BS ISO/IEC 24741:2024

BSI Standards Publication

Information technology — Biometrics — Overview and application

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 24741:2024

National foreword

This British Standard is the UK implementation of ISO/IEC 24741:2024. It supersedes PD ISO/IEC TR 24741:2018, which is withdrawn.

The UK participation in its preparation was entrusted to Technical Committee IST/44/-/4, Technical Implementation of Biometric Systems.

A list of organizations represented on this committee can be obtained on request to its committee manager.

Contractual and legal considerations

This publication has been prepared in good faith, however no representation, warranty, assurance or undertaking (express or implied) is or will be made, and no responsibility or liability is or will be accepted by BSI in relation to the adequacy, accuracy, completeness or reasonableness of this publication. All and any such responsibility and liability is expressly disclaimed to the full extent permitted by the law.

This publication is provided as is, and is to be used at the recipient's own risk.

The recipient is advised to consider seeking professional guidance with respect to its use of this publication.

This publication is not intended to constitute a contract. Users are responsible for its correct application.

© The British Standards Institution 2024
Published by BSI Standards Limited 2024

ISBN 978 0 539 13881 8

ICS 35.240.15

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 30 June 2024.

Amendments/corrigenda issued since publication

Date	Text affected

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 24741:2024

International Standard

ISO/IEC 24741

Third edition
2024-06

Information technology — Biometrics — Overview and application

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

Reference number
ISO/IEC 24741:2024(en)

© ISO/IEC 2024

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 24741:2024

COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2024

All rights reserved. Unless otherwise specified, or required in the context of its implementation, 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
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 24741:2024

Contents

Page

Foreword ... **v**
Introduction ... **vi**
1 Scope ... **1**
2 Normative references ... **1**
3 Terms,definitions and abbreviated terms ... **1**
3.1 Terms and definitions ... 1
3.2 Abbreviated terms ... 1
4 Fundamentals of biometrics ... **2**
4.1 Biometric characteristics ... 2
4.2 Biometric systems ... 3
5 History ... **5**
6 Overview of biometric technologies ... **6**
6.1 Finger and palm ridge recognition ... 6
6.1.1 Fingerprint imaging ... 6
6.1.2 Fingerprint comparison ... 7
6.1.3 Palm technologies ... 8
6.2 Face recognition ... 8
6.3 Iris recognition ... 9
6.4 Dynamic signature recognition ... 9
6.5 Vascular recognition ... 10
6.6 Hand geometry recognition ... 10
6.7 Voice recognition ... 10
6.8 DNA recognition ... 11
6.9 Full body recognition ... 11
6.10 Gait recognition ... 11
6.11 Retina recognition ... 11
6.12 Keystroke recognition ... 12
6.13 Scent and odour recognition ... 12
6.14 Cardiogram recognition ... 12
6.15 Multimodal biometrics ... 12
7 General biometric system ... **12**
7.1 Conceptual representation of general biometric system ... 12
7.2 Conceptual components of a general biometric system ... 13
7.2.1 Data capture ... 13
7.2.2 Transmission ... 13
7.2.3 Signal processing ... 13
7.2.4 Data storage ... 14
7.2.5 Comparison ... 14
7.2.6 Decision ... 14
7.2.7 Administration ... 15
7.2.8 Interface to external application ... 15
7.3 Functions of general biometric system ... 15
7.3.1 Enrolment ... 15
7.3.2 Verification of a positive biometric claim ... 16
7.3.3 Identification ... 17
8 Example applications ... **17**
8.1 General ... 17
8.2 Physical access control ... 17
8.3 Logical access control ... 18
8.4 Time and attendance ... 18
8.5 Accountability ... 18
8.6 Electronic authorizations ... 18

© ISO/IEC 2024 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 24741:2024

8.7 Government and citizen services 18
8.8 Border protection 19
8.8.1 ePassports and machine-readable travel documents 19
8.8.2 Automated border control (ABC) systems 19
8.8.3 Entry/exit systems 19
8.8.4 Visas 19
8.8.5 EURODAC 20
8.9 Law enforcement 20
8.10 Civil background checks 20
8.11 Clustering 20

