Signal Processing for Security Technologies

Richard Jiang
Somaya Al-maadeed
Ahmed Bouridane
Danny Crookes
Azeddine Beghdadi *Editors*

Biometric Security and Privacy

Opportunities & Challenges in The Big Data Era

Springer

Signal Processing for Security Technologies

Series Editor

M. Emre Celebi
Baton Rouge, Louisiana, USA

More information about this series at http://www.springer.com/series/13765

Richard Jiang • Somaya Al-maadeed
Ahmed Bouridane • Danny Crookes
Azeddine Beghdadi
Editors

Biometric Security and Privacy

Opportunities & Challenges in The Big Data Era

Springer

Editors
Richard Jiang
Department of Computer
and Information Science
Northumbria University
Newcastle upon Tyne
United Kingdom

Ahmed Bouridane
Department of Computer
and Information Science
Northumbria University
Newcastle upon Tyne
United Kingdom

Azeddine Beghdadi
Institut Galilée
Université Paris 13
Paris, France

Somaya Al-maadeed
Department of Computer Science
and Engineering
Qatar University
Doha, Qatar

Danny Crookes
School of Electronics, Electrical Engineering
and Computer Science
ECIT Institute, Queen's University Belfast
Belfast, Antrim, UK

Signal Processing for Security Technologies
ISBN 978-3-319-47300-0 ISBN 978-3-319-47301-7 (eBook)
DOI 10.1007/978-3-319-47301-7

Library of Congress Control Number: 2016958827

Printed on acid-free paper

This Springer imprint is published by Springer Nature
The registered company is Springer International Publishing AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface

Biometrics in modern computer science is defined as the automated use of biological properties to identify individuals. The early use of biometrics can be dated back to nearly 4000 years ago when the Babylon Empire legislated the use of fingerprints to protect a legal contract against forgery and falsification by having the fingerprints impressed into the clay tablet on which the contract had been written. Nowadays, the wide use of the Internet and mobile devices has brought out the booming of the biometric applications, and research on biometrics has been drastically expanded into many new domains.

The research trends in biometric research may be categorized into three directions. The first direction is toward the broader Internet and mobile applications. This brings out a number of new topics to utilize biometrics in mobile banking, health care, medical archiving, cybersecurity, and privacy as a service, etc. These new applications have created a huge market of billion dollars for biometric technologies and the industry needs comes back to push the research further and vigorously. The second direction is towards algorithmic development, which includes the investigation of many new AI techniques in biometrics, such as fuzzy approaches, ensemble learning, and deep learning. These new approaches can often help improve the accuracy of automated recognition, making many new applications available for business. Especially, with the vast amount of data coming from billions of users on internet/mobile, biometrics now becomes a new Big Data challenge in its streaming, processing, classification and storage. The third research direction aims at discovering more types of biometrics for various uses. Besides the conventional fingerprints and signatures, other types of biometrics (such as iris, vein pattern, gait, and touch dynamics) have been investigated in recent biometric research. Their combination as multimodal biometrics is another popular way to exploit these types of biometrics in research.

This book includes 16 chapters highlighting recent research advances in biometric security. Chapters 1–3 present new research developments using various biometric modalities including Fingerprints, Vein Patterns and Palmprints. New tools and techniques such as Deep Learning are investigated and presented. Chapter 4 reports a new biometric recognition approach based on the acoustic features of human ears. Chapters 5–9 discuss new research works relating to a number of dynamic behavioural biometric traits. Chapters 10–13 focus on face recognition, which is the most popular topic in biometrics. Chapter 14 carries out a survey of biometric template protection, a very important topic in biometric privacy and security. Chapter 15 investigates the use of biometrics for better security in cloud computing and Internet of Things. Chapter 16 reports the new EU legislation on biometrics, which should help technology developers be aware of the legal aspects of biometric technologies.

The target audience for this book includes graduate students, engineers, researchers, scholars, forensic scientists, police force, criminal solicitors, IT practitioners and developers who are interested in security and privacy related issues on biometrics. The editors would like to express their sincere gratitude to all distinguished contributors who have made this book possible, and the group of reviewers who have offered insightful comments to improve the quality of each chapter. A dedicated team at Springer Publishing has offered professional assistances to the editors from inception to final production of the book. We thank them for their painstaking efforts at all stages of production.

