FRONTEX
EUROPEAN BORDER AND COAST GUARD AGENCY

TECHNOLOGY FORESIGHT ON BIOMETRICS FOR THE FUTURE OF TRAVEL

ANNEX II

Taxonomy of Biometric Technologies and Biometrics-Enabled Technological Systems

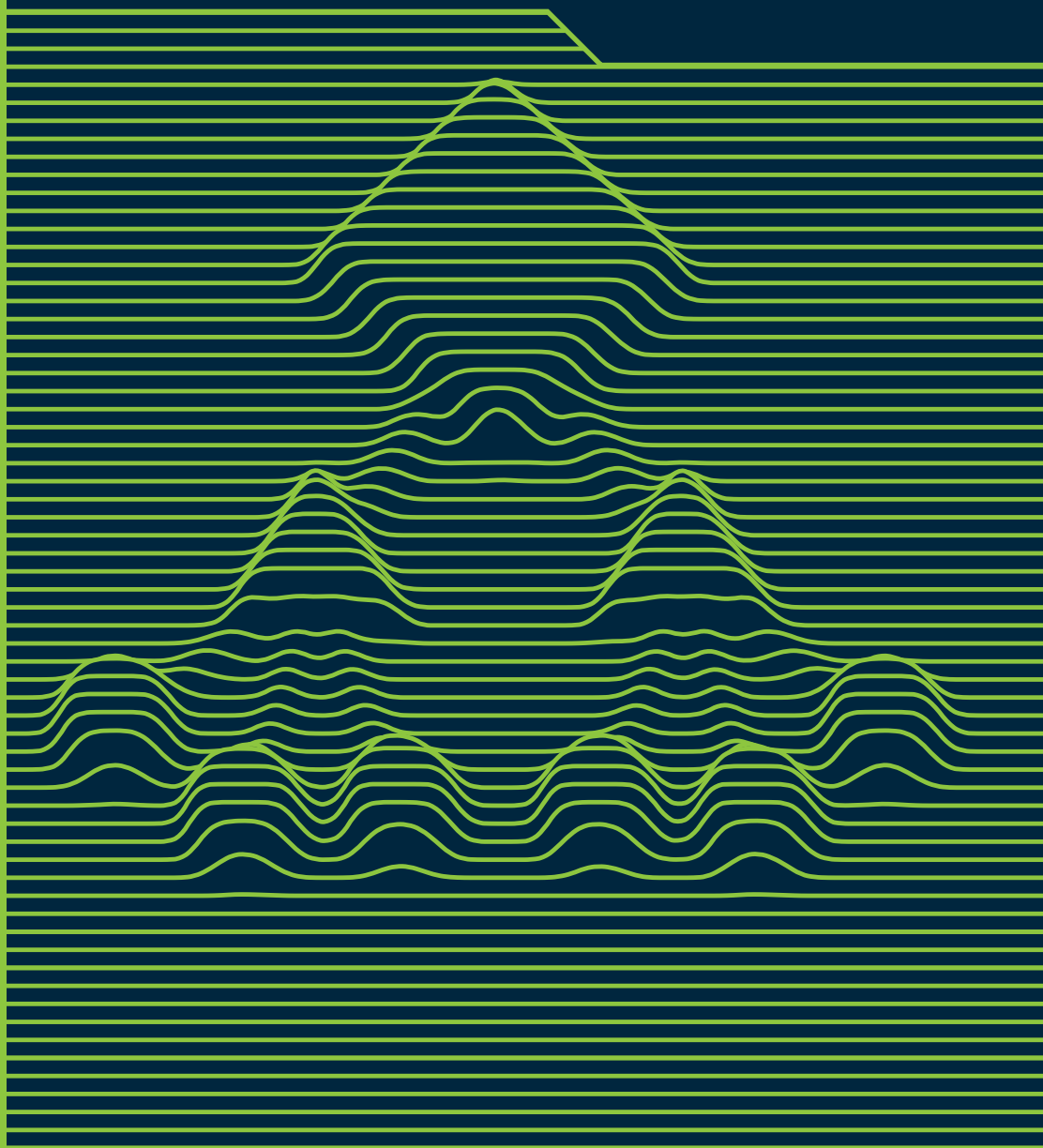
Executive Summary

Research Study

Annex I: Technology Foresight Manual

Annex II: Taxonomy of Biometric Technologies and Biometrics-Enabled Technological Systems

Annex III: Patentometric and Bibliometric Analyses of Biometric Technologies

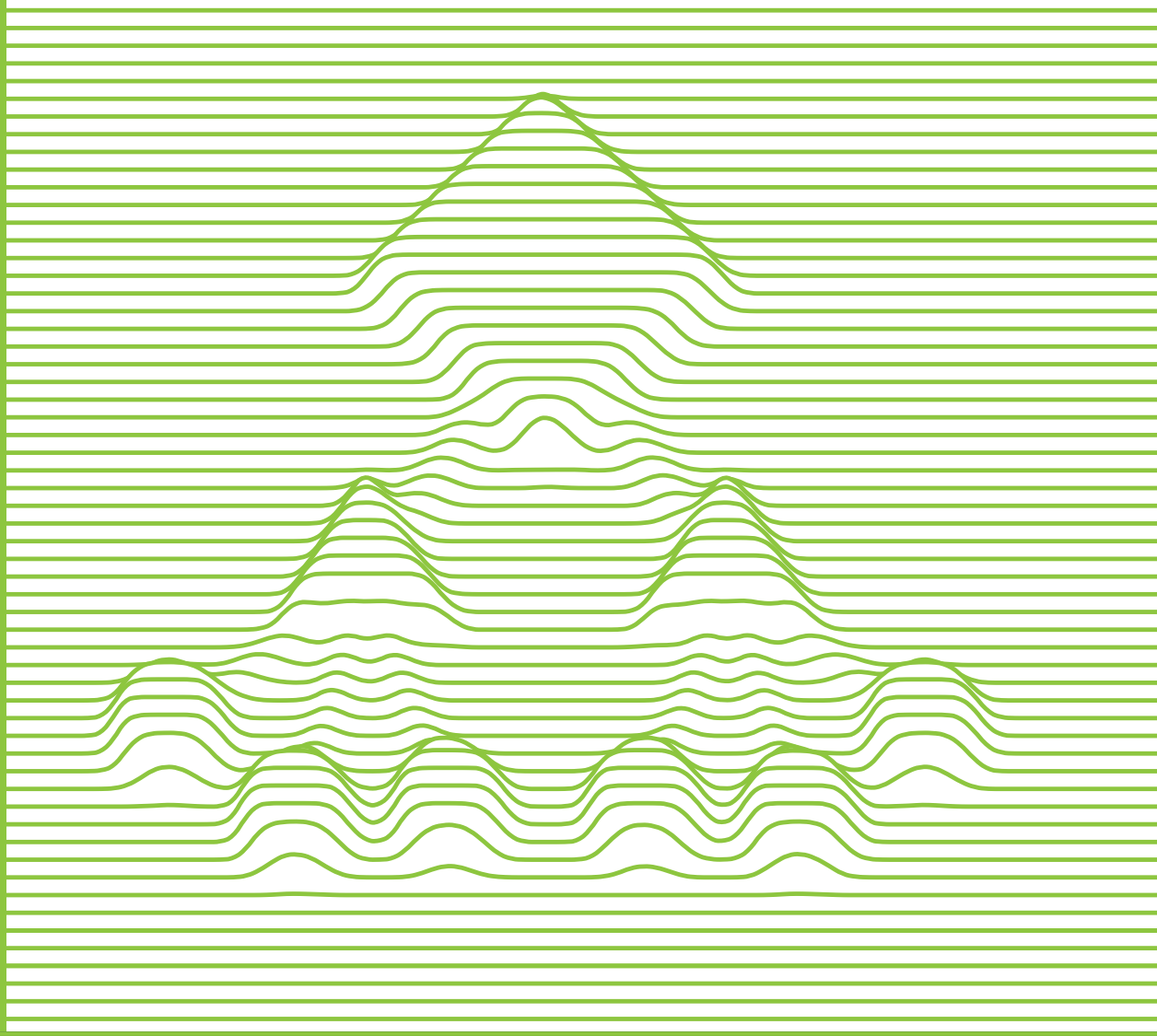


FRONTEX
EUROPEAN BORDER AND COAST GUARD AGENCY

TECHNOLOGY FORESIGHT ON BIOMETRICS FOR THE FUTURE OF TRAVEL

ANNEX II

Taxonomy of Biometric Technologies and Biometrics-Enabled Technological Systems



FRONTEX
EUROPEAN BORDER AND COAST GUARD AGENCY

Legal Disclaimer

Frontex – European Border and Coast Guard Agency
Plac Europejski 6
00-844 Warsaw, Poland
T +48 22 205 95 00
F +48 22 205 95 01

frontex@frontex.europa.eu
www.frontex.europa.eu

Warsaw, September 2021

Table of Contents

Figures and Tables #7
Abbreviations and Acronyms #8
Executive Summary #12
Introduction #14

Part 1 – Taxonomy of biometric technologies #18

1 Methodology #18
2 Taxonomy description #25
2.1 Biomolecular biometrics #26
2.1.1 DNA biometrics #26
2.1.1.1 DNA phenotyping #26
2.1.1.2 DNA profiling #27
2.1.1.3 DNA sequencing #27
2.1.1.4 Techniques for collecting DNA samples #27
2.1.2 Other biomolecular biometrics #27
2.1.2.1 Hand bacteria identification #27
2.2 Morphological biometrics #28
2.2.1 Face recognition #28
2.2.1.1 Thermal infrared face recognition #28
2.2.1.2 Near-infrared face recognition #29
2.2.1.3 Video-based face recognition #29
2.2.1.4 Image-based face recognition #29
2.2.1.5 3D face recognition #30
2.2.2 Friction ridge recognition #30
2.2.2.1 Thermal friction ridge recognition #30
2.2.2.2 Near-infrared friction ridge recognition #30
2.2.2.3 3D friction ridge recognition #30
2.2.2.4 Contactless friction ridge recognition #31
2.2.2.5 Contact-based friction ridge recognition #31
2.2.2.6 Fingerprint recognition #31
2.2.2.7 Palmprint recognition #31
2.2.2.8 Footprint recognition #31
2.2.2.9 Finger-knuckle-print recognition #32
2.2.3 Iris recognition #32
2.2.3.1 Iris recognition in the NIR spectrum #32
2.2.3.2 Iris recognition in the visible spectrum #32
2.2.3.3 Iris recognition at a distance #33
2.2.4 Vascular pattern recognition #33
2.2.4.1 Retina recognition #33
2.2.4.2 Sclera/episclera recognition #33
2.2.4.3 Finger vein recognition #34
2.2.4.4 Palm vein recognition #34
2.2.4.5 Back-of-hand vascular recognition #34
2.2.4.6 Wrist vein recognition #35

2.2.5 Physiological signal biometrics #35
2.2.5.1 Heart-rate variability #35
2.2.5.2 Electrocardiographic signals #35
2.2.5.3 Phonocardiographic signals #35
2.2.5.4 Photoplethysmographic signals #36
2.2.5.5 Encephalographic signals #36
2.2.5.6 Acoustic properties of the ear canal #36
2.2.6 Hand geometry recognition #37
2.2.6.1 Contact-based hand geometry recognition #37
2.2.6.2 Contactless hand geometry recognition #37
2.2.7 Other minor morphological biometrics #37
2.2.7.1 Dental biometrics #37
2.2.7.2 Tongueprint recognition #38
2.2.7.3 Ear print recognition #38
2.2.7.4 Periocular recognition #38
2.2.7.5 Skin texture recognition #38
2.2.7.6 Cranial suture scanning #39
2.2.7.7 Rugoscopy #39
2.2.7.8 MMW and THz wave body imaging #39
2.3 Behavioural biometrics #40
2.3.1 Keystroke recognition #40
2.3.1.1 Dynamic keystroke recognition #40
2.3.1.2 Static keystroke recognition #40
2.3.2 Gait recognition #41
2.3.2.1 Gait recognition based on video sensors #41
2.3.2.2 Gait recognition based on radar sensors #41
2.3.2.3 Gait recognition based on floor sensors #41
2.3.2.4 Gait recognition based on wearable sensors #41
2.3.3 Handwriting recognition #42
2.3.3.1 Dynamic handwriting recognition #42
2.3.3.2 Static handwriting recognition #42
2.3.4 Speaker recognition #42
2.3.4.1 Text-dependent speaker recognition #42
2.3.4.2 Text-independent speaker recognition #43
2.3.4.3 Vocal resonance recognition #43
2.3.5 Other minor behavioural biometrics #43
2.3.5.1 Complex eye movement patterns (eye-tracking) #43
2.3.5.2 Oculomotor plant characteristics #43
3 Technological clusters #44
3.1 DNA biometrics #47
3.2 Infrared face recognition #47
3.3 2D face recognition in the visible spectrum #47
3.4 3D face recognition #47
3.5 Infrared friction ridge recognition #48
3.6 3D friction ridge recognition #48
3.7 Contactless friction ridge recognition #48
3.8 Contact-based friction ridge recognition #48
3.9 Iris recognition in the NIR spectrum #48
3.10 Iris recognition in the visible spectrum #49
3.11 Iris recognition at a distance #49

3.12 Eye vein recognition #49
3.13 Hand vein recognition #49
3.14 Heart signal recognition #49
3.15 Hand geometry recognition #50
3.16 Periocular recognition #50
3.17 Keystroke recognition #50
3.18 Gait recognition #51
3.19 Handwriting recognition #51
3.20 Speaker recognition #51
4 Conclusions #52

Part 2 – Taxonomy of biometrics-enabled technological systems #53

5 Methodology #53
6 Taxonomy description #53
6.1 Self-service systems #56
6.1.1 E-gates #56
6.1.2 Corridors #57
6.1.3 Kiosks #57
6.1.4 Remote on-boarding systems #57
6.2 Identity document readers and verification sub-systems #58
6.2.1 Integrated document readers/scanners #58
6.2.2 Desktop document readers/scanners #58
6.2.3 Forensic document readers/scanners #58
6.2.4 Handheld document readers/scanners #59
6.2.5 Holographic document readers/scanners #59
6.2.6 Document analysis software #59
6.3 Full-body scanning systems #60
6.3.1 Scanners using mm or THz waves #60
6.3.2 Scanners using radar wavebands #60
6.3.3 Systems using quantum sensors #60
6.3.4 Holographic scanning systems #61
6.3.5 Camera-based scanning systems #61
6.4 Systems based on personal devices #62
6.4.1 Smartphone device biometrics #62
6.4.2 Handheld device biometrics #62
6.4.3 Wearable biometric technologies #62
6.4.4 Microchip biometric implants #62
6.5 Movable systems #63
6.5.1 Mobile (non-autonomous) checkpoints #63
6.5.2 Semi-autonomous robotic systems #63
6.5.3 Autonomous robotic systems #63
6.5.4 Systems for the seamless recognition of persons in transport #63
6.6 Large-scale IT systems that deploy biometric comparison components #64
6.6.1 Traveller information and entry-exit registration systems #64
6.6.2 Visa and travel authorisation systems #64
6.6.3 Biometric central databases for border control and law enforcement #54

6.7 Virtual traveller identification schemes for biometrics-enabled technological systems **#66**
6.7.1 ICAO "Digital Travel Credential" (DTC) **#66**
6.7.2 IATA "Travel Pass" **#66**
6.7.3 WEF "Known Traveller Digital Identity" (KTDI) **#66**
6.7.4 Proprietary schemes **#66**
6.7.5 Digital Trust Frameworks **#67**
7 Conclusions **#68**

Figures and Tables

Figure 1: Workflow for constructing the taxonomy of biometric technologies. **#22**

Figure 2: Graphic representation of the taxonomy of biometric technologies. **#25**

Figure 3: Graphic representation of the taxonomy of biometrics-enabled technological systems. **#55**

Table 1: Outline of the results of the Patentometric and Bibliometric Analyses of 20 technological clusters, showing the significance of inventive activity (in terms of number of filed patent families, filed patents and scientific papers) and the inferred stage in the technology lifecycle. The clusters are sorted in descending order according to the number of patent families. The number in the left-hand column is the ordinal number associated with each of the clusters throughout the study. **#24**

Table 2: List of 20 technological clusters and corresponding biometric technologies belonging to the third level of the taxonomy, which were considered for conducting Patentometric and Bibliometric Analyses and used in the various phases of the Tech Foresight on Biometrics. **#45**

Abbreviations and Acronyms

Abbreviation / Acronym	Definition
2D	Two-dimensional
3D	Three-dimensional
ABC	Automated Border Control
API	Advance Passenger Information Information concerning the passengers whom carriers will transport to an authorised border crossing point, through which these persons will enter the territory of a Schengen Member State, which carriers are obliged to transmit, by end of check-in, at the request of the authorities responsible for carrying out checks on persons at external borders Derived from Art. 3 of Council Directive 2004/82/EC (Directive on the obligation of carriers to communicate passenger data)
BCP	Border Crossing Point, as defined in point 8 of Article 2 of Regulation (EU) 2016/399 (Schengen Borders Code)
CBP	US Customs and Borders Protection
DNA	Deoxyribonucleic acid
DOCDB	DOCument DataBase DOCDB is the European Patent Office's master documentation database with worldwide coverage. It contains bibliographic data, abstracts, citations and the DOCDB simple patent family, but no full text or images. The DOCDB simple patent family is defined by the European Patent Office as *"a collection of patent documents that are considered to cover a single invention. The technical content covered by the applications is considered to be identical"* (https://www.epo.org/searching-for-patents/helpful-resources/first-time-here/patent-families/docdb.html)
DTC	ICAO Digital Travel Credential Travel Credentials issued in a digital format, intended to temporarily or permanently substitute a conventional passport with a digital representation of the traveller's identity, which can in turn be validated using the travel document issuing authority's public key infrastructure (see ICAO publication *"Guiding Core Principles for the Development of Digital Travel Credential"*)
EC	European Commission
ECG	Electrocardiographic
ECRIS-TCN	European Criminal Records Information System – Third Country Nationals. Currently under development, ECRIS-TCN will be a centralised system that allows Member State authorities to identify which other Member State(s) hold criminal records on third country nationals or stateless persons Established by Regulation (EU) 2019/816
EEA	European Economic Area
EEG	Electroencephalographic
EES	Entry-Exit System Currently under development, the EES will electronically register the time and place of the entry and exit from the EU of third country nationals as well as calculate the duration of their authorised stay. It will replace the obligation to stamp the passports of third country nationals. Established by Regulation (EU) 2017/2226

Abbreviation / Acronym	Definition
EIS	Europol Information System
eMRTD	Electronic Machine Readable Travel Document
EPO	European Patent Office
ESTA	US Electronic System for Travel Authorisation
ETA	Canadian Electronic Travel Authorisation
ETIAS	European Travel Information and Authorisation System Currently under development, the ETIAS will be a pre-travel authorisation system for visa-exempt travellers. Its key function is to verify whether a third country national meets entry requirements before travelling to the Schengen Area Established by Regulations (EU) 2018/1240 and (EU) 2018/1241
EU	European Union
eu-LISA	European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice Governed by Regulation (EU) 2018/1726
Eurodac	European Asylum Dactyloscopy Database European database that collects and processes the digitised fingerprints of asylum seekers and irregular migrants. It helps determine which Member State is responsible for examining asylum applications Established by Regulation (EU) No 603/2013
Europol	European Union Agency for Law Enforcement Cooperation Governed by Regulation (EU) 2016/794
FKP	Finger-Knuckle-Print
Frontex	The European Border and Coast Guard Agency Governed by Regulation (EU) 2019/1896
Frontex Representatives	Frontex staff who participated in the *Tech Foresight on Biometrics*
GHz	Gigahertz
Group of Experts	Subject-matter experts representative of stakeholders selected to participate in the consultation and collective intelligence activities conducted within the framework of the *Tech Foresight on Biometrics*, such as the workshops and the *Delphi Survey*. This also included members of the Research Team and Frontex Representatives
HRV	Heart-Rate Variability
IATA	International Air Transport Association
ICAO	International Civil Aviation Organization
ID	Identity Document
IEC	International Electrotechnical Commission
IR	Infrared
ISO	International Organization for Standardization
IT	Information Technology
KTDI	Known Traveller Digital Identity
KYC	Know Your Customer
LWIR	Long-Wavelength Infrared; electromagnetic radiation with 8-15 μm wavelength