9 Performance testing 20
9.1 General 20
9.2 Types of technical tests 21

10 Biometric technical interfaces 22
10.1 Biometric data blocks (BDBs) and biometric information record (BIRs) 22
10.2 Management of information on source of biometric data 23
10.3 Service architectures 23
10.4 The BioAPI application programming interface 24
10.5 The BioAPI interworking protocol (BIP) 24

11 Biometrics and information security 25
11.1 General 25
11.2 Security of biometric data 25
11.3 Presentation attack (spoofing) detection 28
11.4 Integrity of the enrolment process 28

12 Biometrics and privacy 29
12.1 General 29
12.2 Privacy protections for biometric applications 30
12.3 Proportional application of biometrics 30
12.4 Biometric technology acceptability 31
12.5 Confidentiality of biometric data 31
12.6 Integrity of biometric data 31
12.7 Irreversibility of biometric data 32
12.8 Unlinkability of biometric information 32

13 Overview of biometric standardisation 32
13.1 Standards development organizations 32
13.2 Types of biometric standards 33
13.2.1 Biometric data interchange format standards 33
13.2.2 Biometric technical interface standards 34
13.2.3 Biometric conformance testing standards 34
13.2.4 Biometric sample quality standards 35
13.2.5 Biometric application profile standards 35
13.2.6 Biometric performance testing and reporting standards 36
13.2.7 Biometric security standards 37
13.2.8 Biometric authentication standards 37
13.2.9 Standards on cross-jurisdictional and societal aspects of biometrics 38
13.2.10 Biometric vocabulary standards 39
13.3 Criteria for selecting a standard 39

Bibliography 41

© ISO/IEC 2024 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 24741:2024

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.

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 or www.iec.ch/members_experts/refdocs).

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents and https://patents.iec.ch. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

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

For an explanation of 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 www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

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

This third edition cancels and replaces the second edition (ISO/IEC TR 24741:2018), which has been technically revised.

The main change is as follows:

— Guidance is given on the international standards that underpin the use of biometric recognition systems.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

© ISO/IEC 2024 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 24741:2024

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: fingerprint recognition, face recognition, hand geometry recognition, speaker recognition and iris recognition.

Some techniques (such as iris recognition) are more biologically based, whereas some (such as signature recognition) are 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 the term "biometrics" has also 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. Within the context of JTC 1/SC 37 documents, biometrics deals with computer-based 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 used to recognize individuals in a wide variety of contexts, such as computer and physical access control, law enforcement, voting, border control, social benefit programs and driver licencing.

© ISO/IEC 2024 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 24741:2024

Information technology — Biometrics — Overview and application

1 Scope

This document describes the history and purpose of biometrics, the various biometric technologies in general use today (for example, fingerprint recognition, face recognition and iris recognition) and the architecture of the systems and the system processes that allow automated recognition using those technologies. It provides information on the application of biometrics in various business domains, such as border management, law enforcement and driver licencing. It also provides information on the societal and jurisdictional considerations that are typically taken into account in biometric systems.

Additionally, this document provides guidance on the use of the International Standards that underpin the use of biometric recognition systems.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 2382-37, *Information technology — Vocabulary — Part 37: Biometrics*

3 Terms,definitions and abbreviated terms

3.1 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 2382-37 apply.

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

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

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

3.2 Abbreviated terms

For the purposes of this document, the following abbreviated terms apply.

