

INTRODUCTION TO BIOMETRICS

The opinions expressed in this publication are those of the authors and do not necessarily reflect the views of the International Organization for Migration (IOM). The designations employed and the presentation of material throughout the publication do not imply expression of any opinion whatsoever on the part of IOM concerning the legal status of any country, territory, city or area, or of its authorities, or concerning its frontiers or boundaries.

IOM is committed to the principle that humane and orderly migration benefits migrants and society. As an intergovernmental organization, IOM acts with its partners in the international community to: assist in meeting the operational challenges of migration; advance understanding of migration issues; encourage social and economic development through migration; and uphold the human dignity and well-being of migrants.

This publication is adhered to the IOM Legal Identity Strategy, in particular contributing to Pillar 2. Assisting Migrants without legal identity documents and Pillar 3. Supporting national civil registration and identity management systems to facilitate regular migration and mobility through supporting Member States in the responsible use of biometrics. In addition, the publication is also in line with Objective 4 of the Global Compact for Safe, Orderly, and Regular Migration, under which States committed to “fulfill the right of all individuals to a legal identity by providing all nationals with proof of nationality and relevant documentation”.

This publication was made through the support provided by the Danish Ministry of Foreign Affairs as part of the IOM RELICA Global Programme, aimed at developing readmission capacities in selected countries across the globe through ID management and assist them in improving their abilities to provide access to legal identity, based on their respective needs and bilateral negotiations on readmission. The overall goal of the project is to establish or strengthen robust identification mechanisms in the selected countries to address the global legal identity gap and lay the fundamental foundations for the global roll-out of the electronic Readmission Case Management System (eRCMS). This comprehensive approach ensures that previously undocumented third-country nationals are better protected at home and on the move on the one hand, while facilitating the identification of irregular migrants in view of their readmission on the other. The opinions expressed herein are those of the author and do not necessarily reflect the views of Danish Government.

This document does not constitute an official IOM biometrics policy.

Publisher: International Organization for Migration
17 route des Morillons
P.O. Box 17
1211 Geneva 19
Switzerland
Tel.: +41 22 717 9111
Fax: +41 22 798 6150
Email: hq@iom.int
Website: www.iom.int

This publication was issued without formal editing by IOM.

Cover photos: Biometrics registration. © IOM 2019/Muse MOHAMMED

Required citation: Hofstetter, S. D., R. Rajeshkumar and A. Kenney (2024). *Introduction to biometrics*. International Organization for Migration (IOM), Geneva.

Coordination: Goncalves, N. and A. Boronbaeva.

ISBN 978-92-9268-799-1 (PDF)

© IOM 2024



Some rights reserved. This work is made available under the [Creative Commons Attribution-NonCommercial- NoDerivs 3.0 IGO License](https://creativecommons.org/licenses/by-nc-nd/3.0/igo/legalcode) (CC BY-NC-ND 3.0 IGO).*

For further specifications please see the [Copyright and Terms of Use](#).

This publication should not be used, published or redistributed for purposes primarily intended for or directed towards commercial advantage or monetary compensation, with the exception of educational purposes, e.g. to be included in textbooks.

Permissions: Requests for commercial use or further rights and licensing should be submitted to publications@iom.int.

* <https://creativecommons.org/licenses/by-nc-nd/3.0/igo/legalcode>.

PUB2023/073/R*

INTRODUCTION TO BIOMETRICS



**MINISTRY OF FOREIGN AFFAIRS
OF DENMARK**

CONTENTS

ACRONYMS	VI
FOREWORD	VII
PART 1. INTRODUCTION TO BIOMETRICS	1
1.1 What is biometric data	2
The purpose	2
How it works	2
1.2 Types of biometrics	4
1.3 Modalities	5
1.4 Uses of biometrics	5
Supporting civil registry	6
Participation in civic activities	6
Border control	6
Humanitarian interventions and site management	8
Balancing benefits and risk	8
PART 2. SOCIETY, HISTORY AND RESPONSIBLE USE	10
2.1 Impacts on society	11
2.2 Ethics and origins	12
2.3 Biometrics and bias	14
2.4 Biometrics and children	14
2.5 Use in humanitarian settings	15
PART 3. GOVERNANCE AND SAFEGUARDING	16
3.1 Responsibility, proportionality, duty of care	17
3.2 Minimum criteria	18
3.3 Accountability	20
3.4 Jurisdictional requirements	20
PART 4. MANAGEMENT OF BIOMETRICS	22
4.1 Data storage	23
Storage models	23
4.2 Maintenance of data and databases	25
Why is maintenance needed	25
Updating biometric data	26
Considering EOI principles	27
Security of biometrics	27
How are biometrics secured on travel documents	28
4.3 Measuring biometric performance: reliability and error	28
4.4 System bias	29
Under-representation in datasets	31
4.5 Vulnerability of biometric systems	31
Presentation attack	31
Presentation Attack Detection (PAD)	32
Morphing	32

4.6	Bilateral sharing of biometric data	32
	Risk and concern	33
	Function creep	33
	Covert collection	33
	Secondary information	33
	Data segregation	34
4.7	On Procurement of biometric technology	34
	Recommendations on procurement for biometrics	34
PART 5. TECHNICAL IMPLEMENTATION		36
5.1	Fingerprint	37
	Representation of fingerprints	38
	Capturing of fingerprints	39
	Quality of fingerprints	40
5.2	Face	40
	Representation of facial biometrics	44
	Capturing of facial biometrics	44
	Quality of facial biometrics	44
5.3	Iris	45
	Representation of iris biometrics	45
	Capture of the iris biometrics	46
	Quality of iris biometrics	46
5.4	Multi-modality	47
PART 6. IOM PROGRAMMING WITH BIOMETRIC COMPONENTS		48
6.1	Use case 1: MIDAS	49
6.2	Use case 2: e-RCMS	52
	e-RCMS and biometrics	53
PART 7. TECHNOLOGY LOOKING AHEAD		57
7.1	Touchless	58
7.2	Self-Service capabilities for users	58
7.3	Presentation attack / deep Fake / liveness	58
7.4	Testing and dataset improvements	59
7.5	Policies	59
7.6	Artificial intelligence	59
7.7	Evolving industry	60
CONCLUSION		61
TECHNICAL TERMINOLOGY		62

LIST OF FIGURES AND TABLES

FIGURES

Figure 1. Initial process of collecting biometric data	3
Figure 2. Process of biometric identification	3
Figure 3. Process of biometric authentication	4
Figure 4. Significant developments contributed to the exponential growth of biometrics over the century	13
Figure 5. Visualization of the equal error rate point in function of the sensitivity respectively level of security, and the percentage of times a false reject and false accept occur	29
Figure 6. Generation of biometric templates	30
Figure 7. Accurate and robust neural networks for face morphing attack detection	32
Figure 8. Arch, Loop and Whorl	37
Figure 9. Greyscale, Phase and Skeleton image	38
Figure 10. Forms of minutiae	38
Figure 11. Eigenfaces	41
Figure 12. Fisherfaces	42
Figure 13. Bayesian Face Recognition. "Dual" Eigenfaces: (a) Intrapersonal, (b) Extrapersonal	42
Figure 14. Elastic Bunch Graph Matching (EBGM – Grids for face recognition)	43
Figure 15. PCANet	43
Figure 16. Iris localization. Left prior to processing; Right after machine processing and localization	45
Figure 17. Detection of the inner and outer boundaries of the iris	45
Figure 18. Iris captured using visible light (left) and infrared light (right)	46

TABLES

Table 1. Suggested frequency for updating biometric data according to age cohort, as discussed in CEN TC224 WG18 in 2023	26
Table 2. IOM projects with biometrics components (past and ongoing)	54

ACRONYMS

1:1	One to one
1:N	One to many
AI	Artificial Intelligence
BC	(Year zero)
DNA	Deoxyribonucleic Acid
DTM	Displacement Tracking Matrix (IOM programme)
EBGM	Elastic Bunch Graph Matching
eMRTD	Electronic Machine-Readable Travel Document
EOI	Evidence of Identity (principles)
FAR	False Acceptance Rate
FNMR	False non-match rate
FRR	False Rejection Rate
iAPI	Interactive Air Passenger Information
ICAO	International Civil Aviation Organization
ID	Identification
IDP	Internally Displaced Person(s)
IOM	International Organization for Migration
ISO	International Organization for Standardization
MIDAS	Migration Information and Data Analysis System (IOM system)
MRTD	Machine Readable Travel Documents
NFIQ	NIST Fingerprint Image Quality
NIST	National Institute of Standards and Technology (of USA)
PAD	Presentation Attack Detection
PCA	Principal Component Analysis
WFP	World Food Programme

FOREWORD

Biometric technologies, simply referred to as “biometrics”, have a broad reputation as a tool for state security, and are widely considered to be a vital part of migration management. Biometrics can streamline and modernize border management processes whereby governments and partner agencies can, for example, carry out verification when issuing identity documents, facilitate and expedite regular and safe cross-border mobility, enhance the digitization and automation of application processes, and play a critical role in border security. Biometrics are increasingly employed as a tool for identity management, which can impact access to and participation in civic and consumer life from the time a person is very young. In other migration contexts such as crisis and displacement, biometrics can be used in the registration of displaced persons and specific groups of vulnerable migrants, including for the distribution of humanitarian assistance.

Biometrics is generally recognized as sensitive personal data, and consequently its processing is subject to relevant legal and data protection legislation. Biometrics has a considerable impact on the rights of the individual, both nationals and non-nationals, especially on the right to privacy. When designing biometric systems and considering the functional requirements of the system, it is crucial to ensure that data subjects are well-informed about how their data is processed, can access their data, understand its usage, and can make decisions regarding its continued processing. Further, the principle of data minimization is effectively applied when processing personal data associated with a biometric profile. This means limiting the collection of information to only what is necessary to fulfill the specified purpose. Pseudonymization techniques should also be employed to enhance privacy and security.

While biometrics are only a tool for identity management and do not confer identity, they can offer significant advantages and benefits to its users in terms of accessibility, eligibility and inclusion across all strata of society.¹ It can simplify processes, replace paper-based systems and their vulnerability to security breaches as well as human error, and reduce the amount of detail required to express verbally at points of contact. Like any technology there are drawbacks, both real and hypothetical, linked to concepts of data protection and privacy, risks of misrepresentation and technical error, and the often suppressed but important historic linkages to the commodification of humans, racialized surveillance and other grave injustices. There can be considerable impacts on the rights of the individual and in the context of migration management, there are implications for nationals and non-nationals alike, in particular their right to move freely in the event of an incorrect or a failure to collect biometric reading.²

If the responsible use of biometrics can be ensured – encompassing the design, implementation, maintenance, and associated training – as well as adherence to policy, principles and standards; not merely perceived as considerations of rights and due protections, but with an explicit aim of fulfilling them, then biometrics can be an effective and essential tool for enhancing migration management and empowering migrants.

The goal of this Biometrics Manual is to provide introductory operational guidance on the recording, matching, and evaluating of biometric data of populations as they move across and within borders, with a particular focus on the technology analysing physical traits: fingerprints, facial recognition and iris scans. While this Manual is primarily directed at IOM’s programme managers and project developers who may support the use of biometric technology in the management of borders and legal identity, it can also serve as a guiding resource for Member States working in this field. Along with a background on the historic development of biometrics and its earlier motivations, the manual elaborates on the science of using various biometrics as well as their quality and reliability, vulnerability to attack, the limitations that inspired the use of “multi-modal” biometrics.

.....
¹ UNICEF, *Faces Fingerprints and Feet*, 2019.

² IOM International Migration Law, No 5, *Biometrics and International Migration*, 2005, Geneva.

Most importantly, the Manual also informs relevant stakeholders of the importance of adhering to minimum data protection standards when implementing any project with a biometric component. For IOM staff, compliance with the IOM Data Protection Legal Framework³ is mandatory. For external stakeholders, compliance with relevant national and regional laws on data protection is required. This Manual also provides insight into the essential discourse on the rights of individuals and the ethical and human rights principles which must steer the use of biometrics. This is guided by standard human rights frameworks, risk analyses, and IOM's commitment to responsible personal data protection, as outlined in institutional and broader United Nations policies referenced throughout.

The Manual highlights not only existing concerns about vulnerabilities, threats and potential discriminatory application of biometrics, but promotes the examination of new risks or potential injustices as they may be identified. This is to equip business line managers of biometric activities to act appropriately on these emerging risks such that biometrics are used only when necessary – when no less invasive alternative means to achieve the purpose of processing are available – and only for purposes of orderly migration management and border governance with objectives of sound identity management, accessibility, and just treatment of migrants.

.....
³ IOM Data Protection Framework is subject to change, please visit the link (<https://intranetportal/en-us/pages/data-protection.aspx>) for updates. Please note that this will not be accessible to the general public as it is an internal link to IOM.

PART 1

INTRODUCTION TO BIOMETRICS



Discussion Session

What are the ethics of using

Moderator: Mick O'Connell, Advisory Council

Panelists:

- Radu Cimpean, Scientist, Joint Intelligence and Information Agency
- Luc Garcia, Face Examiner, Fingerprints and Facial Recognition Unit, INTERPOL
- Nelson Gonçalves, Head of Legal Identity Unit, Immigration and Border Management Division (IBM), International Organization for Migration (IOM)
- Colleen Ryan, Border Adviser, Border Security and Management, Organization for Security and Co-operation in Europe (OSCE)

#Biometrics #BiometricsInstitute

Biometrics Institute

Joint Intelligence, Surveillance and Reconnaissance, NATO Communications

Agency

Luc Garcia, Face Examiner, Fingerprints and Facial Recognition Unit, INTERPOL

- Nelson Gonçalves, Head of Legal Identity Unit, Immigration and Border Management Division (IBM), International Organization for Migration (IOM)
- Colleen Ryan, Border Adviser, Border Security and Management, Organization for Security and Co-operation in Europe (OSCE)

#Biometrics #BiometricsInstitute

Please use Dublin Honor Hall system

BIOMETRICS INSTITUTE

Promoting the responsible and ethical use of biometrics since 2005

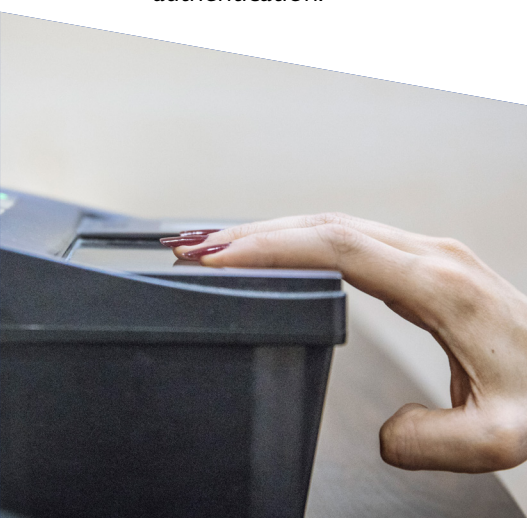
1.1 WHAT IS BIOMETRIC DATA?

Personal data is defined as any information relating to an identified or identifiable individual. Biometric data is personal data resulting from a specific technical processing concerning the physical, biological, physiological or behavioural characteristics of an individual which allows the unique identification or authentication of the individual. Biometric technologies can provide a means for uniquely recognizing humans based upon one or more physical or behavioral characteristics and can be used to establish or verify personal identity of individuals previously enrolled.⁴

Owing to the rapid pace of emerging technologies and the evolving landscape of data protection standards, it is important to routinely reassess the use of biometric data to not inadvertently compromise the rights or safety of data subjects. Such an approach acknowledges the potential advancements in specific biometric identification, as well as the data protection standards with respect to the processing of biometric data.

▶ THE PURPOSE

From a technical perspective, the primary objective of biometric data is to ascertain or verify an individual's identity by analysing distinctive characteristics. Biometric data serves two distinct functions: identification and authentication.



Identification answers the question, "**Who are you?**". In this case, the person is identified as one person among others (1:N matching). Their measurements are identified and compared against the personal data of other persons who already exist in the same database or in some contexts, linked to other databases. This step serves to **demonstrate the uniqueness of an individual** when they come into contact with a system.

Authentication answers the question: "**Are you who you claim to be?**" In this case, a biometric analysis certifies that **the individual presenting their data now, is the same person** who initially provided biometric measurements at an earlier time. Meaning, they are the identity that they claim to be (1:1 matching). This is sometimes referred to as Verification. For the purposes of this document, we shall continue to use the term Authentication.

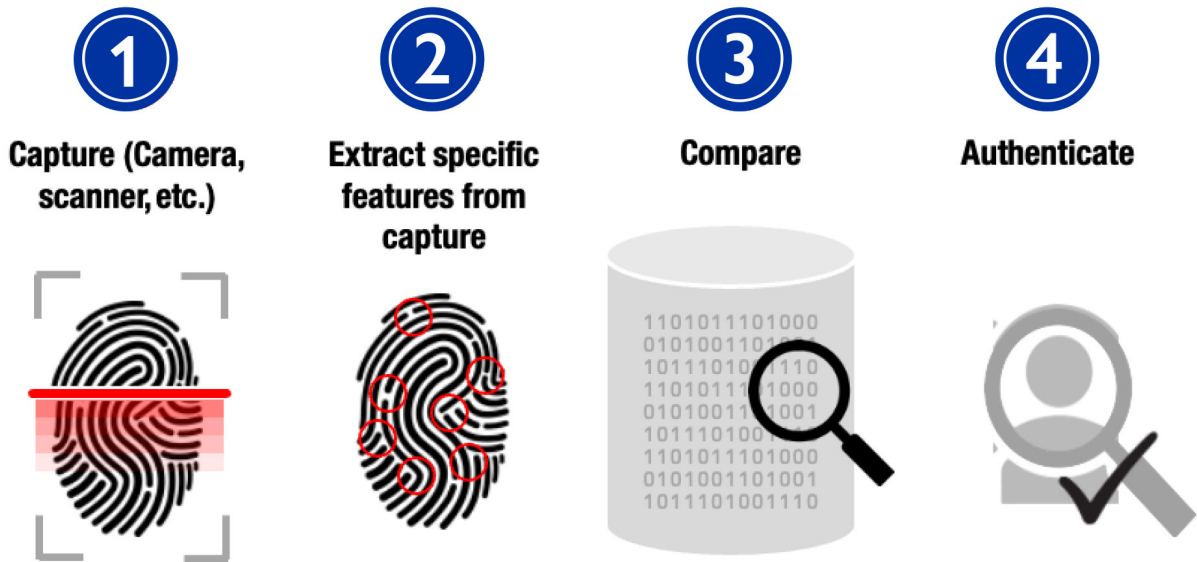
▶ HOW IT WORKS

Enrolment

The initial process of collecting or capturing biometric data is referred to as enrolment. The original image of a trait – a fingerprint, iris, or face, for example – is captured and converted into a template that reflects specific features that were extracted. A template is a configuration of data that should not be able to be reverse engineered back into its original image. Biometrics rely on the digital measurement of these characteristics, not the original image of the trait itself. The system creates a template based on a simplified, digitized version of the trait.

⁴ National Institute of Standards and Technology (NIST), United States Government, [Standards for Biometric Technologies](#), 2013.