Richard Jiang
Newcastle upon Tyne, UK

Contents

Chapter 16
Data Protection and Biometric Data: European Union Legislation

Pedro Miguel Freitas, Teresa Coelho Moreira, and Francisco Andrade

16.1 Introductory Remarks

The protection of personal data is enshrined in several important legal texts. In 1981, under the auspices of the Council of Europe, the first binding international instrument concerning the protection of an individual against misuses in the collection and processing of personal data opened for signature. The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data set as a purpose the protection of personal data in a world of growing automatic data processing on a large scale, although it did not foresee biometric data as a special category of data deserving particular protection.

On a different level, the European Union's Treaty on European Union, on article 39, states that "the Council shall adopt a decision laying down the rules relating to the protection of individuals with regard to the processing of personal data by the Member States when carrying out activities which fall within the scope of this chapter, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities". Meanwhile, the Treaty on the Functioning of the European Union concedes everyone the right to protection of personal data concerning them (article 16). The protection of personal data is also found on the Charter of Fundamental Rights of the European Union. This Charter embodies the core fundamental values of the Member States of the European Union, as important as human dignity (article 1), life (article 2) and the right to physical and mental integrity (article 3). Amongst them emerges the protection of personal data as a fundamental freedom that everyone is entitled to (article 8). This freedom sits right at the heart of the fundamental values that the European Union considers necessary to be promoted and strengthened, especially

P.M. Freitas (✉) • T.C. Moreira • F. Andrade
Law School, University of Minho, Braga, Portugal
e-mail: pfreitas@direito.uminho.pt; tmoreira@direito.uminho.pt; fandrade@direito.uminho.pt

R. Jiang et al. (eds.), *Biometric Security and Privacy*, Signal Processing
for Security Technologies, DOI 10.1007/978-3-319-47301-7_16

"in light of changes in society, social progress and scientific and technological developments" (Preamble). In this sense, the protection of personal data should be safeguarded by all those to whom this charter is addressed to, including not only the institutions, bodies and agencies of the European Union, but also the Member States themselves when implementing European Union legislation. It might appear, in consequence, that, when it comes to the Member States, the Charter has a somewhat limited field of application: it is limited by the powers and competences that have been conferred by the Member States to the European Union. This idea that the European Union has competences that are subjected to the principle of subsidiarity, meaning that, on the one hand, the European Union only acts within the limits of the conferred competences and to meet the objectives set out in the Treaties and, on the other hand, if there is not exclusive competence regarding a certain area, can only act if the objectives should be better achieved at the European level, is an important limitation that should not be overlooked. Yet, it is clear that the protection of personal data is paramount to the objectives of the European Union and, as a fundamental right, portrays an important role in society.

16.2 Data Protection and Personal Data

The concept of data protection as a fundamental right has been further developed in the General Data Protection Regulation (Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data).[1] The reasoning behind the Regulation is the promotion of a consistent level of protection concerning personal data throughout the European Union while allowing a free flow of personal data between Member States. The free flow of personal data is necessary to a deeper economic and social integration of European stakeholders. Without the exchange of personal data, the public and private sector would be severely limited when performing their activities, the European internal market would cave in and public authorities would not be able to perform their tasks. Since 1995, with the directive 95/46/EC of the European Parliament and of the Council of 24 October 1995, that the European Union has a common set of rules on data protection of natural persons. However, globalization and rapid technological developments felt since then made this Directive completely obsolete and incapable of striking a balance between the protection of personal data and the fulfilling of society modern needs.

A conceptual description of personal data is given by the European legislator in the beginning provisions of the Regulation. According to article 4/1 of the

[1] This regulation repealed the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Further developments on the concept of personal data are found on opinion 4/2007 of the Article 29 Working Party (2007).

Regulation, personal data means any information relating to a data subject,[2] including:

- Name;
- Identification number;
- Location data;
- Online identifier; and
- Specific factors such as physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

16.3 Biometric Data as Personal Data

Biometrics involves techniques used to identify[3] individuals based on a particular trait or physical characteristic unique to that individual or on a behavioural characteristic of an individual.[4] Any human physiological and/or behavioural characteristic can be used as a biometric characteristic as long as it satisfies some requirements like universality, distinctiveness, permanence and collectability. Biometric systems record personal information[5] about identifiable individuals.[6]

[2] Only identified or identifiable natural persons are data subjects. The regulation does not afford protection to legal persons, but only natural living persons. The rules concerning the processing of personal data of deceased persons should be established by the Member States and this regulation does not apply to this type of personal data, even when personal data is archived for historical research and genealogical purposes.