ABC	automated border control
API	application programming interface
AFIS	automated fingerprint identification system
ABIS	automated biometric identification system
BDB	biometric data block
BIAS	biometric identity assurance services
BIR	biometric information record

© ISO/IEC 2024 – All rights reserved

Documents Document Sharing Hub
Full document details: BS ISO/IEC 24741:2024

BIP	Biometric Interworking Protocol
CBEFF	Common Biometric Exchange Formats Framework
CNN	convolutional neural network
DET	detection error trade-off
DSV	dynamic signature verification
DNA	deoxyribonucleic acid
EU	European Union
FBI	Federal Bureau of Investigation
ICAO	International Civil Aviation Organization
IR	infrared
MAC	message authentication code
MRTD	machine-readable travel document
PET	privacy enhancing technology
PCA	principal component analysis
PIN	personal identification number
RBR	renewable biometric reference
SB	security block
SBH	standard biometric header
SOA	service-oriented architecture
WSDL	Web Service Description Language

4 Fundamentals of biometrics

4.1 Biometric characteristics

ISO/IEC 2382-37:2022 37.01.03 defines "biometrics" as an "automated recognition of individuals based on their biological and behavioural characteristics".

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

ISO/IEC 2382-37:2022 37.01.02 defines "biometric characteristic" as a "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 "biometric characteristic" is more appropriate.

© ISO/IEC 2024 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 24741:2024

The ideal biometric characteristic for all applications would have the following properties:

— Distinctive: Different across all subjects.

— Repeatable: Similar across time for each subject, over a long time period (several years).

— Accessible: Easily presented to a capture device (for example, camera or fingerprint capture device or finger-geometry measurement device).

— Universal: Observable on all people.

— Acceptable: The subject is prepared to use the biometric characteristic in the given application.

Unfortunately, no biometric characteristic has all of the above properties and practical biometric technologies inevitably compromise on every point.

— There are great similarities among different individuals.

— Biometric characteristics change over time.

— Some physical limitations prevent presentation.

— Not all people have all characteristics.

— "Acceptability" is subjective.

Consequently, the challenge of biometric deployment is to develop robust systems to deal with the vagaries and variations of human beings.

4.2 Biometric systems

It has been recognized since 1970[28] that there are three pillars of automated personal recognition for access control applications:

a) something known or memorized;

b) something carried;

c) a personal physical or behavioural characteristic.

The underlying assumptions are that individuals authorized to access secure data will cooperatively make positive claims (e.g. "I am authorized to access data on the system") and can be counted on to protect their personal identification numbers (PINs) and passwords. In such applications, biometric technologies compete with PINs, passwords and tokens. For example, most web-based access control requires a user ID and an associated password, not biometrics. Passwords have been more widespread than biometrics in such applications because they are easily replaced, can vary across applications, require no specialized acquisition hardware, can be created with different levels of security and are exactly repeatable under conscious control.

However, in many applications, PINs, passwords and tokens cannot meet the security requirements. For example, PINs, passwords and tokens cannot logically be used in applications where enrolled individuals have little motivation to protect their accounts against use by others, such as with amusement parks. Similarly, in applications where the claim is negative (e.g. "I am not enrolled in the system as Pat") PINs, passwords and tokens cannot logically meet the requirements of demonstrating the truth of the claim.

Biometric systems recognize individuals by observing physical and behavioural characteristics of their bodies. Biometric characteristics are not as easy to transfer, forget or steal as PINs, passwords and tokens, so they can be used in applications for which these other authentication methods are inappropriate. Biometrics can be combined with PINs and tokens into "multifactor" systems for added security.

Although biometric technologies cannot directly "identify" individuals, they can link bodies to records of attributes, hereinafter referred to as "identities". Consequently, biometric recognition can become part of an identity management system.

© ISO/IEC 2024 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 24741:2024

Biometric recognition is used in two main classes of applications.

1) Biometric verification applications, i.e. applications that use biometric comparison to verify a biometric "claim of identity".

2) Biometric identification applications, i.e. applications that search a database of the biometric references of known individuals to find and return the identifier attributable to a single individual.

Biometric systems can also be used to "cluster" characteristics, labelling together those that come from the same bodily source (i.e. from the same individual and biometric instance) even when the bodily source cannot be attributed to any known individual. Such types of systems are gaining application in law enforcement.