Figure 1. Initial process of collecting biometric data

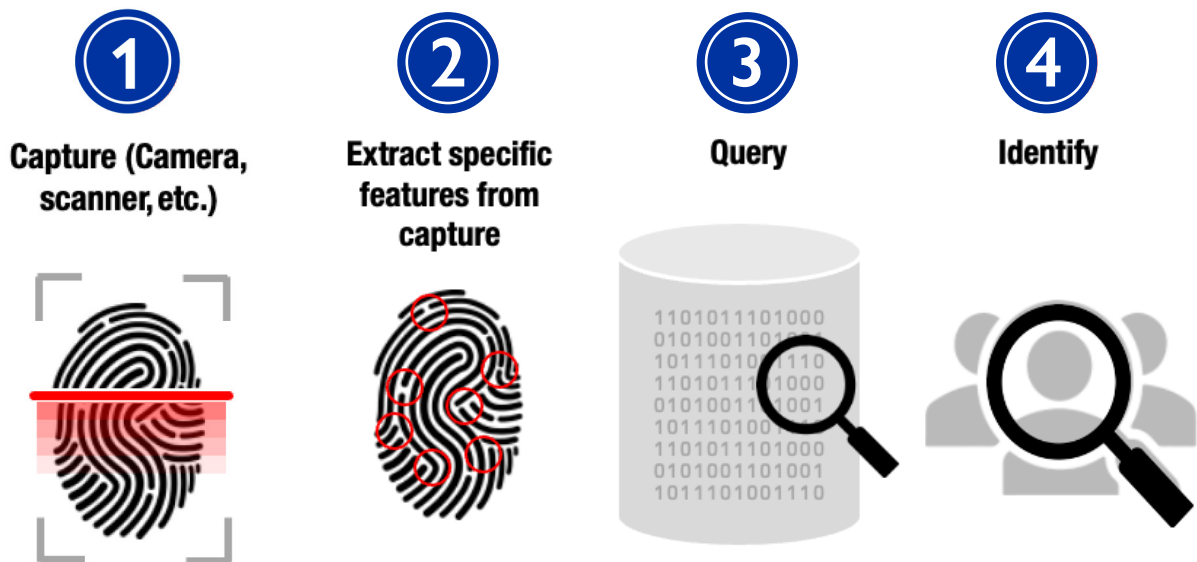


Source: Visualization by the authors with elements from Shutterstock.

Identification

Identification is the process of determining who the subject is. The biometric information presented is cross-referenced to an existing database of registered individuals, identifying who the presenter is. It is also called 1:N matching, in that one person is compared against the rest of the database.

Figure 2. Process of biometric identification

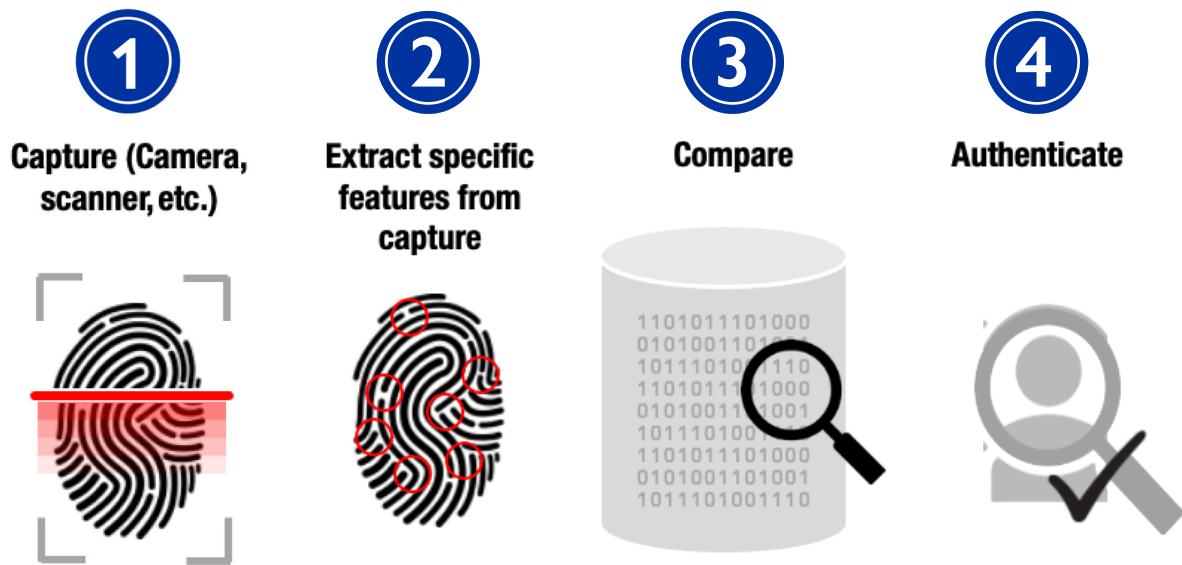


Source: Visualization by the authors with elements from Shutterstock.

Authentication

Authentication is the process of establishing the claimed identity, termed as 1:1 matching. The presented biometric is cross-referenced against the pre-registered information of the claimed identity. As mentioned previously, this is also referred to as Verification.

Figure 3. Process of biometric authentication



Source: Visualization by the authors with elements from Shutterstock.

It is important to recall that biometrics do not confer or establish an individual's identity for the first time.⁵ It can even be said that biometrics cannot *confirm* a person's legal identity; they can only confirm that the biometrics presented do or do not match the data already captured in the system.⁶ It is, however, a powerful tool to strengthen identity management systems that are used across a wide spectrum of social, administrative and security-related functions.

1.2 TYPES OF BIOMETRICS



Physical

While this manual will focus on the physical characteristics of fingerprint, iris or face, there are additional types of biometrics under development which focus on physical attributes such as palm print, vein recognition, as well as forms of DNA.



Behavioural

Though not described in detail in this manual, this type of biometrics looks at how a person does things physically, such as:

- How they write – hand-writing
- How they talk – voice recognition
- How they walk – gait
- Eye movements – blinking
- Facial movements – such as lip motion while talking
- How they type - key strokes

⁵ To-date, the most universal process to establish a legal identity is birth registration, within an appropriate civil registration and vital statistics (CRVS) system.

⁶ The Engine Room, Oxfam. *Biometrics in the Humanitarian Sector*, 2018.

1.3 MODALITIES

Modality

A biometric modality is a category of biometric trait that is taken as an input to the recognition system. Hence, fingerprint, face, iris are considered to be *modalities*.

Unimodal

Usage of only one type of modality for Identification or Authentication is known as a Unimodal biometric method.

Multi-modality

An approach that enlists the use of multiple modalities, to improve the likelihood of accurate results and to compensate for the potential weaknesses in relying on a unimodal form.

Each modality carries inherent limitations in their tangible and theoretical use, which will be examined in later sections of this manual.

1.4 USES OF BIOMETRICS

Biometric data constitutes a category of sensitive data. The reason for this is that biometric data is unique and can't be replaced, in contrast to passwords. Biometric data operations will have a different degree of intrusiveness and impact on the privacy of the Data Subjects depending on the nature, the scope, and the context of the processing. Therefore, additional data protection safeguards are necessary. IOM can only process biometric data in accordance with its data protection framework and in line with "do no harm" approach. This means that biometric processing can only take place following a risk assessment of its use taking into consideration the risks posed to data subjects and whether less invasive alternative means to achieve the purpose of the processing are available. If a decision to process biometric data is subsequently taken, IOM staff are responsible for compliance with the IOM Data Protection Legal Framework when determining the purpose and means for which biometrics are processed, including when they are shared with third parties.

It is important to ensure the data protection principles set out in IOM's data protection legal framework are adhered to, including the principle of minimization, and that technical and organizational measures at a level commensurate with the sensitivity of biometric data are in place to protect the security of the data. Biometric data should only be retained for the duration necessary to fulfill the intended purposes for which it was gathered. Data Protection Impact Assessments should be conducted prior to the collection or processing of biometric data. Data subjects should be duly informed regarding the processing of their data and a lawful basis of the processing must be identified and recorded. Under IOM's current legal framework on data protection,⁷ such lawful basis is the consent of the data subject.

SUPPLEMENTING LEGAL IDENTITY

Biometrics and the establishment of an Automated Fingerprint Identification System (AFIS) can be an essential aid in securing citizen identification in countries where the reliability of traditional identification information is uncertain due to the information itself or the lack thereof, often relating to dates, place of birth, addresses, similarity of names, ambiguity of names and pseudonyms (which may be used interchangeably depending on circumstances.) are the cause of errors.

⁷ IOM, *Data Protection Legal Framework*, 2009. Please note that this will not be accessible to the general public as it is an internal link to IOM.

Biometrics have experienced rapid development in recent decades, becoming a part of daily life in virtually every corner of the world. Biometrics can be used to access smart phones via fingerprints, facial or voice recognition; retailers target consumers by analysing their image and shopping behaviours as captured on closed circuit television (CCTV). It is common to use biometrics to manage work attendance to clock-in and out which directly informs payroll calculations, and to control access to securitized buildings, work sites, or controlled sections of buildings such as banks, casinos and hospitals.

As used by governments on the public, biometrics can serve many functions, such as:



Birth registration process in Mae Sot General Hospital, Mae Sot, Thailand. © IOM 2017/Benjamin SUOMELA

▶ SUPPORTING CIVIL REGISTRY

- Supplementary to standard birth registrations: collecting and storing biometric data at birth (if in accordance with existing national protocols on privacy and child protection).⁸ Birth registration with or without biometrics, is often the basis for creating a legal identity for every individual, which is also typically the precursor to establishing a nationality or citizenship.
- Issuance of travel documents to ensure the right to leave and the right to return to one's country.



Southern Sudanese cast their ballots during the referendum on 9 January 2011. © IOM 2011

▶ PARTICIPATION IN CIVIC ACTIVITIES

- Supplement voting enrolment and verification during voting.
- Supplement verification during census-taking.
- Support exercises to de-duplicate claimed identities.
- For identifying the recipient of a government service face-to-face or remotely, for example, Public Distribution System (PDS), tax related services and others.



Syrian refugees are undergoing biometric registration by Canadian officials as part of their application process to resettle in Canada. © IOM 2016/Muse MOHAMMED

▶ BORDER CONTROL

- Verify identity at international borders for exit and entry.
- Visas: supplement visa applications and verify upon presentation in person.
- Asylum: supplement asylum applications and verify upon presentation in person.
- Resettlement: supplement resettlement applications and verify upon presentation in person.
- Check biometric data in applications against criminal record databases and immigration records.

⁸ Part 2 of this manual, Society, Ethics and Risk explores the usage and ethical questions of using biometrics on children and babies.

Examples – border control

The Canada Border Services Agency collects fingerprints and photographs during the visa application process and in some contexts of refugee resettlement such as the resettlement of Syrian refugees in 2015. This is to search for matches with previous immigration violations or criminal convictions, and/or, to clear the person for entry.

The Schengen Information System (SIS) stores the biometric template external to the document/token itself. The system uses the number of the visa document to determine the appropriate set of templates to compare against the passenger's live fingerprints. Due to the specific characteristics of the SIS, the stored template can be considered as a highly reliable means of identifying the legitimate holder of the visa. The biometric identification would also be used if the identification at the border (deduplication) is implemented. In that case, for each third-country national whose claimed identity is not yet recorded in Entry/Exit System (EES), the biometric identifier is compared with each biometric record of the reference database to confirm that the individual is not yet recorded. If this is confirmed, the individual file is created, and the biometrics are recorded in the database. If the individual is already registered in the database, it is because:

The individual is using the same identity in more than one travel document issued by one or several countries (binationals); in this case, the different travel documents have to be linked to the same individual file.

Law enforcement

Modern biometrics were essentially launched upon developments in forensics, criminal investigations and the cataloguing of convicted criminals. The time and effort consumed by using older manual processes have become untenable as populations grow, and biometrics remain an essential part of this field. For example, portable biometric devices now allow law enforcement officers to scan fingerprints and match them to remote databases. Law enforcement agencies worldwide are moving far beyond fingerprints, building biometric databases that include facial and iris data as well. The use of facial recognition for surveillance and in criminal investigations has been widely adopted.

- Biometrics are used for surveillance, criminal investigations, and verifying targets.
- Forensics and crime detection: establishing a gallery of confirmed offenders to identify perpetrators of a crime.
- Biometrics are used to track prisoners, people with parole obligations, or others of special interest to law enforcement.

COUNTER-TERRORISM

Some States have employed biometrics for counter terrorism purposes in addition to maintaining databases of convicted offenders, and for standard screening passengers at points of entry or during application processes. The global security sector has enrolled biometric data among populations with and without their knowledge, and in some circumstances, is programmed to recognize individuals from considerable distance, including from unmanned aerial vehicles (UAVs, commonly referred to as drones). This is obviously not without controversy and there are considerable ethical questions, but, biometrics have become a key element in many counter-terrorism operations.

Source: Intelligence Advanced Research Projects Activity (IARPA), "Biometric Recognition and Identification at Altitude and Range", Office of the Director of National Intelligence

See also: United Nations Compendium of Recommended Practices for the Responsible Use & Sharing of Biometrics in Counter Terrorism, found here.

Access security

Identity and access control are a regular feature of security for government agencies or other bodies. As fingerprint readers, cameras for the face and microphones for the voice are now widely available on mobile phones, multifactor authentication through mobile biometrics is increasingly possible and a veritable option to improve security in any setting. This can include access to buildings or building zones, storage sites for physical files as well as computer system and databases. Traditional ID cards can be used in conjunction with biometrics on mobile devices to enhance security.

Health-care settings

Possible usage can include, among others:

- Patient identification to ensure the intended patients are receiving care, or to verify eligibility for health-care support.
- Fraud prevention and comparing biometrics against a database of those who have committed health-care fraud or other offences in the past.
- Tracking vaccine distribution (who has received, who has not).
- Biometric authentication-based access for health-care staff in closed settings.
- Enrolment of newborns to prevent kidnapping or switching at birth.⁹

▶ HUMANITARIAN INTERVENTIONS AND SITE MANAGEMENT

While biometrics are being used in humanitarian settings by both host governments and international organizations alike, this manual is not intended to provide explicit guidance on use of biometrics in such contexts, nor present a decisive position on the appropriateness of their use in this environment. Examples are listed below and occasionally referenced; however, it is not the focus of this manual, as such contexts prompt additional questions about necessity, voluntariness, ownership of data among States, the ethics of demanding biometric registration in exchange for potentially life-saving support and other safety considerations.

Biometrics may be employed by governments and/or humanitarian organizations and partners, for the following purposes:

- Family tracing and/or family reunification.
- Registration of displaced or crisis-affected populations for purposes of site management, planning, coordination.
- Registration crisis-affected populations in need of particular services.
- Registration of crisis-affected populations as part of a system for distribution (could include food and non-food items, shelter, cash programming, among others).
- Applications for refugee resettlement.
- Relocation programming, including for internally displaced persons.

▶ BALANCING BENEFITS AND RISK

Traditional methods of identifying a person usually relies on an object they carry or information they know, such as signatures, passwords, identity documents and ID numbers. These methods suffer inconsistencies in that a password can be forgotten, a signature may be forged, an ID card can be misplaced, damaged, or expired. Accurate identification is essential for physical security, information security, financial transactions, contracts and employment, public services, criminal justice, national security and much more. The number and frequency of interactions where identity must be verified is constantly increasing.

⁹ While frequently cited as unchanging, Part 5 of this manual - *Technical Implementation* - remarks on some biometric features that may change in capture and image quality over a person's life.

Older identification systems such as manual passport checks and computer passwords are under considerable pressure as the volume of interaction increases and the speed of day-to-day processes is expected to be instant. Biometrics are hard to falsify or steal, unlike passwords or biographical descriptors. They generally remain consistent over the course of an individual's life and are not transferable between individuals.

Due their convenience and ease of use, biometrics reduce the amount of time required for interactions between the individual and administrator and eliminate the need for paper-based systems and storage. As templates require less storage than original images, even their digital footprint is smaller. The ease at which biometric data can be captured means that greater numbers of individuals can be enrolled, which can strengthen the protection of each person's legal identity.

Biometrics, either on its own or in conjunction with other technologies, offers consumers, businesses and governments enormous opportunities to make identity authentication cheaper, more convenient and arguably, less vulnerable to fraud. Trends suggest that existing biometric applications will expand and new ones will emerge, meaning that biometrics are not only likely to stay, but become increasingly unavoidable.

While biometric technology offers advantages, it also poses several concerns. Biometric data is sensitive personal data and the processing of biometric data entails high risks of abuse and misuse. Biometric systems are not infallible and can incorrectly identify a person or fail to identify a person. Different individuals may also have varying biometric characteristics, making some technologies less suitable for diverse populations (for example, facial recognition has been regarded as being racial and gender biased). The use of biometrics raises privacy and data protection issues as well as human rights concerns, including issues related to discrimination. Responsible and transparent use of biometrics, along with adherence to IOM's data protection legal framework, is essential to counter these risks. Most importantly, relevant stakeholders should conduct a risk-benefit assessment to ensure that the benefits of using biometric technology outweigh the risks.



A registration is underway in Maiduguri. ©IOM 2016/Muse MOHAMMED

PART 2

SOCIETAL, RISK AND RESPONSIBLE USE



IOM staff members are assisting migrants with resettlement. The process includes gathering biometrics, medical assessments and interviews. © IOM 2021/Muse MOHAMMED

As with many technological advancements, the evolution of biometrics is largely be driven by industry leaders and prospective vendors, who are historically bound to consider social impacts and/or negative outcomes on certain populations only after grievances have occurred. Policymakers and civil society often enter the discourse after technology has already had substantial use, whereby analysis, debate and legislation must attempt to keep pace with an industry that is constantly evolving.

The use of biometrics is not only a matter of technical precision and reliability, but carries the potential to impact migration experiences differently among different populations. As described later in Part 4, *System Bias*, biometric technology does not perform equally on all human beings; a discrepancy which could create inequality among the experiences of individuals as well as the legal decisions stemming from their biometric results. Human rights must have a persistent presence in the discourse on biometrics, pertaining especially to freedom of movement¹⁰ and prohibition of discrimination.

Concerns about the use of biometrics are primarily related to privacy and data protection, civil liberties and civil rights: for example, the pervasive and extensive use of biometrics by authoritarian regimes, the intrusive use of biometrics by industry actors and the weaponization of biometric databases in conflict zones are extremely logical concerns. These uses of biometrics ultimately deepen surveillance of daily life which in turn, strips people of what should be their intrinsic anonymity.

2.1 IMPACTS ON SOCIETY

In the context of biometrics employed at borders, the known or anticipated presence of biometric procedures could influence decisions to migrate through particular channels and/or could spur the development of dubious businesses falsely claiming to facilitate immigration processes and/or circumvent established systems. The risk of being falsely identified, or in some situations, correctly identified and then registered at that place and time, may be sufficient to prompt migrants into higher-risk options.

The use of biometrics to access services or entitlements runs the risk of erroneously rejecting users who should qualify and erroneously confirming users who should not; thus excluding people with legitimate needs from their due provisions and protection. In the case of services involving basic needs and rights such as food, shelter or health care, this can have extreme consequences for those who are excluded due to technical error.

The implementation of biometrics as a non-negotiable requirement to access particular services or spaces renders the voluntary nature of compliance questionable. Whereas some individuals or populations may be uncomfortable with the provision of biometric data for various personal, religious or sociocultural reasons, they may feel coerced to prioritize this compliance over their personal beliefs or preferences. As biometrics are increasingly tied to accessing entitlements and services for displaced populations in humanitarian contexts, whether managed by international organizations or government agencies, users may feel there is no choice, whereas in fact an alternate form of authentication must be made available.