[3] Biometric systems are "applications that use biometric technologies, which allow the automatic identification, and/or authentication/verification of a person. Authentication/verification applications are often used for various tasks in completely different areas, for different purposes and under the responsibility of a wide range of different entities", Article 29 Data Protection Working Party "Opinion 3/2012 on developments in biometric technologies", adopted on 27th April 2013.

[4] "Biometric systems are tightly linked to a person because they can use a certain unique property of an individual for identification and or/authentication. While a person's biometric data can be deleted or altered the source from which they have been extracted can in general neither be altered nor deleted", Article 29 Data Protection Working Party "Opinion 3/2012 on developments in biometric technologies", adopted on 27th April 2013.

[5] Although "Biometric systems are not 100 % accurate. Biometric systems accuracy during the template comparison process of authentication depends on external variables, namely, temperature, training level of the enrollment process technicians, physical condition of the individual to be authenticated, etc. Biometric systems accuracy is also dependent on internal variables such as quality of the equipment and the proprietary algorithms being used." Chinchilla, Rigoberto "Ethical and Social consequences of Biometric Technologies".

[6] "While other new technologies that target large populations and have recently raised data protection concerns do not necessarily focus on establishing a direct link to a specific individual—or creating this link requires considerable efforts—biometric data, by their very nature, are directly linked to an individual", Article 29 Data Protection Working Party "Opinion 3/2012 on developments in biometric technologies" adopted on 27th April 2012.

Biometric data is thus implicitly included in the definition of personal data because it implies retrieving and processing unique identification characteristics[7] of an individual.[8] It does not matter the nature of the specific identification processing technique used, e.g., facial recognition,[9] iris scan or dactyloscopic data,[10] insofar this technique allows the identification of a natural living person. Biometric data should be understood, for the purposes of the Regulation, as any technical means of retrieval or confirmation of the identity of a natural living person using their physical, physiological or behavioural characteristics.[11]

The same conclusion—biometric data being conceived as personal data—was already possible with the Directive 95/46/EC. In Article 2 a), "personal data" was defined as "any information relating to an identified or identifiable natural person (. . .); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental (. . .) identity". In accordance with this definition, measures of biometric identification or their digital translation in a template form in most cases are personal data.

Some biometric data could also be considered sensitive data (a special category of personal data) in the meaning of Article 8 of Directive 95/46/EC, because biometric data could reveal the racial or ethnic origin of the data subject or concern

[7] Physical biometrics are faced with the unequivocal fact that people get older and the body changes over time, cfr. Anton Alterman, "A piece of yourself: Ethical issues in biometric identification". See also Rebera, Andrew P. and Mordini, Emilio "Biometrics and ageing: social and ethical considerations": "That the ageing process poses a problem for biometrics is well-understood. No biometric is 100 % permanent: people's biometrics change over time. Hence the technical challenge is to develop techniques whereby an individual may be identifiable by his or her biometrics, throughout his or her lifetime, despite this mutability".

[8] We should be wary when an author writes that "increasingly, the way to keep information secure is to offer up a piece of yourself . . . to be recorded and used to verify your identity", Anton Alterman "A piece of yourself: Ethical issues in biometric identification".

[9] On facial recognition in online and mobile services, see Article 29 Working Party (2012).

[10] Article 29 Working Party (2007) gives as examples of biometric data: "fingerprints, retinal patterns, facial structure, voices, but also hand geometry, vein patterns or even some deeply ingrained skill or other behavioural characteristic (such as handwritten signature, keystrokes, particular way to walk or to speak, etc . . .)".

[11] His concept of biometric data, that is found on article 4/14 of the Regulation is substantially aligned with the opinion of the Article 29 Working Party (2007) that biometric data should be defined "as biological properties, physiological characteristics, living traits or repeatable actions where those features and/or actions are both unique to that individual and measurable, even if the patterns used in practice to technically measure them involve a certain degree of probability".

their health.[12] Biometric data was not explicitly categorized as sensitive data but, taking in consideration the type of data it usually involves, implicitly ought to be regarded as sensitive data.