Abbreviation / Acronym	Definition
MBC	Manual Border Control
MRTD	Machine Readable Travel Document
MMW	Millimetre Waves; electromagnetic radiation with 1-10 mm wavelength
MR	Motion Recording
MV	Machine Vision
MWIR	Medium-Wavelength Infrared; electromagnetic radiation with 3-8 µm wavelength
NEXTT	New Experience Travel Technologies (https://www.nextt.aero/en/)
NIR	Near-Infrared; electromagnetic radiation with 0.78-1.0 µm wavelength
NLP	Natural Language Processing
NZeTA	New Zealand Electronic Travel Authority
OPC	Oculomotor Plant Characteristics
OpenAIRE	Open Access Infrastructure for Research in Europe (https://www.openaire.eu/)
PCG	Phonocardiography
PDA	Personal Digital Assistant
PII	Personally Identifiable Information. Any information related to an identifiable person
PIP	Proximal Interphalangeal
PNR	Passenger Name Record PNR data are unverified information provided by passengers and collected by air carriers to enable the reservation and check-in processes Regulated by Directive (EU) 2016/681
PPG	Photoplethysmography
Research Team	Employees of the of the Contractor selected by Frontex to conduct the *Technology Foresight on Biometrics for the Future of Travel* (Steinbeis 2i GmbH) and its Subcontractors (4CF Sp. z o.o., Erre Quadro S.r.l. and the Instytut Optoelektroniki – Wojskowa Akademia Techniczna), who jointly provided expertise in the following fields: • Project Management • Strategic Technology Foresight • Biometrics for border control systems • Smart and Autonomous Systems • Systems Engineering for border control
Research Team Experts	Members of the Research Team who provided subject-matter expertise in the following disciplines: • Biometrics for border control systems • Smart and Autonomous Systems • Systems Engineering for border control
Schengen Borders Code	Regulation (EC) No 562/2006 of the European Parliament and of the Council of 15 March 2006 establishing a Community Code on the rules governing the movement of persons across borders
SIS	Schengen Information System Supports the exchange of information on persons and objects between the national police, border control, customs, visa and judicial authorities. It acts as a compensatory measure for the removal of border checks in the Schengen Area Established by Regulations (EU) 2018/1860, 2018/1861 and 2018/1862
SMW	Sub-Millimetre Waves; electromagnetic radiation with 1 mm – 0.01 mm wavelength

Abbreviation / Acronym	Definition
SSS	Self-Service System
SWIR	Short-Wavelength Infrared; electromagnetic radiation with 1-3 µm wavelength
Tech Foresight on Biometrics	Technology Foresight on Biometrics for the Future of Travel
TF	Technology Foresight
THz	Terahertz Terahertz waves are electromagnetic radiation with 1 mm – 0.01 mm wavelength
µm	Micrometre
UV	Ultraviolet
VIS	Visa Information System VIS supports the implementation of the EU's common visa policy and facilitates border checks. The system enables dedicated national authorities to enter and consult data, including biometrics, for short-stay visas to the Schengen Area Governed by Regulation (EC) No 767/2008
WEF	World Economic Forum
WTTC	World Travel and Tourism Council
WS	Wearable Sensor

Executive Summary

Biometrics is a broad and diverse scientific field, where physics, engineering, medicine, psychology and more come into contact. Having to deal with such a level of heterogeneity, Frontex has highlighted the importance of categorising the main biometric technologies with potential to find applications in the operational fields of interest for the EBCG community.

Starting from Frontex's requirements, the Research Team designed two different taxonomies, mapping respectively biometric technologies (e.g. *Fingerprint recognition* and *Face recognition*) and biometrics-enabled technological systems (e.g. *e-gates* and *autonomous robotic systems*). To deal with the breadth and complexity of the biometrics domain, as well as to focus on biometric technologies per se, the two taxonomies were designed by following two distinct approaches, featuring different levels of thoroughness and complexity, which are discussed in the two parts of this report.

Together, the two taxonomies represent one of the results of the *State-of-the-Art Review* step in the *Tech Foresight on Biometrics,* and an essential input to the subsequent phases of the adopted Technology Foresight methodology. The taxonomy of biometric technologies, in particular, was used to extract a set of technological clusters on which *Patentometric and Bibliometric Analyses* were conducted and which represented the input to the successive steps in the *Filtering the Results*, *Deep Analysis* and *Mapping Capabilities* phases of the Technology Foresight methodology.

After describing the methodologies we followed, this document reports the results of a systematic categorisation analysis conducted on the set of identified biometric technologies and biometrics-enabled technological systems, for which the scope was limited to applications in border checks, biometric recognition or access control. Technologies and systems finding exclusive application in border surveillance were considered outside the scope of this work, as were solutions aimed at using biometrics for emotion and behaviour detection.

The **taxonomy of biometric technologies** was developed through an iterative process that started from a list of research areas in biometrics, identified *ab initio* by the Research Team. The process then relied on the analysis of the patents gathered from a proprietary database (derived from the EPO database) and the scientific literature collected from OpenAIRE for the scanning of state-of-the-art documentation, the extraction of suitable terminology and the description of technologies. Such analysis was performed through NLP-based automatic tools and the strong involvement of the Research Team Experts. Transverse knowledge is, in fact, necessary to design proper and comprehensive taxonomies. Patents, aiming at describing and protecting inventions, represent a valuable and accessible source of information from which both known and novel technologies, techniques and/or methodologies may be retrieved. However, due to their ontological characteristics, patent databases may not contain sufficient information for developing comprehensive taxonomies. Therefore, to lower the risks arising from patents' limitations, scientific publications and Research Team Experts' knowledge also had to be considered. This approach led to the creation of a three-level taxonomy tree formed by three biometric technological macro-areas, 14 biometric technological fields

and 57 specific biometric technologies and modalities. A definition is provided in this document for every node and leaf of the tree.

The **taxonomy of biometrics-enabled technological systems** was created starting from a set of technological solutions of potential interest for the research study. Such a set was first expanded and then consolidated and validated by exploiting the knowledge and expertise of the Research Team Experts. The outcome of such an approach is represented by a two-level taxonomy tree formed by seven macro-areas and 31 families of technological systems. A definition was provided in this document for every node and leaf of the tree.

In conclusion, through the present work, the Research Team was able to logically map the biometrics realm from the point of view of the basic technologies and technological systems, thus fulfilling the objective of the research study to establish a common understanding of the biometrics domain and create a reference document that could be used in research and innovation activities. The application of NLP methodologies for the analysis of patents and scientific papers was confirmed as a useful practice for intercepting uncommon or niche technologies (e.g. rugoscopy and hand bacteria identification), which were included in the taxonomy of biometric technologies together with the most known ones (e.g. face recognition and iris recognition). It is worth pointing out that due to the need to limit the complexity of the taxonomy, and in general of the overall Research Study, to a manageable level, this work did not consider the mainstream biometrics-enabling and/or cross-cutting scientific and technological fields, such as: artificial intelligence in biometric systems; privacy-preserving and privacy-enhancement solutions for the security of identity; techniques for biometric database construction; document verification and fraud detection; manipulation attack detection and protection against attempts/techniques to falsify biometrics. However, a brief overview of these topics can be found in the Research Study.

Introduction

This document reports the results of a categorisation analysis conducted on a set of biometric technologies and biometrics-enabled technological systems relevant to border checks, whose outcome is represented by:

- a taxonomy of biometric technologies, covered in Part 1,
- a taxonomy of biometrics-enabled technological systems, covered in Part 2.

The term *taxonomy* is a compound word formed by the Greek terms *τάξις* (*taxis*, meaning 'order' or 'arrangement') and *νόμος* (*nomos*, meaning 'law' or 'science') and may be defined as the practice and science of categorisation or classification.[1] The classified units forming a taxonomy are called *taxa*. A taxonomy is a scheme that is generally organised in a hierarchical order of *subtypes* and *supertypes*. A popular example of taxonomy is the one developed by Sneath and Sokal that establishes a classification of organisms based on their similarities.[2] Taxonomies are generally presented as hierarchies where each level is a subset of the level above it. For example, a biology taxonomy would probably include concepts such as *mammals*, as a subset of *animals*, and *dogs* or *cats*, representing subsets of *mammals*.[3]

As explained in Annex I – Technology Foresight Manual, within the Technology Foresight methodology the *State-of-the-Art Review* is executed in two consecutive steps:

1. *Identification of the main areas of research;*
2. *Development of a technological taxonomy.*

The results of Step 1 are reported in Section 3.1 of the Research Study and represented the starting point of the analysis as explained in Chapter 1 of this report.

The work was performed in accordance with the requirements expressed in the *Terms of Reference*[4] for the Research Study, Section 3.1 – Objectives of the assignment, namely:

- *"Comprehensive Technology Taxonomy: Develop a thorough, extensive and detailed technology taxonomy for future biometrics and biometrics-enabled technological systems. A technology taxonomy is understood as the mapping of all the related research topics, sub-topics, and technologies potential to find applications in operational fields of interest for the EBCG community in a categorical and logical manner. The goal is to establish a common understanding and create a reference document, which will be used by Frontex in research and innovation activities".*

1 M. Schatten, M. Baca and K. Rabuzin, "A Taxonomy of Biometric Methods", ITI 2008 – 30th International Conference on Information Technology Interfaces, 2008.

2 P. H. A. Sneath, R. R. Sokal and W. H. Freeman, "Numerical Taxonomy. The Principles and Practice of Numerical Classification", Systematic Zoology, no. 24, pp. 263-268, 1975.

3 R. J. Brachman, "What IS-A Is and Isn't: An Analysis of Taxonomic Links in Semantic Networks", Computer, vol. 16, no. 10, pp. 30-36, 1983.

4 See https://etendering.ted.europa.eu/cft/cft-documents.html?cftId=6982

Considering the breadth and technological complexity of the biometrics domain, and the broad and transversal knowledge needed to create comprehensive taxonomies, two approaches were followed to construct the two taxonomies:

- The methodology used to develop the taxonomy of biometric technologies focused on the analysis of technical and scientific documentation, which were assumed to contain all necessary knowledge. More specifically, patents and scientific papers were considered. Given the significant volume of literature on biometric technologies, automatic tools[5] were used to (a) analyse the textual content of patents and scientific papers, respectively retrieved from the patent database[6] and the *OpenAIRE*[7] database and (b) collect suitable terminology for creating the taxonomy. The Research Team Experts were tasked with amending and validating the information gathered.
- The taxonomy of biometrics-enabled technological systems was developed primarily through desk research conducted by the Research Team Experts.

Moreover, the general structure and the content of both taxonomies were devised to allow a common understanding of the biometrics domain and to make sure they could be used by Frontex as reference documents in its research and innovation initiatives.

In addition to the knowledge requirements, a good definition of the scope and boundaries of the work is essential for a well-designed taxonomy construction process, because it helps the analysts to focus on the target. Therefore, the scope of the categorisation analysis was limited to those biometric technologies and biometrics-enabled technological systems which could find application in ***border checks***, ***biometric recognition***, or ***access control***. Additional constraints were imposed by **not considering *border surveillance* or *emotion and behaviour detection*** within the scope of the taxonomy.[8] Consequently, while constructing the taxonomy of biometric technologies, a specific technology was considered within the scope of interest if and only if at least one reference to its application in at least one field from border checks, access control, or biometric recognition was found during the automated analysis of patents and/or papers. A biometric technology was also taken into consideration if a single 'in-scope' application was known to the Research Team Experts.

Furthermore, due to the need to limit the complexity of the taxonomy, and of the overall Research Study, to a manageable level, the mainstream biometrics-enabling and/or cross-cutting scientific and technological fields were not considered within the scope of the taxonomical categorisation. These include artificial intelligence in biometric systems; privacy-preserving and privacy-enhancement solutions for the security of identity; tech-

5 Erre Quadro's proprietary tools, the Domain Terminology Extractor, Smart Ranker and Weighted Clusterer. For more information, see Annex I – Technology Foresight Manual.

6 Erre Quadro's proprietary patent database based on the Patstat Service provided by the European Patent Office, see Chapter 1.

7 OpenAIRE (Open Access Infrastructure for Research in Europe 2020, https://www.openaire.eu/)) is a European platform whose mission is to provide unlimited, barrier free and open access to research outputs financed by public funding in Europe.

8 Although not considered within the scope of the taxonomy, behaviour detection was in general considered within the scope of the research study, but limited to solutions aimed at the detection of people in need of assistance or special care (e.g. not moving for a long period of time, disoriented children or elderly people).

niques for biometric database construction; document verification and fraud detection; manipulation attack detection and protection against attempts/techniques to falsify biometrics. However, a brief overview of these topics can be found in the Research Study.

The retrieved set of biometric technologies and biometrics-enabled technological systems were categorised and included in two different taxonomy trees, made up respectively of:

- a three-level structure composed of:
  - the ***first level***, consisting of three biometrics macro-areas;
  - the ***second level,*** including 14 technological fields;
  - the ***third level,*** comprising 57 biometric technologies and modalities.
- a two-level structure composed of:
  - the ***first level***, consisting of a set of seven groups;
  - the ***second level***, including 31 categories.

Once created, the taxonomy of biometric technologies was used to identify a set of 20 biometric technological clusters (see Chapter 3) on which *Patentometric and Bibliometric Analyses*[9] were conducted as part of the *Insight Hunt* phase of the Technology Foresight methodology.[10] Since not all the identified technological clusters have the same potential relevance for border check operations, a multi-level assessment was performed with the support of the Group of Experts through a *Delphi Survey*. This consultation was part of the *Filtering the Results* phase of the Technology Foresight methodology and allowed us to shortlist the five most promising clusters suitable for the *Deep Analysis* and the *Mapping Capabilities* phases, where technological roadmaps were finally originated for those clusters and capability readiness analyses were conducted on them.

The taxonomy of biometrics-enabled technological systems played an essential role in guiding the development of roadmaps,[11] where a specific layer was included to envisage future products and systems that might emerge exploiting the selected technological clusters.

This report is divided into two parts:

- **Part 1 – Taxonomy of biometric technologies**. This part of the document is structured in four chapters as follows:
  - *Chapter 1 – Methodology*
  - *Chapter 2 – Taxonomy description*, organised in sections and paragraphs that follow the same hierarchical structure of the taxonomy
  - *Chapter 3 – Technological clusters*
  - *Chapter 4 – Conclusions* includes a set of final considerations about the outcomes of the taxonomical categorisation
- **Part 2 – Taxonomy of biometrics-enabled technological systems**. This part of the document is structured in three chapters as follows:
  - *Chapter 5 – Methodology*

9 See Annex III – Patentometric and Bibliometric Analyses of Biometric Technologies.

10 See Annex I – Technology Foresight Manual, Sections 2.1 and 2.2.

11 See the Research Study, Chapter 9.

- *Chapter 6 – Taxonomy description*, organised in sections and paragraphs that follow the same hierarchical structure of the taxonomy
- *Chapter 7 – Conclusions* provides a set of final considerations about the outcomes of the taxonomical categorisation

Should the reader need a description of basic concepts regarding biometrics, EU border management or patents, or clarifications concerning the meaning of some of the terms used within this document, the Research Study contains, in Appendix 6, a *Glossary of basic terms and definitions* that can be of support in this regard.

Part 1 – Taxonomy of biometric technologies

1. Methodology

This chapter describes in detail the methodology devised by the Research Team to construct the taxonomy through a systematic analysis and categorisation process on the basis of datasets of patents and scientific papers.

The taxonomy of biometric technologies was iteratively created starting from a preliminary list of areas of research potentially relevant to the field of biometrics for border checks, originated, in the initial phases of the Tech Foresight on Biometrics, by the Research Team Experts. In total, 46 main areas of research were identified and preliminarily classified into three categories: applications, biometric technologies and biometrics-enabling technologies (hereinafter also referred to as "transversal scientific fields" or "cross-cutting technologies"). The complete set of results regarding the identification of the areas of research is reported in the Research Study, Section 3.1.

The taxonomy development process relied on a systematic analysis of patents and scientific papers for the retrieval of suitable terminology and descriptions of technologies. Patents, represent a powerful and freely accessible source of information where field-specific technologies, techniques and/or methodologies can be found. Patents represent a privileged source of technical information for several reasons:

- 80% of the technical information contained in patents is not available elsewhere.[12, 13]
- Patents precede market launch as well as scientific publications since the latter may compromise the patentability of inventions.
- Patents entail significant costs for companies, and thus are only filed to protect innovations considered crucial to an enterprise, i.e. innovations worthy of investments likely to be put into production. Thus, the correlation between patents and the economic impact of the innovations they describe is much more direct than that of research papers.
- Patents describe innovative and emerging technologies that are often characterised by a higher level of maturity and feasibility than those presented in papers.
- Finally, patent data are publicly available and are easy to find for any sector.

Scientific publications may also describe cutting edge technologies, but:

- Usually, in high-tech sectors, fewer technologies are discussed in papers than in patents.

12 M. W. Kütt, and M. Schmiemann, "Quick Scan: a novelty search service in the framework of Euro-R&D programmes", World Patent Information, vol. 20, no. 2, pp. 146-147, 1998.

13 P.J. Terragno, "Patents as Technical Literature", IEEE Transaction on Professional Communication, vol. 22, no. 2, pp. 101-104, 1979.

- Technologies that are reported in papers may be less feasible and advantageous from an industrial manufacturing point of view, or may never enter the market at all.
- Although relevant, some technical information might be considered unsuitable for publication.
- The number of papers on a specific technology does not necessarily correlate with its relevance for the economy.
- Freely available information in databases of non-open-access scientific journals is normally limited to titles and abstracts of papers, and the cost for access to a comprehensive database can be very high.
- The available search engines often have severe limitations (e.g. in the *Scopus*[14] database, the search field is limited to 250 characters; no advanced search functions are available and the user cannot download more than 100 articles at a time).

A proprietary patents database,[15] based on the *Patstat Service*[16] provided by the European Patent Office and containing more than 120 million patents, was used as the data source for patent analysis. However, it must be pointed out that patent databases do not contain an exhaustive representation of all existing technologies. Many inventions and innovations are, in fact, not patented. One reason is the strict criteria that inventions must satisfy to be granted a patent, whose interpretation differs over time and across countries, resulting in long and delicate application processes. Furthermore, patenting is not the only possible protection mechanism for innovation. Other important and powerful protection mechanisms include: trade secrets (whose related inventions and innovations could not be discovered using any other source of information); speedy product development; the complexity of product design; control of distinguishing capabilities. This means that not all technologies and innovations will find a place within the patent universe. Furthermore, due to the duration and mechanisms of the application process, patent databases do not exhaustively cover the 18 months[17] preceding the searches (the so-called *blind period*, during which applications are secret).

That being said, the ontological characteristics and the structure of patents (where both the content and the inner organisation of documents are standardised in many ways) allow a reliable and scalable NLP approach to the analysis. Furthermore, even if a particular methodology or technology is not the central object of any invention, thus not being patented in any way, it could still be cited (and therefore intercepted) or referred to within the description of other inventions. This way, the risk of failure in intercepting specific technologies or techniques is low.