The administration of biometric technology should take into account the acceptability and accessibility among particular groups to give their



Displaced people being fingerprinted as part of registration at the Bentiu POC. Bentiu, South Sudan. © IOM 2015/Brendan BANNON

¹⁰ Article 11, paragraph 3 of the International Covenant on Civil and Political Rights 1966 sets forth: “The above-mentioned rights [Liberty of movement and freedom to choose residence; Freedom to leave any country including own] shall not be subject to any restrictions except those which are provided by law, are necessary to protect national security, public order (“order public”), public health or morals or the rights and freedoms of others, and are consistent with the other rights recognized in the present Covenant.”

personal data in the first place. For religious reasons, exposure of the face may be considered unacceptable. Stigmatized populations and targeted groups may not only be uncomfortable in using biometrics, but could be legitimately fearful for their safety, if their non-changing physical features are forever captured in a database. Sex workers, ethnic and religious minorities, political dissidents, people with criminal histories, all have different but valid reasons to resist their deeply personal information becoming eternalized. Individuals presenting at borders may be in hiding or fleeing from harm, whether the threat is from their government, gangs or non-State actors, community, or family, especially in situations of domestic abuse, forced marriage, or threat of honour killing.

Biometric data can reveal more information about a person than was perhaps originally intended. For example, details in the iris can indicate features of a person's health status;¹¹ DNA analysis can confirm parentage or other familial relationships (or lack thereof) which if brought to light, can have devastating effects on families not only in terms of assumptions and trust, but in terms of inheritance, social and financial exclusion, as well as extrapersonal punishment.

An over-reliance on the accuracy of biometric data could potentially infringe upon the right to seek asylum by leading to rejection of entry at the border due to an inaccurate reading of the biometric data. Safeguards should be established to prevent this, such as secondary inspections and a possibility to immediately appeal when biometric data is believed to be inaccurate.

The promotion of biometrics in support of States or select authoritative bodies within States, should undergo at least minimum scrutiny. Prior to equipping authorities to collect and use biometric data, a risk analysis should be undertaken, and baseline criteria met to prevent misuse of the data gathered, especially for discriminatory or abuses purposes. While it is difficult to predict all future scenarios, some States are more vulnerable to interference and/or have a verified history of discrimination and abusive practices towards particular groups or the broader population. This must be taken into consideration and the benefits weighed conservatively against the risks. A related concern would be situations of dramatic changes of power, such as a coup d'état or military takeover as was witnessed in Afghanistan after August 2021. Once the takeover occurred, the country was launched into further turmoil while the Taliban inherited massive amounts of personal data collected on the Afghan population, including those who had worked for foreign bodies, which rendered them immediately vulnerable to attacks and other threats. Even in less severe scenarios, such outcomes can have serious impacts on communities whether they intend to cross a border or not.

2.2 ETHICS AND ORIGINS



Enumerator stamps finger print of beneficiary for registration. © IOM 2018/Rikka TUPAZ

Further, it is important to recognize and reflect upon the racialized past of identification and surveillance; the classification of human beings according to perceived differences, and the social structures that such practices were intended to reinforce. There is evidence that fingerprints – perhaps the earliest known form of biometrics – were used as far back as the year 500 BC to secure contracts or in lieu of a contemporary signature, which may well have been between reasonably equal parties. Fingerprints were also widely used in employment contracting during colonial times between the colonial authority and colonized subjects, which carried over into post-colonial eras, albeit, with sustained power imbalances and discriminatory social structures. These origins and the impact on those who were discriminated against resonate to populations of today, which can continue to influence their experience with the government, law enforcement, and their receptivity to biometrics.

¹¹ Redpath, J. "Biometrics and international migration", *Ann Ist Super Sanità*, 43(1):30.

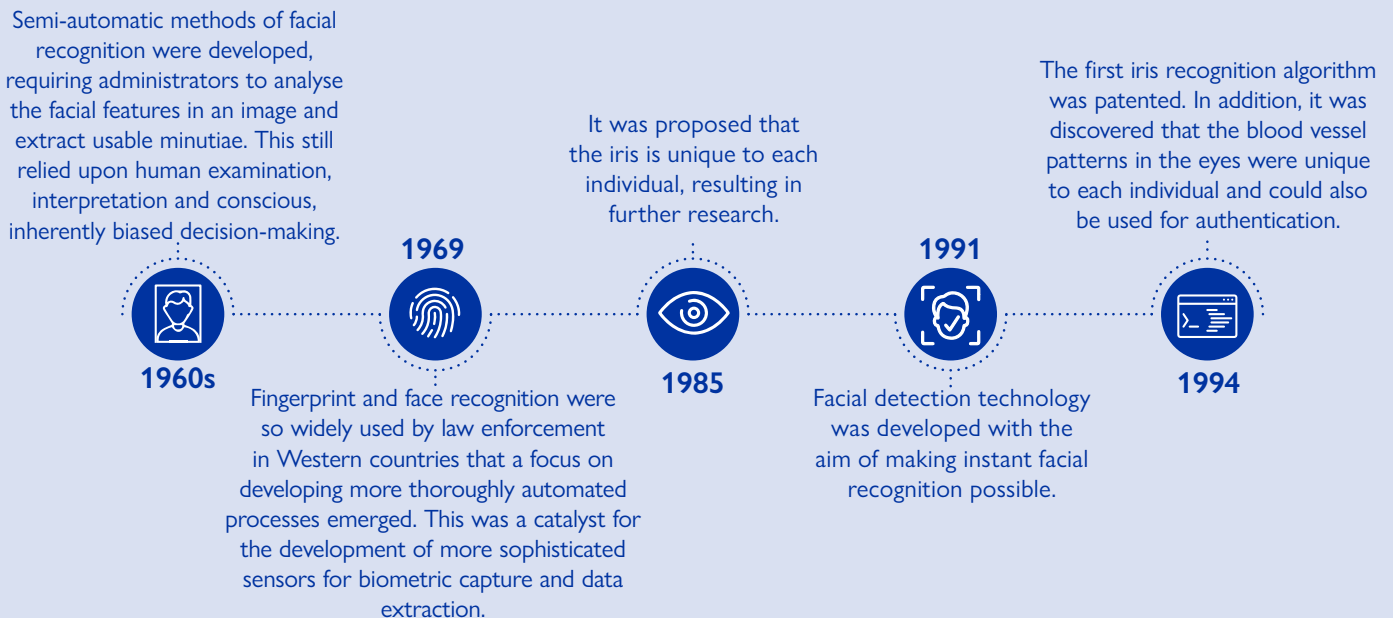
While physical attributes that are acquired during one's lifetime should be viewed differently from the natural attributes or traits that are captured by biometrics, it is relevant to acknowledge alterations to the physical body that have been administered by force for purposes of identification, commodification, and exploitation. In the book *Dark Matters: on the Surveillance of Blackness* (2013),¹² Browne argues that branding and scarification during the transatlantic slave trade was an earlier form of biometric technology. Further, branding in the form of tattoos is widely known to have occurred during horrifying atrocities such as genocide, but also contemporarily among victims of trafficking and people coerced into violent gang membership.

In principle, such practices are divorced from biometrics which use only naturally existing attributes; however, the historic timeline of identification technology and the motivations that drove its development cannot be forgotten, especially when seeking to apply biometrics to populations that have well documented experiences of discrimination and abuse.

A BRIEF HISTORY OF BIOMETRIC DEVELOPMENT

While rudimentary means of identification have been employed over centuries for various purposes, the development of biometric technology was initially advanced through the criminal justice sector, motivated by the desire to measure, document, compare, and identify individuals implicated in or convicted of crimes. When this started to evolve in the 1800s, the main objective was to identify repeat offenders who passed through the criminal justice system but who ostensibly could have changed their name and physical appearance to avoid further detection or linkage to their criminal past. The two technologies that emerged first were anthropometry, which could include measuring limbs and distance between arbitrary physical features, and fingerprinting. The latter was more successful because it was believed to be the easiest to capture. Systems of fingerprinting were adopted by law enforcement agencies in numerous countries and soon became the standard for identifying criminals. This marked the beginning of a century of research into other unique physiological characteristics that could be used for identification. Over the next century, biometrics grew exponentially as a field of research. The following illustrate some of the developments:

Figure 4. Significant developments contributed to the exponential growth of biometrics over the century.



Source: Visualization by the authors.

While ongoing developments have sought to rectify the many flaws of earlier and still current models, caused in part by the technology most often using white male faces as the default blueprint, it has continued to evolve and will likely remain a major element of biometric technology for years to come.

¹² Browne, S. *Dark Matters: on the Surveillance of Blackness*. Duke University Press, 2013.

A selling point in favour of biometrics and indeed any technology, is that – theoretically – it removes the arbitrary nature of human decision-making and potential bias, resulting in equal treatment.¹³ This should, therefore, “increase equality before the law as migrants are not then at the mercy of one individual civil servant’s decision”.¹⁴ And yet biometric data for border management is still sorted as per criteria established during programming of the system, often focusing precisely on nationality and often inevitably, ethnicity, skin colour and associated social background. Thus, a blind, automated system can still introduce “categorical surveillance” and with it, inherent discrimination towards some demographics.¹⁵ This, coined with the well documented reality that some ethnicities experience more false biometric results than others,¹⁶ means that biometric systems risk becoming complicit in the discrimination and miscategorization of migrants, and the criminalization of migration more broadly. Migrants in irregular and other vulnerable situations may find themselves at even greater risk of harm or exclusion from support, if such discrimination is allowed to be systematized and automated.

These risks are very real and hugely consequential and, highlight inherent weaknesses of any automated technology. A conscientious approach to biometric oversight that acknowledges and addresses these risks, is ostensibly more likely to maintain neutrality and fairness in its programming and application.

The use of biometric technology among children, particularly newborns and infants, poses a unique set of challenges. According to UNICEF’s manual,¹⁸ there are limited biometric traits that are suitable for use in this specific age group. This limitation primarily arises from the technical difficulties in capturing high-quality images that can generate usable biometric templates for children. The protection of the right to privacy under Article 16 of the Convention on the Rights of the Child affords all children a strong protection of their right to privacy, and any interference with this right must comply with the principles of legality, necessity and proportionality.

In 2019, UNICEF discouraged the use of biometrics among children in its global programming. This stance reflects a commitment to safeguarding the rights and well-being of children, including their right to privacy. It acknowledges the complexities and concerns associated with capturing and processing biometric data for young children, such as issues related to data quality, consent, and the potential risks of data misuse or abuse.



A newborn’s fingerprint is captured for their birth certificate with the support of an official of the Civil Registry of the state of Chiapas. ©IOM 2022/Cesia CHAVARRÍA

It is important to consider alternative methods of identification and verification that are more suitable and respectful of the unique needs and vulnerabilities of children. This approach ensures that children’s rights and best interests are prioritized when considering the implementation of biometric technologies in programmes and initiatives involving them.

To safeguard the rights of children, it is important to have comprehensive safeguards that establish higher standards and added protective measures. These safeguards should include, but are not limited to provisions for the automatic deletion of children’s data after a predetermined timeframe to prevent unnecessary retention. Furthermore, the access to and sharing of children’s data should be subject to stringent controls, ensuring that their information is handled with the utmost care and respect for their privacy and security.

¹³ Dijkstra, H. and A. Meijer, eds. 2015. *Migration, Minorities and Citizenship*, chapter 7.

¹⁴ Ibid.

¹⁵ Dijkstra, H. and A. Meijer, eds. 2015. *Migration, Minorities and Citizenship*, chapter 4 by Van der Ploeg and Sprengels.

¹⁶ H. Dijkstra and A. Meijer, eds. 2015. *Migration, Minorities and Citizenship*, chapter 7.

¹⁷ UNICEF, *Faces Fingerprints and Feet*, 2019.

As mentioned above, the use of biometrics in the management and distribution of humanitarian aid and services has gained traction in recent years, with many organizations employing biometrics to distribute food, cash, and other goods. It is also used extensively as a method of registration and can record the outcomes of vulnerability screening which could entitle crisis-affected populations to additional support. Biometrics are generally proven to be time-saving, efficient and reduce the amount of personal information gathered that is otherwise susceptible to becoming obscured through language barriers, misinterpretation of names or order of names, as well as establishing family linkages among immediate versus extended members.

Means of safeguarding, however, in particular against data breaches as well as inappropriate or overly risky data sharing arrangements, are in many cases, addressed only after risks arise or demands for data sharing have surfaced. Humanitarian response relies heavily on coordination among agencies which can include sharing of data where appropriate, thereby warranting new and comprehensive data sharing agreements that satisfy standards, but still allow a degree of flexibility to facilitate an efficient operational response. There are significant data protection concerns even for the sharing of biographical data, such as names and dates of birth, much less biometric data, which is considered more permanent, less debatable and often perceived as irrevocable once collected.

In line with the principle of purpose specification, biometric data that is collected for a specific humanitarian purpose may only be used for that specific purpose. Moreover, it is important to conduct a data protection impact assessment before collecting biometric data, adopt data protection by design and by default in all biometric systems, be transparent about the processing, including any sharing of data, and ensure the rights of data subjects are respected and upheld at all times.

Further complications arise when host governments or other entities demand access to the data sets and/or claim ownership of them. There are significant risks to already vulnerable populations if personal data is simply handed over.

The use of biometrics to implement a humanitarian response can be technically effective but remains laden with legal, ethical and protection questions and concerns over safeguarding. IOM's Data Protection Legal Framework should be a core feature of risk analyses, as well as an honest examination of whether the same approach would be considered acceptable if used on a general population, as opposed to a crisis-affected and typically foreign population.

In acknowledgment of the unique risks and challenges posed by biometric data in humanitarian action, IOM staff are required to always comply with IOM's Data Protection Framework and commit to limit the use of biometric data in humanitarian settings for specified, explicit and legitimate purposes where no less invasive alternative means to achieve those purposes are available. If the processing of biometric data may lead to high risks to the data subjects that cannot be sufficiently mitigated through appropriate measures, it is advised not to collect such data in the first place.

Alternative less invasive forms of identification must be concurrently available to data subjects.



At the border area of Haquillas, Venezuelans waiting for their documentation to be formally processed in order to enter in Peru regularly. ©IOM 2019/Muse MOHAMMED

PART 3

GOVERNANCE AND SAFEGUARDING



Legal Identity, Biometrics and Border Management Regional
Conference in Argentina, July 2023. © IOM 2023

While the evolution of biometric systems may have been driven by unrestrained industry momentum, governments seeking to employ biometrics for State purposes must do so cautiously and conscientiously, not necessarily using all available technology simply because it is there. All processes relating to biometrics must be underpinned by internationally recognized standards and principles, codified in national legislation and/or sanctioned by existing laws, and subject to scrutiny and transparent evaluation.

Ultimately, any involvement with the implementation of biometric systems must first reflect on the following questions:

- Is the use of biometrics the only and best solution in order to achieve the objectives; and
- Is the intended use of biometrics and their purpose truly ethical, even if the prevailing law or code does not prohibit its use?

Beyond the compliance with established laws and standards, and in the spirit of consistently re-evaluating the approach to proportionality, governance of biometric usage would be enriched by seeking both formal and informal inputs on a continuous basis. This could include updates from industry leaders on developments in technological performance, as well as recommendations from human rights advocates, legal practitioners, and civil society representatives who are best placed to articulate the impacts on society, both positive and negative. This is not only to respond appropriately to potential rights violations, but ideally to prevent them from happening at all. Any international organization making use of biometric technology as well as direct or indirect implementation in support of States, must first ensure that a minimum list of criteria will be satisfied, and that the State in question is willing, capable, and sufficiently equipped to do so. The criteria described below are guided by the principles in IOM's Data Protection Manual (2015),¹⁸ and the United Nations Principles on Personal Data Protection and Privacy. Adherence is especially important for United Nations agencies which are directly or indirectly providing support to non-United Nations security forces, as enshrined within the United Nations' Human Rights Due Diligence Policy, or HRDDP.¹⁹ The HRDDP stipulates that the provision of any such support must be consistent with United Nations principles and promote respect for human rights, international humanitarian and refugee law. If such standards are unlikely to be met or sustained by a particular authority, the promotion of biometrics should be re-evaluated and/or suspended until appropriate adjustments and safeguards can be established.

▶ IOM'S DATA PROTECTION FRAMEWORK



The IOM Data Protection Manual (to be updated) is available online, and is comprised of three parts: the first part outlines the IOM Data Protection Principles (to be updated); the second part includes comprehensive guidelines on each principle, considerations and practical examples; and the third part provides generic templates and checklists to ensure that data protection is taken into account when collecting and processing personal data. Although the content of this publication was developed for IOM staff to use, it can be used as a resource tool by other organizations engaging in similar operations.

¹⁸ IOM Data Protection Manual, 2015.

¹⁹ United Nations' Human Rights Due Diligence Policy on support to non-United Nations Security Forces.

3.2 MINIMUM CRITERIA

The collection of biometric data must be lawful and undertaken in a fair manner; it should not be an absolute pre-requisite to access basic needs or services, including birth registration or establishing a legal identity. Subsequent processes of using, sharing, updating and discarding biometric data must also be lawful and follow an established process. They cannot be facilitated by threats, coercion, deception, or an abuse of power or a power imbalance.

Under IOM's current data protection framework, **consent is required by all persons** and/or legal guardians on behalf of persons, before acquiring or collecting their biometric data. True consent or true opt-in means that the alternatives need to be viable and non-discriminatory. Consent must be free and informed, and obtained through measures that are void of any coercion, deception, abuse of power or force. The purpose, legal basis, intended use and prevailing management of the biometric data should be explained in a language and method of communication that each individual can understand. People must have the option of not opting in for the biometric process and offered an alternative method of identification. Even if they have given their consent, they should be informed that they may withdraw that consent at any time. Consent to capture, store, and analyse biometric data should facilitate the concept of "true opt-in", whereby the individual expressly agrees to the process, and is not simply complying because they were lacking in information or did not expressly opt out.



Purpose specification: only process biometric data for specified, explicit and legitimate purpose(s).



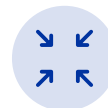
Retention limitation: retain biometric data only for the time period that is necessary for the purposes for which such personal data is being processed. When that purpose has been achieved, and unless personal data is processed or further compatible purposes, the biometric data must be deleted or anonymized, as appropriate, within a reasonable period following the achievement of the purpose.



Confidentiality: biometric data must be filed and stored in a way that is accessible only to authorized personnel on a strictly need-to-know basis and transferred only through the use of protected means of communication.



Transparency: includes the provision of information, as appropriate, in a matter and language that are intelligible to the data subjects concerned about the processing of their biometric data.



Proportion and necessity (data minimization): only process biometric data in a manner that is adequate, relevant, and limited to what is necessary in relation to the purposes for which such personal data is being processed. This requires, in particular, ensuring that the personal data collected is not excessive for the purpose(s) for which it was collected.



Accuracy: take every reasonable step to ensure that biometric data is accurate and, where necessary, kept up-to-date in such a way as to fulfil the purposes for which it is being processed.



Security: implement adequate technical and organizational measures to ensure the integrity, confidentiality, and availability of biometric data at all times. Such measures shall be proportionate to the sensitivity of the personal data and shall guarantee that personal data is protected against unauthorized or accidental access, damage, loss or other risks presented by data processing.



Privacy by Design and by Default is a top priority of biometric systems and should form the core of any biometric platform and its ongoing management. Data protection by design and by default means ensuring that data protection requirements are integrated as early as possible, ideally at the stage of architecture and system design, in data processing operations through technical and organizational measures, such as privacy-friendly standard configurations.



Accessing assistance: in the context of accessing assistance, not limited to but especially in regards to life-saving assistance, the inability or unwillingness of a person to provide biometric data should never impede such access. Other, non-biometric means of identification must be available to provide the required verification; ideally, erring on the side of acquiescence in humanitarian or crisis contexts.

CONCERNING THE CONTEXT OF BORDER GOVERNANCE

Border authorities are encouraged to not only share data among government organs including law enforcement, but under controlled circumstances, to permit direct access to databases in the interest of collaboration, in particular on issues of security and counter terrorism. As flagged in a 2023 study by OHCHR, this means that law enforcement agencies may be able to access data due to an absence of firewalls.

