privacy compliance assessment must be continuously carried out throughout the life of the system.

An example of privacy compliance assessment procedure is sketched in Fig. 1.2 and it comprises the following steps:

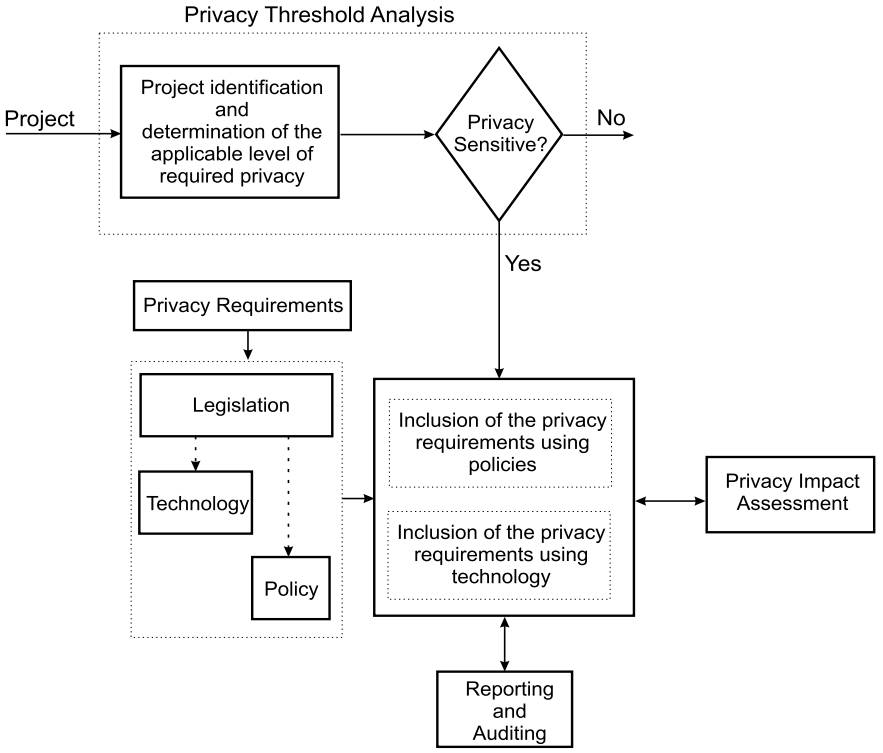

Fig. 1.2 Privacy compliance lifecycle: an example

- Project identification and determination of the applicable level of required privacy. This analysis aims at identifying privacy sensitive applications and for the identified projects further steps, described in the following, need to be performed.
- Inclusion of the privacy requirements in the design and development of the system. In this step, legislation, procedural approaches, and technology concur together in order to embed the identified privacy requirements into the system design.
- The privacy impact assessment is a bidirectional process which is intended to identify and overcome both procedural and technological issues arisen from the inclusion of privacy requirements in the system using both procedural and technological means. In fact the privacy assessment should verify that the system purposes declared by the authority in control of the system are complaint with the actual system. Moreover, the data must be used appropriately, that is, their use should allow achieving the stated purpose of the data collection, and not more. If there is a shift between the declared use and the actual use of the system, a privacy risk is occurring. The privacy assessment should also include an analysis of the control a user has on the way his data are used, if the data are used for the original purpose they were intended for, and if not, if there is an informed user's

agreement. The individual should have the authority to get access to his data and to check if the data are used according to the user's expectations.
- Production of reports on the status of the privacy compliance analysis to be deployment to the proper entities which might include also public deployment.
- Audit procedures to be periodically run to reveal any unauthorized use of both the data and the system.

1.2.4 Privacy vs. Biometrics

Privacy compliance analysis of an automatic biometrics-based recognition system is a key issue both during the system design process and for its deployment in real life applications. Within this respect, both the perception by the user of the potential threats and the real risks to privacy have to be carefully considered when designing a biometric system.

In the following, the main concerns related to the use of biometrics are described.

- Biometrics can be collected or shared without specific user's permission, adequate knowledge, or without specific purpose.
- Biometrics, which has been collected for some specific purposes, can be later used for another unintended or unauthorized purpose. This is known as "function creep", and it can have dramatic consequence since it leads to the loss of the public trust in a given system.
- Biometrics can be used for purposes other than the officially declared purpose or biometrics can be misused to generate extra information.
- Biometrics can be copied or removed from the user and used for secondary purposes.
- Biometrics use can violate the "principle of proportionality" [5], which states that biometric data may only be used if adequate, relevant and not excessive with respect to the system's goal. If this principle is violated, the users may feel that the benefit coming from revealing their biometrics is much less than what they get in exchange.
- Biometrics can be used to reveal gender and ethnicity. Moreover, details on the medical history of the individual can be elicited. Medical conditions can be deduced by comparing biometrics acquired at the time of the enrollment and biometrics acquired later for recognition. Moreover, biometrics can give directly information on health conditions [6]. As a consequence, biometrics can be used to profile people according to their health status.
- Biometrics can be used to pinpoint or track individuals. Since biometric data are considered unique, they have the potential to locate and track people physically as they try to access some facilities or their biometric traits are recorded by some surveillance system. Also associating people's biometrics to their identifiers, such as name, address, passport number, can represent a risk, being then possible to access, gather, and compare a wide range of information starting from a single biometric trait. Moreover the use of biometrics as a universal identifier can allow

user tracking across different databases. All this can lead to covert surveillance, profiling, and social control.
- Biometric use can be associated by the individual to forensic purposes. Therefore the use of biometric traits, such as fingerprints, which are associated, for historical reasons, to criminal investigations and forensic activities, can have a low acceptability rate.
- Biometrics can be improperly stored and/or transmitted. This would expose biometrics to external attacks. Moreover biometrics may also be exposed to administrator or operator abuses, since they could misuse their privileges for accessing a biometric database.