However, to lower the risks arising from patents' characteristics, scientific publications extracted from the *OpenAIRE* database were also considered.

14 https://www.scopus.com/

15 Owned by Erre Quadro, described in more detail in Annex III – Patentometric and Bibliometric Analyses of Biometric Technologies – Section 3.1.

16 https://www.epo.org/searching-for-patents/business/patstat.html

17 It must be highlighted that the Erre Quadro patent database used for the present work was updated to the first quarter of 2021. Thus, the part of the database concerning the period after the first half of 2019 is obviously incomplete.

In the light of the above, to build the taxonomy of biometric technologies, an iterative process was followed and fine-tuned, including the use of specialised software tools as well as frequent collaboration and interaction with both the Research Team Experts and Frontex, thus allowing a continuous alignment on the objectives and the outcomes.

The workflow is shown in Figure 1 and comprises the following steps:

1. *Research areas defined.* The identification of the main areas of research in the Technology Foresight process allowed the creation of the preliminary knowledge and terminology used to query databases of patents and papers.
2. *Terminology construction.* In this step, the terminology for querying the patents and papers databases was created based on a set of keywords. In the first iteration of the process, the preliminary list of research areas compiled in Step 1 was used to extract the first list of biometric technologies.[18] These were directly inputted to Step 6, *Technology validation*, to obtain the first set of keywords for designing search queries. In subsequent iterations, the set of keywords for terminology construction was the one created in Step 6.
3. *Extraction of publications and patents from databases.* Sets of patents and papers were retrieved from the databases through queries which used the terminology created in the previous step.
4. *Extraction of technologies.* The datasets of patents and papers obtained in the previous step were filtered and analysed using the *Domain Terminology Extractor* tool[19] to expand and validate the list of keywords used in Step 2, as well as to extract terms that could be used to describe biometric technologies, techniques and modalities. Technical literature (especially patents) is often full of synonyms and/or multiple ways to describe a single concept.
5. *Desk research.* Concurrently to the automatic extraction of patent and paper sets, brief desk research in industrial literature, online sources and scientific publications was also performed to look for additional terminology and omitted biometric technologies. This step was also conducted to validate possible unfamiliar terms extracted from patents and papers as well as to verify the possible relationships between the technologies encountered. Such assessments were necessary for the initial construction of the taxonomy.
6. *Validation of technologies.* Whenever an additional biometric technology was extracted in Steps 4 and 5, a validation step occurred, consisting of searching in patents or scientific literature for at least one application falling within the scope of the research study. More specifically, a biometric technology or modality was validated if, and only if, at least a relevant application in at least one of the relevant fields (biometric recognition, border checks and/or access control) was described in the retrieved documents. Feedback from the Research Team Experts was also used to corroborate the results and to support drafting the technical descriptions of the validated technologies. Finally, the outcomes of this step consisted in:
   a) validated biometric technologies suitable for inclusion in the taxonomy (input to Step 7);

18 As mentioned in the Introduction, the work described in Part 1 focused on biometric technologies only.

19 Proprietary tool of Erre Quadro. For more information on its functionalities, see Annex I – Technology Foresight Manual – Chapter 19

b) a set of keywords for the identification of other relevant biometric technologies, fed-back to Step 2 to extend and refine the search queries.

7. *Preliminary taxonomy creation*. Once a significant number of technologies were retrieved and validated, a preliminary taxonomy was created. The previous steps (starting from Step 2) were then iterated. This highly iterative process was performed to ensure that no relevant in-scope biometric technologies were missing from the taxonomy. However, it must be highlighted that because biometrics is a broad, complex and expanding domain, it cannot be ruled out that minor, unusual or niche technologies might still have eluded the Research Team Experts' and the automatic tools' grasp.

8. *Taxonomy consolidation*. Once no additional value was created by reiterating Steps 2-7 (meaning that no additional technologies, relationships between the technologies or keywords were found), the preliminary taxonomy was consolidated within this step.

9. *Taxonomy validation*. The taxonomy was reviewed and validated in close collaboration with Frontex before releasing the final version.

10. *Taxonomy of biometric technologies*. The taxonomy was organised into three hierarchical levels:

- The ***first level,*** consisting of three macro-areas: biomolecular biometrics, morphological biometrics and behavioural biometrics;
- The ***second level,*** including 14 technological fields belonging to the three macro-areas;
- The ***third level,*** comprising all 57 specific biometric recognition or acquisition technologies and modalities (five biomolecular, 39 morphological and 13 behavioural), each representing a narrow family of similar applications within a technological field.

A graphical representation of the taxonomy of biometric technologies is reported in Figure 2, while a brief description of all the components of the taxonomy (macro-areas, technological fields and specific technologies/modalities) can be found in the next section.

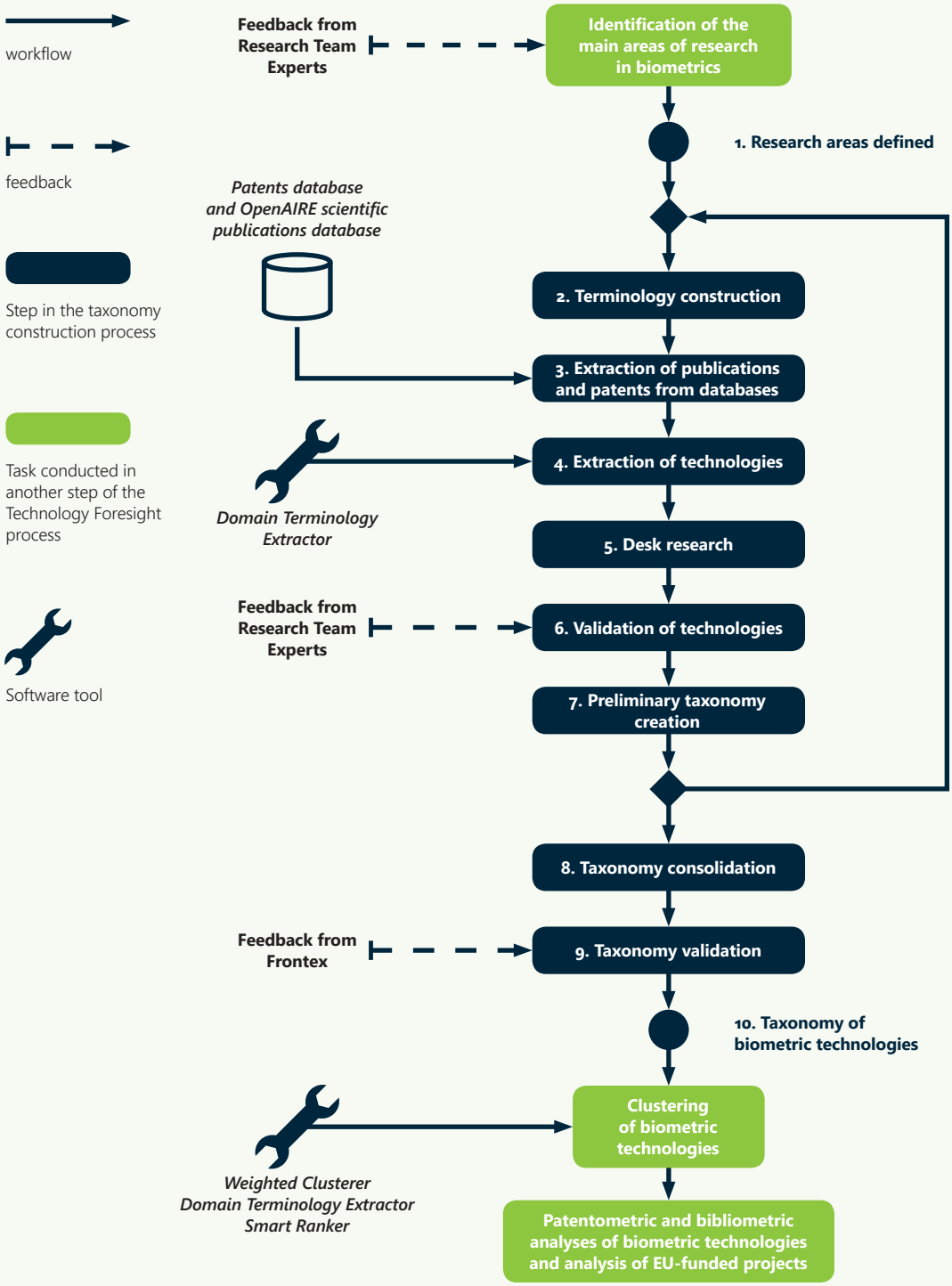


Figure 1: *Workflow for constructing the taxonomy of biometric technologies.*

The workflow in Figure 1 shows that the creation of the taxonomy is followed by two subsequent tasks in the Technology Foresight process: *Clustering of biometric technologies* and *Patentometric and Bibliometric Analyses of Biometric Technologies*.

Within the task of *Clustering of biometric technologies*, the third-level technologies were grouped into a set of 20 technological clusters, each representing a level of abstraction defined in order to enable *Patentometric and Bibliometric Analyses* as well as to assure

the usability of the taxonomy in the successive phases of the *Technology Foresight on Biometrics* (as briefly described in the Introduction). Preliminary identification of the clusters was made by using the *Weighted Clusterer* tool,[20] which thanks to an ML algorithm is able to interpret the content of document sets supporting tasks where documents, as well as technologies or technological applications, have to be categorised.[21] The final identification of the clusters (described in detail in Chapter 3) was based on the **numerosity of the associated documental sets** (patents and scientific publications), the **technological affinity** between taxonomical third-level technologies and the **relevance in target applications** (border checks, biometric recognition, and access control).

Within the following task of *Patentometric and Bibliometric Analyses of Biometric Technologies,* those analyses were conducted on the 20 clusters.[22] Fourteen of the 57 biometric technologies composing the third level of the taxonomy were neither included in the 20 technological clusters, nor considered when performing *Patentometric and Bibliometric Analyses*. This was because either the datasets of patents and scientific publications for this group of technologies were too narrow for quantitative analyses, or the technologies per se were not sufficiently relevant to the domain of border checks.

One of the most significant outcomes of this task is Table 1,[23] where for each cluster the significance of inventive activity (in terms of number of filed *patent families*,[24], filed patents and published scientific papers) is shown, along with the stage in technology lifecycle inferred based on *Altshuller's Theory of Inventive Problem Solving*.[25]

Some succinct considerations are reported here:

- More than half (13) of the clusters were assessed to be in their ***maturity*** stage. Maturity does not imply a rapid decline, since inventive activity may still occur, but usually with a lower rate than in past years. **These are technologies that are ready to be used.**
- Five clusters were assessed as **growing** fields, where *performances* and *profitability*[26] are presumably increasing relatively quickly.
- Two clusters were assessed as being in the **childhood** stage of their lifecycle. These are fields that are expected to grow in the future.
- Three clusters were assessed as being of minor relevance within the scope of the research study.

20 Proprietary tool of Erre Quadro. For more information on the functionalities of the Weighted Clusterer see Annex I – Technology Foresight Manual – Chapter 21.

21 For more details on how this tool was used to analyse technological clusters, please refer to Annex III – Patentometric and Bibliometric Analyses of Biometric Technologies.

22 Annex III – Patentometric and Bibliometric Analyses of Biometric Technologies contains the entire set of results achieved by the execution of this task.

23 This table is an extract of Table 84 in Annex III – Patentometric and Bibliometric Analyses of Biometric Technologies – Section 5.21.

24 Patent families are intended as DOCDB patent families as defined in Abbreviations and Acronyms.

25 G. Altshuller and A. Williams, "Creativity as an exact science", New York: Gordon and Breach Science Publishers, 1984.

26 See Annex III – Patentometric and Bibliometric Analyses of Biometric Technologies – Section 2.2, for a definition of these terms.

Table 1: *Outline of the results of the Patentometric and Bibliometric Analyses of 20 technological clusters, showing the significance of inventive activity (in terms of number of filed patent families, filed patents and scientific papers) and the inferred stage in the technology lifecycle. The clusters are sorted in descending order according to the number of patent families. The number in the left-hand column is the ordinal number associated with each of the clusters throughout the study.*

#	Technological clusters	Patent families	Patents	Papers	Stage in technology lifecycle
20	**Speaker recognition**	1,760	7,468	848	Maturity
8	**Contact-based friction ridge recognition**	1,758	8,599	158	Maturity
3	**2D face recognition in the visible spectrum**	1,437	5,012	580	Maturity
19	**Handwriting recognition**	1,273	6,347	821	Maturity
12	**Eye vein recognition**	1,048	5,117	544	Maturity
2	**Infrared face recognition**	1,047	5,111	151	Maturity
7	**Contactless friction ridge recognition**	811	3,974	25	Maturity
9	**Iris recognition in the NIR spectrum**	650	3,068	30	Maturity
4	**3D face recognition**	561	2,545	269	Maturity
13	**Hand vein recognition**	532	1,958	457	Maturity
1	**DNA biometrics**	473	2,556	168	Maturity – minor relevance
15	**Hand geometry recognition**	428	2,349	186	Maturity – minor relevance
17	**Keystroke recognition**	378	1,482	129	Maturity – minor relevance
14	**Heart signal recognition**	267	1,207	134	Growth
11	**Iris recognition at a distance**	259	1,285	77	Growth
10	**Iris recognition in the visible spectrum**	222	1,212	40	Growth
5	**Infrared friction ridge recognition**	195	843	66	Growth
6	**3D friction ridge recognition**	120	571	41	Growth
18	**Gait recognition**	32	163	67	Childhood
16	**Periocular recognition**	27	197	38	Childhood

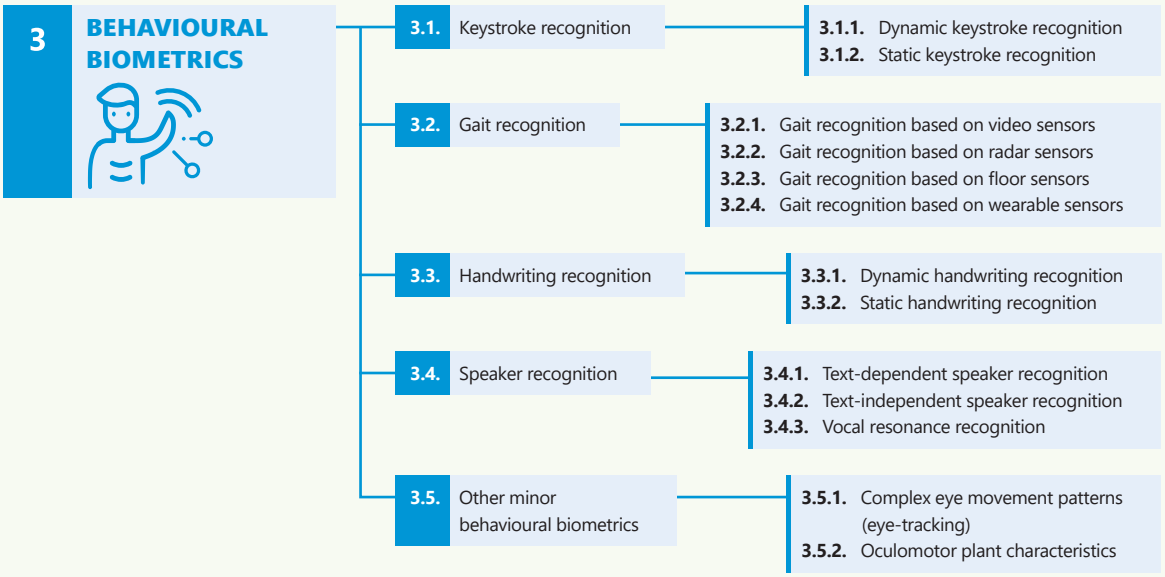
2. Taxonomy description

The final tree-style representation of the proposed taxonomy of biometric technologies is shown in Figure 2. The following sections report a description for each element of the tree.

Figure 2: *Graphic representation of the taxonomy of biometric technologies.*

Continued on pg.26

Continued from pg.25



2.1. Biomolecular biometrics

Molecular and soft biomolecular biometrics is an advancing field that involves the analysis of a person's unique biological markers at a molecular level to ascertain identity.

2.1.1. DNA biometrics

Amongst the various biometric technologies suitable for the recognition of individuals, deoxyribonucleic acid (DNA) provides the most reliable results.[27] This technology is intrinsically digital (in terms of biometric data acquisition and processing) and does not change during a person's life. DNA recognition finds easier applications in forensic science, probably due to the high invasiveness and low efficiency of related modalities. However, other applications in biometric recognition have also been proposed. For example, portable human DNA analysers exist that can conduct DNA analyses in approximately 25 minutes.[28] Although these systems are still unsuitable for applications in the field of access control and border checks, advances are being made to expedite the analysis process.

2.1.1.1. DNA phenotyping

DNA phenotyping is the process of predicting an organism's phenotype (i.e. the set of its observable characteristics or traits) using only genetic information collected from genotyping or DNA sequencing. DNA phenotyping,[29] in particular, refers to the prediction of appearance traits of an unknown sample donor, or an unknown deceased

27 M. Hashiyada, "DNA biometrics", Biometrics, IntechOpen, 2011.

28 S. Bhable, S. Kayte, R. Maher, J. Kayte and C. Kayte, "DNA Biometric", IOSR Journal of VLSI and Signal Processing, vol. 5, pp. 82-85, 2015.

29 M. Kayser, "Forensic DNA Phenotyping: Predicting human appearance from crime scene material for investigative purposes", Forensic Science International: Genetics, vol. 18, pp. 33-48, 2015.

(missing) person, directly from sampled biological materials. In general, biometric information from DNA phenotyping can only provide investigative leads to trace unknown persons who are unidentifiable with current comparative DNA profiling.

2.1.1.2. DNA profiling

DNA profiling[30] (also called DNA fingerprinting) is used to assist in the recognition of individuals by their respective DNA profiles. Although more than 99.1% of the genome is the same throughout the human population, the remaining 0.9% of human DNA shows variations between individuals. These variable DNA sequences, termed polymorphic markers, can be used to both differentiate and correlate individuals.

2.1.1.3. DNA sequencing

DNA sequencing[31] is the process of determining the nucleic acid sequence (the order of nucleotides in DNA). One possible technology to perform DNA sequencing is capillary electrophoresis, which offers high resolution and high throughput, automatic operation, and data acquisition.

2.1.1.4. Techniques for collecting DNA samples

This group refers to all the techniques used for the acquisition of DNA samples. This relates strongly to the field of forensics, where saliva samples, swab samples, tape samples, etc.,[32] may be used in order to collect DNA.

2.1.2. Other biomolecular biometrics

2.1.2.1. Hand bacteria identification

Bacteria communities found on the skin of the human hand have shown to be highly diverse and to have a low percentage of similarity between individuals. Some studies focus on this type of biometrics, and some claim to recognise individuals with high accuracy.[33]

30 E. Giardina, "DNA Fingerprinting", Brenner's Encyclopedia of Genetics (Second Edition), Elsevier, 2013, pp. 356-359.

31 G. Murugesan and G. W. Procop, "Direct Genome Sequencing in Diagnostic Pathology", Cell and Tissue Based Molecular Pathology, Churchill Livingstone, 2009, pp. 56-62.

32 J. Mitchell, R. Van Oorschot and K. Ballantyne, "Forensic trace DNA: a review. Investigative genetics.", Investigative Genetics, vol. 1, no. 14, 2010.

33 A. B. Holbert, "Hand bacteria as an identifier: a biometric evaluation", Network Modeling Analysis in Health Informatics and Bioinformatics, vol. 4, no. 22, 2015.