This permissibility has implications for the minimum criteria indicated above, and calls into question whether the initial body gathering biometric data can maintain standards of legality, purpose, data protection, function and consent, among others.

As an example, the European Union has enhanced interoperability of databases such that authorized actors can search across all six databases depending on access privileges, which is in contrast to earlier European Union ideals of compartmentalizing migration-related databases.

The OHCHR report also notes that border governance has expanded beyond the physical border, including “insourcing” of border control through the policing of migrants already in the country, resulting in detecting, detaining, and deportation. In parallel, there is increasing outsourcing of border control through the remote collection of biometric data and social media monitoring to gather information on individuals before arriving at borders. This outsourcing means that migrants can be under surveillance and subject to potentially discriminatory scrutiny long before leaving their country of origin. The report describes emerging digital technologies making use of interoperable databases, which can share much broader data than is collected only via standard border control procedures.

Similar to the challenge of putting policy before practice, this has implications for informed policy development, decision-making, and how far ahead such practices can reach before being codified and guided by a legal and ethical framework.

See OHCHR’s September 2023 study, *Digital Border Governance: a Human Rights Based Approach*.

3.3 ACCOUNTABILITY

Prior to launching any initiative using biometrics, and as a recurrent review of existing biometric activity, it is essential to interrogate each context with a set of questions to establish legitimacy, proportionality, risk and compliance with rights and protection. This reflection is essential for all actors and future Controllers, but especially for international organizations supporting or promoting the use of biometrics in their programming. Organizations must consider all ethical, legal, and social elements prior to project design and certainly before implementation. This remains true whether the activity will support host State functions or not:

- Are biometrics the only means to achieve the objectives of the programme?
- Is there an established legal basis for collecting, receiving, or sharing biometric data?
- Is biometric technology appropriate for the target group(s)?
- Is the biometric technology accurate and reliable for the proposed project use?
- Is the technology suitable for the setting?
- How acceptable are biometrics among the target community?
- Could the introduction of biometrics potentially exclude children or families from services or protection?
- Can the data be appropriately protected at all stages from collection (or receipt) through to destruction?
- In the settings where the technology is being rolled out or promoted, do reasonable data protection and privacy laws exist?
- Are capacity-building and sustainability assured?
- Have monitoring and evaluation mechanisms been established?

These questions are in addition to the questions listed above about meeting overall objectives, ethics regardless of prevailing laws, as well as the questions indicated in the section on Use in Humanitarian Settings. This demonstrates the many angles that must be examined prior to undertaking biometric programming, especially on the part of international organizations.

If any of the questions listed above cannot be adequately answered nor guaranteed as per the prevailing rights and standards, then the application of biometrics should be swiftly re-evaluated.

As is detailed later in Part 4, under System Bias, biometrics do not result in equal performance outcomes for every individual, nor across certain combined demographic groups. The risk of false acceptance and false rejection are significant for some populations under specific circumstances. Misidentification can lead to delays in travel, missed connections and lost resources at best; or discrimination, criminalization, grave maltreatment, and denial of rights or due entitlements at worst. Even accurate performance can be influenced by inherent system bias and the inevitable “social sorting” that can emerge over time. Governance of biometrics systems should include not only a complaint and feedback mechanism to receive reports and claims of compensation for erroneous decisions made on the basis of problematic biometric analysis, but also formal means of submitting complaints amounting to legal claims or other recourse. The process for this should not be obscured or made conveniently over-complicated; rather, data subjects should be made aware of these options and guided towards the appropriate first steps and/or a trusted body that can support them in the process.

3.4 JURISDICTIONAL REQUIREMENTS

The entity deploying a biometric system needs to take into account a number of issues related to specific jurisdictional requirements. In the field of migration, these requirements might not be limited to the place of

operation alone, but also to cross-border jurisdiction and international best practice. A list of issues to be considered are provided here:²⁰

- Anti-discriminatory laws;
- Disclosure laws;
- Redress mechanisms;
- Provision of biometric data to agencies or subsidiaries;
- Provisions for law enforcement agencies for access to biometric and associated information;
- Opt-in and opt-out rights and associated requirements for fallback processes;
- Specific data retention conditions (including period of time and security standards);
- Evidentiary requirements for use of biometric data in a court of law;
- Specific instances where Biometrics are required by organizations or governments (e.g. for secure access to critical national infrastructure);
- Applicability of legal domains in use of Biometrics on the internet;
- Alignment with border control protocol.



Biometric registration procedures at the Canada Visa Application Centre. © IOM 2019/Muse MOHAMMED

²⁰ Based on ISO TR 24714-1.

PART 4

MANAGEMENT OF

BIOMETRICS



Birth registration in the Chiure district, Mozambique
© IOM 2023

Beyond the overarching governance and safeguarding of biometric technology, the practical design, technical maintenance, troubleshooting, security, and day-to-day management plays a critical role in maintaining the required standards and principles, as well as technical performance.

Depending on the entity involved and their objective, the modality of biometrics to be used is a foundational decision after evaluating the suitability of biometrics in and of itself.

4.1 DATA STORAGE

One of the first decisions prior to setting up a biometric system is the representation that will be used to store the biometric data. This will depend on the type of biometric data envisioned for recognition (fingerprint, face, iris, or others).

Biometric analysis uses algorithms that work on templates, or transformed versions of the original image, therefore, a possible choice of storage representation could be the template itself.

If in future, the system was altered or upgraded and a new algorithm used for recognition, the templates used for the previous algorithm may become obsolete or incompatible. This implies that it might be better to store the raw data as images so these are always available; however, this carries additional ethical and data protection concerns as they are more immediately identifiable and subject to attack.

A common solution is to have two databases: one with raw images archived securely for future use and another with templates. In case of a change in system and algorithm, the archived raw data can be recalled creating templates for the new algorithm. This is not without risk; however, as various databases can be vulnerable to attack and must comply with legal, policy, and ethical terms for their establishment and maintenance.

STORAGE MODELS

There are three basic models for storing and sharing considerable amounts of data:

- Local database
- Peer-to-peer network
- Cloud storage

Local database

Local storage involves storing data on physical drives such as hard drives, or Network Attached Storage (NAS) drives directly on an entity's premises. Although pre-built features are unavailable when using local storage, there is greater control over the data to determine where files are stored and who has access. Local storage devices, like hard drives, are usually not connected to the internet and if so, the network and firewalls must be set up accordingly. As a result, the chances of malicious cyberattacks and data breaches are reduced, provided this is done professionally with sufficient resources invested in qualified staff, and appropriate infrastructure.

This conventional model is often migrated to the private cloud approach, described below.

Peer-to-peer network

In a peer-to-peer network, computers on the network are considered equal, with each workstation providing access to resources and data. This is a simple type of network where computers are able to communicate with

one another and share what is on or attached to their computer with other users. It is also one of the easiest types of architectures to create. Here are some of the characteristics of a peer-to-peer network:

- Individual users have responsibility over who can access data and resources on their computers.
- Operating systems such as Windows XP and Windows Vista allow accounts to be set up that will be used when other users connect to an individual user's computer.
- Accounts, passwords, and permissions are saved in a local database and are used to determine what someone can do when connecting to the specific computer.

This type of federated, distributed data storage is – on the upside – a rather robust architecture, avoiding a single point of failure. While one specific storage might be off-line for a certain time, the whole system will remain available. On the downside, the management of policy and security is non-trivial and therefore, often not suitable for storage of sensitive data.

Cloud storage

Amazon AWS describes cloud storage form of storage as “Cloud storage is a cloud computing model that stores data on the Internet through a cloud computing provider who manages and operates data storage as a service. It's delivered on demand with just-in-time capacity and costs, and eliminates buying and managing your own data storage infrastructure.”

Biometric data or any sensitive data should not be stored or processed in a public cloud environment due to the possible exposure to legal risks, namely the risks that certain domestic laws may pose to IOM's privileges and immunities including the inviolability of IOM data.

There are two main types of cloud storage solutions:



1. Private cloud storage

Private cloud storage is also known as enterprise or internal cloud storage. Data is stored on the organization's server in this case. This data is protected by the organization's own firewall. Private cloud storage is a great option for companies with expensive data centres and can manage data privacy in-house. A major advantage of saving data on a private cloud is that it offers complete control to the user. The responsibility of managing private cloud storage lies with the host organization.



2. Hybrid cloud storage

Hybrid cloud storage is a combination of private and public cloud storage. As the name suggests, hybrid cloud storage offers the best of both worlds to the user – the security of a private cloud and the personalization of a public cloud. In a hybrid cloud, data can be stored on the private cloud, and information processing tasks can be assigned to the public cloud as well, with the help of cloud computing services. In a hybrid cloud storage, the actual biometric data should be segregated and only processed in the private cloud due to the sensitivity of biometrics and the legal risks of public cloud computing. Hybrid cloud storage is affordable and offers easy customization and greater user control.

There are benefits and drawbacks on the cloud storage model. These are always in context of the specific use-case and the circumstances.



Benefits of private and hybrid cloud storage:

- Flexibility and easy access: storage in the cloud means that data is not tied to a specific location. Different stakeholders can access data stored in the cloud from a location and device of their choice without having to download or install it.
- Remote management support: cloud storage also paves the way for remote management by internal IT teams or by managed service providers (MSPs). They can troubleshoot without being on-site, which speeds up problem resolution.
- Rapid scalability: a major benefit of cloud storage is that new resources can be acquired with just a few clicks, without the need for additional infrastructure. With unprecedented growth in data volumes, this feature supports business continuity.
- Redundancy for data backup: data redundancy (such as replicating the same data across multiple locations) is essential for an effective backup mechanism. The cloud ensures that data is kept safe at a remote location in the event of a natural disaster, accident or cyberattack.



Drawbacks of cloud storage:

- Data protection and security governance can be inconsistent, depending on the hosting countries or the jurisdictions to which the cloud service providers (CSPs) are subject and their public and covert laws (with respect to sharing of the data with the government of the country) relative to cloud storage.
- Data breaches: the lack of strong and robust access controls and authentication mechanisms might enable unauthorized access.
- Risk of vendor lock-in: if all data is stored in a single cloud platform, there is a risk of vendor lock-in and potential inflexibility.
- Security and legal issues related to multi-tenancy: cloud environments may be shared by multiple tenants, which can multiply security risks, as well as legal risks with respect to the application of IOM's Privileges and Immunities to the data.
- Fragmentation of the IT landscape: the unplanned introduction of cloud storage can lead to the IT landscape becoming fragmented over time.
- Risk of failures and downtime: cloud platforms managed by external providers can experience outages, making the data and applications stored in these environments inaccessible.

4.2 MAINTENANCE OF DATA AND DATABASES

WHY IS MAINTENANCE NEEDED?

When setting up an enrolment and/or data collection platform, it is common to begin with an extensive list of data elements to be collected. This will usually be reduced once aligning to the concept of data minimization; only collecting that which is necessary and justifiable for the objective at hand. When designing a system, the Data Controllers, and those with oversight must be aware that the data-elements need to be maintained for multiple reasons:

- Legal limitations on the storage time;
- Information becoming outdated such as residential address, employer;
- Expiry of data, such as expiry of identity documents;
- Name change, such as marriages/divorces.

In the context of biometrics, the usability of data degrades as well. The performance of biometric authentication systems is affected by discrepancies between data stored in biometric templates and corresponding data derived from the actual owners of biometric templates upon presentation. Such discrepancies are mainly attributed to

within-person variations of biometric features. Among all types of within-person variations, aging-related variation displays unique characteristics that make the process of dealing with aging a challenging task.

- The biometrical features of a person change in time due to natural ageing, sun exposure, accidents or disease, surgery – cosmetic or otherwise.
- The recording devices / sensor technology also evolve with time, requiring data legacy conversions.

▶ UPDATING BIOMETRIC DATA

The principles of Evidence of Identity (EOI) require that an identity must be continuously verified over time through interactions to verify the individual is indeed still alive. Re-enrolment of biometrics can be part of this process of intermittent interaction.

There are several ways that the physical body and associated biometric templates can change over time. The ridges on the fingers become smoother as we age, and fingerprint capture in the elderly can be a challenge. The appearance of the human face is significantly affected by the ageing process. Facial ageing is mainly due to exposure to elements (sun, wind, dryness); reduced skin elasticity and decreased muscle strength; the movement and growth of bones and skin-related deformities. Age-related changes in appearance due to bone growth usually occur during childhood and puberty, while effects related to general exposure over time are most visible among the elderly.

In addition to the direct effects of ageing, the human face can also be subject to indirect effects due to health conditions that occur over time. Depending on the condition, the human face is affected in different ways, making it almost impossible to define precisely the indirect effects of ageing on faces. For example, some conditions may cause weight gain and others weight loss – both conditions affect the human face in different ways.

There is no generally accepted or recommended practice on the updating frequency of biometrics in function of age or other factors. The considerations vary on the chosen biometric modality, the user group, and the intended objective of the biometric capture.

Aligning with generalized age brackets whereby changes in the face are sufficiently variable to warrant an updating of biometric enrolment, the table below can serve as indicative guidance:²¹

Table 1. Suggested frequency for updating biometric data according to age cohort, as discussed in CEN TC224 WG18 in 2023

Infants	weeks
Children	2 years
Youth	5 years
Adults	10 years
Senior	5 years

²¹ Recall that enrolling biometric data of children and babies carries additional ethical and protection-related concerns; their presence on this table does not implicitly endorse the use of biometrics on children. This is instead, a reflection of the pace of potential physical changes to the face at different age ranges.

▶ CONSIDERING EOI PRINCIPLES

Identification is the process of associating identity-related attributes with a particular person. Typically, EOI²² processes are based on a three-component approach for establishing identity:

- Evidence that the claimed identity is valid; meaning that the person was born and, if so, that the owner of that identity is still alive.
- Evidence that the presenter links to the claimed identity; that the person claiming the identity is who they say they are and that they are the only claimant of the identity.
- Evidence that the presenter uses the claimed identity; meaning, that the claimant is operating under this identity in society.
- The first point above relates to the maintenance of biometric databases, implying that people should occasionally present themselves to authorities as a means to confirm that records on file are still claimed by a unique, living person. Records that have not been confirmed / updated could be flagged as possibly abandoned identities. The flagging could mean, for example, that the individual is deceased, has emigrated or is simply non-compliant for any number of reasons.
- The other two points are linked to the usual use of Biometrics and can provide opportunities to enrich or update the Biometrics database.



Recommended further reading: *ICAO TRIP Guide on Evidence of Identity*.

▶ SECURITY OF BIOMETRICS

While significant attention must be dedicated to the security of biometric systems, on a technical level this is a colossal endeavour requiring intense technical comprehension, and apart from reiterating its importance, is not the immediate focus of this guide.

The vulnerability of biometric systems and thus, the importance of security, are highlighted in this manual but without detailed descriptions on how it functions. Some key considerations include:

- Analysis of the threats to and countermeasures inherent in a biometric and biometric system application model;
- Security requirements for secure binding between a biometric reference and an identity reference;
- Biometric system application models with different scenarios for the storage of biometric references and comparison; and
- Guidance on the protection of an individual's privacy during the processing of biometric information.

Recommended further reading for technical detail on data security:



ISO/IEC 24745:2022 -Information security, cybersecurity and privacy protection — Biometric information protection.

.....
²² ICAO, *TRIP Guide on Evidence of Identity*, 2018.

▶ HOW ARE BIOMETRICS SECURED ON TRAVEL DOCUMENTS

ICAO Doc 9303 specifies the use of biometrics in electronic machine-readable travel documents (eMRTDs), establishing the face as the primary biometric, with fingerprint and iris as optional biometrics.

While the facial image can be read from a chip using Basic Access Control (BAC) or Password Authenticated Connection Establishment (PACE), fingerprint and Iris are defined as confidential and hence Doc 9303 requires that these two features should be protected under “Extended Access Control” or EAC; whereby only terminals authorized by the passport issuing country are able to read this data. One of the most widely used protection schemes is the European Union Implementation of Extended Access Control.

In this scheme, a specific Inspection System is “permitted” to read the fingerprint and/or Iris for a limited time. This permission is given by the issuer of the document. The holder of the document does not have control over when or if the permission is given.

4.3 ▶ MEASURING BIOMETRIC PERFORMANCE: RELIABILITY AND ERROR

Biometrics are often perceived as the silver bullet for reliably identifying individuals. While technology has evolved in terms of sensor ability and complexity of algorithms, demographic variables play an important role in technical performance. Vendors, policymakers, technical specialists as well as the end-users – meaning, the public – should be aware of the limitations and potential for discrimination.

There are two main metrics that are used to measure the performance of a biometric system: false acceptance and false rejection.

The matching between the anchor biometric and the presentation biometric is never 100 per cent. The returned value is the one that is the “closest match” to the anchor image (in the case of 1:N matching) or a percentage of similarity (in the case of a 1:1 match). Hence biometric systems are set up to assume that a match above a certain threshold is a valid match. This threshold is also known as the Biometric Match threshold.

Since the match threshold is below a 100 per cent match, it is still possible that a presented biometric may not be the right person, but their match percentage is above the threshold due to similarity with the anchor image. This is called False Acceptance and the proportion of such false acceptances to the total number of matches is termed as the **False Acceptance Rate (FAR)**.

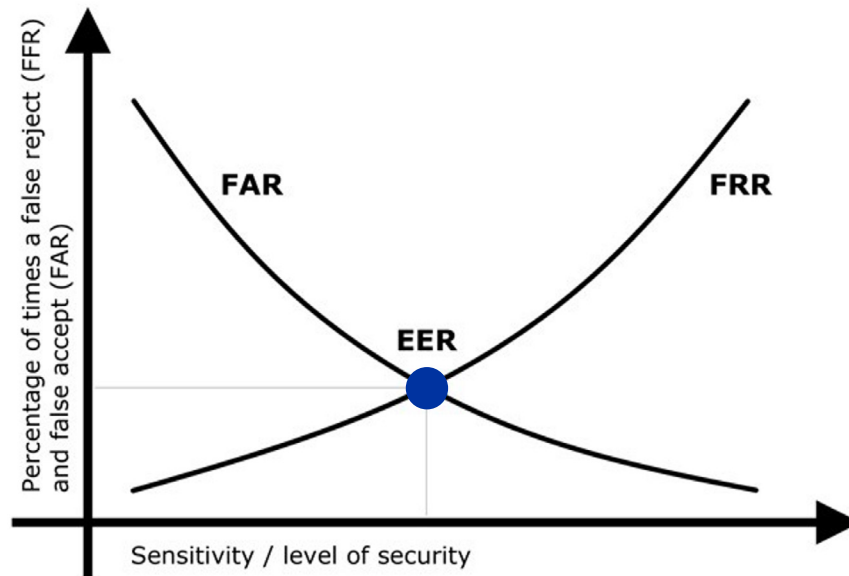
It is also possible that the threshold is set very high, and the match is below that threshold or a true biometric claim, and this will result in a rejection of a valid biometric claim. This is called False Reject and the proportion of such transactions over the total number of transactions is termed as **False Rejection Rate (FRR)**.

The false non-match rate (FNMR) is the rate at which a biometric matching miscategorizes two captures from the same individual as being from different individuals. It can be thought of as the false rejection rate (FRR) for a typical classification algorithm.

It is important to note that all of these values are dependent on the value of the match threshold. If the threshold is set very low, then there will be more cases of false acceptance and less cases of false rejection. If the match threshold is set very high, the FAR will be low, but FRR will be high.

If plotting the FAR and FRR against the match threshold, a graph as depicted below will be generated. The point at which the two graphs meet is called the **Equal Error Rate (EER)**.

