TECHNICAL REPORT

ISO/IEC TR 24741

Second edition
2018-02

Information technology — Biometrics — Overview and application

Technologies de l'information — Biométrie — Aperçu général et applications

Reference number
ISO/IEC TR 24741:2018(E)

© ISO/IEC 2018



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2018, Published in Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

Contents

Page

Foreword ..... **v**

Introduction ..... **vi**

1 Scope **1**

2 Normative references **1**

3 Terms and definitions **1**

4 Introduction and fundamental concepts **1**
4.1 What are biometric technologies? 1
4.2 What biometric systems do 2

5 History **4**

6 Overview of biometric technologies **5**
6.1 Eye technologies 5
6.1.1 Iris recognition 5
6.1.2 Retina recognition 5
6.2 Face technologies 6
6.3 Finger and palm ridge technologies 6
6.3.1 Fingerprint imaging 6
6.3.2 Fingerprint comparison 7
6.3.3 Palm technologies 8
6.4 Hand geometry technologies 8
6.5 Dynamic signature technologies 8
6.6 Speaker recognition technologies 9
6.7 Vascular patterns 9
6.8 Keystroke dynamics 9
6.9 Scent/Odour 9
6.10 DNA 9
6.11 Cardiogram 10
6.12 Gait and full body recognition 10

7 Example applications **10**
7.1 Physical access control 10
7.2 Logical access control 10
7.3 Time and attendance 10
7.4 Accountability 11
7.5 Electronic authorizations 11
7.6 Government/citizen services 11
7.7 Border protection 11
7.7.1 ePassports and machine-readable travel documents 11
7.7.2 Automated border crossing (ABC) systems 11
7.7.3 Visas 12
7.7.4 EURODAC 12
7.8 Law enforcement 12
7.9 Civil background checks 12
7.10 Clustering 12

8 General biometric system **13**
8.1 Conceptual representation of general biometric system 13
8.2 Conceptual components of a general biometric system 13
8.2.1 Data capture subsystem 13
8.2.2 Transmission subsystem 14
8.2.3 Signal processing subsystem 14
8.2.4 Data storage subsystem 14
8.2.5 Comparison subsystem 14
8.2.6 Decision subsystem 14

© ISO/IEC 2018 – All rights reserved

8.2.7 Administration subsystem 15
8.2.8 Interface 15
8.3 Functions of general biometric system 15
8.3.1 Enrolment 15
8.3.2 Verification of a positive biometric claim 16
8.3.3 Identification 17

9 Performance testing 17
9.1 General 17
9.2 Types of technical tests 18

10 Biometric technical interfaces 19
10.1 BDBs and BIRs 19
10.2 Service architectures 20
10.3 Common Biometric Exchange Formats Framework (CBEFF) 20
10.4 The BioAPI International Standard 21
10.5 The BIP International Standard 21

11 Biometrics and information security 22
11.1 General 22
11.2 Security of biometric data 22
11.3 Presentation attacks (Spoofing) 25
11.4 Integrity of the enrolment process 25

12 Biometrics and privacy 26
12.1 General 26
12.2 Proportional application of biometrics 27
12.3 Biometric technology acceptability 28
12.4 Confidentiality of biometric data 28
12.5 Integrity of biometric data 28
12.6 Irreversibility of biometric data 29
12.7 Unlinkability of biometric information 29

Bibliography 30

 © ISO/IEC 2018 – All rights reserved

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see the following URL: www.iso.org/iso/foreword.html.

This document was prepared by ISO/IEC JTC 1, *Information technology*, SC 37, *Biometrics*.

This second edition cancels and replaces the first edition (ISO/IEC TR 24741:2007), which has been technically revised with the following changes:

— terminology is revised to align with that of ISO/IEC 2382-37;

— clauses on “Overview of biometric technologies” and “Example applications” have been updated to reflect state of art;

— clauses on “Biometrics and information security” and “Biometrics and privacy” have been considerably expanded.

© ISO/IEC 2018 – All rights reserved

Introduction

"Biometric recognition" is the automated recognition of individuals based on their biological and behavioural characteristics. The field is a subset of the broader field of human identification science. Example technologies include, among others: fingerprinting, face recognition, hand geometry, speaker recognition and iris recognition.

Some techniques (such as iris recognition) are more biologically-based, some (such as signature recognition) more behaviourally based, but all techniques are influenced by both behavioural and biological elements. There are no purely "behavioural" or "biological" biometric systems.

"Biometric recognition" is frequently referred to as simply "biometrics", although this latter word has historically been associated with the statistical analysis of general biological data. The word "biometrics", like "genetics", is usually treated as singular. It first appeared in the vocabulary of physical and information security around 1980 as a substitute for the earlier descriptor, "automatic personal identification", in use in the 1970s. Biometric systems recognize "persons" by recognizing "bodies". The distinction between person and body is subtle, but is of key importance in understanding the inherent capabilities and limitations of these technologies. In our context, biometrics deals with computer recognition of patterns created by human behaviours and biological structures and is usually associated more with the field of computer engineering and statistical pattern analysis than with the behavioural or biological sciences.

Today, biometrics is being used to recognize individuals in a wide variety of contexts, such as computer and physical access control, law enforcement, voting, border crossing, social benefit programs and driver licensing.

© ISO/IEC 2018 – All rights reserved

Information technology — Biometrics — Overview and application

1 Scope

This document describes the history of biometrics and what biometrics does, the various biometric technologies in general use today (for example, fingerprint recognition and face recognition) and the architecture of the systems and the system processes that allow automated recognition using those technologies. It also provides information about the application of biometrics in various business domains such as border management, law enforcement and driver licensing, the societal and jurisdiction considerations that are typically taken into account in biometric systems, and the international standards that underpin their use.

2 Normative references

There are no normative references in this document.

3 Terms and definitions

No terms and definitions are listed in this document.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— IEC Electropedia: available at http://www.electropedia.org/

— ISO Online browsing platform: available at http://www.iso.org/obp

4 Introduction and fundamental concepts

4.1 What are biometric technologies?

The definition of biometrics in ISO/IEC 2382-37[27] is “automated recognition of individuals based on their biological and behavioural characteristics”.

NOTE 1 The all-encompassing term “biometrics” refers to “the application to biology of the modern methods of statistics”. In the context of this document, we are concerned with automated technologies that analyse human characteristics for recognition purposes; the general application of statistics to biological systems is a separate discipline.

The term “biometric characteristic” is defined as “biological and behavioural characteristic of an individual from which distinguishing, repeatable biometric features can be extracted for the purpose of biometric recognition”. So, biometric technologies are related to physical parts of the human body or the behavioural traits of human beings, and the recognition of individuals based on either or both of those parts or traits. A fuller explanation of the various biometric technologies is given in Clause 6.

NOTE 2 ISO/IEC 2382-37 recommends the use of the term “biometric” only as an adjective and deprecates its use as a noun in places where the fuller term biometric characteristic (as above) would be more appropriate.

The perfect biometric characteristic for all applications would be:

— *Distinctive*: different across all subjects;

— *Repeatable*: similar across time for each subject, over a long time period (several years);

© ISO/IEC 2018 – All rights reserved