2.2. Morphological biometrics

Morphological biometrics refers to biometric recognition modalities relying on the identification of the shape, size and distinctive features of the human body.

2.2.1. Face recognition

Facial recognition analyses a digital image or a video frame, using one of three approaches:

- *Global (holistic) approach*[34] uses the entire face as the input data, which are then projected onto a subspace of smaller dimension;
- *Local (feature-based) recognition approaches*[35] considers local features or areas of the face such as the eyes, nose or mouth. These are extracted first and then their locations and local statistics (geometric and/or appearance) are used to classify human faces according to well-defined rules and statistics;
- *Hybrid approaches*[36] make use of the features of both techniques and have the potential to offer better performance.

Facial recognition may be performed in the visible[37] or invisible spectrum of light. *Infrared face recognition* includes various approaches for recognising human faces using infrared (IR) imaging. This is commonly sub-divided into:[38] near-infrared (NIR, 0.78-1.0 µm in wavelength) imaging; short-wavelength infrared (SWIR, 1-3 µm) imaging; mid-wavelength infrared (MWIR, 3-8 µm) imaging; long-wavelength infrared (LWIR, 8-15 µm) imaging. NIR and SWIR, usually with active illumination, are sometimes called "reflected infrared" while passive MWIR and LWIR techniques are sometimes referred to as "thermal infrared" (thermal IR).

2.2.1.1. Thermal infrared face recognition

Face recognition based on images captured using imaging sensors operating in the thermal IR portion of the electromagnetic spectrum (i.e. thermal cameras), including MWIR and LWIR. The human face emits thermal infrared radiation[39] detectable by thermal cameras. Temperature variations on the surface of the face produce a heat pattern, which can be captured as a 2D image (thermal image) and used for recognition. Thermal IR imagery is independent of illumination[40] and only requires passive IR sensor

34 S. Karamizadeh, S. Abdullah and M. Zamani, "An Overview of Holistic Face Recognition", International Journal of Research in Computer and Communication Technology, vol. 2, pp. 738-741, 2013.

35 P. N. Divyarajsinh and M. B. Brijesh, "Face Recognition Methods & Applications", International Journal of Computer Technology & Applications, vol. 4, pp. 84-86, 2013.

36 G. Prince and W. Heena, "A review on facial recognition including local, holistic and hybrid approaches", Journal of Natural Remedies, vol. 21, pp. 210-216, 2020.

37 D. Sliney, "What is light? The visible spectrum and beyond", Eye, vol. 30, pp. 222-229, 2016.

38 K. B. Mrinal, S. Kankan, M. Sharmistha, M. Goutam, S. Ashim, Aniruddha, S. Nath, B. Debotosh, K. B. Dipak and N. Mita, "Thermal Infrared Face Recognition – A Biometric Identification Technique for Robust Security system", Reviews, Refinements and New Ideas in Face Recognition, IntechOpen, 2011.

39 G. Bebis, "Face Recognition, Thermal", Encyclopedia of Biometrics, Springer, Boston, MA., 2009.

40 S. Ashim, S. Aniruddha Nath, B. Debotosh, K. B. Dipak and N. Mita, "Thermal Infrared Face Recognition – A Biometric Identification Technique for Robust Security system", Reviews, Refinements and New Ideas in Face Recognition, IntechOpen, 2011.

technology, because thermal IR sensors measure the heat energy emitted from objects, not reflected light. More importantly, thermal IR emission can be viewed in any visible light conditions and is less subject to scattering and absorption by smoke or dust than visible light. Therefore, thermal imaging has great advantages in face recognition under low illumination conditions and even in total darkness (without the need for IR illumination), where visual face recognition techniques fail.

2.2.1.2. Near-infrared face recognition

Face recognition based on images captured using NIR sensors. Near-infrared-based face recognition[41], as opposed to the conventional visible light-based, is an effective approach to overcome the impact of illumination changes on face recognition. Since NIR imaging is based on reflected light (i.e. is due to the reflective material properties), it uses a special purpose imaging acquisition hardware based on active IR sensor technology in which NIR lights illuminate the face from the near frontal direction, and an NIR camera captures front-lit NIR face images. This is similar to a camera flash, but the imaging is done in the invisible NIR spectrum. With such NIR face images, problems caused by uncertainties in uncontrollable environmental illumination are minimised, and difficulties in building the face matching engine are much alleviated. The NIR approach usually achieves significantly higher performance than the visible light approach.

2.2.1.3. Video-based face recognition

Video-based face recognition,[42] applied within the visible spectrum of light, is a technique for recognising one or multiple persons present in a video. Given the input face video, a typical video-based face recognition approach combines the temporal characteristics of facial motion with appearance changes. This often involves the temporal characterisation of faces.[43] As the face moves, its appearance as captured in a video varies due to changes in the pose, illumination conditions, expression, etc. The pattern of these variations is often specific to the individual, containing distinguishing information that can be used by video-based face recognition systems for improved performance.

2.2.1.4. Image-based face recognition

Image-based face recognition, applied within the visible spectrum of light, is the technique of recognising one or multiple persons present in a single image based on their facial characteristics. Generally, the first step in an image-based face recognition process is the detection of a face in the image. If a face is detected, the successive step consists in locating its position within the image. Factors such as variations in illumination, facial expressions (such as smiling or yawning) or individuals' appearances (presence of moustaches, glasses, etc.) all hinder face detection. Device-related factors, such as limited resolution, lighting artifacts, image file format or compression, can also lower the performance of the biometric system. After a face is detected in an image, its features must be represented in vectorial form for biometric comparison.[44]

41 S. Z. Li and A. K. Jain, "Face Recognition, Near-Infrared", Encyclopedia of Biometrics, Springer, Boston, MA, 2009, pp. 352-355.

42 R. Chellappa, G. Aggarwal and K. S. Zhou, "Face Recognition, Video-Based", Encyclopedia of Biometrics, Springer, Boston, MA, 2015, pp. 514-521.

43 S. Z. Li and A. K. Jain, "Temporal Characterization of Faces", Encyclopedia of Biometrics, Springer, Boston, MA, 2009, pp. 1327-1327.

44 C. Mejda, E. Akram, B. Wajdi and B. A. Chokri, "A Survey of 2D Face Recognition Techniques", Computers, vol. 5, no. 21, 2016.

2.2.1.5. 3D face recognition

Face recognition technologies that make use of the three-dimensional features of the facial components acquired by using visible or near-infrared[45] light illumination. Once the three-dimensional geometry of the human face is acquired, it is used to extract distinctive features on its surfaces, such as the contour of the eye sockets, nose and chin. Recognition is then based on matching the metadata extracted from the 3D shapes of the face. *3D face recognition* is claimed to have the potential to achieve better accuracy than its 2D counterpart.[46]

2.2.2. Friction ridge recognition

The skin of the palms of the hands and fingers, as well as of the soles of the feet and toes, is distinctly different from that of the rest of the body and is known as *friction ridge skin* in the biometric and forensic communities.[47] This technological field includes the different biometric recognition modalities used to recognise individuals based on the unique geometrical features of the friction ridges of various parts of the human body.

2.2.2.1. Thermal friction ridge recognition

Friction ridge recognition based on signals captured using thermal scanners capable of sensing the temperature differences on the contact surface in between friction ridges and valleys of the aforementioned body parts.[48]

2.2.2.2. Near-infrared friction ridge recognition

Recognition that uses friction ridge biometric data captured using near-infrared light illumination. For example, near infrared palmprint images have been shown to be reliable for efficient recognition.[49]

2.2.2.3. 3D friction ridge recognition

Biometric recognition technologies based on scanning technologies and image detection systems capable of acquiring the frictional ridges of one or multiple body parts (i.e. fingers, palms, feet or finger knuckles) and producing a three-dimensional representation of them in order to recognise an individual. For example, extracted features from 3D palmprint data usually include depth and curvature of the palm lines and wrinkles on the palm surface.[50]

45 G. A. Atkinson, M. F. Hansen and M. L. Smith, "A efficient and practical 3D face scanner using near infrared and visible photometric stereo", Procedia Computer Science, vol. 2, pp. 11-19, 2010.

46 Z. Eng, Y. Yick, Y. Guo, H. Xu, M. Reiner, T. Cham and S. Chen, "3D faces are recognized more accurately and faster than 2D faces, but with similar inversion effects", Vision Research, vol. 138, pp. 78-85, 2017.

47 A. R. Hicklin, "Anatomy of Friction Ridge Skin", Encyclopedia of Biometrics, Springer US, 2009, pp. 23-28.

48 J.-s. Han, Z.-y. Tan, K. Sato and M. Shikida, "Thermal characterization of micro heater arrays on a polyimide film substrate for fingerprint sensing applications", Journal of Micromechanics and Microengineering, vol. 15, pp. 282-289, 2015.

49 A. Meraoumia, S. Chitroub and B. Chitroub, "Are infrared images reliable for palmprint based personal identification systems?", Saudi International Electronics, Communications and Photonics Conference, 2013.

50 D. Zhang and V. Kanhangad, "Palmprint, 3D", Encyclopedia of Biometrics, Springer, Boston, MA, 2009, pp. 1037-1042.

2.2.2.4. Contactless friction ridge recognition

Recognition modalities in which the friction ridge mark signature is acquired without direct contact of the relevant body part with a sensing surface, mostly employing the video or image acquisition of fingerprints, palmprints, footprints and knuckle prints. *Contactless friction ridge recognition* is characterised by low constrained acquisition processes, which determines high levels of usability and hence, user acceptance. Further, finger/palm/foot/knuckle images acquired by a contactless sensor exhibit no deformation.[51]

2.2.2.5. Contact-based friction ridge recognition

Recognition modalities in which the friction ridge mark signature is acquired through the contact of the body part with an acquiring surface. For example, contact-based palmprint capture may be performed by asking the users to put their hands on a planar surface where their fingers are typically restricted by pegs. The biometric samples captured by a *Contact-based friction ridge recognition* system can be directly used for feature extraction, while the corresponding contactless friction ridge images require further pre-processing.[51]

2.2.2.6. Fingerprint recognition

Methods and technologies for the recognition of individuals based on the unique geometrical features of the friction ridges of human fingers. A fingerprint[52] is the representation of the dermal ridges of a finger that form through a combination of genetic and environmental factors: the genetic code in DNA gives general instructions on the way the skin should form in a developing foetus, but the specific way in which it forms is a result of random events such as the exact position of the foetus in the womb at a particular moment. This is the reason why even the fingerprints of identical twins are different.

2.2.2.7. Palmprint recognition

Methods and technologies for the recognition of individuals based on the unique geometrical features of the friction ridges of human palms. A palmprint[53] is formed by the skin patterns of the inner surface of the human hand from the wrist to the root of the fingers and is rich in physical characteristics such as lines, points, and textures, which provide stable and distinctive information sufficient for recognition. *Palmprint recognition* is a relatively new biometric technology and recognition systems use palmprint features that may or may not be observable to the naked eye.

2.2.2.8. Footprint recognition

Methods and technologies for recognising individuals based on the unique geometrical features of the friction ridges of the feet. Prior work on footprint biometrics mainly explored the use of foot shape features such as length, width, major axis, minor axis and centroid, but proved unreliable due to similarity in those features amongst individuals. Instead, footprint texture features coming from creases of the soles of the feet and minutiae of toes are unique and permanent like palmprint texture features. Recent-

51 J. Priesnitz, C. Rathgeb and N. Buchmann, "An overview of touchless 2D fingerprint recognition", EURASIP Journal on Image and Video Processing, vol. 2021, no. 8, 2021.

52 D. Maltoni, "Fingerprint Recognition, Overview", Encyclopedia of Biometrics, Springer, Boston, MA, pp. 510-513.

53 D. Zhang and L. L. Liu, "Palmprint Features", Encyclopedia of Biometrics, Springer, Boston, MA, 2009, pp. 1043--1049.

ly, various recognition techniques based on the extraction and classification of those features have been investigated.[54]

2.2.2.9. Finger-knuckle-print recognition

Methods and technologies for the recognition of individuals based on the unique geometrical features of the friction ridges of human finger-knuckles. The finger-knuckle surface[55] is defined as the skin pattern present on the backs of the fingers. This region has three joints: the *metacarpophalangeal joint* which joins the finger to the hand; the *proximal interphalangeal (PIP) joint* in the middle of the finger; and the final *distal joint*. The presence of these joints in the finger dorsum surface forms the flexion shrinks on the outer region of the skin, which creates the dermal patterns consisting of lines, wrinkles, contours etc. The pattern generated by the PIP joint on the finger back region is referred to as *finger-knuckle-print (FKP)*. The area of the captured finger-knuckle-print is very small as compared to the area captured for *Palmprint recognition*, and also has highly unique features well suited for a biometric recognition system.

2.2.3. Iris recognition

The iris is a thin, circular structure in the eye that controls the diameter and size of the pupils. The iris consists of muscle tissues that cause the pupil to contract and dilate. The back surface is covered by a layer of pigmented epithelial tissue, which gives an eye its distinctive colour. Iris recognition is the field of biometrics that deals with the recognition of individuals through the textural features of the iris muscular patterns.

2.2.3.1. Iris recognition in the NIR spectrum

Iris recognition based on images captured using near-infrared (NIR) illumination. Due to the presence of melanin (the pigment which attributes the iris its appearance) absorption by the iris is significant for light within the visible spectrum while it is almost negligible for infrared wavelengths.[56] High reflectance (i.e. low absorption) enables good visibility of the iris texture details even for dark irises. For this reason, most commercial iris scanning cameras acquire images using NIR illumination.[57]

2.2.3.2. Iris recognition in the visible spectrum

Biometric recognition technology based on images of the iris captured in the visible spectrum of light. This presents many challenging aspects, especially in the case of individuals with dark irises[58] (caused by higher melanin pigmentation and collagen fibrils) because the unique pattern of the iris is not clearly observable under visible light.

---

54 R. Kushwaha and N. Nain, "Person Identification Using Footprint Minutiae", Advances in Intelligent Systems and Computing, vol. 1024, 2020.

55 K. Usha, "Personal recognition using finger knuckle shape oriented features and texture analysis", Journal of King Saud University – Computer and Information Sciences, vol. 28, pp. 416-431, 2016.

56 M. Trokielewicz and B. Ewelina, "Cross-spectral Iris Recognition for Mobile Applications using High-quality Color Images", Journal of Telecommunications and Information Technology, pp. 91-97, 2016.

57 M. Hosseini, B. Araabi and H. Soltanian-Zadeh, "Pigment Melanin: Pattern for Iris Recognition", IEEE Transactions on Instrumentation and Measurement, VOL. 59, NO. 4, APRIL 2010, vol. 59, no. 4, pp. 792-804, 2010.

58 K. B. Raja, R. Raghavendra and C. Busch, "Visible iris imaging: A novel imaging solution for improved iris recognition", IEEE International Conference on Imaging Systems and Techniques

2.2.3.3. Iris recognition at a distance

This modality refers to capturing iris images metres away from the subject and analysing them. With the right detection equipment, *Iris recognition at a distance* might be implemented even for a person walking.[59] This would enhance the traveller's experience at border checks, especially where a large number of people move through a bottleneck (e.g. a border check point), reducing the need for user cooperation and achieving low intrusiveness, and thus high acceptance and transparency.

2.2.4. Vascular pattern recognition

Vascular pattern recognition, also commonly referred to as *Vein pattern recognition*, uses a powerful light source (usually near-infrared light[60]) to acquire images of blood vessels. Researchers have determined that the vascular pattern of the human body is unique to a specific individual and does not change as people age. Two main acquisition approaches exist to *Vascular pattern recognition*: *reflection* and *transmission* modes. In the first, NIR illumination is emitted towards the body part of interest (retina, finger, palm, etc.) and the reflected light is captured by a sensor. The traces where veins occur are captured as darker parts because veins absorb more near-infrared illumination than their surrounding elements due to the high absorption of haemoglobin. In the second, the illumination device and the sensor must be placed opposite one another so that the sensor may capture an image formed by the light transmitted through the skin of the person.[61]

2.2.4.1. Retina recognition

The retina is the innermost, light-sensitive layer of tissue in human eyes, which serves a function analogous to that of the film or image sensor in a camera. The optics of the eye create a focused two-dimensional image of the visual world on the retina, which translates that image into electrical neural impulses to the brain to create visual perception. It has two distinct vascular networks, the *choroidal network* and the *retinal network*, whose unique patterns enable biometric recognition. Generally, subjects are requested to position their eyes in front of a capture system at a distance ranging from 8 cm to one metre. The person must then look at a series of markers, viewed through the eyepiece, and line them up. During this process, the retina is scanned by near-infrared radiation and the pattern of the blood vessels is captured. This technology is not to be confused with other ocular-based biometric technologies such as iris recognition and scleral/episcleral scanning.[62]

2.2.4.2. Sclera/episclera recognition

This is a biometric technique that uses unique patterns on a person's sclera blood vessels. The sclera, also known as the *white of the eye*, is the opaque, fibrous and pro-

(IST), 2015.

59 H. Proença, "Iris Recognition in the Visible Wavelength", Handbook of Iris Recognition, Springer, London, 2013, pp. 151-169.

60 W. Wu, "Selection of Typical Wavelength for Palm Vein Recognition", Acta Optica Sinica, vol. 32, no. 12, pp. 1-7, 2012.

61 A. Uhl, "State of the Art in Vascular Biometrics", Handbook of Vascular Biometrics. Advances in Computer Vision and Pattern Recognition., Springer, Cham, 2020.

62 Y. Seto, "Retina Recognition", Encyclopedia of Biometrics, Springer, Boston, MA, 2009, pp. 1128-1130.

tective outer layer of the human eye that surrounds the iris. The human sclera mostly contains collagen and some crucial elastic fibres and is formed from four layers which, from outermost to innermost, are: *episclera, stroma, lamina fusca, and endothelium*.[63] The vasculature of the sclera has several desirable characteristics that make it appealing for biometric recognition systems:[64] unlike the iris and the periocular region, the sclera has a rich vascular structure that is considered unique for each individual and even differs between identical twins; the vein patterns are discernible despite potential eye redness and also in the presence of contact lenses that may adversely affect iris recognition systems. The vasculature is relatively stable over time and difficult to forge, so sclera recognition systems are commonly considered to be resistant to presentation attacks and spoofing.

2.2.4.3. Finger vein recognition

Scanning technologies aiming to recognise an individual by their fingers' unique vascular pattern. Finger vein network patterns are visible under NIR or visible illumination.[65] In this definition, the term *finger* includes all 5 fingers of the hand.

2.2.4.4. Palm vein recognition

Scanning technologies aiming to recognise an individual by their palms' unique vascular pattern. These palm patterns[66] are normally captured under NIR illumination using the reflection method. Palm veins emerge as dark traces in the captured images because they absorb a high percentage of the near-infrared illumination. With this method, contactless pattern-capturing and recognition systems can be created.

2.2.4.5. Back-of-hand vascular recognition

Back-of-hand (or dorsal hand) vascular recognition[67] is based on the subcutaneous vascular network on the back of the hands. According to large-scale experiments, this pattern of blood vessels is unique to everyone, even amongst identical twins. *Dorsal hand vein recognition* is known for high accuracy, stability, and resistance to attacks.[68] The crucial factor in achieving accurate recognition is the quality of the vein image that can be captured in real-life scenarios. These images are captured using similar principles to those for palm veins: the back of the hand is illuminated using near-infrared radiation and the reflected light is used to acquire an image of its vascular pattern. The deoxidised haemoglobin in blood vessels absorbs more infrared rays than surrounding tissues and causes the blood vessels to appear as black patterns in the resulting image captured by an NIR camera.