It is worth pointing out that the evaluation of the "real" risk of privacy invasiveness must be performed considering both the final application and the employed biometric trait. For example biometric overt applications are less privacy-invasive than covert ones. Mandatory biometrics-based recognition systems bear more privacy risks than optional ones. Privacy is considered to be more at risk when physiological data are used since they are more stable in time and allow a higher accuracy than behavioral biometrics. If the biometrics-based recognition system is used in the verification mode, less privacy concerns are implied than those involved in a system operating in the identification mode. This is due to the fact that in the identification mode, one-to-many comparisons have to be performed through a database search. This action introduces more privacy threats than the ones introduced when one-to-one comparison is performed as in the verification mode. The privacy risks increase when the biometric data are stored for an unlimited amount of time. In fact, if the system deployment is indefinite in time, threats such as function creep may arise. If the database is violated, biometric traits related to several users are compromised. Biometric systems where identifiable biometrics, such as faces, voice patterns, and so on, are retained are more prone to privacy risks than those which store templates. Moreover, if the biometric data are stored in a centralized database, serious privacy concerns arise since data are stored out of user's control, whereas if the user can maintain the ownership of the biometric data, less privacy risks can occur since the user can control the collection, usage, etc. of biometric information. The use of biometrics can have secondary purposes when both either governmental institutions or private companies are involved. In different societies, one or the other can be perceived more threatening to privacy. Also the role of the individual in the biometric system, employee, citizen or customer, impacts on the privacy assessment.

1.3 Biometric System Security

Although the definition of the notion of security for a biometric based system is a very challenging task, a significant effort has been done by the scientific community to highlight the main security concerns related to a biometrics-based recognition system (see for example [7–11]).

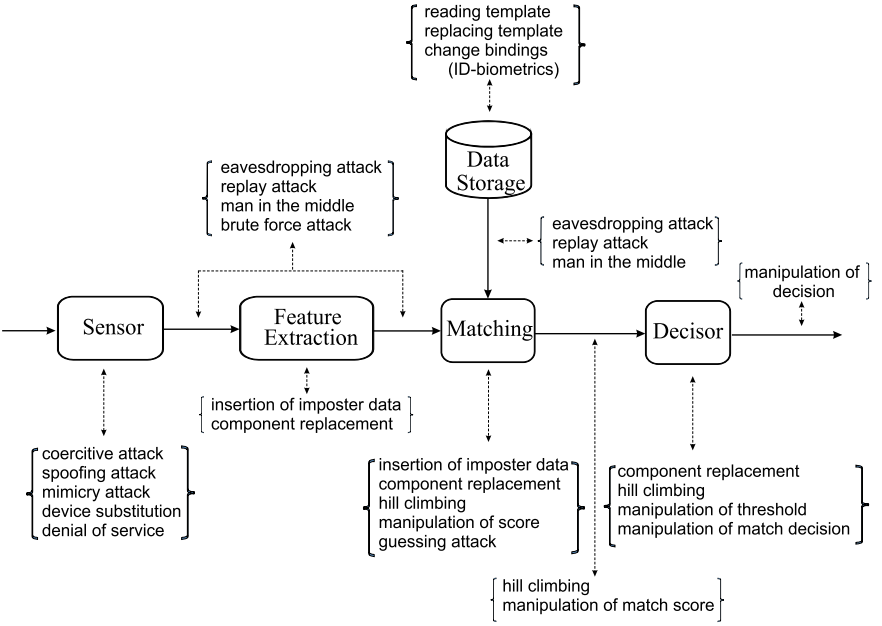

Fig. 1.3 Points of attack in a generic biometric system

Roughly speaking a biometric system can be vulnerable either because of intrinsic failure or because of intentional attacks.

A system characterized by a high False Acceptance Rate is very prone to be violated since it is likely that an arbitrary biometric feature presented to the system will match. This can happen also if there is no adversary willing to attack the system, case usually referred to as *zero-effort attack*.

In Fig. 1.3 a biometric system is sketched as the cascade of the acquisition sensor, the feature extractor module, the module that performs matching between the output of the feature extractor and the templates stored in the database, and finally the decisor that drives the application device. As discussed in [8–12] and also illustrated in Fig. 1.3 the major potential intentional attacks that can be perpetrated against the different blocks of a biometric system can be summarized as follows:

- *Sensor*
  - *coercive attack*: the true biometric is presented but in some unauthorized manner, e.g. when an impostor forces a legitimate user to grant him access to the system;
  - *spoofing attack* and *mimicry attack* related to physiological and behavioral biometrics respectively. These attacks consist in copying, by means of different strategies, the biometric feature of the enrolled user, and to transfer it to an impostor in order to fool the system;

  - *device substitution*: substitution of a legitimate biometric capture device with a simulated, modified or replacement unit;
  - *denial of service*: massive attacks on the system cause the system failure.