Biometric verification systems verify claims (test hypotheses) regarding the source of a biometric data record in a database. The claim can be made by the individual presenting a biometric sample (e.g. "*I am the source of a biometric data record in the database*") or the claim can be made about the source by another actor in the system (*"She is the source of a biometric data record in the database"*). The claims can be positive (*"I am the source of a biometric record in the database"*) or negative (*"I am not the source of a biometric record in the database"*). Claims can be specific ("*I am the source of biometric record A in the database*") or unspecific (*"I am not the source of any biometric record in the database"*). Any combination of specific or unspecific, positive or negative, first-person or third-person, is possible in a claim.

According to ISO/IEC 2382-37, an individual's biometric data record in a database is referred to as a "biometric reference" and the biometric sample used for comparison with the stored biometric reference is referred to as a "biometric probe". It is possible to either look for a "match" between the biometric probe of an individual and an identified biometric reference stored in the database, or to search a population of biometric references in a database for a match with the supplied biometric probe and return an identifier for any reference that matches. In both cases, it is necessary to set thresholds for how close the similarity has to be before the biometric probe and the biometric reference can be considered to have come from the same bodily source (a "match"). Of course, errors can be made, either by a "false non-match" failing to correctly declare a "match" when the probe and reference are indeed from the same bodily source, or by a "false match" incorrectly declaring a match when the probe and reference are from different bodily sources. The proportion of such errors over the total number of comparisons are referred to as the "false match rate" and the "false non-match rate" for a given technology and a given population in a given application environment.

Systems requiring a positive claim to a specific enrolled reference treat the biometric reference as an attribute of the enrolment record. These systems verify that the biometric reference in the claimed enrolment record matches the probe sample submitted by the subject. Some systems, such as those for social services and driver licencing, verify negative claims of no biometric data record already in the database by treating the biometric reference as a record identifier or pointer. These systems search the database of biometric pointers to find one matching the submitted biometric probe (this process is one of biometric identification). However, the act of finding an identifier (or pointer) in a list of identifiers also verifies an unspecified claim of enrolment in the database, and not finding a pointer verifies a negative claim of enrolment. Consequently, the differentiation between "identification" and "verification" systems is not always clear and these terms are not mutually exclusive.

Usernames, identification numbers, personal smart cards or security tokens are often used to enter specific biometric claims into biometric verification systems.

For example, a subject can claim to be the source of the fingerprint biometric reference stored on an immigration card. To prove the claim, the subject inserts the card into a card reader which reads the reference record, then places their finger on the fingerprint capture device. The system compares the biometric characteristics of the fingerprint on the reader with those of the reference recorded on the card. The system can conclude, in accordance with defined thresholds, that the subject is indeed the source of the reference on the card, and therefore is afforded the rights and privileges associated with the card. This does, of course, assume that the card has not been forged. All that the biometric verification achieves is to determine that the human being has presented biometric characteristics that are a close match to those recorded on the card.

Simple "identification" can require the comparison of the submitted biometric sample with all of the biometric references stored in the database. The state of California requires applicants for social service benefits to verify the negative claim of no previously enrolled identity in the system by submitting

© ISO/IEC 2024 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 24741:2024

fingerprints from both index fingers. Depending upon the specific automated search strategy, these fingerprints can be searched against the entire database of enrolled benefit recipients, or just the part of the database corresponding to subjects of the same sex as the applicant, in order to verify that there are no matching fingerprints already in the system. If matching fingerprints are found, the enrolment record pointed to by those fingerprints is returned to the system administrator to confirm the rejection of the applicant's claim of no previous enrolment.

The number of comparisons to be made, and the prior probabilities that those comparisons will result in a match (determination that biometric probe and reference have the same bodily source) depend upon both the claim and the system architecture. The security risk posed by a wrong determination will also vary by system function. Consequently, some systems are very sensitive to false matches (false positives), while some systems are very sensitive to false non-matches (false negatives) for any comparison. Depending upon the claim, either a false positive or a false negative can result in either a false acceptance or false rejection of the claim.