63 B. Cassin and S. Solomon, "Dictionary of Eye Terminology", Triad Publishing Company, 1990.

64 M. Vitek, P. Rot, V. Štruc and P. Peer, "A comprehensive investigation into sclera biometrics: a novel dataset and performance study", Neural Computing and Applications, vol. 32, p. 17941–17955, 2020.

65 N. Miura, "Technology and Future Prospects for Finger Vein Authentication Using Visible-light Cameras", Hitachi Rev, vol. 67, 2018.

66 T. Aoki and T. Shinzaki, "Palm Vein", Encyclopedia of Biometrics, Springer, Boston, MA, 2009, pp. 1195-1202.

67 A. H. Choi, "Back-of-Hand Vascular Recognition", Encyclopedia of Biometrics, Springer, Boston, MA, 2009, pp. 55-60.

68 R. Raghavendra, J. Surbiryala and C. Busch, "Hand Dorsal Vein Recognition: Sensor, Algorithms and Evaluation", in 2015 IEEE International Conference on Imaging Systems and Techniques (IST), 2015.

2.2.4.6. Wrist vein recognition

Technologies aiming to recognise an individual by their wrists' unique vascular pattern, which has similar usability as palm vein and finger vein modalities. The wrist vein variant, with wider veins, provides clear visualisation and definition of a person's unique vein patterns.[69]

2.2.5. Physiological signal biometrics

Physiological signals are characteristics of individuals that do not rely on morphological characteristics of the human body, but rather refer to those signals that can be acquired and monitored to assess a person's clinical state. The same signals can be used for recognition. However, in general, the acquisition modalities of physiological signals can be uncomfortable and may require expensive equipment.[70] Part of the current research is focused on the combination of multiple physiological signals to reduce the vulnerability of biometric systems based on these signals to external attacks, as their level of security can still be regarded as insufficient.

2.2.5.1. Heart-rate variability

Heart-rate variability (HRV) is an intrinsic property of the heart and an active research domain within the medical research community for the last two decades.[71] Its application in biometrics is still in its infancy. Irvine et al.[72] proposed one of the very few attempts specifically aimed at HRV-based biometric recognition, but the actual techniques used and the results obtained are not fully known.

2.2.5.2. Electrocardiographic signals

Electrocardiographic (ECG) signals describe the electrical activity of the heart over time, recorded with electrodes attached to the surface of the body. Traditionally, physicians use ECG characteristics to gain insights into the heart's condition, usually with complementary tests required in order to finalise a diagnosis. From a biometrics perspective, it was demonstrated[73] that the ECG has sufficient details for applications in biometric recognition. The advantages of using ECG signals for biometric recognition can be summarised as universality, permanence, uniqueness, robustness to attacks, live detection, continuous recognition and data minimisation.

2.2.5.3. Phonocardiographic signals

Phonocardiographic (PCG) signals are the sounds and murmurs made by the heart during a cardiac cycle. A *phonocardiogram* is a plot of a high-fidelity recording of PCG

69 R. Garcia-Martin and R. Sanchez-Reillo, "Wrist Vascular Biometric Recognition Using a Portable Contactless System", Sensors, vol. 20, p. 1469, 2020.

70 M. Moreno Revelo, M. Ortega Adarme, D. Peluffo Ordoñez, K. Alvarez Uribe and M. Becerra, "Comparison Among Physiological Signals for Biometric Identification", Lecture Notes in Computer Science, vol. 10585, 2017.

71 A. Nazneen, S. Tharewal, V. Kale, A. Bhalerao and K. Kale, "Heart Based Biometrics and use of Heart Rate Variability in Human Identification Systems", Advanced Computing and Systems for Security, vol. 395, Springer India, 2015, pp. 15-29.

72 J. Irvine, B. Wiederhold, L. Gavshon, S. Israel, S. McGehee, R. Meyer and M. Wiederhold, "Heart rate variability: a new biometric for human identification", International Conference on Artificial Intelligence (IC-AI'2001), 2001.

73 A. Foteini, G. Jiexin and H. Dimitrios, "Heart Biometrics: Theory, Methods and Applications", Biometrics, IntechOpen, 2011, pp. 199-217.

signals made using a machine called a *phonocardiograph*, while *phonocardiography* is the recording of the PCG signals. The use of these signals for biometric recognition represents a novel approach[74] and has the potential to reduce the risks of vulnerability faced by other biometric systems.[75]

2.2.5.4. Photoplethysmographic signals

Photoplethysmographic (PPG) signals are optically obtained signals (e.g. by illuminating the skin using a light-emitting diode and detecting the intensity changes in the reflected light) that can be used to detect blood volume changes in the microvascular bed of tissue. The corresponding temporal plot is called the *photoplethysmogram*. Compared to other commonly used physiological signals, PPG signals offer important advantages.[76] First, the acquisition of PPG signals may be performed in a more comfortable manner, as the sensor placement does not require the use of gels, and the acquisition devices are often widely diffused in medical applications. For example, PPG biometric samples can be captured by using pulse oximeters, which are non-invasive devices for monitoring haemoglobin saturation and are usually attached to the earlobe or fingertip. Another advantage is that pulse oximeters are usually less expensive and smaller than the acquisition devices used for ECG, EEG, and PCG signals.

2.2.5.5. Encephalographic signals

An emerging approach in physiological biometrics is cognitive biometrics,[77] which relies on the measurement of the brain's response to stimuli performed through several devices, including measurements performed by using Electroencephalography (EEG) systems. EEG is an electrophysiological monitoring method to record the electrical activity of the brain. It is typically executed by placing a set of electrodes along a person's scalp.

2.2.5.6. Acoustic properties of the ear canal

The ear canal is a resonant system, which together with the *pinna* (the visible part of the ear that is outside the head) provides rich acoustic features. In a coarse approximation, it is a one-dimensional system that resonates at one-quarter of the acoustic wavelength. The resonance frequency of the ear canal will typically be around 2500 Hz, but this will vary from person to person, as it depends on the lengths and shapes (curvatures) of the pinna and ear canal which have dimensions that vary from millimetres to a few centimetres. The acoustic properties of the ear canal can be used as a biometric characteristic, can be measured relatively easily with an inexpensive sensor, and feature vectors can be derived with little effort.[78]

74 A. Singh and A. K. Singh, "Biometric identification using phonocardiogram", thesis submitted for partial fulfillment of the requirements for the degree of Bachelor of Technology in Electronics and Communication Engineering – National Institute of Technology, Rourkela, Orissa, India, 2011.

75 T. Meitei, A. Sinam and S. Majumder, "PCG based biometric", Handbook of Research on Information Security in Biomedical Signal Processing, 2020, pp. 1-25.

76 A. Bonissi, R. D. Labati, L. Perico, R. Sassi, F. Scotti and L. Sparagino, "A Preliminary Study on Continuous Authentication Methods for Photoplethysmographic Biometrics", 2013 IEEE Workshop on Biometric Measurements and Systems for Security and Medical Applications, 2013.

77 R. J. Rodriguez, "An Electroencephalogram (EEG) Based Biometrics Investigation for Authentication: A Human-Computer Interaction (HCI) Approach", NSUWorks, 2015.

78 T. Akkermans, K. T.A.M. and S. D.W.E., "Acoustic Ear Recognition", Lecture Notes in Computer Science, vol. 3832, 2005.

2.2.6. Hand geometry recognition

Hand geometry is a widely accepted biometric characteristic that allows the recognition of individuals from the shape of their hands. Hand geometry readers measure the individual's hand along many dimensions including height, width, deviation and angle, and compare those measurements to a reference sample. Although these measurements are not very distinctive amongst people, hand geometry can be very useful for biometric recognition. Major advantages of hand geometry systems include: simple requirements in imaging resolution (hand features can be extracted from low-resolution images); the ability to operate under harsh environmental conditions (hand geometry biometrics are immune, for example, to dirt on the hand and other external factors); and low data-storage requirements. In addition, hand geometry acquisition and recognition are extremely fast. This technique is widely accepted, and the recognition process involves simple data processing.[79]

2.2.6.1. Contact-based hand geometry recognition

Contact-based (also known as platform-based) hand geometry scanning uses flat platforms with which the hands must be placed in contact, facilitating not only the acquisition procedure but also the segmentation and post-acquisition feature extraction. Depending on the use of pegs or pins to restrict the hand's degrees of freedom, contact-based solutions may be further sub-divided into *constrained* and *unconstrained*.[80]

2.2.6.2. Contactless hand geometry recognition

In contactless hand geometry recognition technological solutions, neither pegs and pins nor platforms are required for the hand geometry acquisition, which may be conducted using static video cameras,[81] web cams,[82] or other digital contactless image-capturing devices.

2.2.7. Other minor morphological biometrics

As ascertained during the study, other morphological biometrics exist that are less relevant than the above-mentioned primary ones to the fields of border checks and access control. For the sake of completeness, these minor morphological biometrics were included in this taxonomical group.

2.2.7.1. Dental biometrics

Dental biometrics uses information about dental structures for the recognition of individuals. This methodology is mainly applied to the identification of individuals in forensic analyses. The process of dental recognition consists of measuring dental features, labelling individual teeth with tooth indices, and matching these dental features with

79 D. Zhang and V. Kanhangad, "Hand Geometry Recognition", Encyclopedia of Cryptography and Security, Springer, Boston, MA, 2011, pp. 529-531.

80 M. Bača, P. Grd and T. Fotak, "Basic Principles and Trends in Hand Geometry and Hand Shape Biometrics", New Trends and Developments in Biometrics, IntechOpen, 2012.

81 X. Jiang, "New directions in contact free hand recognition", International Conference in Image Processing: Proceedings of the IEEE International Conference in Image Processing, 2007.

82 A. Morales, M. A. Ferrer, J. B. Alonso and C. M. Travieso, "Comparing infrared and visible illumination for contactless hand based biometric scheme", 2008 42nd Annual IEEE International Carnahan Conference on Security Technology, pp. 191-197, 2008.

biometric samples. Commonly used dental features are based on tooth morphology (shape) and appearance (grey level). Dental radiographs are the major source for obtaining morphological dental features.[83]

2.2.7.2. Tongueprint recognition

Biometric technology for automatically recognising a person using tongue information. As the tongue can be extended out from the body for inspection, shape and texture information can be acquired from images (e.g. using a machine vision system) as a *tongue print* for the recognition process. Unlike other biometrics (e.g. face and fingerprint), the tongue is an internal organ and well protected in the mouth, so it is basically immune to forgery. This is advantageous for protecting users' privacy and security.[84] Furthermore, the involuntary squirming of the tongue is not only convincing proof that the subject is alive, but also a characteristic for recognition. The tongue can also present both *static* and *dynamic* features for recognition.

2.2.7.3. Ear print recognition

Ear print analysis is mainly used as a means of forensic identification intended as a characteristic similar to fingerprinting. An ear print is a two-dimensional reproduction of the parts of the outer ear that have touched a specific surface (most commonly the *helix, antihelix, tragus, and antitragus*). Although ear prints do not have powerful distinctiveness information, they are useful as forensic evidence and are a promising soft biometric.[85]

2.2.7.4. Periocular recognition

The full region around the eye, including the *sclera, eyelids, lashes, brows, and skin*, is known as the *periocular region*,[86] and can be acquired non-intrusively and used as a biometric characteristic.[87] *Periocular recognition* offers advantages over full-face recognition as it is least affected by expression variations, ageing effects, and changes due to the growth of facial hair. Moreover, this biometric technology may perform better in the case of extreme pose changes when only one eye is completely visible.

2.2.7.5. Skin texture recognition

Skin texture is the surface texture pattern of any part of the human body with bare skin (e.g. face, hand and palm). In the context of biometrics, this term commonly refers to the technologies and methods of face recognition using highly detailed facial skin texture in high-resolution images. A person's skin texture pattern is, to some extent, a

83 H. Chen and A. K. Jain, "Dental Biometrics", Encyclopedia of Biometrics, Springer, Boston, MA, 2015, pp. 343-351.

84 S. Z. Li and A. K. Jain, "Tongue-Print Recognition", Encyclopedia of Biometrics, Springer, Boston, MA, 2009, pp. 1340-1340.

85 A. Morales, M. Diaz, G. Llinas-Sanchez and M. A. Ferrer, "Earprint recognition based on an ensemble of global and local features", International Carnahan Conference on Security Technology (ICCST), 2015.

86 K. Hernandez-Diaz, F. Alonso-Fernandez and J. Bigun, "Periocular Recognition Using CNN Features Off-the-Shelf", International Conference of the Biometrics Special Interest Group (BIOSIG), 2018.

87 M. Uzair, A. Mahmood, A. Mian and C. McDonald, "Periocular Biometric Recognition using Image Sets", IEEE Workshop on the Applications of Computer Vision (WACV), pp. 246-251, 2013.

unique physical trait and is distinguishable from those of others, and thus can be used for biometric recognition.[88]

2.2.7.6. Cranial suture scanning

Cranial sutures are fibrous joints providing malleability to the head that allows the growth of the brain during its early development[89] and can be used for biometric recognition. More specifically, cranial sutures in preadolescent skulls are known to present distinctive patterns, whose significance reduces in adulthood.[90]

2.2.7.7. Rugoscopy

The *palatal rugae* are asymmetrical and irregular elevations of the *mucosa* located in the anterior third of the palate. The study of palatal rugae patterns for human identification is described as *rugoscopy*.[91] Palatal rugae were shown to be highly individualistic and unique, and maintain consistency in shape throughout life. In forensic dentistry, palatal rugae patterns can lead to important information and help in recognition.

2.2.7.8. MMW and THz wave body imaging

The use of millimetre waves (MMW) and submillimetre waves (SMW, also called THz radiation) within body imaging systems is an active field of research due to various interesting properties. Penetration through clothing and other nonpolar dielectric materials, even at standoff ranges, is one of the most important abilities of MMW and SMW. Therefore, security screening (e.g. detection of concealed weapons under clothing), non-destructive inspection of goods and medical and biometric imaging are the most relevant applications of MMW/SMW imaging. In the biometrics domain, only works for presentation attack detection in the THz range are currently known.[92]

88 X. Zhu, Z. Lei and S. Z. Li, "Skin Texture", Encyclopedia of Biometrics, Springer, Boston, MA, 2009, pp. 1229-1232.

89 J. Crompton and J. Black, "Chapter 28 – Craniofacial abnormalities", Pediatric Ophthalmology and Strabismus (Fourth Edition), W.B. Saunders, London, 2013, pp. 243-264.

90 P. T. Jayaprakash, "Skull Sutures: Radiographic Contour of Wormian Bone as an Individualizing Epigenetic Marker", Journal of the Canadian Society of Forensic Science, vol. 30, pp. 39-47, 1997.

91 M. Rezwana Begum, "Rugoscopy: Human identification by computer-assisted photographic superimposition technique", Journal of forensic dental sciences, vol. 5, pp. 90-95, 2013.

92 N. Palka and M. Kowalski, "Towards Fingerprint Spoofing Detection in the Terahertz Range", Sensors, vol. 20, no. 12, p. 3379, 2020.

2.3. Behavioural biometrics

Behavioural biometrics is a class of biometrics based on various human actions as opposed to physical characteristics.[93] It is related to the measurement of uniquely identifiable and measurable patterns in human activities. Within the scope of this study, this group of biometric technologies was considered only in relation to its possible application to the recognition of individuals and access control. Possible usages for emotional analysis or the prediction of human intensions were not considered.

2.3.1. Keystroke recognition

Keystroke dynamics is a behavioural biometric characteristic suitable for the automated recognition of an individual based on their own unique typing rhythm. It refers to the detailed timing information and patterns describing how a person is typing on a digital device keyboard. Unlike morphological biometric characteristics, such as fingerprint or iris, where specialised sensors are necessary to collect the biometric data from the captured subject, keystroke dynamics can be detected using off-the-shelf physical computer keyboards or virtual keyboards in smartphones and PDAs. Thus, keystroke dynamics represents a low-cost solution and is easily deployable in a variety of scenarios. On the other hand, one of the major drawbacks is that a person's typing varies substantially during the day and from day to day, and may be affected by multiple external factors. Although other measurements are conceivable, patterns used in keystroke dynamics are derived mainly from the two events that make up a keystroke:[94] *Key-Down* and *Key-Up*. The Key-Down event takes place at the initial depression of a key, and the Key-Up occurs at the subsequent release of that key. Various unique features are then calculated based on the intra-key and inter-key timing variations between these events.

2.3.1.1. Dynamic keystroke recognition

Keystroke recognition modality that uses the keystroke dynamics acquired when the biometric capture subject types any text. This is often used for continuous recognition, i.e. to continuously ensure the validity of an initial recognition throughout the interaction period of the subject with the keyboard. Such a system will continuously monitor the typing behaviour of a user so that the system can be locked if a different user is detected.[95]

2.3.1.2. Static keystroke recognition

Keystroke recognition modality that uses the keystroke dynamics acquired when the biometric capture subject types a predefined text or a password. Static *Keystroke recognition* is in general used to recognise the individual at the initial instance of interaction with the biometric system (for example, to supplement the password in order to avoid password sharing) providing a more robust user verification than simple passwords, but does not provide continuous security, as it cannot detect substitution of the user after the initial verification.[96]

93 S. Z. Li and A. K. Jain, "Behavioral Biometrics", Encyclopedia of Biometrics, Springer, Boston, MA, 2009, p. 62.

94 N. Bartlow, "Keystroke Recognition", Encyclopedia of Biometrics, Springer, Boston, MA, 2009, pp. 877-882.

95 P. Bours, "Continuous keystroke dynamics: A different perspective towards biometric evaluation", Information Security Technical Report, vol. 17, pp. 36-43, 2012.

96 F. Monrose and A. Rubin, "Keystroke dynamics as a biometric for authentication", Future Generation Computer Systems, pp. 351-359, 2000.

2.3.2. Gait recognition

Gait allows to recognize individuals by their walking style (or manner) and pace. Gait has several advantages compared to other biometric characteristics: in most modalities, *Gait recognition* is non-intrusive, does not require cooperation from the individual and can function at moderate distances from the subject.[97]

2.3.2.1. Gait recognition based on video sensors

In this modality, gait is captured from a distance using a video camera. Video and image processing techniques are employed to extract gait features for the recognition process. Most of the Machine Vision (MV)-based *Gait recognition* algorithms are based on using the human silhouette: the image background is removed, and the silhouette of the biometric captured subject is extracted and analysed for recognition. The primary advantage of video-based *Gait recognition* compared to other modalities is that it is captured from a distance when other biometric characteristics are not accessible.[98]

2.3.2.2. Gait recognition based on radar sensors

Detailed radar signal processing can reveal many characteristics of human motions and of the human body morphology, including gait characteristics. The transmitted radar signal is insensitive to the environmental light conditions of day and night, while smoke, dust, and fog only slightly reduce the signal. Therefore, radar can be effectively used in situations where other sensors perform poorly or cannot be used at all.[99] Radar signals also penetrate most clothing, preventing disguises from being effective. Using radar-based *Gait recognition* in conjunction with other biometric recognition technologies can help to reduce the susceptibility of the combined system to poor visibility conditions and intentional deception.

2.3.2.3. Gait recognition based on floor sensors

In this modality, a set of sensors or force plates are installed on the floor that enable gait biometric feature extraction when a person walks on them.[98] Floor sensor-based *Gait recognition* systems are usually installed along corridors leading to check-points.

2.3.2.4. Gait recognition based on wearable sensors

In this modality, gait biometric features are acquired using wearable Motion Recording (MR) sensors, which can be worn or attached to various places on the human body. Examples of sensors can be accelerometers, gyro sensors, force sensors and bend sensors, capable of measuring various characteristics of walking.[100] Typically, the acceleration of gait, recorded by the MR sensor, is used for subject recognition. One of the main advantages of WS-based *Gait recognition* over several other biometric technolo-

97 R. Chellappa, A. Veeraraghavan and N. Ramanathan, "Gait Biometrics, Overview", Encyclopedia of Biometrics, Springer, Boston, MA, 2009, pp. 628-633.