Figure 5. Visualization of the equal error rate point in function of the sensitivity respectively level of security, and the percentage of times a false reject and false accept occur



Source: Original author unknown.

If aiming to reduce False Acceptance, the system becomes very secure, but the convenience is low, as it will also have a high False Rejection Rate. In practice, it is a trade-off between security and convenience, and the thresholds for this trade-off vary for different use cases.

4.4 SYSTEM BIAS

Facial recognition algorithms can become biased if their training datasets are not diverse. Recent research on face classification algorithms from IBM, Microsoft, and few other companies shows all to be most accurate with light-skinned men, and least accurate with dark-skinned women.²⁴

Although technological and hardware providers continue to strive for absolute accuracy, existing research suggests that no algorithm will ever perform ideally for everyone: there will be users who are prone to being misidentified, which may make them targets for impersonation or unusually, able to impersonate others.²⁵ Beyond impersonation, this is an integral element to the reality that some ethnicities or demographics may be discriminated against through errors in representation.

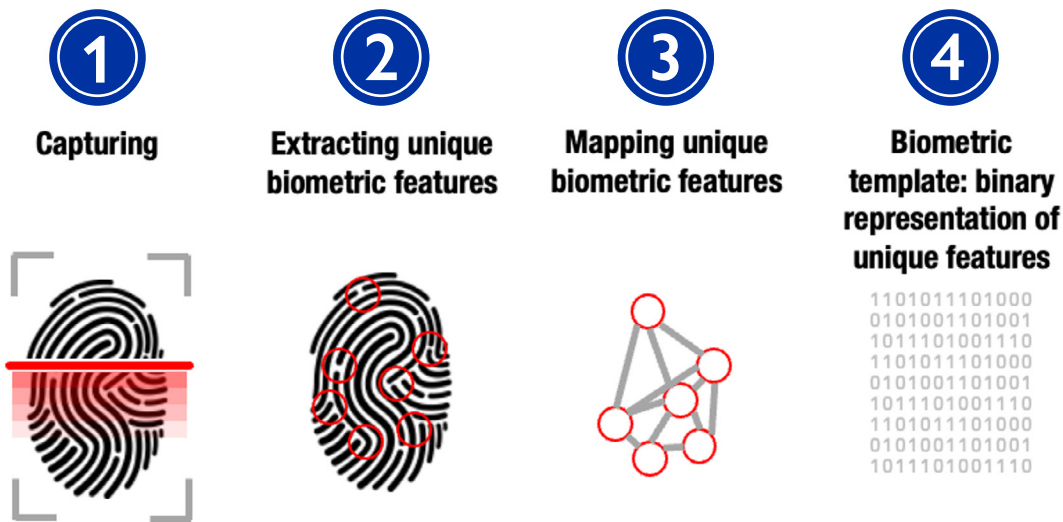
Although some argue that Artificial Intelligence (AI) technology is impartial because it is void of emotion or opinion, it is important to recognize that the developers behind the machine are not. Much like the categorical surveillance mentioned above, unconscious or even conscious bias at the time of design and scaling can influence coding and machine learning.

As has been described, a biometric system is a system that allows the recognition of a certain characteristic of an individual using mathematical algorithms and biometric data. These algorithms compute from a biometric sample from a capture device such as a camera or fingerprint scanner, into a biometric template. A template is a set of stored biometric features as depicted here:

²³ Buolamwini, J. and T. Gebru, "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification" in Proceedings of Machine Learning Research 81:1–15, 2018.

²⁴ Yager, N. and T. Dunstone, "The Biometric Menagerie" in IEEE Transactions on Pattern Analysis and Machine Intelligence, 32(2), 2010.

Figure 6. Generation of biometric templates



Source: Visualization by the authors with elements from Shutterstock.

The generation of templates are based on research that relies on past system performances, working on typically under representative training datasets. Traditionally, these datasets have been populated by Caucasian persons. MIT research found typical datasets to be 77 per cent male versus 23 per cent female; 83 per cent white versus 17 per cent “other”.²⁵

The empirical evidence is stark. A ground-breaking study published in December 2018 by the U.S.-based National Institute of Standards and Technology (NIST), which analysed 189 software algorithms from 99 developers, observed higher rates of inaccuracy for Asian and African-American faces relative to images of Caucasians, often by a factor of ten to one hundred times.

A 2018, an MIT Media Lab study also found that the facial recognition systems from companies such as IBM, had a 0.8 per cent error on white men versus a 34.7 per cent error on dark-skinned women. Thus, it is increasingly evident that a reliance on facial recognition can result in severe miscarriages of justice in the form of false rejection and/or false identification; false arrests and erroneous convictions, in particular among people of color.²⁶

Key findings from the cited study include:

- There is a significant demographic differential bias.
- False positives are substantially higher than false negatives, but with different root causes:
 - False negatives originating from poor quality photos;
 - Large false positive variations by ethnicity or skin colour;
 - Higher false positives among women, elderly and young;
 - Twins are not separable, creating false positives;²⁷
 - Human review capability is poor;
 - Morphing, as both individuals will be recognised as the same person by the Facial Matching System.

²⁵ Massachusetts Institute of Technology (MIT), [Study finds gender and skin-type bias in commercial artificial-intelligence systems](#), MIT News 2018.

²⁶ National Institute of Standards and Technologies, U.S. Department of Commerce, [Study Evaluates Effects of Race, Age, Sex on Face Recognition Software](#), 2019.

²⁷ The mentioned finding results from the referenced NIST test setting. Work from Muard Ali Rahat et al, in the paper “*Monozygotic and Dizygotic Twins Differences in Fingerprint patterns of Swat District*”, August 2020, provides the following conclusion of their research: “The results concluded that the fingerprints of identical twins are more similar to each other as that of the non-identical twins, when two fingers both the left and right thumbs were compared each with eight (8) points. In both cases there are matching on the first six (6) points out of the total eight (8) points while the rest of the two (2) points remained unmatched. The matching percentage for each of these pairs of fingers is 75% whereas, that of the mismatched is 25%. But when both fingers rotated on 180°, and then compared with a total of 8 points and the matched percentage was 87.5%, while the mismatched percentage was 13.5. However, these 8 points were found enough for differentiation of identical and non-identical twins.”

These weaknesses are significant while some of this can be mitigated by employing multi-modality approaches to biometrics, it is clear that the industry has a responsibility to improve and equalize such outcomes.



Resource: Study on Fingerprint Recognition for Children, Final Report, European Commission Joint Research Centre, Institute for the Protection and Security of the Citizen, Digital Citizen Security Unit, September 2013. Chapter 7.1

▶ UNDER-REPRESENTATION IN DATASETS

As noted above, and as a common starting point for subsequent limitations, under-representation in testing datasets and lack of compensation for technical weakness can result in system bias and discrimination. This could be based on some of the following factors:

- Age group (minors / elderly)
- Sex, due to underrepresentation in testing datasets, not accounting for different physical attributes, and/or cultural boundaries as well as explicit exclusion, limiting the participation of some groups;
- Persons with physical, cognitive or mobility impairments, as well as groups with medical conditions causing intended biometric features to be absent;
- Various ethnicities and especially ethnic minorities, due to underrepresentation in testing datasets;
- Work sector such as academic versus field or manual labourers, which could have an impact on damaged or altered biometric features;
- Persons who are unable to provide free and informed consent;
- Objections to certain modalities due to personal or societal beliefs.



VULNERABILITY OF BIOMETRIC SYSTEMS

▶ PRESENTATION ATTACK

Attacking a biometric system can have valuable outcomes for the perpetrators, and it is not surprising that such attacks rise each year in frequency and creativity. Presentation attacks are attacks targeted at biometric recognition system data capture devices with the intention to tricking the system and manipulating the results, also known as “spoofing”. A presentation attack may also be an attempt at obfuscation, whereby the user is trying to evade being recognized by the system.



Types of attacks on fingerprints:

- Paper printout of a fingerprint
- Direct use of latent print on the scanner
- An artificial cast of a finger



Types of attacks on face:

- A picture
- Mobile phone-based display
- Masks



Types of attacks on iris:

- A picture of Iris either as a printout or on a mobile phone screen
- Video display of Iris to simulate movement
- Contact lenses

It is to be noted, that presentation attacks are most likely to succeed where the collection of the biometric is not supervised such as during entry of a building using biometrics, or an automated border control station.

► PRESENTATION ATTACK DETECTION (PAD)

To prevent such presentation attacks from being successful, it is necessary to be able to detect them.

The detection of attack could be done at the sensor itself. For example, a fingerprint scanner may also have the ability to check for the liveness of the finger presented, meaning, that the presentation is occurring in real time. Similarly, liveness detections can be done for facial recognition, using two types: one is called “active detection”, which requires the user to execute a certain set of instructions like looking up, left, etc., and the software checks if the presented image can be considered a plausible response to the instruction. The other is called “passive detection”, where the software tries to determine whether the subject is actually present.

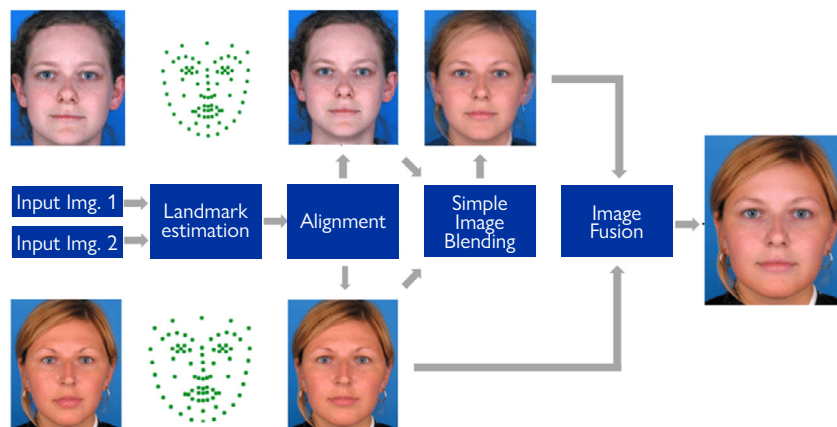
Another method would be for the matching software to check for additional artefacts that might indicate a presentation attack. The field of presentation attack detection is an evolving field and a lot of effort is being put into solving this issue.

► MORPHING

Morphing is the creation of a synthetic face image using the faces of two different individuals and then presenting this image for acceptance as an anchor image. In this case, both the individuals will be recognized as the same person by the Facial Recognition System.

Morphing is not a problem in cases where live enrolment of biometrics is done; however, if people are permitted to send in a photograph for enrolment, then morphing attacks can be carried out.

Figure 7. Accurate and robust neural networks for face morphing attack detection



Source: Journal of information security and applications. Process of morphing. Seibold, C., W. Samek, A. Hilsmann and P. Eisert, (2020).

4.6 ► BILATERAL SHARING OF BIOMETRIC DATA

The use of biometrics must be lawful, responsible, and for a specified, explicit and legitimate purpose. A Data Protection Impact Assessment should be conducted prior to any disclosure of biometric data. If the risks of disclosure do not outweigh the benefits and a decision is taken to share biometric data with other entities, there should be appropriate legal and contractual safeguards between data sharing stakeholders, public or private; States or institutions, guided by the IOM data protection legal framework, to protect the biometric data of all data subjects.

▶ RISK AND CONCERN

The increasing use of biometric systems introduces significant concerns regarding their vulnerability. The risk of security breaches, unauthorized access, and potential data manipulation poses a threat to individual privacy and can lead to identity theft. As stated before, storing biometric data in centralized databases or a public cloud environment raises additional questions about data protection and cybersecurity. Moreover, as these systems become more interconnected, the potential for sophisticated attacks like spoofing or tampering amplifies the need for stern security measures. A comprehensive approach, including robust encryption, strict access controls, regular security audits, and compliance with IOM's data protection legal framework, is essential to ensure the secure deployment of biometric technologies.



Sharing personal data with **governments** can lead to particular risks for persons in need of international protection. They or their families may be subject to retaliation measures, ranging from criminal sanctions upon return to persecution of family members.



Sharing biometric data with **private entities** can also potentially lead to the use of the data for purposes which are incompatible with the humanitarian purpose for which the data was originally collected as well as accountability issues: who is responsible and accountable if there is improper use of the information?

▶ FUNCTION CREEP

Function creep occurs when information is used for a purpose other than that for which it was collected. This becomes a concern when the secondary use is not communicated to the individual at the time of providing their information.²⁸ Generally, biometric data collection protocols should ensure that the data subject understands who controls the biometric data and the purposes for which it is collected and otherwise processed. The data subject should be informed about the entities to which the data will be transferred. IOM's data protection legal framework sets out the minimum information that should be provided to a data subject when their data is collected.

▶ COVERT COLLECTION

The covert or passive collection of individuals' biometric information means data being collected without the subject's informed consent, participation, or knowledge. Facial biometric information, for example, can be captured from photographs that individuals do not know are being taken, and latent fingerprints can be lifted to collect biometric information long after an individual has made contact with a hard surface.

▶ SECONDARY INFORMATION

Depending on the biometric data and how it is processed, whether as a template or raw data, some biometric data could potentially reveal secondary information about an individual beyond the purpose for which the biometric data was initially collected. A raw image of a facial biometric, for example, could potentially reveal health information that an individual may not want to provide, or to which they did not consent.

.....
²⁸ Recall the increased access of databases specific to border governance, as referenced in OHCHR's 2023 study on [Digital Border Governance: A Human Rights Based Approach](#).

▶ DATA SEGREGATION

Biometric and associated biographic data should always be stored in separate isolated databases. This serves to mitigate risks related to unauthorized system intrusions and unlawful data extractions. The data from each system should only be linked to authorized IOM personnel using a common unique identifier when required. Finally, secure logs should record who accessed the system, what activity they undertook and for what reason.

4.7 ▶ ON PROCUREMENT OF BIOMETRIC TECHNOLOGY

Procurement is the act of acquisition or purchase of goods or services, which can include the procurement of biometric technology. The framework for procurement by governments or agencies can vary. In most cases, there is a specialized agency or department that provides procurement services to the project-owning agencies. In the case of multiple agencies and/or approaches to procurement, the lowest thresholds in terms of risk and limitations should be employed, and stakeholders and procurement professionals can perform best when there is good cooperation and coordination. All procurement through IOM and partners must adhere to IOM's established General Procurement Principles and Processes²⁹ for vendors and IOM's internal Procurement Manual, IN 168. There are various reasons for a coordinated procurement process when using biometrics, such as:

- Interoperability
- Economies of scale
- Capacity-building and improvement
- Establishing requirements / Terms of Reference
- Avoidance of lock-ins

▶ RECOMMENDATIONS ON PROCUREMENT FOR BIOMETRICS



Ensure integrity

Contracting officers must ensure the integrity of the procurement process.



Get involved early

The procurement process can be facilitated by advance work being done with the internal clients. This includes helping with needs identification and requirement definition, procurement strategy development, and drafting of solicitation documents before a requisition is actually received. Facilitating the process also includes ensuring that accessibility has been considered by clients and, where appropriate or necessary, is incorporated into the procurement process, including in the requirement definition and solicitation documents.



Consult with peers

Contracting officers should consult with colleagues, particularly when working with an unfamiliar situation, such as a new commodity, or incorporating accessibility into procurement requirements or solicitation documents.

²⁹ IOM General Procurement Principles and Processes.



Liaise with the client

The contracting officer should keep clients informed and involved, and in order to develop responsive, creative and flexible procurement strategies, their departmental needs must be understood, as well as their specific technical and accessibility requirements. When consulting the client, make the purpose plain, so that if there is a problem with a proposed approach a solution that achieves the purpose can be developed. The contracting officer must work with the client towards their operational objectives.



Use specialists

The contracting officer should seek advice from the following specialists: legal services, policy advisors, access to information and privacy officers, quality control officers, cost analysts and risk management advisors.



Commodity knowledge

Contracting officers should develop their understanding of their commodity's industry, the market conditions, opportunities, accessibility standards and options, and other pertinent factors of each commodity, which then affects the choices made by contracting officers in determining, for example, such things as the basis of payment and the selection methodology. Clients should also use their understanding of the commodity, including relevant standards or best practices, when defining their technical and accessibility requirements and scope. This would include any market analysis of capacity when the procurement is subject to a Comprehensive Land Claims Agreement.



Maintain confidentiality

The contracting officer must treat all information of a confidential or personal nature, including bid information, in a secure and confidential manner.



Communicate effectively

Contracting officers should be very clear in communications. Written instructions accompanying each bid solicitation, for example, should be clear with no ambiguity, and be easily understood by all parties.



Obtain confirmation

The contracting officer should obtain written confirmation of significant information, agreements and discussions, such as confirmation of an unusually low price, or extension of a bid validity period by the bidder.




Life Cycle Management of Assets

Life Cycle Management of Assets (LCMA) is an integrated approach to materiel management that looks at the process as a complete system rather than separate activities.



Maintain records

Contracting officers must keep procurement files up to date for reasons of good management, access to information requests as well as for audit purposes.

A close-up photograph of a person's hand being scanned on a biometric device. The device has a glowing green light on the scanning area. A barcode sticker is visible on the device. The background is dark and out of focus.

PART 5

TECHNICAL IMPLEMENTATION

Syrian refugees are undergoing biometric registration by Canadian officials as part of their application process to resettle in Canada. © IOM 2016/Muse MOHAMMED

5.1 FINGERPRINT

A fingerprint is a mark made by the pattern of ridges on the pad of a human finger. This has been used extensively over history for forensic analysis and criminal investigations, as well as authentication for access to mobile phones or secure buildings, in contemporary times.

The pads of the fingers and thumbs have a unique pattern of friction ridges (which are the raised part of the skin surface) and furrows (which are the recessed part of the skin surface). They have certain patterns and these patterns are grouped into specific types.



Arch

Arches create a wave like pattern on the surface of the finger. Arches that rise to a sharper point are termed tented arches and ones that do not rise to a sharp point are termed plain arches.



Loop

Loops are patterns that recurve back on themselves to form a closed loop and hence the name. The loops that point towards the thumb (also known as radius bone) are termed radial loops, and the ones that point towards the little finger (known as the ulna bone) are termed as ulnar loops. These form the majority of the patterns in a fingerprint

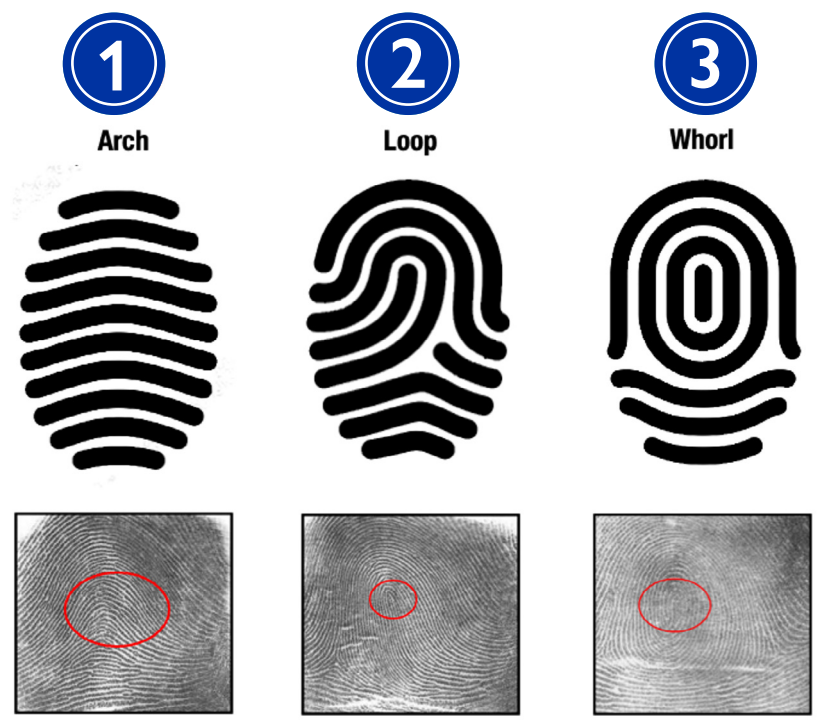


Whorl

The circular or spiral patterns on the skin surface are termed whorls. They look like miniature whirlpools.