- *Feature extractor* that could be forced by an attacker to produce pre-selected features by inserting impostor data or component replacement.
- *Matcher* that can be attacked to produce fake scores. This task can be achieved in different ways:

  - *manipulation of the match scores*: capturing and changing the value of a match score before it affects the decision;
  - *reply attack*: a recorded version of the true data is injected in the channel;
  - *component replacement*: substitution of one of the software/hardware components in order to control its behavior:
  - *hill climbing attack*: iterative attack [13] that can be performed when access is granted to the match scores. Specifically, given an input, a slight modification of the input is performed. If the match score is increased the modification is kept, otherwise the modification is discarded. The procedure is iterated until the matching score is greater than the threshold.

- *Channels* interconnecting the different parts of a biometric system, like the channel between the sensor and the feature extractor, between the feature extractor and the matcher, between the database and the matcher, and between the matcher and the application device, can be intercepted and controlled by unauthorized people. Among the possible attacks we can mention the:

  - *eavesdropping attack*: the act of surreptitiously listening to biometric data transmission;
  - *man in the middle attack*: an attacker is able to manipulate the messages exchanged between two parties without the parties knowing that the link has been compromised;
  - *brute force attack*: exhaustive presentation of a large set of biometrics inputs to the recognition system to find one that works;
  - *replay attack*;
  - *hill climbing attack*;
  - *manipulation of match score*;
  - *manipulation of the decision*: capturing and changing the value of the decision.

- *Database*: reading templates, modification of one or more records in the database, replacing templates, changing links between ID and biometrics, are very threatening attacks.

It is also worth pointing out that automatic biometrics-based recognition systems are also prone to enrollment threats related to identity proofing, since forged ID cards could be used in the enrollment stage. This could lead to having a valid enrolled biometric but bound to a false identity. On the other hand a valid identity could be bound to fake biometrics.

Different kind of attacks or vulnerabilities require different kind of countermeasures. For example liveness detection techniques could be used as countermeasure

Table 1.1 Most feasible system architectures for a biometrics-based recognition system

Storing \ Matching	Server	Client	Device	Token
Server	YES	–	–	YES
Client	–	YES	–	–
Device	–	–	YES	YES
Token	–	–	–	YES

against spoofing, the hill climbing can be counteracted using encrypted channels or matching scores coarsely quantized, eavesdropping using secure channels, and so forth.

Furthermore some threats may be eliminated by the actual implementation of the system. In fact, different security requirements need to be considered according to the location where storage and matching are performed. Specifically, in [12] the different threats of the general architecture of a biometrics-based recognition system shown in Fig. 1.3 are particularized to the most feasible system architectures summarized in Table 1.1. Each of these architectures presents its own pros and cons. For example the one based on the template storage on a physical token has the advantage not to have any central storage to protect. On the contrary the architecture where the storage is made on the server poses many security and privacy concerns for the central database storage, although the use of centralized storage allows simplified administration.

The use of multibiometric systems [14] can be also foreseen to increase the level of security of biometrics-based recognition systems. In fact the increase of the number of credentials required for proper recognition can deter the spoofing attack, improving the matching accuracy and increasing the population coverage. On the other end multibiometric systems also increase the cost and the complexity of the system.

1.4 Privacy and Security

Within the biometric framework, the term "security" refers to making the data available for authorized users and protected from non-authorized users, whereas the term "privacy" is used to limit the use of shared biometrics only to those individuals who need to know the data and to limit it to the original purposes for which the data have been collected in the first place in agreement with the OECD purpose specification, use limitation, and collection limitation principles. Moreover, within the security framework the ultimate control over the data is made by the system owner/administrator, whereas within the biometric framework, the ultimate control over the data is made by the individual in agreement with the OECD Individual participation principle. Therefore privacy means something more than keeping biometric data secret. Most biometric characteristics like face images, voice, iris images, fingerprints, gait, to cite a few, are exposed and therefore not secret, and technology is available to covertly capture with different degrees of difficulty. As stated in [15],

privacy and security have been treated in the recent past as requirements hindering each other, which imply that when more emphasis is given to security, less emphasis will be given to privacy. Moreover, since in general the public concern for security is very high, privacy has been often penalized. However, in the recent past an always increasing level of attention towards the problems of privacy protection has lead to the development of techniques that allow both to enhance security and minimize privacy invasiveness.

1.5 Privacy Enhancing Technologies: An Historical Perspective

The unauthorized access to biometric templates is among the most dangerous threats to users' privacy and security [16]. In fact, although it was commonly believed that it is not possible to reconstruct the original biometric characteristics from the corresponding extracted template, some concrete counter examples, which contradict this assumption, have been provided in the recent literature as in [13] where it is shown that the knowledge of the face biometric template and of the match score can lead to face reconstruction and in [17] where an efficient algorithm has been proposed to generate a fingerprint from its matching minutiae points.

Therefore, storing biometric templates would not be secure enough and in case the template is compromised it is highly desirable to revoke or to renew it, and also to obtain from the same biometrics different keys to access different locations, either physical or logical, in order to avoid unauthorized tracking.