98 D. Gafurov, "A survey of biometric gait recognition: Approaches, security and challenges", Proceedings of the Annual Norwegian Computer Science Conference, 2007.

99 D. Tahmoush and J. Silvious, "Radar micro-Doppler for long range front-view gait recognition", IEEE 3rd International Conference on Biometrics: Theory, Applications, and Systems, BTAS, pp. 1-6, 2009.

100 D. Gafurov and E. Snekkenes, "Gait Recognition Using Wearable Motion Recording Sensors", EURASIP Journal on Advances in Signal Processing, vol. 2009, no. 7, pp. 1-16, 2009.

gies is its unobtrusive acquisition process. The WS-based approach has been recently proposed for device protection and user recognition in mobile and portable devices.[101]

2.3.3. Handwriting recognition

Handwriting recognition is the process of recognising the author of a text from their handwriting style, and includes (and mostly refers to) signature recognition. *Handwriting recognition* can be implemented in several ways, and applied to a generic text or to a specific predefined text (usually a signature).

2.3.3.1. Dynamic handwriting recognition

In this approach (also known as *online handwriting recognition*), the biometric capture subject writes a text on a digitising screen, which acquires the signature in real time. Another possibility is the acquisition by means of stylus-operated PDAs. Some systems also operate on smartphones or tablets equipped with a touchscreen, where users can sign using a finger or an appropriate pen. *Dynamic handwriting recognition* usually consists of a multi-dimensional temporal analysis, considering multiple variables at a time, e.g. including spatial coordinates x(t) and y(t), pressure, azimuth, inclination, pen up/down and velocity.[102]

2.3.3.2. Static handwriting recognition

In this approach (also known as *off-line handwriting recognition*), the biometric capture subject is requested to write a certain text (usually a signature) on paper (which is subsequently digitally scanned) or directly on a digital device so that, in any case, the written text is acquired as a digital image. This is then analysed by a system that evaluates the shape of the written text to perform biometric recognition.[102]

2.3.4. Speaker recognition

Speaker recognition refers to a group of technologies that use information extracted from a person's speech to perform biometric operations such as speaker identification and verification.[103] It is based on the extraction of acoustic features of speech that differentiate individuals. These features convey two kinds of biometric information: physiological properties (anatomical configuration of the vocal apparatus) and behavioural traits (speaking style).[104]

2.3.4.1. Text-dependent speaker recognition

In this modality, the set of words (or lexicon) used during the biometric acquisition process is the same or is a subset of the words used during the enrolment phase. A major drawback of text-dependent systems lies in the replay attacks that can be performed easily with a simple recording device.[105]

101 H. Zhan, C. Xuejie, L. Shiyun and G. Hongyang, "Gait Recognition of Acceleration Sensor for Smart Phone Based on Multiple Classifier Fusion", Mathematical Problems in Engineering, vol. 2019, 2019.

102 G. A. Khuwaja and M. S. Laghari, "Offline Handwritten Signature Recognition", World Academy of Science, Engineering and Technology, 59, 2011.

103 J. Markowitz, "Speaker Recognition, Standardization", Encyclopedia of Biometrics, Springer, Boston, MA, 2009, pp. 1270-1277.

104 J. Hennebert, "Speaker Recognition, Overview", Springer, Boston, 2009, pp. 1262-1270.

105 S. Z. Li and A. K. Jain, "Text-Dependent", Encyclopedia of Biometrics, Springer, Boston, MA, 2009, pp. 1332-1332.

2.3.4.2. Text-independent speaker recognition

In text-independent *Speaker recognition*, there are no constraints on the words which the speakers are allowed to use. Thus, the reference (what is spoken during the training phase for a *Speaker recognition* algorithm) and the test (what is uttered in actual use) may have completely different content, and the recognition process must take this phonetic mismatch into account. This modality is most often used for *Speaker recognition*, as it requires very little (or no) cooperation by the speaker, thus resulting in more flexible solutions than the text-dependent ones.[106]

2.3.4.3. Vocal resonance recognition

Vocal resonance is the sound of a person's voice as it travels through the person's body. To conduct vocal resonance scanning, a microphone may be placed in contact with the body in order to record audio samples and then compare them with a model built earlier during the training phase. The same methodology may be performed through a wearable microphone and reliably distinguish amongst individuals.[107]

2.3.5. Other minor behavioural biometrics

As ascertained during this study, other behavioural biometrics exist that are less relevant, than the above-mentioned primary ones, to the fields of border checks and access control. For the sake of completeness, these minor behavioural biometrics were included in this taxonomical group.

2.3.5.1. Complex eye movement patterns (eye-tracking)

Class of biometric techniques that use patterns identifiable in human eye movements to recognise individuals. The distribution of a set of primitive eye movement features is compared with eye movement recordings. This biometric modality is sometimes used to ensure robustness against presentation attacks.[108]

2.3.5.2. Oculomotor plant characteristics

Biometrics modality where recognition is performed via the internal non-visible anatomical structure of the eye. To recognise the subject by this method, the anatomical characteristics of the oculomotor plant (comprising the eye globe, its muscles, and the brain's control signals) are estimated. The estimation of the oculomotor plant characteristics (OPC) is achieved by analysing the recorded eye movement trajectories via a 2D linear homoeomorphic mathematical representation of the oculomotor plant. The derived OPC allows recognition via various statistical methods and information fusion techniques.[109]

106 K. Tomi and L. Haizhou, "An Overview of Text-Independent Speaker Recognition: from Features to Supervectors", Speech Communication, vol. 52, no. 1, pp. 12-40, 2010.

107 R. Liu, "Poster: Vocal Resonance as a Passive Biometric", Proceedings of the 15th Annual International Conference on Mobile Systems, Applications, and Services, 2017.

108 C. D. Holland and O. V. Komogortsev, "Complex Eye Movement Pattern Biometrics: Analyzing Fixations and Saccades", 2013 International Conference on Biometrics (ICB).

109 O. V. Komogortsev, A. Karpov, L. R. Price and C. Aragon, "Biometric authentication via oculomotor plant characteristics", 5th IAPR International Conference on Biometrics (ICB), 2012.

3. Technological clusters

As previously mentioned in the Introduction and in Chapter 1, the 57 third-level biometric technologies and modalities of the taxonomy were grouped into a set of 20 technological clusters, each representing a level of abstraction defined in order to enable *Patentometric and Bibliometric Analyses* (see Annex III – Patentometric and Bibliometric Analyses of Biometric Technologies) and to ensure the usability of the taxonomy in the various phases of the Tech Foresight on Biometrics. The definition of the clusters, also formulated by applying the *Weighted Clusterer* software tool, was based on:[110]

- The **numerosity of document sets** (patents and scientific publications) associated with third-level technologies. *Patentometric and Bibliometric Analyses* mostly rely on statistical interpretations of document sets. Therefore, it is preferable to conduct these analyses on numerous datasets as, in general, low numerosity implies a lower level of statistical consistency and significance. But it is hard to indicate the minimum number of patents and scientific publications that a dataset must contain in order to be suitable for a proper statistical analysis, since this value strongly depends on the ontological features of the technical fields of interest. For the present work, 200 was considered the indicative lower limit. Nevertheless, in some cases, less numerous data sets were considered to fulfil the need to include some specific technological fields within the analyses.
- The **technological affinity** between third-level technologies. This was assessed by the Research Team also conducting desk research on the scientific literature. Then, every time the documental set related to a biometric technology resulted in low numerosity, the technology was grouped together with one or more other third-level affine technology (if any) to form a cluster.
- The **relevance of biometric technologies in target applications** (border checks, biometric recognition and access control). This was assessed by crossmatching the stated fields of applications of the selected biometric technologies in patents and in the scientific literature with the objectives of the research study.

Table 2 lists the 20 technological clusters that were considered for *Patentometric and Bibliometric Analyses* along with the corresponding biometric technologies belonging to the third level of the taxonomy. The table does not include the following technologies:

- 1.1.4 Techniques for collecting DNA samples
- 1.2.1 Hand bacteria identification
- 2.5.5 Encephalographic signals
- 2.5.6 Acoustic properties of the ear canal
- 2.7.1 Dental biometrics
- 2.7.2 Tongueprint recognition
- 2.7.3 Ear print recognition
- 2.7.5 Skin texture recognition
- 2.7.6 Cranial suture scanning
- 2.7.7 Rugoscopy
- 2.7.8 MMW and THz wave body imaging

110 For detailed information on the methodology used to define technological clusters, please refer to Annex III – Patentometric and Bibliometric Analyses of Biometric Technologies – Chapter 4.

- 3.4.3 Vocal resonance recognition
- 3.5.1 Complex eye movement patterns (eye-tracking)
- 3.5.2 Oculomotor plant characteristics

These were not considered for *Patentometric and Bibliometric Analyses* because either the associated datasets of patents and scientific publications were too narrow for quantitative analysis, or the technologies per se were deemed not sufficiently relevant to border-check applications.

Table 2: *List of 20 technological clusters and corresponding biometric technologies belonging to the third level of the taxonomy, which were considered for conducting Patentometric and Bibliometric Analyses and used in the various phases of the Tech Foresight on Biometrics.*

#	Technological Clusters	Third-level biometric technologies included in each technological cluster
1	**DNA biometrics**	1.1.1 DNA phenotyping
		1.1.2 DNA profiling
		1.1.3 DNA sequencing
2	**Infrared face recognition**	2.1.1 Thermal Infrared face recognition
		2.1.2 Near-Infrared face recognition
3	**2D face recognition in the visible spectrum**	2.1.3 Video-based face recognition
		2.1.4 Image-based face recognition
4	**3D face recognition**	2.1.5 3D face recognition
5	**Infrared friction ridge recognition**	2.2.1 Thermal friction ridge recognition
		2.2.2 Near-Infrared friction ridge recognition
		2.2.6 Fingerprint recognition
		2.2.7 Palmprint recognition
		2.2.8 Footprint recognition
		2.2.9 Finger-knuckle-print recognition
6	**3D friction ridge recognition**	2.2.3 3D friction ridge recognition
		2.2.6 Fingerprint recognition
		2.2.7 Palmprint recognition
		2.2.8 Footprint recognition
		2.2.9 Finger-knuckle-print recognition
7	**Contactless friction ridge recognition**	2.2.4 Contactless friction ridge recognition
		2.2.6 Fingerprint recognition
		2.2.7 Palmprint recognition
		2.2.8 Footprint recognition
		2.2.9 Finger-knuckle-print recognition

Continued on pg.46

Continued from pg.45

#	Technological Clusters	Third-level biometric technologies included in each technological cluster
8	**Contact-based friction ridge recognition**	2.2.5 Contact-based friction ridge recognition
		2.2.6 Fingerprint recognition
		2.2.7 Palmprint recognition
		2.2.8 Footprint recognition
		2.2.9 Finger-knuckle-print recognition
9	**Iris recognition in the NIR spectrum**	2.3.1 Iris recognition in the NIR spectrum
10	**Iris recognition in the visible spectrum**	2.3.2 Iris recognition in the visible spectrum
11	**Iris recognition at a distance**	2.3.3 Iris recognition at a distance
12	**Eye vein recognition**	2.4.1 Retina recognition
		2.4.2 Sclera/episclera recognition
13	**Hand vein recognition**	2.4.3 Finger vein recognition
		2.4.4 Palm vein recognition
		2.4.5 Back-of-hand vascular pattern recognition
		2.4.6 Wrist vein recognition
14	**Heart signal recognition**	2.5.1 Heart-rate variability
		2.5.2 Electrocardiographic signals
		2.5.3 Phonocardiographic signals
		2.5.4 Photoplethysmographic signals
15	**Hand geometry recognition**	2.6.1 Contact-based Hand geometry recognition
		2.6.2 Contactless Hand geometry recognition
16	**Periocular recognition**	2.7.4 Periocular recognition
17	**Keystroke recognition**	3.1.1 Dynamic Keystroke recognition
		3.1.2 Static Keystroke recognition
18	**Gait recognition**	3.2.1 Gait recognition based on video sensors
		3.2.2 Gait recognition based on radar sensors
		3.2.3 Gait recognition based on floor sensors
		3.2.4 Gait recognition based on wearable sensors
19	**Handwriting recognition**	3.3.1 Dynamic Handwriting recognition
		3.3.2 Static Handwriting recognition
20	**Speaker recognition**	3.4.1 Text-dependent Speaker recognition
		3.4.2 Text-independent Speaker recognition

In the following sections, a brief description of each technological cluster is provided. As the reader may notice, these descriptions are often an abridged (and in some case combined) version of the definitions provided in Sections 2.1, 2.2 and 2.3 concerning the third-level biometric technologies. Such concise descriptions were also meant to

facilitate the quantitative assessment of the 20 technological clusters within the *Delphi Survey* as mentioned in the Introduction. Therefore, if necessary, the readers are referred to previous sections for more detailed descriptions and references.

3.1. DNA biometrics

Amongst the various biometric technologies suitable for the recognition of individuals, deoxyribonucleic acid (DNA) provides the most reliable results. This technology is intrinsically digital (in terms of biometric data acquisition and processing) and does not change during a person's life or even after their death. *DNA biometrics* finds easier applications in forensic science, due to the high invasiveness and low efficiency of related modalities. However, other applications in biometric recognition have also been proposed. For example, portable human DNA analysers exist that can conduct DNA analyses in approximately 25 minutes. Although these systems are still unsuitable for applications in the field of access control and border checks, advances are being made to expedite the analysis process. This technological cluster includes **DNA phenotyping, DNA profiling and DNA sequencing**.

3.2. Infrared face recognition

Technologies for the recognition of human faces using infrared (IR) imaging, commonly sub-divided into: near-infrared (NIR, 0.78-1.0 µm in wavelength) imaging; short-wavelength infrared (SWIR, 1-3 µm) imaging; mid-wavelength infrared (MWIR, 3-8 µm) imaging; long-wavelength infrared (LWIR, 8-15 µm) imaging. NIR and SWIR, usually with active illumination, are sometimes called "reflected infrared", while passive MWIR and LWIR techniques are sometimes referred to as "thermal infrared" (thermal IR). This cluster includes **thermal infrared face recognition** and **near-infrared face recognition**.

3.3. 2D face recognition in the visible spectrum

This technological cluster deals with the automated recognition of individuals through the matching of a face, from a digital image or a video frame acquired in the visible spectrum of light, against a database of face images or a specified biometric reference image. It encompasses **video-based face recognition** and **image-based face recognition.**

3.4. 3D face recognition

This cluster includes solutions aimed at recognising an individual by the three-dimensional features of their facial components. Once the three-dimensional geometry of the human face is acquired, it is used to extract distinctive features on its surfaces, such as the contour of the eye sockets, nose, and chin. Recognition is then based on matching the metadata extracted from the 3D shapes of the face. *3D face recognition* is claimed to have the potential to achieve better accuracy than its 2D counterpart.

3.5. Infrared friction ridge recognition

The skin of the palms of the hands and fingers as well as of the soles of the feet and toes is distinctly different from that of the rest of the body and is known as *friction ridge skin* in the biometric and forensic communities. This technological cluster includes biometric recognition modalities (such as *Fingerprint recognition*, *Palmprint recognition*, *Footprint recognition* and *Finger-knuckle-print recognition*) implemented through **thermal imaging or near-infrared imaging of friction ridge skin**.

3.6. 3D friction ridge recognition

This cluster includes the modalities, scanning technologies and image detection systems capable of acquiring the frictional ridges of one or multiple body parts (i.e. fingers, palms, feet or finger-knuckles) and producing a three-dimensional representation of them in order to recognise an individual. For example, extracted features from 3D palmprint data usually include depth and curvature of the palm lines and wrinkles on the palm surface.

3.7. Contactless friction ridge recognition

This cluster includes the modalities in which the friction ridge mark signature of a finger, palm, foot or finger-knuckle is acquired without direct contact of the relevant body part with a sensing surface, mostly employing video or image acquisition of fingerprints, palmprints, footprints, and knuckle prints.

3.8. Contact-based friction ridge recognition

This cluster includes the modalities in which the friction ridge mark signature of a finger, palm, foot or finger-knuckle is acquired through the contact of the body part with an acquiring surface. For example, contact-based palmprint capture may be performed by asking the users to put their hands on a planar surface where their fingers are typically restricted by pegs.

3.9. Iris recognition in the NIR spectrum

The iris is a thin, circular structure in the eye that controls the diameter and size of the pupils. The iris consists of muscle tissues that cause the pupil to contract and dilate. The back surface is covered by a layer of pigmented epithelial tissue, which gives an eye its distinctive colour. *Iris recognition in the NIR spectrum* is the field of biometrics that deals with the recognition of individuals through images of the textural features of the iris captured using near-infrared illumination.

3.10. Iris recognition in the visible spectrum

This cluster includes iris recognition technologies based on images of the iris captured in the visible spectrum of light. This presents many challenging aspects, especially in the case of individuals with dark irises (caused by higher melanin pigmentation and collagen fibrils) because the unique pattern of the iris is not clearly observable under visible light.

3.11. Iris recognition at a distance

This cluster refers to technological solutions for capturing iris images metres away from the subject and analysing them. With the right detection equipment, *Iris recognition at a distance* might be implemented even for a person walking. This would enhance the traveller's experience at border checks, especially where a large number of people moves through a bottleneck (e.g. a border check point), reducing the need for user cooperation and achieving low intrusiveness, and thus high acceptance and transparency.

3.12. Eye vein recognition

In general, vein (or vascular) pattern recognition uses a light source (usually near-infrared light) to acquire images of blood vessels. In the case of *Eye vein recognition*, scanners typically use harmless low-energy lasers to scan the blood vessels of the eye, and users are typically asked to position their eyes in front of the scanner, as eyes must be very close to the sensors for the vein patterns to be acquired. This cluster encompasses **retina recognition** and **sclera/episclera recognition technologies**.

3.13. Hand vein recognition

This cluster refers to recognition of individuals through images of the complex structure of larger blood vessels near the skin of the hand. These may be readily captured from the back and the palm of the hand as well as from fingers and wrist, using non-invasive and safe imaging techniques (typically in the near-infrared). This vein structure, which is mostly invisible to the human eye, forms a pattern of interconnecting lines that is different from one individual to another and can be used as a morphological biometric. This technological cluster includes **finger vein recognition**, **palm vein recognition**, **back-of-hand vascular recognition,** and **wrist vein recognition**.

3.14. Heart signal recognition

Heart signals belong to the wider group of physiological characteristics of an individual, i.e. those that do not rely on the morphological characteristics of the human body but rather refer to physiological signals that can be acquired and monitored to assess a person's clinical state. This technological cluster includes biometric recognition technologies based on the detection and acquisition of **heart-rate variability (HRV), electrocardiographic (ECG) signals, phonocardiographic (PCG) signals,** and **photoplethysmographic (PPG) signals**.

3.15. Hand geometry recognition

Hand geometry is a widely accepted biometric characteristic that allows the recognition of individuals from the shape of their hands. Hand geometry readers measure the individual's hand along many dimensions including height, width, deviation and angle, and compare those measurements to a reference sample. Although these measurements are not very distinctive amongst people, hand geometry can be very useful for biometric recognition. Major advantages of hand geometry systems include: simple requirements in imaging resolution (hand features can be extracted from low-resolution images); the ability to operate under harsh environmental conditions (hand geometry biometrics are immune, for example, to dirt on the hand and other external factors); and low data-storage requirements. In addition, hand geometry acquisition and recognition are extremely fast. This technique is widely accepted, and the recognition process involves simple data processing. This cluster includes **contact-based hand geometry recognition** and **contactless hand geometry recognition.**

3.16. Periocular recognition

The full region around the eye, including the *sclera, eyelids, lashes, brows and skin*, is known as the *periocular region* and can be acquired non-intrusively and used as a biometric characteristic. *Periocular recognition* offers advantages over full-face recognition as it is least affected by expression variations, ageing effects and changes due to the growth of facial hair. Moreover, this biometric technology may perform better in the case of extreme pose changes when only one eye is completely visible.