16.4 The New Data Protection Regulation: Requirements and Challenges for the Treatment of Personal Data

This state of affairs has substantially changed with the new data protection regulation. The European legislator makes now absolutely clear that biometric data is a species of personal data, alongside sensitive personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, genetic data, data concerning health or data concerning a natural person's sex life or sexual orientation (article 9). The immediate consequence of categorizing certain data as a special category of personal data is the general prohibition of its processing.[13] Simply put, processing biometric data is forbidden. There are, however, exceptions: if the data subject consents (article 9/a) or, if he or she is—physically or legally—incapable of giving consent, and there is the need of protection of vital interests (article 9/c); for employment, social security or social protection law purposes (article 9/b); data concerning members of a legal entity related to political, philosophical, religious or trade-union aims and the data is not disclosed outside the legal entity (article 9/d); data made public by the data subject (article 9/e); processing of data necessary to the exercise of judicial activity (article 9/f); reasons of substantial public interest (article 9/g); purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services (article 9/h); reasons of public health (article 9/i); archiving purposes in the public interest, scientific or historical research purposes or statistical purposes (article 9/j). Each of these exceptions to the referred prohibition is herein only superficially mentioned.

[12] Article 29 Working Party (2003): "Some biometric data could be considered sensitive in the meaning of Article 8 of Directive 95/46/EC and in particular, data revealing racial or ethnic origin or data concerning health. For example, DNA data of a person often include health data or can reveal the racial or ethnic origin. In this case DNA data are sensitive data and the special safeguards provided by article 8 must apply in addition to the general data protection principles of the Directive. In order to assess the sensitivity of data processed by a biometric system the context of the processing should also be taken into account", Article 29 Data Protection Working Party "Opinion 3/2012 on developments in biometric technologies", referred.

[13] "'Processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction" (article 4/2 of the Regulation).

A thorough analysis would be necessary in order to fully understand the scope and limitation of each and every one of the exceptions. To perform a full-depth analysis of each and every exception to the general rule that prohibits processing of biometric data would be inopportune and even bothersome given the objective of this chapter but these exceptions will be of utmost importance to those whose field of activity is connected, to some extent, to biometric data.

The sensitive nature of biometric data means that it can only be used in very restrictive and specific situations.[14] The misuse of biometric information in various domains, e.g., medical, commercial and security profiling, is a matter of concern to a vast number of individuals. According to survey done in the United Kingdom up to 45 % of respondents considered biometric data to be extremely sensitive [1], which makes a strong argument in favour of conceding a strong legal protection to this type of personal data. This major concern over one's privacy means, in turn, that the use cases of biometric data are severely limited, especially when free, informed and explicit consent[15] is not given by the individual, and even if there this consent exists some legal restrictions may withdraw its validity.[16] In the online technology sector consent might be given by ticking a box when visiting an internet website that processes personal data (recital 32 of the Regulation). On mobile phones that rely on security features such as fingerprint[17] or facial recognition the consent requisite implies explicit agreement of the user with the processing of biometric data during the enrolment stage. The data controller, in other words, the natural or legal person responsible for determining the purposes and means of the processing of personal data, must be able to demonstrate that the data subject has given consent to the processing after being made aware of the fact that he or she was consenting and the extent of the consent. Irrespective of being located in European territory, this consent must be obtained for the purposes of the Regulation, as long as the data subjects are

[14] Even as a means of identification of the individual, according to the new regulation on electronic identification and trust services for electronic transactions (Regulation EU Nr 910/2014) electronic identification must comply with the principles relating to the protection of personal data provided for in Directive 95/46/EC (still in force but that will be replaced in 2018 by the new European Regulation 2016/679 of the European Parliament and Council of the 27th April 2016) and authentication for online service should concern processing of only those identification data that are adequate, relevant and not excessive to grant access to that service online.

[15] A definition of consent is found on article 4/11 of the Regulation.

[16] The European Union and national laws may foresee situations where the general prohibition of processing biometric data or other special personal data is not lifted by consent of the data subject (article 2/a, *in fine* of the Regulation).

[17] Even this kind of biometric data may encompass difficulties of application: "How will population with disabilities (or lacking physical traits) be enrolled or authenticated in biometric databases? People with just one hand, no iris or retina, no fingers, and in general people lacking physicals characteristics in need of using a biometric facility, may suffer discrimination and unnecessary delays in biometric systems. A well-developed, well-designed biometric system should allow these persons alternative ways to enroll and authenticate, yet delays and processes of bypassing the biometric systems may give them hardships each time they want to access a resource or use a facility which may be an ethical violation of their rights", Chinchilla, Rigoberto "Ethical and Social consequences of Biometric Technologies".

in the European Union and the processing activities relate to the offering of goods or services to such data subjects in the Union, or to the monitoring of their behaviour as far as their behaviour takes place within the Union.