5 History

Biometric characteristics have been used for centuries in a non-automated way. Parts of our bodies and aspects of our behaviour have historically been used, and continue to be used, as a means of identification. The use of fingerprinting dates back to ancient China, individuals are remembered and identified by their face or by the sound of their voice, and signatures are the established method of authentication in banking, for legal contracts and many other ways of life.

The modern science of recognizing people based on physical measurements owes much to the French police clerk, Alphonse Bertillon, who began his work in the late 1870s.[4] The Bertillon system involved multiple measurements, including: height, weight, the length and width of the head, width of the cheeks, and the lengths of the trunk, feet, ears, forearms, and middle and little fingers. Categorization of iris colour and pattern was also included in the system. By the 1880s, the Bertillon system was in use in France to identify repeat criminal offenders. Use of the system in the United States (US) for the identification of prisoners began shortly thereafter and continued into the 1920s.

Although research on fingerprinting, began in the late 1850s, knowledge of the technique did not become widespread in the western world until the 1880s[16][26] when it was popularized scientifically by Sir Francis Galton[20] and in literature by Mark Twain.[60] Galton's work also included the identification of individuals from profile facial measurements.

By the mid-1920s, fingerprinting had completely replaced the Bertillon system within the U.S. Bureau of Investigation (later to become the Federal Bureau of Investigation). However, research on new methods of human identification continued in the scientific world. Handwriting analysis was recognized by 1929[45] and retinal identification was suggested in 1935.[55] However, at this time, none of these techniques were automated.

Work in automated speaker recognition can be traced directly to experiments with analogue filters done in the 1940s[49] and early 1950s.[13] With the computer revolution picking up speed in the 1960s, speaker[50] and fingerprint[58] pattern recognition were among the very first applications in automated signal processing. By 1963, a wide, diverse market for automated fingerprint recognition was identified, with potential applications in credit systems, industrial and military security systems and for personal locks.[59] Computerized face recognition research followed.[6][21] In the 1970s, the first operational fingerprint and hand geometry recognition systems were fielded, results from formal biometric system tests were reported,[44] measures from multiple biometric devices were combined[39][17] and government testing guidelines were published.[38]

Running parallel to the development of hand recognition technology, fingerprint recognition was making progress in the 1960s and 1970s. During this time, a number of companies were involved in automating the identification of fingerprints to assist law enforcers. The manual process of comparing fingerprints against criminal records was laborious and used up too much manpower. Various fingerprint identification systems developed for the FBI in the 1960s and 1970s increased the level of automation, but these were ultimately based on fingerprint comparisons by trained examiners. Automated fingerprint identification systems (AFIS) were first implemented in the late 1970s, most notably by the Royal Canadian Mounted Police in

© ISO/IEC 2024 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 24741:2024

1977. The role of biometrics in law enforcement has grown exponentially since then and AFIS are used by a significant number of police forces across the globe. Building on this early success, biometric applications are now being explored in a range of civilian markets.

In the 1980s, fingerprint capture devices and speaker recognition systems were connected to personal computers to control access to stored information. Based on a concept patented in the 1980s,[19] iris recognition systems became available in the mid-1990s.[14] Today, there are close to a dozen approaches used in commercially available systems, utilizing hand and finger geometry, iris and fingerprint patterns, face images, voice and signature dynamics, computer keystroke, and hand/finger vein patterns.

Today's speaker verification systems have their roots in technological achievements of the 1960s, while biometric technologies such as iris, finger vein, and face recognition are relative newcomers to the industry. Research in universities and by biometric vendors throughout the globe is essential for refining the performance of existing biometric technologies, while developing new and more diverse techniques. The challenge is bringing a product to market and proving its operational performance. It takes time for any laboratory technology to migrate to a fully operational system. However, such systems are currently in place and are proving effective across a range of diverse applications.