There are different types of whorls and these constitute the second largest group of patterns on a fingerprint.

Figure 8. Arch, Loop and Whorl



Source: Visualization by the authors with elements from unknown source.

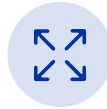
▶ REPRESENTATION OF FINGERPRINTS

There are mainly four types of fingerprint representation systems.



Grayscale image

The image is saved in an 8-bit monochrome representation of the actual capture. It is a perfect reproduction of the captured biometric without any enhancements being done to the image.



Phase Image

The image is enhanced for contrast through a pre-processing before the image is stored.



Skeleton image

The circular or spiral patterns on the skin surface are termed whorls. They look like miniature whirlpools.

The width of the ridgelines is reduced using a thinning algorithm.

Figure 9. Greyscale, Phase and Skeleton image



Source: Visualization by the authors with elements from unknown source.



Minutiae

The two most prominent characteristics of a ridge are (a) ending and (b) bifurcation.

Figure 10. Forms of minutiae

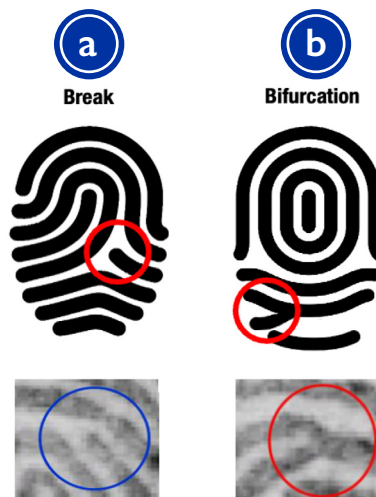


Diagram (a) shows the place where a ridge line ends. It represents a break in the ridge line, after which it does not continue.

Diagram (b) shows a bifurcation of ridgelines. It marks the place where a single ridgeline separates into two distinct ridgelines.

Source: Visualization by the authors with elements from unknown source.

Apart from ridge endings and bifurcation, other features that can be marked on a fingerprint are as follows:

- **Independent ridge** – a ridge that starts and ends within a short distance.
- **Island** – a very short ridge that is not connected to any other ridges.
- **Ridge enclosure** – a single ridge that bifurcates and then unites to become a single ridge.
- **Spur** – a short ridge than bifurcates from a longer ridge but ends within a short distance.
- **Bridge** – a short ridge than connects two parallel ridges.
- **Delta** – a Y-shaped ridge bifurcation.
- **Core** – a circular ridge.

The collection of these features and its location in the fingerprint is known as a minutiae. It is a representation of the information collected from the fingerprint. However, it is not the original fingerprint and the fingerprint itself cannot be recreated from the minutiae.

▶ CAPTURING OF FINGERPRINTS

For fingerprint comparison, the capture of the anchor fingerprint data is important. Before the advent of computers, fingerprints were captured by inking the surface of the finger and then rolling it on a piece of paper.

Electronic devices that can be used to capture fingerprints. The choice of representation to store the fingerprint is not dependent on the device. That is, irrespective of the device used to capture the fingerprint, they can be stored as grayscale image, phase image, skeletal image or minutiae.



Capacitive scanners

These scanners use a capacitor, which induces an electrical current, which is then used to form an image of the fingerprint. These are the most accurate fingerprint scanners.



Ultrasonic scanners

This is the newer form of fingerprint capture. It uses high frequency sound waves to penetrate the outer layer of the skin. Some of the sound waves are reflected back depending on the ridges and valleys and these enable creating an image of the fingerprint.



Other type

Other types of fingerprint scanners are:

- Thermal scanners – use the temperature difference between the ridges and valleys to construct the fingerprint image;
- Radio frequency scanners – use radio frequency waves to construct the image.



Optical scanners

Optical scanners have a built-in digital camera. The image of the finger is captured using this camera.



Touchless fingerprinting

All of the scanners listed above have a scanner panel on which the finger is placed for the capture. When pressing the finger against this panel, there is a deformation of the skin, which depends on the pressure applied and also the position in which the finger has been placed. Hence, no two captures are the same. Touchless fingerprint scanners use a camera (similar to optical scanners), but do not require the finger to be placed on a scanner panel. However, the surface area that is available for capture is then reduced as there is a certain distance between the camera and the finger. To overcome this, scanners have multiple cameras or mirrors, which then combine the images to recreate a composite image of the finger. It is to be noted that at the present time, the interoperability between devices in terms of comparison accuracy is not as good as contact scanners.

▶ QUALITY OF FINGERPRINTS

For fingerprint comparison, the quality of the captured fingerprint data is important. The thickness of the captured ridges must be sufficiently wide and uniform. There needs to be sufficient separation between ridges and the valleys. The image has to be of sufficient size (area of surface contact) to be able to extract useful information for matching.

Factors that can affect fingerprint quality.



Age

Age (**elderly people**) – as people age, the skin becomes smoother and the ridges may not be prominent enough for capture.

Age (**infants**) – it is unclear if the changes in finger structure as children grow, impact the ability of matching systems to verify someone years after their initial enrolment.

- It is not confirmed whether the smaller size of a juvenile fingerprint provides sufficient information for accurate enrolment and matching.
- The 2022 NIST report cautions on the matching performance of fingerprinting in children: “Younger subjects give considerably higher False Non-Match Rate (FNMR)”.³⁰
- The finger, palm and footprint scanners for infants and children require very high resolution. Scanners with lower ppi for adults will not be able to cope with the lack of definition in smaller children’s or infants’ fingerprints.



Damage

People who work their hands (carpenters, farmers, masons, violinists, nurses, working with chemicals) and those who participate in sports such as rock climbing will wear out the skin surface and make it challenging to capture fingerprint information.



Skin texture

Different populations can have variations in skin texture which may respond differently or ineffectively to fingerprint scanners. Individually, people can have more prominent ridges and valleys in their fingerprints than others, which can also affect scanner results. Scanners can be tuned to capture fingerprints of various textures, but it is quite difficult to tune a single device to work effectively for diverse populations.



Medical / dermatological reasons

People with oily skin or eczema may have a challenge in presenting fingerprints that are sufficient for matching.

Resources:



ISO/IEC 19794-4:2009 – Biometric data interchange formats – Part 4: fingerprint Image data.
ISO/IEC 19794-2:2011(en) Biometric data interchange formats — Part 2: Finger minutiae data.
ISO/IEC 29794-4:2017 Biometric sample quality — Part 4: Finger image data.
NFIQ 2 - NIST Fingerprint Image Quality (NFIQ).

³⁰ NIST: «Ongoing Face Recognition Vendor Test (FRVT) Part 1: Verification», 30.08.2022. Available at : www.nist.gov/programs-projects/face-recognition-vendor-test-frvt-ongoing; Chapter 3.5.3.

5.2 FACE

Facial Recognition is a generic term that encompasses Face Detection (detecting the position and size of a face in an image) and Face Matching (comparing to pre-registered faces to identify the person). It is a form of image recognition. Recognizing faces is an inherent trait for human beings. Instances where a person presents an identity document which contains his or her face and the verifier does a visual comparison between the presenter and the face stored in the identity document, uses this basic and ancient ability of human beings to recognize a face.

The theory of automated facial recognition is quite complex, and this section aims to simplify the description for the intended audience of this manual.

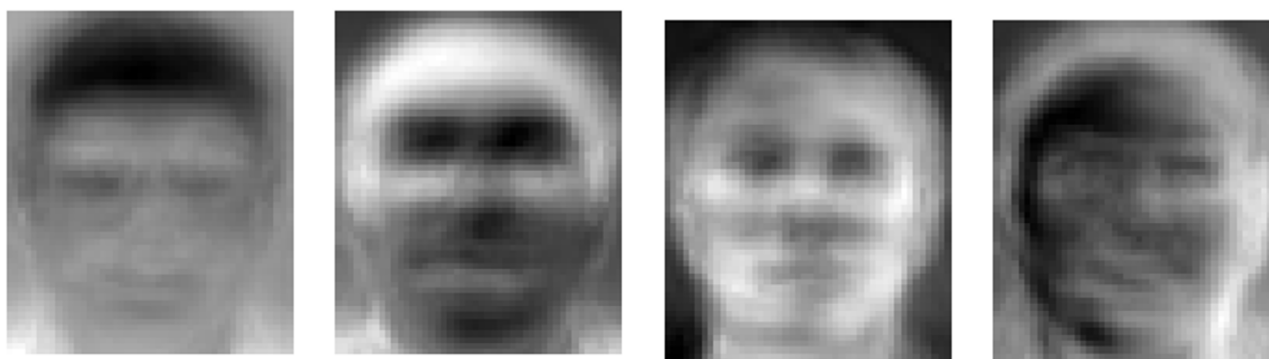
Facial recognition can be distinguished as either *feature-based* recognition, whereby the face is compared feature by feature like distance between eyes; or *image-based* recognition, whereby the image is compared based on the pixels of the image by doing some form of transformation of these pixels.

Automated facial recognition is generally accepted as beginning in the 1960s whereby facial features and their coordinates were manually established by a human operator from a photograph.³¹ There were twenty such parameters that were mapped from each of the sample photographs. A computer program would then take a photograph and do the same measurements and return a photograph that was closest in terms of these measurements. This method falls into the category of feature-based recognition. The rest of this section deals with image-based recognition.

A later development was what is known as *Eigenfaces*. In this approach, a training data set is necessary. Each image is converted to multiple images, with each image covering a single component of the face, called an Eigenface. This process is also known as Principal Component Analysis (PCA). The images in the data set can be recreated by combining the Eigenfaces. However, a smaller set of Eigenfaces, which are sufficient to arrive at a close approximation to the original images in the data set, are maintained.

To do facial recognition, the anchor image for comparison, are saved as a collection of the Eigenfaces that can recreate that image along with the contribution weightage of each of those Eigenfaces to the anchor image. When a face is presented for comparison (the presented image), the Eigenfaces that can be used to recreate this face are taken along with the contribution weightage of each of them, and then these values are compared to the weightages of the stored anchor images. The one with the closest match in terms of numbers is then returned as the match.

Figure 11. Eigenfaces



Source: AT&T Laboratories Cambridge.

The value of the different Eigenfaces will depend on the conditions of capture of the anchor image and also the capture of the presented image. The size of the original anchor image and the size of the presented image will also impact this comparison.

³¹ This could include, for example, the distance between the eyes, the width of the mouth; however, this is quite arbitrary of a measurement and further, linked to historic attempts to quantify the physical attributes among different ethnic groups for discriminatory purposes.

A different method known as **Fisherfaces** attempts to improve on the limitations of Eigenfaces. In the case of Eigenfaces, one attempts to find contributing weights for each datapoint. In the case of Fisherfaces, the attempt is to focus on a single datapoint whereby the different images in the training data set are as far apart from each other as possible. Finding the datapoints that allow for such separation between the images is the essence of Fisherfaces. This aims to reduce the limitations associated with image capture conditions while maintaining the ability to differentiate between the images.

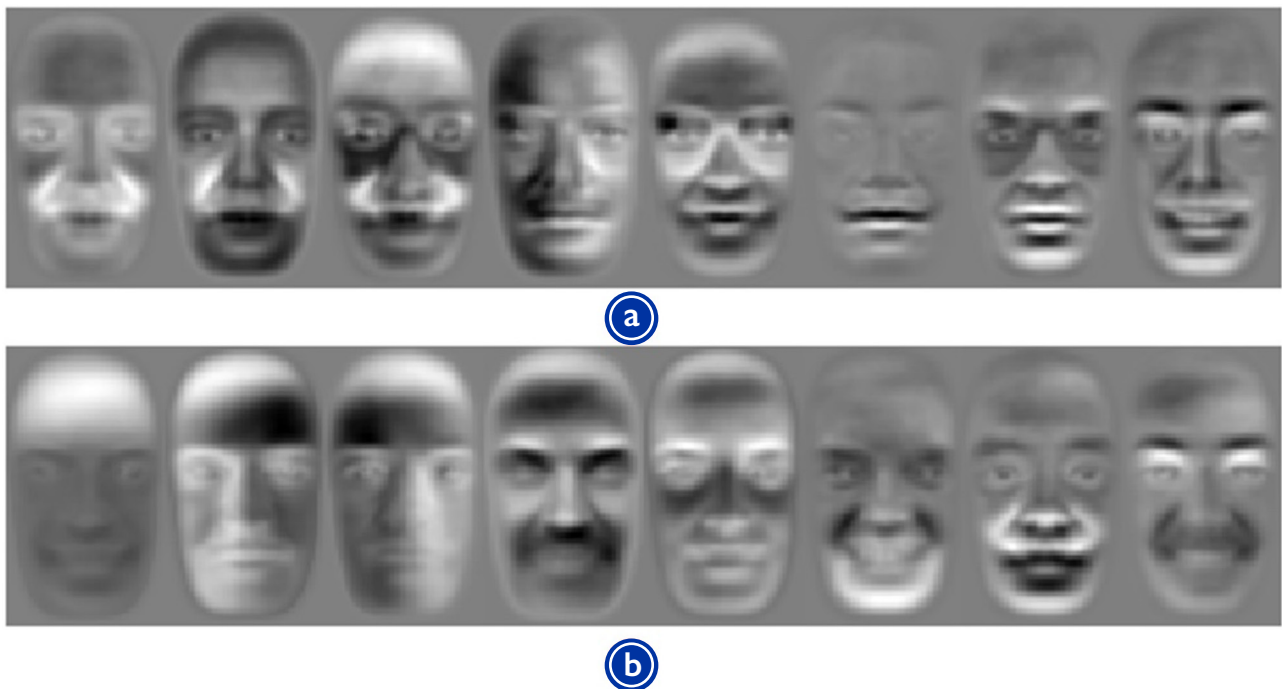
Figure 12. Fisherfaces



Source: www.scholarpedia.org/w/images/b/b0/Fisherfaces.jpg.

The **Bayesian face recognition** method uses a statistical approach to facial recognition. At a very simplistic level, the logic is as follows: First assume that the two faces belong to the same person (intrapersonal hypothesis). Next assume that the two faces belong to two different persons (extrapersonal hypothesis); then classify the differences between the two as either intrapersonal or extrapersonal variances, based on previously learned logic. The match is a likelihood ratio of the intrapersonal variations versus the extrapersonal variances.

Figure 13. Bayesian Face Recognition. “Dual” Eigenfaces: (a) Intrapersonal, (b) Extrapersonal



Source: Moghaddam, B., T. Jebara and A. Pentland: Bayesian face recognition. Pattern Recognition 33 (2000) 1771–1782.

The past two decades have seen an explosion of activity in the area of face recognition and some algorithms may be too complex for the purposes of this document. However, the following is a list of some of the terminologies commonly referenced in this field.

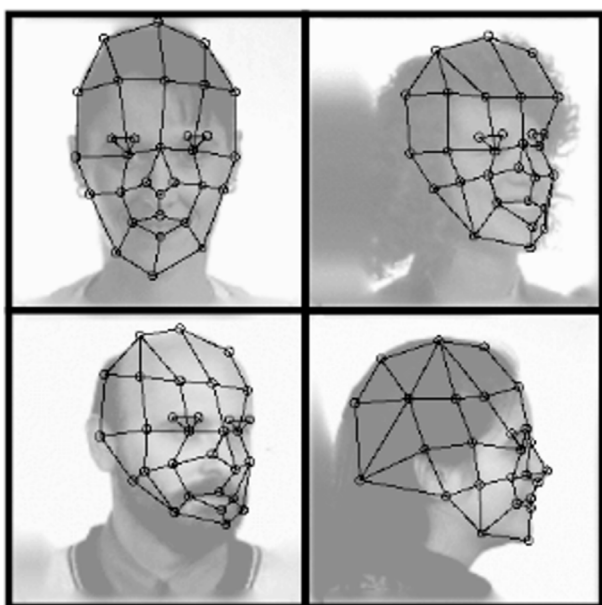


Elastic Bunch Graph Matching (EBGM)

A system that works by extracting concise face descriptions from an image, which describes reference points in an image as an image graph. The matching is done by a comparison of the image graphs.

While innovative and efficient, experts have noted that biometric technologies exacerbate discrimination and human rights' abuses when deployed for control and surveillance by States and that "the use of new technology tools could deepen racism and xenophobia.³²" With the inception of AI wherein algorithms and deep learning mimic human behaviour, this abuse and exclusion will be further aggravated. Recommendations emphasize that the use of security technology should be free of racial biases to comply with human rights and thus, great caution must be exercised in the employment of these technologies, with foresight on their control and management by authorities.

Figure 14. Elastic Bunch Graph Matching (EBGM) – Grids for face recognition



Source: Wiskott, L., J.M. Fellous, N. Krüger, and C. von der Malsburg, (1999). Face recognition by elastic bunch graph matching.



Deep Learning

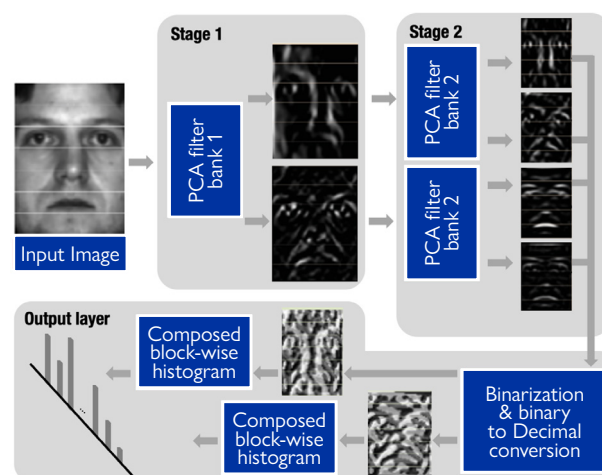
Deep Learning is a subset of AI. The goal is to allow machines to analyse a large volume of data and make decisions/predictions with as little human intervention as possible.



PCANet

This deep machine learning has multiple stages of Principal Component Analysis (PCA, as with Eigenfaces) and then does further processing to extract useful information for facial matching.

Figure 15. PCANet



Source: PCANet: A Simple Deep Learning Baseline for Image Classification? - Tsung-Han Chan, Kui Jia, Shenghua Gao, Jiwen Lu, Zinan Zeng, Yi Ma.

Deepface is a deep learning facial recognition system created by a research group at Facebook. Deepface is a lightweight face recognition and facial attribute analysis (age, gender, emotion and race) framework for python. It is a hybrid face recognition framework wrapping state-of-the-art models: VGG-Face, Google FaceNet, OpenFace, Facebook DeepFace, DeepID, ArcFace, Dlib and SFace.

³² OHCHR, [Special Rapporteur on Contemporary Forms of Racism Calls for a Moratorium on the Use of Surveillance Technology in the Immigration Enforcement Context](#). Press release, 2021.

▶ REPRESENTATION OF FACIAL BIOMETRICS

The representation of the facial image depends very much on the algorithm that is used for facial recognition. Each of the methods first requires a “training process”, whereby the machine transforms the input images into a form that it can use for comparison, and then presentation of another image for matching.