Apart from the consent requisite, the data controller is also responsible for complying with additional requisites. The collection of personal data must be done with a specified, explicit and legitimate purpose. The so-called purpose limitation means that the data controller must process the data in accordance with the purpose that initially motivated the processing. If the data controller desires to process data for a purpose that is incompatible[18] with the one that the data was initially collected for then either the data subject gives consent for further processing or the further processing falls within the scope of public interest, scientific or historical research purposes or statistical purposes.

Another concern has to do with data accuracy. The data controller must show that has taken all reasonable steps to ensure that personal data, including biometric data, under his control, is accurate and up to date. The Regulation states that personal data shall be "accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay". Having in regard that the accuracy of biometric data is challenged [2] and that biometric data may need updating by force of natural factors such as ageing [3], this requisite demands from the data controller an ongoing effort of compliance.

One final remark concerning integrity and confidentiality of personal data. Processing and storage of personal data, especially biometric, must be carried out with strong security measures.[19] Reality displays numerous examples of how insecure information systems are. Hospitals, for instance, have become a prime target of cyber-attacks. Old and insecure computer systems coupled with poor security policies seem to create the perfect prey for hackers after easy money. The increasing economic value of health records in the black market, often surpassing credit card information, make the health industry an attractive victim of cyber-attacks such as data theft or crypto-ransomware. High security standards are not usually implemented and the exponential computerization of health care records creates new opportunities for security breaches. Although the regulation does not describe which security measures should be put in place, it requires proper security of the personal data that is object of processing, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures (article 5/f of the Regulation). The legislative choice of not determining exactly the security measures

[18] Incompatibility of purposes arises when there is not any link between the initial purpose and the further purpose, for instance. The data controller should also evaluate the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller; the nature of the personal data; the possible consequences of the intended further processing for data subjects and the existence of appropriate safeguards, which may include encryption or pseudonymization.

[19] "If biometric databases are not protected properly and information is stolen, the consequences can be permanently devastating", Chinchilla, Rigoberto "Ethical and Social consequences of Biometric Technologies".

is an understandable one. Security measures as well as attack techniques change over time in their nature and complexity. They are a product of the technological state of the art. Given this, a neutral approach to wording is wiser, meaning that the European legislator opted for establishing certain objectives, e.g., confidentiality, integrity, availability and resilience, while stating the factors that should be taken into account when deciding which security measures to deploy. In this sense, the required technical and organizational security measures depend on the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.

16.5 Conclusions

Since 1995, with the Directive 95/46/EC of the European Parliament and the Council, the European Union has established minimum rules concerning the protection of personal data which is thus enshrined in several important legal texts.

The concept of data protection as a fundamental right has been further developed in the General Data Protection Regulation (Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data).

Human physiological and/or behavioural characteristic can be used as a biometric characteristic as long as it satisfies some requirements like universality, distinctiveness, permanence and collectability. Biometric systems record personal information about identifiable individuals.

Biometric data should be understood, for the purposes of the Regulation, as any technical means of retrieval or confirmation of the identity of a natural living person using their physical, physiological or behavioural characteristics.

Some biometric data must also be considered as sensitive data and the processing sensitive biometric data is generally forbidden, but there are exceptions such as situations whenever there is a free informed consent or if someone is—physically or legally—incapable of giving consent, and there is the need of protection of his/her vital interests, among many others. Anyway, the sensitive nature of biometric data means that it can only be used in very restrictive and specific situations.

The collection of personal data must be done with a specified, explicit and legitimate purpose. Besides that, biometric data may need updating by force of natural factors such as ageing.

Processing and storage of personal data, especially biometric, must be carried out with strong security measures.

References

1. Bustard, J. (2015). The Impact of EU Privacy Legislation on Biometric System Deployment: Protecting citizens but constraining applications. IEEE Signal Processing Magazine, 32(5), 101–108.
2. Liu, Y. (2008). Identifying Legal Concerns in the Biometric Context, Journal of the International Commercial Law and Technology, 3(1), 45–54
3. Mordini E. & Rebera A. (2013). Social Factors in Ageing and Relevance to Biometrics. in M. Fairhurst (ed.), Age Factors in Biometric Processing, Springer: Berlin, 37–62