3.17. Keystroke recognition

Keystroke dynamics is a behavioural biometric characteristic suitable for the automated recognition of an individual based on their unique typing rhythm. It refers to the detailed timing information and patterns describing how a person types on a digital device's keyboard. Unlike morphological biometric characteristics, such as fingerprint or iris, where specialised sensors are necessary to collect the biometric data from the captured subject, keystroke dynamics can be detected using off-the-shelf physical computer keyboards or virtual keyboards in smartphones and PDAs. Thus, *Keystroke recognition* represents a low-cost solution and is easily deployable in a variety of scenarios. On the other hand, one of the major drawbacks is that a person's typing varies substantially during the day and from day to day, and may be affected by multiple external factors. Although other measurements are conceivable, patterns used in keystroke dynamics are derived mainly from the two events that make up a keystroke: *Key-Down* and *Key-Up*. The Key-Down event takes place at the initial depression of a key, and the Key-Up occurs at the subsequent release of that key. Various unique features are then calculated based on the intra-key and inter-key timing variations between these events. This technological cluster includes **static keystroke recognition** and **dynamic keystroke recognition**.

3.18. Gait recognition

Gait is a type of behavioural biometric characteristic used to recognise individuals by their walking style (or manner) and pace. Gait has several advantages compared to other biometric characteristics: in most modalities, *Gait recognition* is non-intrusive, does not require cooperation from the individual and can function at moderate distances from the subject. This technological cluster is formed by *Gait recognition* technologies based on **video sensors, radar sensors, floor sensors and wearable sensors**.

3.19. Handwriting recognition

Handwriting recognition is the process of recognising the author of a text from their handwriting style, and includes (and mostly refers to) signature recognition. *Handwriting recognition* can be applied to a generic text or to a specific predefined text (usually a signature) and implemented according to two main modalities, included in this technological cluster: **dynamic handwriting recognition** and **static handwriting recognition**.

3.20. Speaker recognition

Speaker recognition refers to a group of technologies that use information extracted from a person's speech to perform biometric operations such as speaker identification and verification. It is based on the extraction of acoustic features of speech that differentiate individuals. These features convey two kinds of biometric information: physiological properties (anatomical configuration of the vocal apparatus) and behavioural traits (speaking style). This technological cluster includes **text-dependent speaker recognition** and **text-independent speaker recognition**.

4. Conclusions

The work presented in *Part 1 – Taxonomy of biometric technologies* focused on a systematic taxonomical categorisation, conducted on a set of identified biometric technologies relevant for border checks. The output of the process consisted of:

a) a **taxonomy of biometric technologies** (whose tree-style graphical representation is shown in Figure 2), developed to establish a common understanding of the biometrics technological domain and to create a reference document that could be used in research and innovation activities in the future.

b) the detailed **description** of the 57 biometric technologies and modalities.

The taxonomy was organised in a three-level hierarchical structure with a progressively increasing degree of complexity: ***first-level*** biometrics macro-areas; ***second-level*** biometric technological fields; ***third-level*** biometric recognition or acquisition technologies and modalities.

Morphological biometrics is the most copious group of biometric technologies pertinent to the investigated application domains of border checks, biometric recognition and access control. Meanwhile, biomolecular biometrics, mostly formed by DNA-related technologies, turned out to be the narrowest macro-area. In fact, even though the DNA-related biometric technologies provide the most reliable results, they are still characterised by highly invasive and low-efficiency sample capture and processing. Behavioural biometrics was also found to be significantly less represented than morphological biometrics. This is possibly due to the high levels of reliability and efficiency required in the investigated domains, which may be difficult for behavioural biometric technologies to achieve.

Patents and scientific literature proved to be suitable sources of information for taxonomy development. Moreover, patents allowed the Research Team to retrieve a higher number of less-known technologies than with the scientific literature. Examples of these are:

- Hand bacteria identification,
- Encephalographic signals,
- Acoustic properties of the ear canal,
- Dental biometrics,
- Tongueprint recognition,
- Cranial suture scanning,
- Rugoscopy,
- Complex eye movement patterns (eye-tracking),
- Oculomotor plant characteristics.

Given the small amount of related documentation, these technologies were not considered in *Patentometric and Bibliometric Analyses*. Nonetheless, their inclusion within the proposed taxonomy is useful as they may be considered for research and innovation activities in the future.

The scientific literature and the knowledge of the Research Team Experts represented the most reliable sources of information to validate and to provide a description of the technologies to be included in the taxonomy. Patents are, in fact, generally written to enlarge the scope of application of the reported inventions, thus often resulting in abstract and non-specific descriptions.

Part 2 – Taxonomy of biometrics-enabled technological systems

5. Methodology

The taxonomy of biometrics-enabled technological systems was developed to provide an indicative reference, definition and classification guide to the systems and sub-systems that will make use of, or rely on, the various individual biometric technologies reported in *Part 1 – Taxonomy of biometric technologies*, within the context of new and emerging methodologies and processes worldwide for border checks and management.

To provide information within the Tech Foresight on Biometrics about the possible future use of biometric technologies within the context of border checks, the Research Team considered the system aspects and use cases to which these various biometric technologies may be applied, as well as how the individual traveller would interact with them.

We analysed the end-to-end journey of a traveller as they encounter various technological systems along their way, from first booking the travel to arrival, passing control and being accepted into their final destination point. Sources such as the vision presented in *IATA NEXTT – Building the journey of the future*,[111] the *World Economic Forum*'s[112] project on *Shaping the Future of Security in Travel*[113] and the *World Travel and Tourism Council*'s[114] (WTTC) publicly available information on the future of travel provided valuable background information. The *2021-26 vision and strategy report*[115] of the *US Customs and Border Protection Agency*[116] (CBP) also provided insight into CBP's thinking about how to facilitate travel while reducing the friction of interaction with the traveller, yet maintaining and enhancing the prerequisites of national security.

The taxonomy of biometrics-enabled technological systems took into consideration the Research Team Experts' knowledge regarding existing and projected systems worldwide, along with *EU-funded* projects such as *PROTECT*[117] and *D4FLY*,[118] which are part of the EU's Horizon 2020 research and innovation funding programme focused on researching and evaluating the security and convenience aspects of potential future traveller management systems.

111 https://www.nextt.aero/en/
112 https://www.weforum.org/
113 https://www.weforum.org/videos/shaping-the-future-of-security-in-travel
114 https://wttc.org/
115 https://www.cbp.gov/newsroom/national-media-release/cbp-releases-2021-2026-strategy
116 https://www.cbp.gov/
117 http://projectprotect.eu/
118 https://d4fly.eu/

The taxonomy first identified, at the top level, groups of systems that may use biometric technologies a traveller would knowingly or unknowingly interact with along their journey. For example, the top level includes the group of large-scale IT systems that form the all-important data analysis and decision-making back-end infrastructure that ultimately provides the informative distillation of data on which a border guard authority, or in the case of automation an ABC system, permits or denies the traveller passage across a state border.

Each of these top-level groups was then sub-divided into second-level categories that encompass all the possible types of instantiations of a particular group. In each category, there is a specific element of biometric data acquisition and evaluation that relates to an aspect of recognising travellers and ascertaining their entitlement to travel.

The taxonomy should be read in conjunction with the *Technical Guide for Border Checks on EES-related equipment*[119] recently published by Frontex. This technical guide provides an overview of the minimum technical requirements for Manual Border Control (MBC) Systems; Self-Service Systems (SSS); e-Gates & Automated Border Control (ABC) Systems; and Mobile Systems. One of its primary aims is the technical support of Member States' procurements related to the implementation of the EU Entry/Exit System. The technical guide does make significant reference to MBC Systems, which were not explicitly covered in the taxonomy. However, current MBC Systems and their likely evolution in the immediate future use many of the technological sub-systems detailed in the taxonomy.

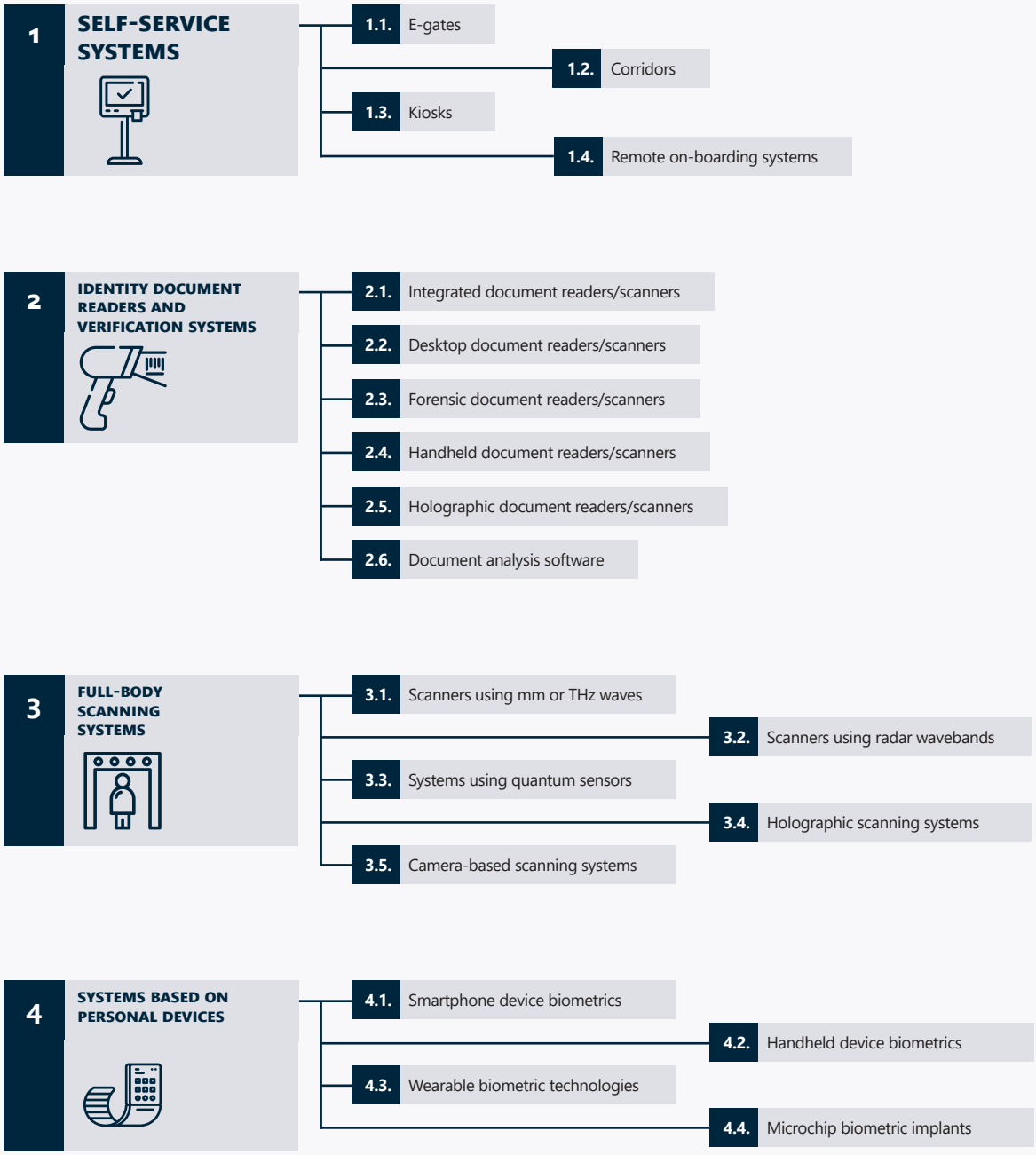
The proposed taxonomy of biometrics-enabled technological systems focuses on solutions that can be used to design and implement a preferred service architecture over a period in which seamless and automated border checks are expected to become the norm rather than the exception.

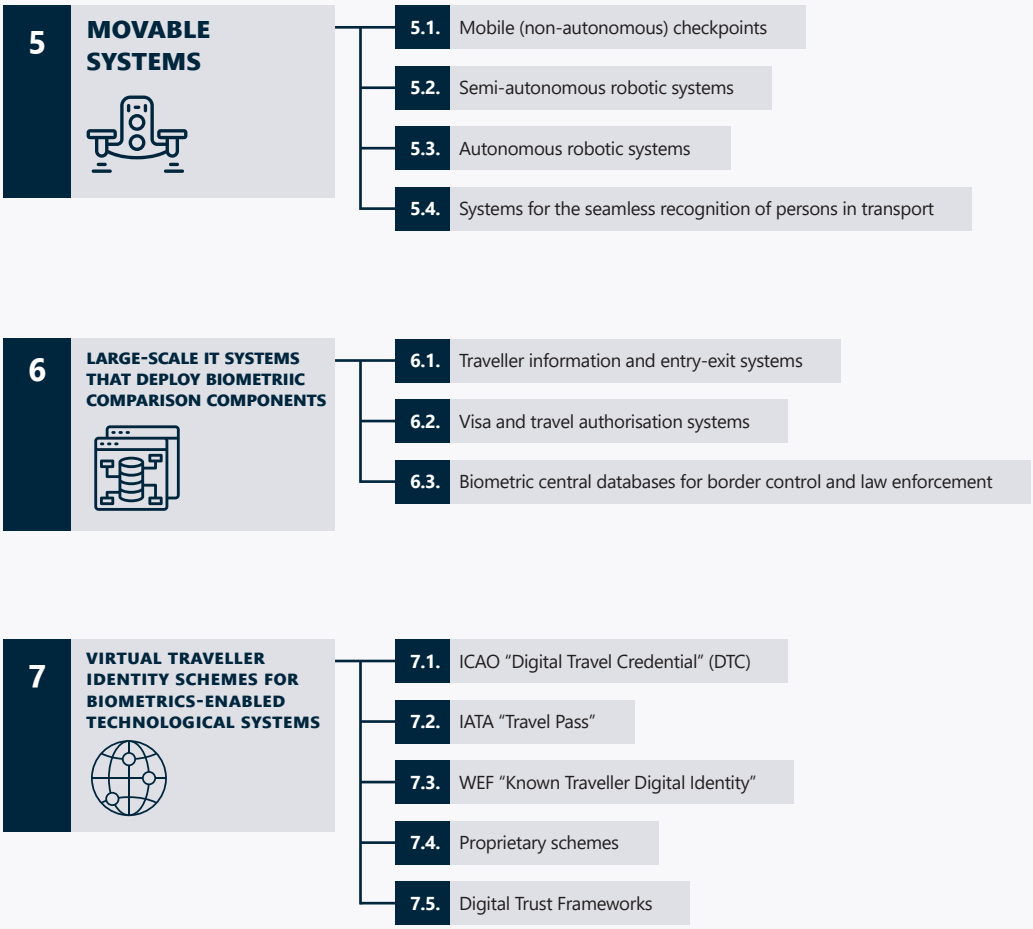
119 European Border and Coast Guard Agency, "Technical Guide for Border Checks on Entry/Exit Systems (EES) related equipment", Publications Office of the European Union, Luxembourg, 2021.

6. Taxonomy description

The final tree-style representation of the proposed taxonomy of biometrics-enabled technological systems is shown in Figure 3. The following sections contain a description for each element of the tree.

Figure 3: *Graphic representation of the taxonomy of biometrics-enabled technological systems.*





Please note that the references given below include publicly available materials provided by several commercial companies. References do not imply any commercial interest by EU entities nor make any recommendation. The reference citations are simply intended to assist with the illustration or description of a specific use case or examples of products and services useful for the construction of the taxonomy.

6.1. Self-service systems

Systems with which a traveller can interact on their own without requiring direct supervision or interaction with another person or official.

6.1.1. E-gates

This category includes Automated Border Control (ABC) and Assisted Border Control gates that are connected to a system with sensors that automatically or semi-automatically

recognises the traveller using protocols and checks approved for the purpose of a state's immigration policy.[120, 121, 122, 123]

6.1.2. Corridors

This category refers to multi-sensor deployments designed to operate within corridors/spaces where travellers walk/ride, for the purpose of guiding and performing the biometric acquisition and recognition of those individuals within the corridor or space.

There are possible sub-categories:[124, 125, 126]

- 6.1.2.1 single person, single lane,
- 6.1.2.2 single person, multi-lane,
- 6.1.2.3 multi-person, single lane,
- 6.1.2.4 multi-person, multi-lane,
- 6.1.2.5 defined space, without lanes or files.

6.1.3. Kiosks

This category refers to self-service systems that may be deployed in various locations within an international travel terminal, e.g. check-in, pre-entry, pre-exit, and transit. Kiosks provide system-connected functions such as document and ticket checking, issuing boarding passes, baggage check-in, verification of API/PNR manifests, and verification back to the system that a traveller is within the terminal complex.[127]

6.1.4. Remote on-boarding systems

This category refers to systems[128] in which a personal device (e.g. a device belonging to Category 6.4 in this taxonomy) is used to collect initial data, potentially including biometrics, for the purpose of verifying a traveller, their journey and their rights to travel.

120 See for example https://www.cbp.gov/newsroom/national-media-release/cbp-enhances-biometrics-non-us-travelers-entering-and-exiting-united

121 J. Sanchez del Rio, "Automated border control e-gates and facial recognition systems", Elsevier Computers and Security, vol. 62, pp. 49-72, 2016.

122 C. Morosan, "Information Disclosure to Biometric E-gates: The Roles of Perceived Security, Benefits, and Emotions", Journal of Travel Research, vol. 57, no. 5, pp. 644-657, 2017.

123 See also Section 3.3 in: European Border and Coast Guard Agency, "Technical Guide for Border Checks on Entry/Exit Systems (EES) related equipment", Publications Office of the European Union, Luxembourg, 2021.

124 See also https://www.futureairport.com/contractors/airport-security/kaba-gallenschuetz-gmbh/

125 O. Hamdoun, "Person re-identification in multi-camera system by signature based on interest point descriptors collected on short video sequences", 2nd ACM/IEEE International Conference on Distributed Smart Cameras (ICDSC-08), Stanford, Palo Alto, 2008.

126 M. M. Kalayeh, E. Basaran, M. Gökmen, M. E. Kamasak and M. Shah, "Human Semantic Parsing for Person Re-Identification", Proc IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2018.

127 See for example https://www.idemia.com/morphomaestro-kiosks-and-gates-supervision

128 Two of many examples of typical commercial offerings are given in:
https://www.idemia.com/news/future-remote-identity-verification-and-digital-onboarding-2020-05-14
https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/identity-verification

Further functions might include pre-populating traveller information (e.g. API/PNR) into the system that will eventually verify the traveller throughout their journey, from departure to destination arrival and immigration check. Analogous to KYC (Know Your Customer) systems used for on-boarding in online and digital banking systems.

6.2. Identity document readers and verification sub-systems

Equipment and software for reading and verifying the data contained in eMRTDs and managing its transfer to other sub-systems, including the large-scale IT systems of Category 6.6.