To summarize, a template protection scheme should satisfy the following properties [10]:

- *Renewability*: it should be possible to revoke a compromised template and reissue a new one based on the same biometric data.
- *Diversity*: each template generated from a biometrics should not match with the others previously generated from the same data. This property is needed to ensure the user's privacy.
- *Security*: it must be impossible or computationally hard to obtain the original biometric template from the stored and secured one. This property is needed to prevent an adversary from creating fake biometric traits from stolen templates.
- *Performance*: the biometric recognition error rates in terms of False Rejection Rate or False Acceptance Rate should not degrade significantly with the introduction of a template protection scheme, with respect to an unprotected approach.

The design of a template protection scheme able to properly satisfy each of the aforementioned properties is not a trivial task, mainly due to the unavoidable intra-user variability shown by every biometric trait. In the recent years, many different solutions have already been proposed for the generation of secure and renewable templates. A variety of possible classifications for template protection algorithms have been proposed so far and some attempts to harmonize the vocabulary have already been done [18] although a common vocabulary has not been established yet

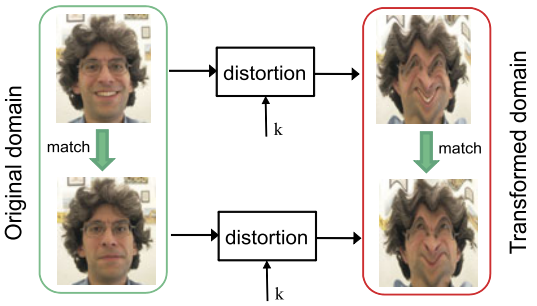

Fig. 1.4 Scheme of principle of a transform-based approach

in the scientific community. In the following, among the possible classifications of template protection algorithms, we will refer to two categories [10], namely *biometric cryptosystems* and *feature transformation* approaches.

1.5.1 Features Transformations for Template Protection

In a feature transformation approach, a function dependent on some parameters, which can be used as key, is applied either in the original biometric domain or in the feature domain to generate either transformed biometrics or transformed feature vectors. The matching is then performed in the transformed domain (see Fig. 1.4 for a simple schematization). The employed function can be either *invertible*, resulting in a *salting* approach, whose security is based on the protection of the function parameters, or *non-invertible*, when a one-way function is applied to the template and it is computationally hard to invert the function even if the transformation parameters are known. The use of the methods belonging to the first category typically results in low false acceptance rates, but if a user-specific key is compromised, the user template is no longer secure due to the invertibility of the transformation. On the contrary, when non-invertible transforms are used, even if the key is known by an adversary, no significant information can be acquired on the template, thus obtaining better security than the one achievable when using a salting approach. Specifically, the security of the non-invertible transform-based schemes relies on the difficulty of *inverting* the transformation to obtain the original biometric data. Moreover, differently from the cryptosystem approaches, the transformed templates can remain in the same feature space of the original ones, being then possible to employ standard matchers to perform recognition in the transformed domain. This allows achieving performances similar to those of an unprotected approach. In addition to the benefits on the performance deriving from using standard matchers in the transformed domain, transformation-based approaches typically result in matchings scores which can be fused in multi-biometric approaches. Therefore, the use of transform based approaches for template protection in multi-biometrics systems allows using either score level fusion techniques or decision level fusion techniques [14], whereas only the latter, less effective than the former, can be employed when biometric cryptosystems are considered.

The transformation function should be designed in order to keep the intra-class and inter-class distances in the transformed domain similar to the corresponding ones in the original domain in such a way to preserve the features discriminability. Moreover the transformation should be non-invertible. Unfortunately, it is difficult to design transformation functions which preserve both the template discriminability and the non-invertibility properties simultaneously. Furthermore, a rigorous security analysis concerning the non-invertibility of the scheme is very difficult especially when the transformation algorithm and related keys/parameters are also compromised. Therefore, extra care should be taken when designing and analyzing this type of schemes.

The concept of achieving template security through the application of non-invertible transformations has been first presented in [8], where it has been referred to as *cancelable biometrics* although this expression has been later used in a more general sense. Since then many approaches have been proposed with application to different biometric modalities. Without any claim of completeness, some examples follow. In [19] cancelable face biometrics are obtained by convolving the face image with a two-dimensional array of random numbers, generated via a password, and a cancelable correlation filter is designed from such "randomized" biometric signature. In [20] a geometric transform has been employed to protect minutiae templates but obtaining a significant performance degradation. More general geometric transforms, specifically, Cartesian, polar, and functional, have been later studied in [21], where better recognition performances have been achieved, but with a very limited amount of non-invertible data in practice. Moreover, the approaches presented in [20] and [21] are vulnerable to a record multiplicity attack: having access to two or more different transformed versions of the same minutiae pattern, it is possible to identify the original position of the considered minutiae [22]. A registration free construction of cancelable fingerprint templates has also been proposed in [23]. From each detected minutia, a square patch is extracted and transformed using an orthogonal transformation matrix. The approach presented in [23] is more robust than the one proposed in [21], being able to withstand also a record multiplicity attack, but it exhibits lower verification performances than the one obtained in [21]. A voice based cancelable template method has been proposed in [24], where a non invertible transformed version of the originally acquired voiceprint is generated. The original biometrics cannot be obtained from the template stored in the server during enrollment, even if the keys employed for transformations are disclosed. In [25, 26], a set of non-invertible transformations, based on the convolution operator, has been introduced in order to generate multiple transformed versions of a template. The framework in [25, 26], applicable in principle to any biometrics whose template can be represented by a set of sequences, has been there applied as proof of concept to an on-line signature recognition system, where a Hidden Markov Model based matching strategy is employed.