Since these systems work on a normal image as the input, the training data and/or the anchor images are stored as images without any transformation. On starting the system, it then takes these images and does the processing necessary to convert them into the form that can be used for comparison.

▶ CAPTURING OF FACIAL BIOMETRICS

The capture of a facial image is done with a camera, suffering the usual drawbacks of camera-captured imagery in terms of clarity, light balance, exposure, shadow and angle, which must be taken into account.



The capture of the anchor image needs to be of good quality to allow for effective Facial Recognition using this anchor image. One of the biggest uses of facial recognition is in the area of MRTDs. The document www.icao.int/Security/FAL/TRIP/Documents/TR%20-%20Portrait%20Quality%20v1.0.pdf lists the quality requirements for capturing images for purposes of using in travel document.

▶ QUALITY OF FACIAL BIOMETRICS

On a general basis, the quality issues are as follows:



Image size

Depending on the field of application, size of the captured image is mandated by the specifications.



Width to Height Ratio

The ratio between the horizontal dimensions and the vertical dimensions are also determined by the use case. For MRTDs, the ratio is mandated as being between 74 per cent and 80 per cent.



Sharpness

This refers to the image’s clarity in terms of both focus and contrast.



Background pattern

The photo must be taken on a clear background that does not interfere with the clarity of the person’s features. Usually, it is grey with a plain, dull flat surface. Colour backgrounds like light blue and white may be used as long as there is sufficient distinction between the face/hair and the background.



Lighting

Lighting plays an important role in highlighting the face with the correct brightness and contrast with respect to the background.



Other measures

Some other measures that are usually specified include:

- Distance between eyes measured in pixels;
- Width of the eye;
- Width of the head;
- Length of the head;
- Distance of the face from the border of the photograph.

While significant strides have been made in facial recognition, the possibility of presentation attack as well as false identification and/or false rejection and the subsequent consequences remain. As described above, facial recognition is based on a training data set. If the training data set is not sufficiently diverse, it can increase the risk of inaccurate identification or non-identification.

References



ISO/IEC 19794-5:2005 – Biometric data interchange formats – Part 5: face Image data.

ISO/IEC 29794-5:2017 Biometric sample quality — Part 5: Face image data.

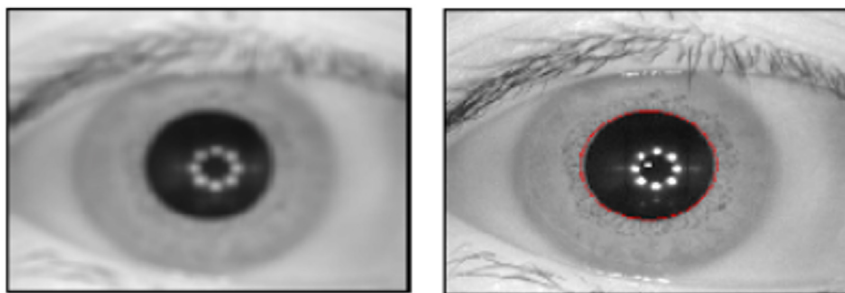
ICAO Technical Report – Portrait Quality (Reference Facial Images for MRTD) – Version 1.0 – 2018.

5.3 IRIS

Iris recognition uses many of the same models that were mentioned in face recognition, as it is also a case of image comparison. The Iris is a thin ring-shaped muscle structure in the eye that is used to control the diameter and size of the pupil, thereby controlling the amount of light that can reach the retina.

In iris detection, an image of the eye is taken. Then the pupil is detected.

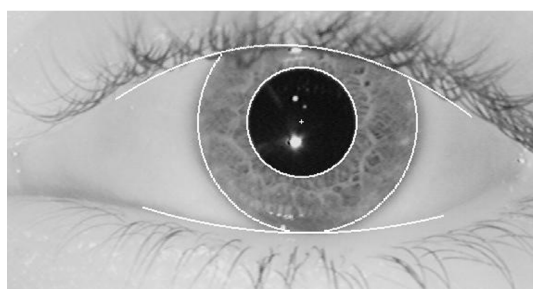
Figure 16. Iris localization. Left prior to processing; Right after machine processing and localization



Source: Suhad, A., E. Loay and G. Loay (2013). New Approach of Iris Localization for Personal Identification.

In the next step, the inner and outer boundaries of the iris are detected by excluding the pupil and the other artefacts such as eyelids, eyelashes.

Figure 17. Detection of the inner and outer boundaries of the iris



Source: www.cl.cam.ac.uk/~jgd1000/iris_recognition.html.

The image is then used for feature extraction, which are then used for matching. Almost all the methods used in Iris recognition are based on Deep Learning models.

▶ REPRESENTATION OF IRIS BIOMETRICS

Similar to facial recognition, the representation that is stored is dependent on the algorithm that is used to detect the iris and its features. Hence, the reference images are usually stored as images themselves and the system then takes the image and does the transformation before actual matching is done.

▶ CAPTURE OF THE IRIS BIOMETRICS

The Iris can be captured using Visible light or Infrared light.

Figure 18. Iris captured using visible light (left) and infrared light (right)



Source: https://en.wikipedia.org/wiki/Iris_recognition

The image on the left uses visible light and the one on the right is in Infrared light.

Effective capture and matching usually requires a camera with an Infrared light source and sensor and the capture is usually done in close proximity.

There are new developments; however, which allow for Iris capture and recognition up to a distance of 10 metres, or even allow capture and recognition will the subject is walking (called iris on the move). This is, naturally, a controversial option as it calls into the question of consent and informing individuals that they are inadvertently providing their biometric data for comparison. The accuracy of images taken on a distant and moving target is also called into question, especially in the context of law enforcement, surveillance and investigations.

▶ QUALITY OF IRIS BIOMETRICS

Iris quality depends on the quality of the captured image. Particular considerations include:



Sharpness – the image's clarity in terms of both focus and contrast.



Pupil to iris **ratio** – affected by pupillary dilation.



Iris pupil **contrast**.



Presence of **eyelashes** – reduces the size of the outer boundary of the iris.

Limitations with iris scanning:



Eye diseases – have an impact on iris affecting biometric recognition.



The **ambient circumstances** – of capture (lighting, gaze) can have an impact on the accuracy of recognition.

References



ISO/IEC 19794-6:2005 – Biometric data interchange formats – Part 6: Iris Image data.
ISO/IEC 29794- 6:2015 Biometric sample quality — Part 5: Iris image data.

Using a multimodal approach reduces the chance of exclusion of certain individuals who may be unable to use a specific form of biometrics or the quality of one form is unsatisfactory.

It is believed that a combination of modalities allows for a more accurate recognition of a person and spoofing becomes more challenging as attackers will have to spoof more than one type of biometric.

The drawback is that the user is required to present their biometrics to different scanners and sensors which is often not a seamless process especially if two types must be presented simultaneously (face and finger on respective scanners at the same moment). Since multiple matches are being performed, the total time taken for a multi-modal biometric match will be higher. This can be an issue for time sensitive scenarios, such as an Automated Border Gate.

The cost of the multi-modal system is generally higher as additional sensors/scanners must be deployed and multiple matching engines are running in parallel.



Chinese migrants get biometric registration at a migrant reception centre after crossing the Darien jungle. A growing number of Chinese citizens set their sights on the United States via the perilous Darien between Colombia and Panama. © IOM 2023/Gema CORTÉS

PART 6

IOM PROGRAMMING WITH BIOMETRIC COMPONENTS



On 12 November, 2019 the Nigerian Ministry of interior launched IOM's Migration Information and Data Analysis System (MIDAS) in Abuja airport. © IOM 2019/ Jorge GALINDO

▶ IOM USE CASES

Biometrics is only one part of a functioning system. IOM developed an integrated solution for governments that streamlines different governmental functions, including but not limited to Migration Management, Border Security, Data exchange and analysis, integrating Biometrics as an identification component. This chapter introduces to the Migration Information and Data Analysis System (MIDAS) developed by IOM and offered to the Member States, and the Electronic Readmission Case Management Systems (e-RCMS), which is an IT platform that digitizes the return and readmission process between two countries in line with the readmission cooperation frameworks in place between them.

6.1 ▶ USE CASE 1: **MIDAS** MIGRATION INFORMATION AND DATA ANALYSIS SYSTEM

Developed by IOM in 1997, MIDAS is a high-quality and user-friendly Border Management Information System (BMIS) for Member States in need of comprehensive cost-effective solution. The system is entirely customizable and can be tailored to the specific requirements of governments for them to identify border monitoring needs and prioritize the tasks. The data collected by the system can set the foundations for improving national statistics and enhance evidence-based migration policymaking. Worth noting that governments have full and exclusive ownership of the system as well as of any data recorded by MIDAS.

Currently operational in countries across Africa, Asia, and the Americas, MIDAS has been designed to be compliant with ICAO and ISO international standards. To date, more than 150 border crossing points (BCPs) are equipped with MIDAS core border management module (+ approximately 50 BCPs coming soon). In addition to this module, MIDAS can be equipped with additional modules available, such as:

- Foreigner Registration Module
- e-Visa Module
- Health Module
- Passport Module
- Citizenship Module

With the capability to collect, process, store, and analyse traveller information in real time and across an entire border network, MIDAS enables governments to manage and monitor inbound and outbound movements more effectively, providing in return a sound statistical basis for decision-making as well as migration policy-related planning. IOM has no access to the data collected through MIDAS, and it ensures that receiving States have full and exclusive ownership of the system as well as any data recorded by MIDAS.

MIDAS automatically captures and verifies traveller's biographic and biometric data through the use of document readers, webcams and fingerprint scanners. The automation of data collection processes allows for faster and more accurate capture of information – alleviating the workload at borders and minimizing to the maximum extent possible human errors.



Standard MIDAS workstation. © IOM 2015



MIDAS training in Moshi, United Republic of Tanzania, September 2019. ©IOM 2019

MIDAS features four core use-cases:



Managing Migration

MIDAS can also be used to assist with in-country immigration and emigration management functions, such as the recording and management of cases and the issuance of residence, employment, and other types of permits, but also serve as case management system for naturalization/citizenship processes.



Border Security

MIDAS automatically checks all recorded entry and exit data against national alert lists. Where a bilateral agreement with the government exists, MIDAS can be interconnected with INTERPOL Alert Lists, so to streamline and expedite border controls. As such, this feature helps States to curtail security risks by automatically cross-checking entry and exit data against national and INTERPOL alert lists (if connected), the latter enabling the timely identification of suspect travellers flagged by law enforcement agencies of other countries. Moreover, such connectivity provides valuable support to the protection of vulnerable people and, for example, in locating missing children and adults.



Exchanging Data

MIDAS-equipped border-crossing points can be connected to a central server to ensure that the collected traveller data is shared between all border crossing points in real time. The system is designed to work in centralized or decentralized mode, the latter allowing MIDAS to function in remote areas with poor or in-existent network connection between the Headquarters and the border post, thus addressing border management imperatives in very challenging network and power conditions.



Analysing Data

MIDAS allows assigned user to easily generate different reports and statistics according to the types of traveller data needed, to mention few: per country of origin, age, gender, type of document, travel purpose or whether the person has been detected in an Alert List. In addition, MIDAS provides a powerful data analysis and reporting tool that produces fully customizable visual dashboards and reports. Processing and analysing the data collected contributes towards a more complete understanding of a country's migration dynamics and mobility patterns. Data collected through MIDAS can thus serve as the basis for the development of well-founded evidence-based migration policies.

Data captured by MIDAS includes:

- Biographic data
- Biometric data (photographs, including for facial comparison and fingerprints)
- Travel document images under Infrared, Ultraviolet and White Light
- Entry and exit data and information
- Visa data
- Vehicle/flight/vessel data
- Health information (where relevant, e.g. during a pandemic)

MIDAS is prepared for facial comparison and recognition as well as comparing travellers' fingerprints. Various modalities and equipment brands are supported. MIDAS can capture traveller photo at the point of entry/exit (PoE) and conduct biometric verification via facial comparison through:

- Live photo versus the photo on the bio page of travel document;
- Live photo versus the photo in the chip of the eMRTD;
- Photo on the bio page versus photo in the chip of eMRTD.

The system can capture either 1, 2, or 10 fingerprints, and compare the travellers' fingerprints against:

- Travellers fingerprint against the fingerprints recorded in the database (1:1; 1:N);
- Travellers fingerprints against recorded fingerprints in Alert Lists (1:N; N:N);
- Travellers fingerprint against recorded fingerprints in the ePassport (1:1; 1:N).

When requested by the receiving Government, MIDAS allows also biometric authentication, i.e. to ensure that MIDAS users access to the system use unique identifiers, namely: Username, User password and User fingerprint.

MIDAS CASE STUDY: MIDAS INSTALLATIONS IN HAITI

Due to its geographical location, the Haitian population is particularly exposed to natural catastrophic events, such as earthquakes, tropical storms, and hurricanes. The most recent earthquake in August 2021 caused more than 15,000 lives. In addition, poverty has intensified, due to the deep political crisis exacerbated by the murder of President Jovenel Moïse in July 2021. These events have led to a significant increase in Haitian migration within and across the region.

Haiti shares the island of Hispaniola with the Dominican Republic, with a border of 388 km. This area is marked by an active cross-border commercial exchanges, driving a continuous migratory and mobility flows. This zone has four official land border control posts: Dajabón, Belladère, Malpasse, and Anse-à-Pitre; additionally, it is estimated that there are around ninety-six unofficial border crossings.

In this highly porous border, there is a proliferation of illegal activities, such as human trafficking, migrant smuggling, organ trafficking, arms trafficking, and other forms of crime. Therefore, IOM has jointly worked with the government since 2016 to strengthen border management by improving the capacity for the border agency to record and monitoring inbound and outbound movements, as until then this was done manually on paper-based logbooks. IOM Haiti, starting in 2019, gradually implemented the MIDAS system at the country's land border control posts, as well as at the Toussaint Louverture international airport.

IOM provided logistical support between 2019 and 2022 to install MIDAS at the four border control posts mentioned above. A MIDAS pilot scheme was carried out at the official border control post of Malpasse. The team used a contextualized MIDAS assessment form to examine, among other things: the border post security, travellers processing (daily registrations), energy supply, connectivity, technological tools, and political implications. Additionally, IOM team suggested the installation of solar systems to ensure business continuity of the MIDAS system also when power supply fails.

MIDAS installation and configuration were coordinated with an expert group of IOM MIDAS team, who trained IOM focal points (IT staff and project team) and the DIE IT staff (as well as the Technology and Communication Director). DIE officials in charge of recording the travellers' information received specific training about MIDAS. This process ensured that staff members understood how to use the system and could disseminate their knowledge to other inspectors.

One of the good practices of the IOM team was to ensure on-the-job mentoring period at the point of installation to ensure that the system was properly working and that immigration inspectors were correctly registering travellers. In addition, monitoring, evaluation, and follow-up were carried out to incorporate the improvements into future facilities.

This methodology was replicated on the other three border points where MIDAS is installed. The system installation was carried out gradually. In 2019 the first installation was completed at the Malpasse border post; in 2020, two installations were carried out, one at the Cap Haïtien International Airport and the other at the Juana Méndez border post; in 2021, another installation was completed in Belladère; and by the end of 2022, MIDAS is expected to be installed at the Anse-a-Pitre border post.

MIDAS installation facilitated the Haitian Government to gain a comprehensive view of a person's migratory history rather than managing each record as an isolated case. Among the benefits of implementing the MIDAS in Haiti, as well as in other countries, we have a more effective border management, more accurate capture of relevant information, a better allocation and use of human and financial resources, resulting in alleviated workload at borders and greater efficiency in migration management.

6.2

USE CASE 2: e-RCMS

The electronic Readmission Case Management System (e-RCMS) is a digital platform that supports rights-based readmission cooperation by allowing two or more governments to securely exchange returnee data on a reciprocal basis, thereby supporting the identity verification or travel document issuance processes required for State-led returns and readmissions. As it uses a standardized, IOM-owned IT architecture and deployment model, the system has the potential to connect governments across regions and continents, while ensuring that each hosting Member State retains full ownership of its own e-RCMS.

The e-RCMS draws on a decade of IOM experience in supporting the development of similar systems at the national level, including in Bangladesh, Georgia, Pakistan and Sri Lanka. It comes with the unique added value of the Organization's thorough knowledge of returns, in addition to its nearly global membership and deep commitment to serving migrants.

Throughout 2022, countries in the European Union, the South Caucasus, the Western Balkans, the Middle East, Central and South Asia, and Africa have engaged with IOM on awareness-raising and targeted preparations for tailored e-RCMS deployment in future. The first places to receive their respective e-RCMS segments will be Azerbaijan and the European Union, whose Member States will benefit from this connection to Azerbaijan in 2023. In Communication C(2020) 2516 on the implementation of relevant European Union provisions in the area of asylum and return procedures on resettlement during the COVID-19 pandemic, the European Commission stressed the importance of using electronic tools to maintain communication and cooperation channels open with third countries' consular authorities in order to advance on individual cases in the return and readmission, at a time when the COVID-19 restrictive measures make the procedures of physical identification a re-documentation more difficult due to lack of human resources.

IOM developed the e-RCMS, to facilitate the return and readmission process as defined in applicable readmission cooperation frameworks. The e-RCMS facilitates the exchange of information necessary for identity verification which includes returnee personal data, identity documents, and biometric data, as well as the exchange of information relevant to transfer, such as flight details. Moreover, the system also allows for direct, real-time communication between competent authorities concerning readmission applications. With all workflows being performed digitally, using the e-RCMS significantly reduces delays in manual case processing, improves the quality of applications submitted, and facilitates higher levels of data protection and information security, ensuring only competent government authorities have access to returnee data with the system.

▶ E-RCMS AND BIOMETRICS

The data processed through the e-RCMS is not limited to any specific type of biometrics. The biometrics to be used are decided by each country and then the e-RCMS is configured accordingly. As of now, facial images and fingerprints are in use. IRIS might be requested in future implementation. The e-RCMS platform can also include voice recognition if this is necessary. The purpose of using biometrics in e-RCMS is to simplify the identity verification of a returnee. Biometrics are usually captured outside of e-RCMS and then uploaded in the system. Integration with capturing devices might be requested for some implementations to avoid manual errors. The biometrics are attached to a return case and sent to the relevant authority for verification. The e-RCMS has a configurable workflow where each agency can decide to have a partly manual process or a fully digital process, where e-RCMS would perform an online check with the biometrics database(s).





The use of biometrics in e-RCMS is based on existing cooperation frameworks between States, for example, readmission agreements and standard operating procedures. The requirements stipulated in the agreement are configured in the e-RCMS to be available for specific country-to-country communication. The e-RCMS helps both countries to handle biometrics by its configured functionality, only as intended. The configuration will define aspects such as types of biometrics, retention times, and permissions to view, add, change, and delete biometrics, in line with applicable international, regional, and national data protection standards. The basic principles are that each country owns and is responsible for its data. Each country is recommended to assess if the security measures and functionalities of the system meet its requirements.

E-RCMS CASE STUDY: AZERBAIJAN

IOM has been implementing the EU-funded European Readmission Capacity Building Facility since 2016 (EURCAP) to contribute to effective and efficient cooperation in migration governance between the European Union and its partner country through capacity-building initiatives. The e-RCMS was piloted under the programme between Azerbaijan and 6 European Union Member States to implement the readmission process as defined in the European Union-Azerbaijan readmission agreement. Along with the readmission application fingerprints and facial image are attached. Copies of other means of evidence could also be attached when present such as passports or national id-cards, in line with the accepted means of evidence defined in the European Union-Azerbaijan readmission agreement. This evidence, together with biometrics, will be used by the authorities in the country of origin to verify the identity and, depending on the outcome, approve or reject the readmission application.