6.2.1. Integrated document readers/scanners

These systems typically include a *video spectral comparator* equipped with multiple illumination sources (usually Visible, NIR, UV) for scanning and verifying high resolution images of government-issued documents such as passports, visas, and ID cards including eMRTDs.[129] They also usually include ICAO-compliant chip reading and verification functions, e.g. for reading biometric and biographic data (accessing stored biometric data from a chip or other source) and verification (confirming a biometric claim through biometric comparison[130]). Deployed in kiosks and e-gates.[131]

6.2.2. Desktop document readers/scanners

Similar to 6.2.1, but with a different form-factor more suitable for stand-alone use at BCP desks for first-line inspection.[132]

6.2.3. Forensic document readers/scanners

Scanners that may be deployed as second- or third-line document inspection devices, where checks conducted using a Category 6.2.1 or 6.2.2 device fail or flag a suspicious document. These instruments offer higher resolution imaging, special-purpose image extraction capabilities and the ability to visualise holographic/diffractive security features. They may also include ICAO-compliant chip reading and verification.[133]

129 See for example:
https://regulaforensics.com/en/products/
https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/document-readers/oem-kiosk-readers
https://www.desko.com/en/products/overview/desko-penta-scanner/

130 ISO, International Standard ISO/IEC 2382-37:2017 — Information technology — Vocabulary — Part 37: Biometrics, 2017.

131 See Paragraph 2.2.2 in: European Border and Coast Guard Agency, "Technical Guide for Border Checks on Entry/Exit Systems (EES) related equipment", Publications Office of the European Union, Luxembourg, 2021.

132 One example of commercial offering: https://www.desko.com/en/products/overview/desko-penta-scanner/

133 See for example this commercial offering: https://regulaforensics.com/en/products/special_equipment/8850/

6.2.4. Handheld document readers/scanners

Handheld devices with a dedicated, multi-illumination document reader/scanner[134] function, providing similar functionality to devices described in Categories 6.2.1 or 6.2.2.

6.2.5. Holographic document readers/scanners

Specialised document readers, or adjunct devices to document readers, which scan documents' holographic/diffractive optical security features.[135] So far, equipment that truly separates imagery from holographic or diffractive optically variable security features appears to be limited to equipment specifically aimed at forensic document inspection tasks, for example[136] Category 6.2.3.

6.2.6. Document analysis software

Category that refers to the dedicated software that works with data fed into the underlying border management IT system for the purpose of verifying data and images acquired through identification document readers of the type described in Categories 6.2.1–6.2.5 of this taxonomical group. This software may include biometric data extraction (e.g. photos from the chip) and potentially biometric matching functions.[137]

134 See an example of commercial offering at: https://regulaforensics.com/en/products/machine_verification/7308/

135 See https://www.biometricupdate.com/202012/new-id-document-scanning-technologies-address-security-privacy-concerns

136 One example of commercial offering may be found at: http://www.fosterfreeman.com/product/qde-products/580-vsc8000.html

137 See an example of commercial offering at: https://regulaforensics.com/en/products/advanced_verification/frontline-documents-system/

6.3. Full-body scanning systems

Equipment that acquires images for biometric purposes from a traveller's whole body, using techniques described in the following paragraphs. The subsequent analysis of the acquired images may occur within the scanner equipment itself or may be passed to another sub-system.

6.3.1. Scanners using mm or THz waves

This category refers to full-body imaging systems designed to use stimulus and detection devices operating in the 30 GHz to 300 GHz frequency bands (10 mm-1 mm wavelength or "mm wave") or in the 300 GHz to 10 THz frequency bands (1 mm to 30 um wavelength or "THz wave") of the electromagnetic spectrum. Such systems are currently used in security screening for concealed item detection but have the technical potential to be used for biometrics.[138, 139, 140]

Note that mm-wave radars (see 6.3.2) operating at ~30 GHz could also be considered in this category, as their spectral band overlaps with the lowest frequency considered in this category.

6.3.2. Scanners using radar wavebands

This category refers to full-body imaging systems designed to use stimulus and detection devices operating in the parts of the electromagnetic spectrum associated with radars[141] (wavelength in the range of 30 cm to 10 mm or frequency from 1 to 30 GHz).[140]

6.3.3. Systems using quantum sensors

A quantum sensor is a quantum device (usually referring to quantised energy levels and the exploitation of quantum mechanical phenomena) that responds to a stimulus using quantum coherence to measure a physical quantity,[142] or using entanglement to improve measurements beyond what can be achieved with classical sensors.[143] Making quantum measurements of human body attributes for application in biometrics is at a very early stage of research.

138 J. Laviada, A. Arboleya-Arboleya and F. Las Heras, "Multistatic Millimeter-Wave Imaging by Multiview Portable Camera", IEEE Access, vol. 5, pp. 19259-19268, 2017.

139 D. McMakin, "New Improvements to Millimeter-Wave Body Scanners", 3D BODYTECH 2017 – 8th Int. Conf. and Exh. on 3D Body Scanning and Processing Technologies, Montreal, Canada, 2017.

140 D. McMakin, D. M. Sheen, T. E. Hall, M. O. Kennedy and H. P. Foote, "Biometric identification using holographic radar imaging techniques", Defense and Security Symposium, Orlando, Florida, United States, 2007.

141 Radar wave-band definitions can be found at: https://www.radartutorial.eu/07.waves/Waves%20and%20Frequency%20Ranges.en.html

142 See for example https://www.quantumsensors.org/technology/sensing-the-brain

143 T. Bowler, "How quantum sensing is changing the way we see the world", BBC News, 8 March 2019.

6.3.4. Holographic scanning systems

Category of systems that refers to a real-time optical recording technique in which holographic information about a three-dimensional (3D) object (in this case all or part of a human body) is acquired using a single two-dimensional (2D) active optical scan.[144]

6.3.5. Camera-based scanning systems

This category encompasses camera-based data acquisition systems intended for multi-purpose sensing, e.g. face, gait, and somatotype. They may typically deploy an array of cameras, whose spatial geometry may be important to the biometric acquisition process, and require specific image analytic techniques for decoding the biometric data so acquired, e.g. photogrammetry. The camera array may include devices specialised for different wavelengths, e.g. Visible, NIR, SWIR, MWIR, and LWIR.[145]

144 T. Chung Poon, "Optical Scanning Holography – A Review of Recent Progress", Journal of the Optical Society of Korea, vol. 13, no. 4, pp. 406-415, 2009.

145 A. Jirafe, M. Jibhe and V. Satpute, "Camera Handoff for Multi-camera Surveillance", Applications of Advanced Computing in Systems. Algorithms for Intelligent Systems, Springer Singapore, 2021.

6.4. Systems based on personal devices

Personal devices such as smartphones and smartwatches contain many sensors from which biometric data may be acquired and analysed, either within the device itself where appropriate or by transmitting the data via a suitable route to another sub-system.

6.4.1. Smartphone device biometrics

This category comprises system use cases where biometric data is acquired and aggregated using the built-in sensors of a smartphone, and where such data is either completely or partially processed locally on the device and includes the associated data analysis and communication methodology.[146, 147]

6.4.2. Handheld device biometrics

This category comprises system use cases similar to 6.4.1 but where a dedicated handheld device (which may or may not be based on commercial smartphone technology) is used.[148, 149] Typically, such use cases refer to the trusted usage of the device by an official and may circumvent the issue of trust in the data source.

6.4.3. Wearable biometric technologies

This category refers to biometric sensors embedded within devices or clothing worn by a user and from which biometric data may be acquired, aggregated, analysed and communicated to an external system.

6.4.4. Microchip biometric implants

This category encompasses chip-based devices embedding biometric sensors, implanted in a user's body for the purpose of acquiring, aggregating, analysing, and communicating biometric data to an external system.[150] Such biometric implants would typically comprise three components: an integrated circuit with embedded sensors for acquiring, pre-processing, and possibly temporarily storing biometric information, an antenna for receiving and transmitting signals between that circuit and an external reader/processor, and a means for supplying power to the whole assembly.[151]

146 R. Blanco-Gonzalo and R. Sanchez-Reillo, "Biometrics on Mobile Devices", Encyclopedia of Biometrics, Springer, Boston, 2014, pp. 1-8.

147 See also Digital Mobile equipment and application for travellers within Paragraph 1.5.3 in: European Border and Coast Guard Agency, "Technical Guide for Border Checks on Entry/Exit Systems (EES) related equipment", Publications Office of the European Union, Luxembourg, 2021.

148 An example of a commercial offering: https://news.northropgrumman.com/file?fid=57d963042c-fac27bff90edeb

149 Another example of a commercial offering: https://www.irisid.com/productssolutions/hardwareproducts/icam-m300/

150 P. Rotter, B. Daskala and R. Compañó, "RFID implants: Opportunities and challenges for identifying people", Technology and Society Magazine, vol. 27, pp. 24-32, 2008.

151 For example, a commercial offering may be found at: https://www.vivokey.com/ecosystem

6.5. Movable systems

Systems for collecting data about an individual traveller or user but comprising equipment that can be moved either under human control or autonomously to interact with the user (rather than the user deliberately moving into place).

6.5.1. Mobile (non-autonomous) checkpoints

These systems represent a variation of the kiosk theme of Category 6.1.3 but refer to devices that can be moved up to a user, either under supervised, remote control or self-service operation.[152]

6.5.2. Semi-autonomous robotic systems

Devices or equipment that carry biometric sensors (e.g. cameras), and that move under remote or supervised control to detect and recognise persons within a controlled area; for example drones which are remotely controlled by a human operator to locate the subject of interest.[153] Data acquisition and analysis tasks will be largely or entirely automated.

6.5.3. Autonomous robotic systems

Devices or equipment that carry biometric sensors (e.g. cameras) and that move autonomously (i.e. without explicit human control) to detect and recognise persons within an area; for example drones with autonomous "seek and detect" capability.[154]

6.5.4. Systems for the seamless recognition of persons in transport

Systems capable of seamless biometric acquisition and recognition of persons staying inside various vehicles or modes of transport, i.e. in trucks, cars, coaches, trains, and ships.[155]

152 In the EU EES context, such mobile checkpoints are covered in Paragraph 1.5.3 in: European Border and Coast Guard Agency, "Technical Guide for Border Checks on Entry/Exit Systems (EES) related equipment", Publications Office of the European Union, Luxembourg, 2021.

153 H.-J. Hsu and K.-T. Chen, "Face Recognition on Drones: Issues and Limitations", DroNet '15: Proceedings of the First Workshop on Micro Aerial Vehicle Networks, Systems, and Applications for Civilian Use, Florence, Italy, 2015.

154 Y. Kortli, M. Jridi, A. Al Falou and M. Atri, "Face Recognition Systems: A Survey", Sensors, vol. 20, no. 2, p. 342, 2020.

155 M. Ruby, "The Mertens Unrolled Network (MU-Net): a high dynamic range fusion neural network for through the windshield driver recognition", DeepAI, 2020.

6.6. Large-scale IT systems that deploy biometric comparison components

These are the back-end systems and infrastructure that analyse and evaluate the data collected from individual travellers and users as they interact with the data collection front-end systems.

6.6.1. Traveller information and entry-exit registration systems

Large-scale IT systems capable of electronically registering the time and place of transit (entry and exit) of travellers through a border crossing point and calculating the duration of their authorised stay. These systems usually deploy document readers as well as biometric acquisition and recognition systems and have access to central or federated biometrics data repositories that are used for biometric comparison and identification in the context of border checks (at exit or entry). Typically, biometric samples, along with other data associated with the individual in question, are submitted to the system and a pass/fail result for verification or an identification result is returned, often with a confidence score, and with watchlist detection which may be via associated queries to other databases that are not an integral part of the Entry-Exit System itself. Examples of this are the EU Entry/Exit System[156] (EES) and the Biometric Facial Comparison system used within the US CBP[157] proposed Biometric Entry/Exit Program.[158, 159, 160, 161, 162]

EU large-scale IT systems that use biometrics and may be queried during part of an entry/exit process include[163] the Entry/Exit System (EES), the Schengen Information System (SIS), the Visa Information System (VIS), the European Asylum Dactyloscopy Database (Eurodac) and the European Criminal Records Information System – Third Country Nationals (ECRIS-TCN).

6.6.2. Visa and travel authorisation systems

Large-scale IT systems that underpin visa policies and electronic visa waiver schemes to facilitate border checks as well as pre-travel authorisation systems to verify whether a traveller meets entry requirements before travelling to a certain destination. In the EU,

156 https://ec.europa.eu/home-affairs/what-we-do/policies/borders-and-visas/smart-borders/ees_en

157 https://biometrics.cbp.gov/

158 G. Glouftsios, "Governing border security infrastructures: Maintaining large-scale information systems", Security Dialogue, 2020.

159 A. Helala, H. Muhammad, A. Hatim and A. Mansour, "A Large-Scale Study of Fingerprint Matching Systems for Sensor Interoperability Problem", Sensors, vol. 18, no. 4, p. 1008, 2018.

160 S. Hemalatha, "A systematic review on Fingerprint based Biometric Authentication System", 2020 International Conference on Emerging Trends in Information Technology and Engineering (IC-ETITE), 2020.

161 European Agency for the operational management of large-scale IT systems in the area of freedom, Biometrics in Large-Scale IT. Recent trends, current performance capabilities, recommendations for the near future, 2015.

162 Congressional Research Service (CRS), Biometric Entry-Exit System: Legislative History and Status, 2020.

163 A description of such large-scale IT systems may be found at: https://www.eulisa.europa.eu/Activities/Large-Scale-It-Systems

systems that perform these functions include the Visa Information System (VIS)[164] and the European Travel Information and Authorisation System (ETIAS).[165] Examples outside the EU are ESTA[166] (in the US), the eTA[167] (in Canada), and the NZeTA[168] (in New Zealand). These systems may have potential to collect biometric data, e.g. by reading the biometric information stored in an e-passport chip where this is used to facilitate the traveller's enrolment into the visa or travel authorisation system.

6.6.3. Biometric central databases for border control and law enforcement

Databases of biometric data that may be accessed as part of a border check on an individual, for example, to ascertain whether that person is a known criminal, terrorist or on a wanted watchlist, or to deal with asylum seekers and irregular migrants. Examples of such databases in the EU are the Schengen Information System (SIS II)[169], the European Asylum Dactyloscopy Database (Eurodac)[170] and the European Criminal Records Information System – Third Country Nationals (ECRIS-TCN)[171] managed by eu-LISA,[172] and the Europol Information System (EIS).[173]

164 https://www.eulisa.europa.eu/Activities/Large-Scale-It-Systems/Vis
165 https://www.eulisa.europa.eu/Activities/Large-Scale-It-Systems/Etias
166 https://www.cbp.gov/travel/international-visitors/esta#
167 https://www.canada.ca/en/immigration-refugees-citizenship/services/visit-canada/eta.html
168 https://www.immigration.govt.nz/new-zealand-visas/apply-for-a-visa/about-visa/nzeta
169 https://www.eulisa.europa.eu/Activities/Large-Scale-It-Systems/Sis-Ii
170 https://www.eulisa.europa.eu/Activities/Large-Scale-It-Systems/Eurodac
171 https://www.eulisa.europa.eu/Activities/Large-Scale-It-Systems/Ecris-Tcn
172 https://europa.eu/european-union/about-eu/agencies/eu-lisa_en#overview
173 https://www.europol.europa.eu/operations-services-and-innovation/services-support/information-exchange/europol-information-system

6.7. Virtual traveller identification schemes for biometrics-enabled technological systems

Systems and processes aimed at facilitating the journey of an individual traveller to ultimately make it seamless, from initial journey booking, through the verification of entitlement, to arrival and acceptance into their destination.

6.7.1. ICAO "Digital Travel Credential" (DTC)

Virtual traveller identity scheme conforming to the specifications defined by the *ICAO*, including its issuance and verification protocols.[174]

6.7.2. IATA "Travel Pass"

Virtual traveller identity scheme conforming to specifications defined by *IATA*, including its issuance and verification protocols.[175] Travel Pass is part of the *IATA NEXTT*[176] initiative and uses the *OneID*[177] traveller digital identity concept developed by IATA.

6.7.3. WEF "Known Traveller Digital Identity" (KTDI)

Virtual traveller identity scheme conforming to specifications defined by the World Economic Forum (WEF), including its issuance and verification protocols. It uses open-source techniques described in the *Commons project*.[178]

6.7.4. Proprietary schemes

Other commercial proprietary schemes for preparing, issuing, and verifying virtual traveller identity credentials, which may or may not conform to or implement techniques described in Categories 6.7.1, 6.7.2 or 6.7.3 and which may include biometric content, as proposed by various companies.[179]

174 ICAO Technical Advisory Group on the Traveller Identification Programme (TAG/TRIP), Subgroup of the New Technologies Working Group (NTWG), "Guiding Core Principles for the Development of Digital Travel Credential (DTC)", 2020.

175 Find more at: https://www.iata.org/en/programs/passenger/travel-pass/

176 https://www.nextt.aero/en/

177 https://www.iata.org/en/programs/passenger/one-id/

178 https://ktdi.org/
https://www.weforum.org/agenda/2020/08/covid19-coronavirus-travel-data-privacy-commonpass/

179 Some examples:
Zamna (https://zamna.com/)
Travizory (https://www.travizory.com/)
Daon (https://www.daon.com/verifly-seamless-travel/verifly-solution)
HID (https://www.hidglobal.com/citizen-identity)
Idemia (https://www.idemia.com/easy-and-legitimate-border-crossing)
SITA (https://www.sita.aero/pressroom/news-releases/sita-steps-up-smart-border-solutions-to-support-new-regulations-for-entry-and-exit-to-the-eu-schengen-zone/)

6.7.5. Digital Trust Frameworks

This category includes systems and protocols that typically deploy privacy-enhancing techniques to protect Personally Identifiable Information (PII), including biometric data, while facilitating the querying and verification of such PII data.[180] They are an important mechanism to be considered for the implementation of virtual traveller identity schemes.

180 For example, see:
https://www.gov.uk/government/publications/the-uk-digital-identity-and-attributes-trust-framework/
https://www.dta.gov.au/our-projects/digital-identity/trusted-digital-identity-framework
https://digital-strategy.ec.europa.eu/en/library/building-trusted-and-secure-european-digital-identity-brochure

7. Conclusions

It is hoped that the proposed taxonomy of biometrics-enabled technological systems provides an informative starting point from which forward-thinking into the deployment of biometrics, as well as the systems and sub-systems that use the biometric data, may be further developed for a more efficient management of border control.

Three key aspects are suggested to be considered when implementing future biometrics-enabled technological systems:

1. Ways in which individual travellers, including those with differing levels of ability and understanding, are likely to interact with and react to the systems and processes they encounter or are presented with.
2. The progress of technology and its capabilities within the various categories identified in the taxonomy, taking into account how the sub-systems might interact with and complement each other.
3. The progress of legislation related to the employment and ethics of biometrics as well as the balance between protecting fundamental rights and maintaining the security and integrity of external borders.

Furthermore, as anticipated in the introduction, this taxonomy played an essential role within the Tech Foresight on Biometrics in guiding the development of technological roadmaps, where a specific layer was included to envisage future products and systems that might emerge exploiting the biometric technologies included in the clusters.

FRONTEX
EUROPEAN BORDER AND COAST GUARD AGENCY

Plac Europejski 6, 00-844
Warsaw, Poland
T +48 22 205 95 00
F +48 22 205 95 01
frontex@frontex.europa.eu
www.frontex.europa.eu

PDF:
TT-07-22-749-EN-N
ISBN 978-92-9467-444-9
doi 10.2819/349227

Print:
TT-07-22-749-EN-C
ISBN 978-92-9467-443-2
doi 10.2819/181163

FPI 22.0060

EPUB:
TT-07-22-749-EN-E
ISBN 978-92-9467-509-5
doi 10.2819/517194

MOBI:
TT-07-22-749-EN-L
ISBN 978-92-9467-510-1
doi 10.2819/212160