It is worth pointing out that, when using templates distortions techniques, with either invertible or non-invertible transforms, only the distorted data are stored in the database. This implies that even if the database is compromised, in principle, that is if the keys are unaccessible and the transformation perfectly non invertible,

the biometric data cannot be retrieved. Moreover, different templates can be generated from the original data, simply by changing the parameters of the employed transforms.

1.5.2 Biometric Cryptosystems for Template Protection

Biometric cryptosystems provide the means to adapt cryptographic protocols to biometric data which are inherently noisy data. They can be classified into *key generation* schemes, where binary keys are directly created from the acquired biometrics, and *key binding* schemes, which store information obtained by combining biometric data with randomly generated keys.

The main issue affecting key generation approaches regards the possibility of creating multiple keys from the same biometrics without using any external data, and the stability of the resulting cryptographic key. Moreover, due to the difficulties in managing the intra-class variability of biometric data, the recognition performance of such schemes are typically significantly lower than those of their unprotected counterparts [27].

A key binding system can be twofold: it can be used to protect a biometric template by means of a binary key, thus securing a biometric recognition system, or to release a cryptographic key only when its owner presents a specific biometric trait. In both cases a secret key, independent of the considered biometrics, is combined during enrollment with a reference template to generate some publicly available data, the so-called *helper data*, from which it should be impossible, or at least computationally hard, to retrieve information about the original biometric trait or the key. The helper data is then used in conjunction with a query biometrics during recognition to retrieve the secret. Typically, these approaches are able to manage the intra-user variations in biometric data by exploiting the capabilities of error correcting codes. However, it is generally not possible to use sophisticated and dedicated matchers, thus reducing the system matching accuracy.

In a key generation scenario the major design problem is related to the variability of the biometric traits. Therefore many efforts have been devoted to obtain robust keys from noisy biometric data. In [28] and in [29] cryptographic keys have been generated from voice and faces respectively. Significant activity has been devoted to the generation of keys from signature. As proposed in [30] and further detailed in [31] a set of parametric features has been extracted from each dynamic signature and an interval matrix has been used to store the upper and lower admitted thresholds for correct recognition. A similar approach has been proposed in [32]. Both methods provide protection for the signature templates. However, the variability of each feature has to be made explicitly available, and both methods do not provide template renewability. In [33] biometric secrecy preservation and renewability have been obtained by applying random tokens, together with multiple-bit discretization and permutation, to the function features extracted from the signatures. In [34] biometric keys have been generated using a genetic selection algorithm and applied to

on–line dynamic signature. In [35] a technique to increase the level of entropy offered by a generic biometric modality has been presented. In [36] key generation for iris biometrics has been investigated by selecting the most reliable feature of each subject.

In a key binding scenario, among the cryptographic protocols most commonly employed, we can mention the fuzzy commitment [37] where a secret key is chosen by the user, encoded, and the result is XORed with the biometric template to ensure the security and privacy of the template. More in detail the approach proposed in [37] stems from the one described in [38], where the role of error correction codes used within the framework of secure biometric recognition is investigated and provides better resilience to noisy biometrics. In order to cope with set of unordered data in [39] the fuzzy vault protocol based on polynomial-based secret sharing has been introduced. Both the fuzzy commitment and the fuzzy vault have been widely used for biometric systems relying on different identifiers. The fuzzy commitment scheme has been applied to ear biometrics [40], fingerprint [41, 42], 2D face [43], 3D face [44], iris [45, 46], and online signatures [47, 48] among the others. The fuzzy vault scheme has been applied to fingerprint [49–51], signature [52], face [53], iris [54], and palmprint [55], to cite just a few.

In [56] two primitives, namely the *fuzzy extractor* and the *secure sketch*, have been introduced. The first extracts a uniformly random string from an input in a error tolerant way, that is, in such a way that even if the actual input differs from the original one, still remaining close, the string can be exactly recovered. The second allows an exact reconstruction of the input by using some public information extracted from it, namely the *sketch*, which does not reveal significant information about the input itself, and a noisy replica of the input close enough to the original one. Constructions and rigorous analysis have been given for three metrics: Hamming distance, set difference, and edit distance. In [57] the practical issues related to the design of a secure sketch system have been analyzed with specific application to face biometrics. In [58] fuzzy extractors have been employed in a setting where data obtained in enrollment and verification are stored in different representations. A proof of concept has been given with application to fingerprints. In [59] fuzzy extractors for continuous source data have been considered and in [60] fuzzy extractors for continuous domain with application to faces have been proposed.