Legacy systems implemented in Bangladesh, Georgia, Pakistan and Sri Lanka, apply the same principles, tailored to the requirements of their respective readmission cooperation frameworks.

Table 2. IOM projects with biometrics components (past and ongoing)

MISSION	PROJECT TITLE	BRIEF SCOPE
 Bahrain	The Arab Centre for Technical Cooperation on Migration and Border Management	<p>IOM experts will lead the design, development and delivery of a 6-month seminar on Legal Identity, geared towards equipping NAUSS students with knowledge of systems and processes to operationalize legal identity of individuals.</p> <p>Emphasis will be put on migrant populations, with particular attention given to improving mechanisms for accessing documentary proof of legal identity, verification of presented documentary proofs and how these processes could be improved by national institutions.</p> <p>A combination of academic excellence with practical case-studies, this 6-month programme will provide the tools, skills and vision to advance students' careers by providing the opportunity to work with and learn from a range of highly experienced field professionals, governmental representatives and private sector, while cementing a multidisciplinary approach to Legal Identity</p> <p>Core semester topics include:</p> <ul style="list-style-type: none"> • IOM's Legal Identity Agenda • Supporting national identity management systems • Civil registration and ID/travel documents issuance services • Assisting migrants and displaced populations without proof of legal identity • Identity Management and Biometrics
 Chad	(MEFM) Emergency Shelter assistance for households displaced by flooding in N'Djamena and Lac provinces of Chad	<p>The proposed project has the objective of improving humanitarian support for the most vulnerable IDPs, returnees and migrants in N'Djamena and Lac province through two overarching outcomes, falling in line with Chad's 2021 and ongoing 2022 Humanitarian Needs Overview and Humanitarian Response Plan as well as the Humanitarian Country Team-designed biometric registration strategy.</p>
 Chad	Humanitarian assistance to displaced population in Lac province, Chad	<p>To provide lifesaving assistance in the Lac province, IOM suggests the implementation of a two-fold response:</p> <ol style="list-style-type: none"> 1. Enhancement of displacement data management to support decision-making, planification and direct assistance, through the Displacement Tracking Matrix (DTM)'s Mobility tracking and continuation of the implementation of rapid biometric registration. 2. Shelters and Non-Food Items procurement and distribution for most vulnerable displaced people.
 IOM Headquarters	Supporting the visa application processing of former national staff of "German Organizations in Afghanistan" or "Operation of Visa Acceptance Office"	<p>The objective of the project is supporting the German Federal Foreign Office to facilitate the visa processing of former GOIA national employees and other vulnerable Afghans. Visa facilitation, in this context, is implemented as form of protection for the targeted beneficiaries. The project will include the daily activities related to the administrative tasks of visa application, these including information dissemination, identity verification, document completeness checks, filling of the VIDEX visa application form online, case management, biometrics enrolment, and visa application, biometrics data and document logistics.</p>

 IOM Headquarters	Data and Displacement: Assessing the Practical and Ethical Implications of Targeting Humanitarian Protection	<p>This project contributes to a new understanding of the ways that contemporary humanitarian risk is generated, resolved and/or perpetuated in situations of conflict and development, specifically by assessing protection interventions that are grounded in the use of largescale quantitative, biometric and visual data with IDPs. By juxtaposing data sources with an overview of coordination mechanisms and operational activities across each site, the resonance between complex data and humanitarian assistance will be assessed and highlight problems of interference that impact the transposition of data into practice.</p>
 Mali	Strengthening the evidence base around population displacement in Mali	<p>This project is implementing a novel biometric registration system to identify beneficiaries and provide a new comprehensive baseline on population movements, identifying the urgent needs of internally displaced persons (IDPs) as well as returnees and repatriated individuals, finding durable solutions to forced displacement through identification of pockets of stability, and strengthening the data capacities of government agencies in order to inform optimal and targeted interventions by humanitarian and State actors in Mali.</p>
 Mexico	Strengthening the Capacities of the Government of Mexico for a Safe, Orderly and Humane Border Management	<p>Provide support to the Government of Mexico's ability to effectively implement integrated immigration and border management (IBM) processes such as humanitarian border management to counter migrant smuggling, border security, travellers' identification, biometric data collection, screening and referral, etc.</p>
 Nigeria	Enhancing Land Border Management Information Systems in Nigeria-Seme Border	<p>To support the Federal Government of Nigeria in its efforts to process the identities of individuals upon entry or exiting the country as well as foreigner registration and regularization; manage migration, and build the requisite migration in the country, IOM launched the MIDAS initiative which can be deployed in States. The system is based on an automated acquisition of standardized and interoperable data set that comprises individuals' biometrical and biographical information, some basic travel document info (white light, ultraviolet and IR passport images), as well as additional relevant data.</p>
 Nigeria	Enhanced displacement and mobility tracking and multi-sectoral support for displaced populations in Nigeria	<p>The overall objective of this action is to reinforce protection and resilience of displaced and conflict affected populations in Nigeria while providing an overall picture of the movements and evolving needs of displaced populations. IOM will continue providing information packages through IOM's Displacement Tracking Matrix (DTM); continue conducting biometric registration of beneficiaries and verification of biometric data; continue conducting DTM assessments in the North West / North Central regions and producing flash reports in response to displacements.</p>
 Nigeria	Enhancing the understanding of displacement and human mobility flows in conflict-affected states of north-east Nigeria	<p>Through the Displacement Tracking Matrix (DTM), IOM will provide quarterly Mobility Tracking reports from the three conflict-affected states (Borno Adamawa, and Yobe) in Nigeria's North-east Geopolitical Zone. As a result of the fluid displacement situation, the Emergency Tracking Tool (ETT)/Point of entry (POE) will be implemented in Adamawa, Borno and Yobe when necessary to complement the Mobility Tracking. Additionally, in several preselected camps and camp-like settings, DTM will set up Biometric Registration assessments to assist partners (WFP) with verification exercises and support other organizations with distributions.</p>



Philippines

Capacity-building support to the Government of Philippines for improved emergency preparedness and response

Providing provide technical assistance for the Government Departments to develop a Biometric information management system that can support the preparedness, response and monitoring based on IOM's Biometric Registration and Verification System (BRaVe). The system can serve as basis for the vulnerability profiling and shelter damage reporting system.



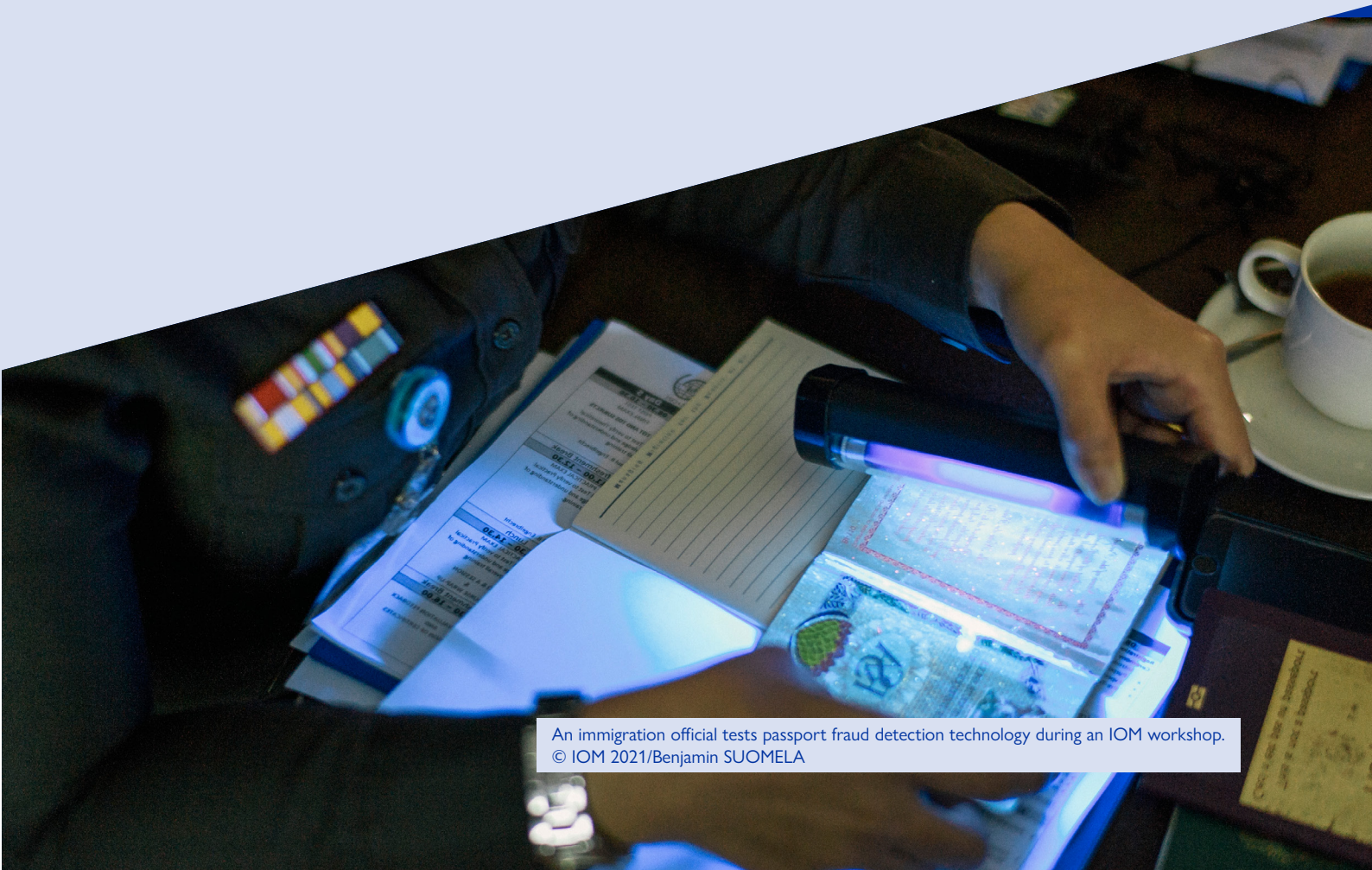
South Sudan

Data collection for evidence-based response and provision of CCCM services to address the needs of populations displaced by the Tonga crisis

IOM will implement IOM Displacement Tracking Matrix (DTM) to scale up data collection by utilizing the existing network of enumerators and key informants to provide partners with up-to-date, actionable, and verified information on population movement, displacement as part of the early warning system in the context of ongoing insecurities and tensions. IOM DTM will undertake a comprehensive biometric registration maintenance activity within the Protection of Civilians (sites) to establish reliable population estimates within the camp and hence support response planning.

PART 7

TECHNOLOGY LOOKING AHEAD



An immigration official tests passport fraud detection technology during an IOM workshop.
© IOM 2021/Benjamin SUOMELA

“Border and immigration enforcement, too, has been subject to rapid digitization, a phenomenon that has only escalated in response to the COVID-19 pandemic. Our age is unquestionably the age of the rise of what other scholars have termed “digital borders”³³ – borders whose infrastructure increasingly relies upon machine learning, big data, automated algorithmic decision-making systems, predictive analytics, and related digital technologies. These technologies form part of identification documents and systems, facial recognition systems, ground sensors, aerial video surveillance drones, biometric databases, and in some places, even part of visa and asylum decision-making processes.”³⁴

Various trends are anticipated in the field of Biometrics-based identity management. While each usage scenario will have its own priorities, the following aspects are a summary of the main priorities in the near future.

These are touchless biometrics, making use of mobile devices for enrolling, combating fraud related to presentation attacks and deep fakes, improving liveness checks, enhancing the datasets used for training the systems, enhancing policies, and improving systems performance by use of artificial intelligence.

7.1 TOUCHLESS

During the COVID-19 pandemic, touchless recognition technologies received much attention, favouring the established face recognition in the travel continuum, and being seconded by touchless fingerprint capturing. For touchless fingerprint capturing, instead of placing the hand on a reader, an individual holds or waves their hand across a sensor. This can be beneficial for non-cross-border use cases and in cases where the use of specialized equipment is not practical. Recall that the interoperability between devices in terms of comparison accuracy is not as good as contact scanners.

7.2 SELF-SERVICE CAPABILITIES FOR USERS



The use of mobile devices for performing Know-Your-Customer (KYC) procedures known in the financial industry, or for device access procedures are continuing to become a popular model. We expect to see major progress in the field of enrolling identities for using mobile devices for different use-cases.

The performance of feature phones for enrolment continues to improve. The key challenges remaining to be solved are related to usability, impact from the environment on the recording quality, the broad variety of hardware and software environments creating data sets of diverse qualitative nature.

7.3 PRESENTATION ATTACK / DEEP FAKE / LIVENESS

With recent advances in artificial intelligence (AI) and computer vision, biometric systems have become dramatically more accurate, faster, and more resilient to environmental and user variables. However, even biometric systems can be attacked and bypassed without the right technology in place. The process of a biometric system detecting a biometric spoof is known as Presentation Attack Detection (PAD). PAD systems utilize a combination of

³³ Broeders, D., *The New Digital Borders of Europe: EU Databases and the Surveillance of Irregular Migrants*, 22 INT'L SOC. 71 (2007).

³⁴ Tendayi Achiume, E., (2021). *Digital Racial Borders*. Published by Cambridge University Press on behalf of The American Society of International Law.

hardware and software technologies to determine whether or not a presented biometric is genuine. A subset of this is liveness detection, which refers to a PAD system's specific ability to differentiate between human beings and non-living spoofs.

While the anti-spoofing landscape is much better than previous years, adversaries will likely increase the frequency and complexity of presentation attacks. Investments need to be made to improve our abilities to mitigate these attacks and detect and counter them faster and with greater confidence.

It is expected that there will be further advances in this field, not only in responding to known attacks, but to take an active role in fraud prevention. Liveness detection will be receiving growing attention in the systems, as systems could become decentralized and effective liveness detection will become a pre-requisite for enrolment taking place on private devices like mobile phones.

7.4 TESTING AND DATASET IMPROVEMENTS

Continued standards development and expanded testing are underway. While, on one hand, the performance criteria and attack detection need constant work, there is, on the other hand, a widely acknowledged need for improved testing datasets. Testing institutes such as NIST, as well as Governments, such as the UK Homeland Security, have been investing in developing and providing datasets for performance tests. The identified bias towards male Caucasians is being addressed, such that the datasets continue to become more representative to the expected community intended to use the systems.

7.5 POLICIES

A Biometrics Institute analysis states: "As digital identity capabilities mature and expand across government and private organizations, there will be new options in how policies and governance are planned and implemented as we advance interoperability and achieve improved responses. A centralized approach offers a strong central governance structure along with its associated protocols and standards. A de-centralized approach relies heavily on point-to-point agreements across independent, interdependent organizations. Hybrid organizations implement portions of centralized and de-centralized concepts. Further analyses, research and development in this area should prove helpful to capability progression."³⁵

Within the policies, there has to be a balance between privacy requirements and ethical use of Biometrics on the one side, and on the other side, not blocking innovation and system enhancement. Further evolution of risk management frameworks for access to biometric data are to be expected, also in order to support an improvement of data sharing across systems.

7.6 ARTIFICIAL INTELLIGENCE

The use of artificial intelligence methods applied in Biometrics will continue to grow. Main benefits are:

- a. in the reduction of False Acceptance Rates / False Rejection Rates;
- b. in the detection of various attack vectors, including deep fake, image/video injection and various other forms of Presentation Attacks;
- c. in the speed.

³⁵ Biometrics Institute, *State of Biometrics Report 2021*, Chapter 5.



Artificial intelligence helps spot attack vectors like deep fakes, image/video injection, and other Presentation Attacks. © 2020/Arif RIYANTO

7.7 EVOLVING INDUSTRY

The number of market entrants will continue to grow over the next few years for as long as barriers to entry remain low, opportunities remain untapped, and no single vendor, or limited group of vendors, dominates the marketplace. At the same time, a considerable number of brands have disappeared from the market, being absorbed by other companies, or having folded down.

This makes the selection of technologies, products and suppliers a challenging process. It is to be anticipated, that this consolidation especially in the field of facial and fingerprint biometrics will continue over the next years.



A Venezuelan migrant undertaking biometric migratory registry with the Ministry of Interior. ©IOM 2023/Gema CORTÉS

CONCLUSION

There is no doubt that biometric technology will continue to exist and will play an ever-increasing role in how populations, administration and migration are managed. The industry carries significant risk and ethical questions, which must be taken seriously and examined closely from multiple perspectives, especially those of intersectionality; minorities, marginalized groups, and populations who already experience discrimination.

Biometrics have the potential to revolutionize how our systems function and in theory, improve data security, identity management and access for all. The potential to improve even protective measures is evident, though this can only be implemented with parallel and even greater caution towards data breaches, abuse of power, the right to privacy, and freedom from discrimination. It is up to each organization to carefully weigh the risks and ensure that biometric interventions adequately address all ethical questions; implement adequate safeguards, and can stand up to scrutiny at any point. The ability to adapt to new threats and adjust approaches – both in advance of potential rights violations as well as in response to them – will be the key to implementing ethically sound and effective biometric programming.



Legal Identity Sensitization during Community Safety Council Session Quilawa, Cabo Delgado, November 2023. ©IOM 2023

TECHNICAL TERMINOLOGY

Authentication	ISO 24760-1 defines authentication as a formalized process of authentication that, if successful, results in an authenticated identity for an entity . Authentication typically involves the use of a policy to specify a required level of assurance for the result of a successful completion. Identification is usually done as authentication to obtain a specific level of assurance in the result.
Credential or access	The intended license, privilege, or status granted as a result of approved checks. It remains valid until the credential/access expires and/or is revoked.
Enrolment	Collection of biographic and biometric information through in-person and virtual platforms, where applicable.
iAPI	The Interactive Advance Passenger Information (iAPI) provides opportunities for governments to communicate an instant response to carriers based on vetting results. This information helps airlines determine whether or not passengers have the appropriate travel document and requirements in order to enter the country of destination (i.e. Visa). www.icao.int/Security/FAL/SitePages/API%20Guidelines%20and%20PNR%20Reporting%20Standards.aspx .
Identity proofing	Validation of provided biographic and biometric information in accordance with TSA's standards (derived from NIST 800-63A) by confirming that provided information matches with a trusted source.
Identity management	The holistic process of enabling the right person to have the right access or credential based on their biographic and biometric information.
Identity verification	Matching a person's physical or digital identification/Biometrics against vetted information to verify a person's identity at credential or access use (e.g. access to secure area, differentiated level of physical screening).
Industry	Including but not limited to Air Carriers, Air-Carrier Representation, All-Cargo Air Transportation, Labor Organizations Representing Air Carrier Employees and TSOs, Airport Operations.
Issuance / credentialing	Entire process (from application through issuance, use, and expiration or potential revocation of the issued credential) of determining a person's suitability for a particular credential, access, or status and assigning a token that enables use of the credential, access, or status.
Population	A managed group of individuals applying for similar credentials or access within the transportation security enterprise.
Provisioning	Assigning a token that enables use of the credential, access, or status.
Reservation	Collection of biographic information, or biometric information where applicable, from passengers at the time of booking travel.
Vetting	Acquiring the appropriate data and running the appropriate checks to determine if the credential or access can be granted.
Verification	For the guide, the term "Verification" is used interchangeably with "Authentication". ISO 24760-1 defines Verification: process to determine that presented identity information associated with a particular entity is applicable for the entity to be recognized in a particular domain at some point in time.



17 route des Morillons, P.O. Box 17, 1211 Geneva 19, Switzerland
Tel.: +41 22 717 9111 • Fax: +41 22 798 6150
Email: hq@iom.int • Website: www.iom.int