6 Overview of biometric technologies

6.1 Finger and palm ridge recognition

6.1.1 Fingerprint imaging

Historically, fingerprints were collected by placing inked fingers onto collection cards. In the early days of automated fingerprint recognition, those cards were then scanned into a computer. With the advent of technologies that collect fingerprints without the use of ink, these historic methods are considered obsolete. However, there can be occasions when an inked collection is still necessary, e.g. when the capture device is unable to acquire the biometric subject's fingerprint or is unavailable. Very recently, contactless capture devices have been developed that use either laser or standard lighting that do not require the fingers to touch any surface.

Fingerprints derived from finger friction ridges can vary from sample to sample for many reasons. For example, the images captured are determined by the following:

— finger moisture;

— angle of placement;

— pressure;

— ridge damage.

The way in which a subject interacts with a finger capture device has an important effect on the images captured. This includes the height and angle of the fingerprint capture device in relation to the data subject. Vendors are addressing these problems by designing ergonomic capture devices in order to optimize the fingerprinting process.

A key difference between the various contact-based fingerprint technologies on the market is the means of capturing an image. Most large-scale systems capture finger images using optical technique or by electronically scanning inked images from paper. Other capture techniques include capacitive, thermal and ultra-sonic devices.

In contact fingerprint systems, the optical image technique is based on the concept of "frustrated total internal reflection". A glass platen is illuminated from below at an angle of incidence just beyond the critical angle at which light becomes reflected. If nothing is touching the topside of the platen, all of the light is reflected into the camera sensor. But where a finger ridge is touching the platen, the internal reflection is "frustrated", i.e. the light rays are not reflected but pass through to the finger. Consequently, the resulting fingerprint image is dark where there are ridges and light where there are valleys, replicating the pattern obtained through traditional ink impressions.

© ISO/IEC 2024 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 24741:2024

With capacitive fingerprint sensors, the platen comprises an array of tiny cells, each smaller than the width of a fingerprint ridge. Measurement of capacitance over the cells in the array indicates where the finger ridges are in contact with the sensor, generating a fingerprint image.

Thermal techniques use silicon chip technology to acquire fingerprint data as the subject moves a finger across the sensor. Variation in temperature between the ridges and the valleys are sensed and converted into a black and white image.

Ultra-sonic imaging uses sound waves beyond the limit of human hearing. A finger is placed on a capture device and acoustic waves are used to measure the density of the fingerprint pattern.

Fingerprints can be imaged one at a time, or in combinations of two or four. An image of four fingers (index through little finger) is known as a "slap". A slap is taken from each hand, followed by a single image of both the thumbs to create a "ten-print" image. In large-scale identification systems, individuals are enrolled using the optical live-scan capture process using multiple fingers, often taken as slaps. Law enforcement AFIS or ABIS capabilities can include a biometric collection kit or booking station to capture prints of all ten fingers. A booking station can operate in a standalone capability without connection to an AFIS or ABIS system. A civil AFIS or ABIS, however, need not capture all fingerprints and can operate effectively using as few as two.

Regardless of the fingerprint imaging technology employed, the fingerprint capture device develops a matrix of numbers, each corresponding to a pixel, representing the fingerprint. The standard spatial sampling rate for finger images is 197 pixels per centimetre (500 pixels per inch). The numbers in the matrix generally range from 0 (dark) to 255 (light), but some non-optical capture devices can output only a matrix of 0s and 1s.

Fingerprint imaging is one example of the biometric trait of friction ridges. Just as the friction ridges of a fingerprint can be captured by the appropriate technology, so can the friction ridges of palms, feet, and toes. ISO/IEC 19794-4 and ISO/IEC 39794-4 provide data interchange formats for exchange and processing of fingerprint and palm images.

6.1.2 Fingerprint comparison

There are many ways to compare fingerprints computationally (optical comparison methods developed in the 1960s and 1970s are not covered in this document). The major computational approaches are:

a) transform-based;

b) local correlation;

c) minutiae-based.

All three have been used in commercial systems. While minutiae-based systems were once the most popular, new uses of fingerprint recognition (for example on smartphones with small area sensors) and breakthrough in accuracy due to convolutional neural networks have made transform-based approaches at least as common.