In the recent years many efforts have been devoted to the analysis of the applicability of biometric cryptosystems in real life applications with respect to the level of security and privacy that can be actually achieved. Specifically in [61] the secrecy and privacy leakage properties in fuzzy commitment schemes have been investigated. In [62] an empirical analysis on the security and privacy of the fuzzy commitment scheme with application to an existing system for 3D face recognition has been given. In [63] the cross-matching attack within the framework of the fuzzy commitment scheme has been theoretically analyzed, the analysis has been applied to real world datasets, and some possible countermeasures have been proposed. In [64] the security of the fuzzy commitment has been analyzed from a practical point of view with application to iris biometrics. Also the vulnerabilities of the fuzzy vault have been investigated. Specifically in [65] some criteria to distinguish chaff points

of a fuzzy vault scheme from minutiae in a fingerprint based recognition system have been given and experimentally validated. Moreover, it has been proven that the fuzzy vault is vulnerable to the cross-matching attack [66]: if an adversary has access to two different vaults obtained from the same data, he can easily identify the genuine points in the two vaults. A practical implementation of the cross-matching attack for the fuzzy vault scheme for fingerprints has been presented in [67].

In [68] it has been shown that some implementations of the fuzzy extractor and of the fuzzy sketch are not adequate when the same secret is employed for multiple uses and some models and conditions that allow reusable secrets are given. Some improved solutions are presented in [69]. In [70] it has been demonstrated that fuzzy sketches always leak some information about their inputs and in [71] the analysis of weather an attacker can determine whether two documents are encrypted using the same biometrics is addressed. In [72] a theoretical framework for the analysis of privacy and security trade-offs in secure biometric recognition systems has been given. Specifically a comparative information-theoretic analysis of both fuzzy commitment and secure sketch-based protection schemes has been provided.

In the last few years some efforts have been also devoted to the design of template protection mechanisms for multi-biometric systems. Although the development of the topic is still in its infancy some interesting contributions have already been proposed. In [73] face and fingerprints templates have been fused at a feature level and secured using the fuzzy commitment scheme. In [74] a multi-biometric system based on the fusion at the feature level of fingerprints and iris and secured by using the fuzzy vault scheme has been proposed. In [75] different forms of fusion, specifically feature, score, and decision level fusion have been investigated within the framework of the fuzzy commitment construct. In [76] a multibiometric system combining iris and face to obtain a long cryptographic key having high entropy has been proposed. In [77] a feature level fusion approach for the implementation of multibiometric cryptosystems based on the use of both the fuzzy commitment and the fuzzy vault has been proposed. Specifically fingerprint, iris, and face have been simultaneously employed.

1.6 Research Projects on Privacy and Security in Biometrics

The privacy and security aspects of emerging biometric identification technologies have been object of research in several funded projects worldwide. Specifically, within the framework of the European Union Framework Programs, the BITE (Biometric Identification Technology Ethics) project [78], which ended in February 2007, and the HIDE (Homeland Security, Biometric Identification & Personal Detection Ethics) project [79], which ended in 2011, focused on the ethical and privacy issues of biometrics and personal detection technologies with specific reference to those applications which require cooperation among National and International agencies is crucial. Moreover the project PRIME (Privacy and Identity Management in Europe), which ended in February 2008, focused on solutions for

privacy-enhancing identity management that supports end-users' sovereignty over their private sphere and enterprises' privacy-compliant data processing. The IRISS (Increasing Resilience in Surveillance Societies) project [80], a two year project which started in October 2011, is aimed at investigating the development and deployment of surveillance technologies and their impact on the citizen's democratic rights and their social and economic costs. The SurPRISE (Surveillance, Privacy and Security) project [81], a three year project which started in February 2012, is aimed at identifying those factors which contribute to the shaping of security technologies as effective, non-privacy-infringing and socially legitimate security devices. European projects with the objective of implementing some of the discussed privacy enhancing technology are the 3DFace [82] and the TURBINE (TrUsted Revocable Biometric IdeNtitiEs) [83] projects. The 3DFace project is a three-year project which started in April 2006. The objective of the 3DFace project was to develop a prototype of an automated border control biometric system incorporating privacy enhancing technology based on 2D and 3D face images. The TURBINE project is a three-year project which started in February 2008. Its aim was to develop innovative digital identity solutions by combining secure, automatic user identification based on electronic fingerprint authentication and reliable protection of the biometrics data through privacy enhancing technology. The BEAT (Biometrics Evaluation and Testing) project [84], a four year project which started in March 2012, aims at proposing a framework of standard operational evaluations for biometric technologies with emphasis on the analysis of the performance of the underlying biometric system, of the robustness to vulnerabilities such as direct (spoofing) or indirect attacks, and of the strength of privacy preservation techniques. The TABULA RASA (Trusted Biometrics under Spoofing Attacks) project [85], a 42 month project which started in November 2011, aims at addressing some of the issues of spoofing attacks to trusted biometric systems.

However, despite the efforts devoted in these projects, privacy and security within biometrics still pose a wide range of challenging problems that need to be further investigated.

1.7 Research Agenda on Privacy and Security

The design of secure and privacy compliant biometric based systems is a challenging problem which involves several disciplines ranging from legislation and ethics to signal processing, pattern recognition, information theory and cryptography. Therefore, although on one side the aforementioned goal is a very demanding one, on the other side it can offer several research opportunities in heterogeneous fields of research in which scientists necessarily need to act synergically in order to achieve tangible results. Some examples follow.

As for the security, a system is usually referred to as a *strong* system when the cost of attacks is greater than the potential advantage to the adversary. On the contrary, a *weak* system is a system for which the cost of attacks is lower than the

corresponding potential advantage. The definition of the level of security in biometric systems has been performed so far through the identification of possible attacks, vulnerabilities, possible countermeasures, and a global cost analysis. It is not straightforward to define the security which is ensured by a specific system and in particular by a biometric system in a quantitative rather than in a qualitative way. Therefore, major efforts need to be done towards the definition of metrics to be employed for assessing the performance of a system in terms of the level of security achieved.

With specific reference to biometric template protection schemes, different taxonomies have been proposed so far, with the risk to potentially generate confusion. Therefore a vocabulary harmonization is really needed by the scientific community. Currently, some activities are being carried out in standardization bodies to achieve this goal. Moreover, although several biometric template protection approaches have been proposed in literature, still a systematization on the benchmark metrics need to be done. It is worth pointing out that some metrics tailored to characterize specific biometric template protection systems have already been proposed. However, their applicability is limited to those approaches which share the same basic principles. For example, within the *fuzzy extractor* and *secure sketch* framework introduced in [56], the concepts of *min-entropy* and *entropy loss* related to the length of the extracted biometric key and to the information leakage given by the public data respectively are given. On the other hand, when transformation based template protection approaches are considered, different performance evaluation metrics need to be defined. Therefore the definition of a holistic approach able to cope with the performance assessment of a generic template protection approach would be a significant achievement. Some preliminary attempts within this regard have been performed, see for example [86], but a significant amount of research effort needs to be still put in place.

In the recent past, multi-biometric systems are witnessing an always increasing interest from the scientific community due to their intrinsic capabilities of addressing the universality issue better than uni-modal systems and to the increasing level of security they can potentially achieve. However, a comprehensive analysis on the possible additional threats, attacks, vulnerabilities, and countermeasures, specific to multi-biometric systems still needs to be systematically carried out. Moreover, the issue of designing template protection approaches tailored to multi-biometric systems, still in its infancy, is a fertile field of research. Also, the assessment of the effectiveness of the aforementioned systems requires proper procedures and metrics, yet to be designed.

It is worth pointing out that in the past it has been given more emphasis to ensure security rather than designing privacy compliant systems. Only recently privacy and security have been treated as two factors to be jointly optimized and not as two requirements hindering each other. This has lead to the need to include the privacy requirements in the early stage design of a biometric system. Appealing research topics include analyzing the privacy risks, defining the needed requirements to guarantee individual's privacy, developing proper best practices, architectures, and systems with the purpose to implement the needed privacy constraints. Finally

a testing stage to assess whether the privacy requirements have been fulfilled is required. The modeling and quantification of privacy properties such as anonymity, unlinkability, etc. are essential steps towards the deep understanding of what is intended for privacy and towards the definition of metrics which are needed to assess the level of privacy protection provided by different biometric systems. However privacy preservation is a multidisciplinary area of research which has relevant legal, social, economic, political, and cultural aspects which must be understood in depth and developed in order to design effective approaches for the protection of individual's privacy. Therefore research expertise beyond engineering is needed in order to tackle the privacy protection problem in biometric systems effectively.

References

1. Privacy & biometrics building a conceptual foundation. NSTC, Committee on Technology, Committee on Homeland and National Security, Subcommittee on Biometrics. Tech rep, September 2006
2. Woodward JJD (2008) The law and use of biometrics. In: Jain AK, Flynn P, Ross AA (eds) Handbook of Biometrics. Springer, New York
3. Guidelines on the protection of privacy and transborder flows of personal data. OECD (Organisation for Economic Co-operation and Development), Paris, France. Tech rep, 1980 (accessed in December 2012). [Online]. Available: www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html
4. Privacy technology implementation guide. Homeland security. Tech rep, 16 August 2007 (accessed in December 2012). [Online]. Available: http://www.dhs.gov/xlibrary/assets/privacy/privacy/guide/ptig.pdf
5. Article 29—data protection working party 2003, working document on biometrics 12168/02/en. Tech rep
6. Mordini E (2008) Biometrics, human body and medicine: a controversial history. In: Duquenoy P, George C, Kimppa K (eds) Ethical, Legal and Social Issues in Medical Informatics. Idea Group Inc, Hershey
7. Biometric security concerns. UK biometric working group. Tech rep, September 2003
8. Ratha N, Connell J, Bolle R (2001) Enhancing security and privacy in biometrics-based authentication systems. IBM Systems Journal 40(3):614–634
9. Uludag U, Jain A (2003) Attacks on biometric systems: a case study in fingerprints. In: Proc SPIE-EI 2004, Security, Steganography and Watermarking of Multimedia Contents VI, 18–22 January 2003, pp 622–633
10. Jain AK, Nandakumar K, Nagar A (2008) Biometric template security. EURASIP Journal on Advances in Signal Processing 2008
11. Roberts C (2006) Biometric attack vectors and defences. Computers & Security 26(1)
12. INCITS-M1/07-0185rev, Study report on biometrics in e-authentication. InterNational Committee for Information Technology Standards, INCITS Secretariat, Information Technology Industry Council (ITI). Tech rep, 30 March 2007 (accessed in December 2012). [Online]. Available: http://standards.incits.org/apps/group_public/download.php/24528/m1070185rev.pdf
13. Adler A (2003) Can images be regenerated from biometric templates? In: Proc Biometrics Consortium Conference, September 2003
14. Ross A, Nandakumar K, Jain AK (2006) Handbook of Multibiometrics. Springer, Berlin
15. Cavoukian BA, Stoianov A (2007) Biometric encryption: a positive-sum technology that achieves strong authentication, security and privacy, Toronto, Canada. Tech rep, 2007 (accessed in December 2012). [Online]. Available: www.ipc.on.ca