No two fingerprints are alike. That is, even the same finger placed twice on a fingerprint platen will produce two different images of the ridge structure. There are no two identical fingerprints, even from the same finger. The within-class variation of fingerprints from the same finger has many causes, including changes in pressure and orientation of finger placement, finger moisture and ridge damage, as well as changes of imaging device.

Fingerprints can be compared using transform-based methods, correlation-based methods, or minutiae-based methods. Transform-based methods were generally based on two-dimensional Fourier transforms and Hough transforms applied to the matrix of pixels representing the fingerprint. In recent years, convolutional neural networks (CNNs) have been successfully used to significantly increase accuracy. The idea is to mathematically transform the image in some way, then compare coefficients of the transformed images. In this context, the fingerprints' features are the transform coefficients. See ISO/IEC 19794-3 for information on transform-based fingerprint transmission and storage.

Correlation-based methods recognize that fingerprints, and their representative matrices from the capture device, cannot simply be overlaid owing to all the variation. However, small areas of two fingerprints, when

© ISO/IEC 2024 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 24741:2024

overlaid, can be correlated. If the geometrical relationship between centres of the small areas remains about the same when overlaid to maximize correlation between the two images, it is possible that the images are of the same finger friction ridges.

Minutiae-based methods analyse small friction ridge features of the finger and emulate what forensic fingerprint examiners do. The minutiae are the ridge endings, and bifurcations (branching of fingerprint ridges). Minutiae also have a direction associated with the ridge at the point they occur, and the distance between ridges can also be analysed. The mathematical algorithm moves over the image searching for ridges, as well as where they split or end, and creating a minutiae map. To compare two fingerprints, their minutiae maps are laid on top of each other and are either spun or slid around or both. If some minutiae produce overlay in position and direction, it is a match. ISO/IEC 19794-2 and ISO/IEC 39794-2 provide data interchange formats for systems processing, generating and storing fingerprint minutiae data.

6.1.3 Palm technologies

Palm biometrics can be closely aligned with finger-scanning, and in particular with AFIS or /ABIS technology. As with fingers, friction ridges containing minutiae points are found on the palm. These can be captured using optical techniques as with fingerprinting. This area of the biometrics industry is particularly focused on the law enforcement community, as latent palm prints are as useful in criminal investigation as latent fingerprints. The capture and comparison processes for palm prints are essentially the same as those for fingerprints. Some collection platforms are suitable for both fingerprint and palmprints.

Other palm biometrics based on palm creases rather than on friction ridge structures have been developed in laboratory programs.

6.2 Face recognition

Automatically identifying an individual by analysing a face is a complex process for which there are a variety of algorithmic approaches. A number of biometric vendors and research institutions have developed face recognition systems that use digital photographs or video to capture images in visible, near infrared (IR) or far IR (thermal) wavelengths. Face recognition is made difficult by changes in images of the same face owing to pose angle, lighting, facial expression or adornment, and by the basic structural similarity of all faces (that is, generally a mouth placed under a nose placed below and between two eyes). Face recognition is also subject to ageing effects, more strongly than most other modalities, a large timespan between the capture of the probe and reference samples can significantly degrade recognition accuracy.

Algorithms often start the identification process with image enhancement and normalization: finding eye centres, reposing the facial image to a full-frontal orientation, and adjusting for shadows, etc. On the normalized image, a variety of image processing techniques are available to extract abstract measures from the image by the placement of filters over all or parts of the face. The extracted facial features are abstract measures not related directly to distances between “landmarks” on the face, such as nose, mouth and ears. Such measures, however, need to be both stable (not changing significantly for each individual from image to image) and distinctive (varying greatly between individuals).