16. Tuyls P, Skoric B, Kevenaar T (2007) Security with Noisy Data. Privacy Biometrics, Secure Key Storage and Anti-counterfeiting. Springer, Berlin
17. Ross A, Shah J, Jain AK (2007) From template to image: reconstructing fingerprints from minutiae points. IEEE Transactions on Pattern Analysis and Machine Intelligence 29(4):544–560
18. Breebaart J, Busch C, Grave J, Kindt E (2008) A reference architecture for biometric template protection based on pseudo identities. In: BIOSIG, Darmstadt, Germany, September 2008
19. Savvides M, Vijaya Kumar BVK, Khosla PK (2004) Cancelable biometric filters for face recognition. In: Proceedings of the 17th International Conference on Pattern Recognition, ICPR 2004, vol 3, Cambridge, UK, August 2004, pp 922–925
20. Ang R, Safavi-Naini R, McAven L (2005) Cancelable key-based fingerprint templates. In: ACISP. Lecture Notes on Computer Science, vol 3574, pp 242–252
21. Ratha NK, Chikkerur S, Connell JH, Bolle RM (2007) Generating cancelable fingerprint templates. IEEE Transactions on Pattern Analysis and Machine Intelligence 29(4):561–572
22. Quan F, Fei S, Anni C, Feifei Z (2008) Cracking cancelable fingerprint template of Ratha. In: International Symposium on Computer Science and Computational Technology, ISCSCT'08, Shanghai, China, December 2008, pp 572–575
23. Chikkerur S, Ratha N, Connell J, Bolle R (2008) Generating registration-free cancelable fingerprint templates. In: IEEE Second International Conference on Biometrics: Theory, Applications and Systems, BTAS'08, Washington, DC, USA, 28 September–1 October 2008
24. Xu W, He Q, Li Y, Li T (2008) Cancelable voiceprint templates based on knowledge signatures. In: Proceedings of the 2008 International Symposium on Electronic Commerce and Security, ISECS'08, Guangzhou, China, August 2008
25. Maiorana E, Martinez-Diaz M, Campisi P, Ortega-Garcia J, Neri A (2008) Template protection for hmm-based on-line signature authentication. In: IEEE Intl Conf on Computer Vision and Pattern Recognition, Anchorage, Alaska, USA, 23–28 June 2008
26. Maiorana E, Campisi P, Fierrez J, Ortega-Garcia J, Neri A (2010) Cancelable templates for sequence based biometrics with application to on-line signature recognition. IEEE Transactions on Systems, Man and Cybernetics. Part A 40(3):525–538
27. Ballard L, Kamara S, Reiter M (2008) The practical subtleties of biometric key generation. In: 17th Annual USENIX Security Symposium, San Jose, CA, USA, 28 July–1 August 2008
28. Monrose F, Reiter M, Li Q, Wetzel S (2001) Cryptographic key generation from voice. In: IEEE Symp on Security and Privacy, Oakland, CA, USA, May 2001
29. Goh A, Ngo D (2003) Computation of cryptographic keys from face biometrics. In: International Federation for Information Processing. Lecture Notes on Computer Science, vol 2828
30. Vielhauer C, Steinmetz R, Mayerhoefer A (2002) Biometric hash based on statistical features of online signatures. In: 21st International Conference on Pattern Recognition, ICPR 2012, Tsukuba Science City, Japan, November 2012
31. Vielhauer C, Steinmetz R (2004) Handwriting: feature correlation analysis for biometric hashes. EURASIP Journal on Applied Signal Processing 4:542–558. Special issue on biometric signal processing
32. Feng H, Chan C (2002) Private key generation from on-line handwritten signatures. In: Information Management and Computer Security, pp 159–164
33. Kuan Y, Goh A, Ngo D, Teoh A (2005) Cryptographic keys from dynamic hand-signatures with biometric secrecy preservation and replaceability. In: Proc Fourth IEEE Workshop on Automatic Identification Advanced Technologies, AUTO ID 2005, Buffalo, New York, USA, October 2005, pp 27–32
34. Freire M, Fierrez J, Galbally J, Ortega-Garcia J (2007) Biometric hashing based on genetic selection and its application to on-line signatures. In: Lecture Notes on Computer Science, vol 4642, pp 1134–1143
35. Ballard L, Kamara S, Monrose F, Reiter MK (2008) Towards practical biometric key generation with randomized biometric templates. In: Proceedings of the 15th ACM Conference on Computer and Communications Security, CCS'08, Alexandria, VA, USA, October 2008