Face recognition technology can work accurately with high resolution (more than 100 pixels between the eye centres), full frontal images in good lighting. However, performance degrades as resolution reduces or pose angle increases. Lighting variations also cause a decrease in accuracy. In the mid-2010s, the usage of CNN to detect and encode face data provided a major technological breakthrough in the accuracy of face recognition algorithms. Error rates dropped by orders of magnitude in the span of a few years, and this fast improvement is still ongoing. This improvement has allowed face recognition to be used effectively in previously challenging settings. At the current level of development, face recognition technology can work quite accurately, even with limited resolution (from 30 pixels between the eye centres) and is resilient to most defects (lighting, pose, angle, etc.). Only when several strong defects are present simultaneously will a decrease in accuracy be noticeable.

Three-dimensional maps of the face can be created through various means, such as:

— laser ranging;

— the projection of a grid on to the face to observe grid distortion owing to facial structure;

© ISO/IEC 2024 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 24741:2024

— merging of multiple images;

— using shading information in a single image.

Thermal imaging analyses heat that is caused by the flow of blood under the face. A thermal camera captures the hidden, heat-generated pattern of blood vessels underneath the skin. Because IR cameras are used to capture facial images, lighting is not important and systems can capture images in the dark. However, such cameras are significantly more expensive than standard video cameras and face recognition systems based on this technology have not been commercially available since the 1990s.

ISO/IEC 19794-5 and ISO/IEC 39794-5 provide a face image format for face recognition applications requiring exchange of face image data. ISO/IEC 29794-5 specifies methodologies for computation of objective, quantitative quality scores for facial images.

6.3 Iris recognition

After the expiry of patent protection, iris recognition technology became available from a variety of commercial sources and has been used successfully in border control, benefit programs and access control environments. Iris recognition has been successfully used in access control applications without the need for any form of claim of identity by the data subject. The data subject can be verified for system access by searching through the entire database of enrolled individuals. Technologies vary by vendor, with some systems collecting images from a single eye and some systems collecting images of both eyes simultaneously. Technologies are now available that can collect iris images from distances of over a metre or from individuals walking through a portal.

In most implementations, a grayscale image of the iris is acquired in the near IR spectrum to maximize the detail in eyes of all colours. To ensure pupil constriction to maximize the area of the iris, capture should be done in a well-lit environment. Non-patterned contact lenses and glasses do not interfere significantly with image capture. Sunglasses, however, should not be worn as they can affect the capture process. The computer algorithms unwrap these images to form a rectangular matrix of pixels, over which a smaller filter is placed in multiple locations. The filter represents a smooth wave with a frequency and direction. At every filter placement, the phase of the same frequency and direction in iris image is observed relative to the filter and used to create a pattern of 0s and 1s. These 0s and 1s are the iris features and do not directly represent any of the visible patterns on the iris such as crypts, filaments and freckles. Features of two iris patterns are compared by counting the percentage of 0s and 1s that coincide over the length of this binary vector, a function that can be performed by a computer at the bit level with extreme efficiency. If over about two-thirds of the 0s and 1s coincide, the patterns are assumed to be from the same eye. This value of two-thirds represents a threshold that can be varied to aid in balancing the false negatives and false positives.

ISO/IEC 19794-6 and ISO/IEC 39794-6 provide a data record format for storing and transmitting the iris images, including compact data formats and compression targets. ISO/IEC 29794-6 provides quantitative methodologies for characterizing the quality of iris images and for assessing their potential for high confidence biometric match decisions.

6.4 Dynamic signature recognition

Dynamic signature verification (DSV) is based on the hand movements made during the signing of our names. It is the method of signing rather than the finished signature that is important. Thus, DSV can be differentiated from the study of static signatures on paper. The technology was developed in the 1960s and is one of the oldest forms of automated personal recognition.

Signature data can be captured via a special pen or tablet. The pen-based method incorporates sensors inside the pen. The tablet method relies on the tablet to sense the distinctive signature characteristics.

A number of features can be extracted and measured by DSV. For example, the time taken to sign, the velocity and acceleration of the signature, the pressure exerted when holding the pen and the number of times the pen is lifted from the paper can all be extracted as distinctive characteristics. DSV is not based solely on the static image, so even if a signature is traced, a forger would need to know the dynamics of that signature.

© ISO/IEC 2024 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 24741:2024