ISO/IEC FDIS 24741

ISO/IEC JTC 1/SC 37~~/N0000~~

~~Date: 2023-05-24~~

~~ISO/IEC DIS 24741:2023~~

~~ISO/IEC JTC 1/SC 37/WG 4~~

Secretariat: ANSI

Date: 2024-02-20

Information technology — Biometrics — Overview and application

~~*Technologies de l'information — Aperçu général et applications*~~

~~Copyright notice~~

~~This ISO document is a working draft~~FDIS stage

Published in Switzerland

Contents

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

The main ~~changes are~~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.

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 ~~this latter word~~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 ~~being~~ 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.

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 ~~also~~ provides information ~~about~~on the application of biometrics in various business domains, such as border management, law enforcement and driver licencing. ~~And it~~It also provides information on the societal and ~~jurisdiction~~jurisdictional considerations that are typically taken into account in biometric systems.

Additionally, this document ~~identifies and~~ 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: ~~Harmonized biometric vocabulary~~Biometrics*

3 Terms,definitions and abbreviated terms

~~2.1~~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 systems
ABIS	automated biometric identification system
BDB	biometric data blocks
BIAS	biometrics identity assurance services
BIR	biometric information record
BIP	biometric interworking protocol

CBEFF	common biometric exchange formats framework
CNN	convolutional neural networks
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 documents
PET	privacy enhancing technology
PCA	principal component analysis
PIN	personal identification numbers
RBR	renewable biometric reference
SB	security block
SBH	standard biometric header
SOA	service-oriented architecture
WSDL	web services description language

~~3~~4 Fundamentals of biometrics

~~3.1~~4.1 Biometric ~~Characteristics~~characteristics

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

NOTE 1 The all-encompassing term "biometrics" refers to the application ~~to~~of biology ~~of~~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.

~~The term~~ISO/IEC 2382-37:2022 37.01.02 defines "biometric characteristic" ~~is defined~~ as a "biological and behavioural characteristic of an individual from which distinguishing, repeatable biometric features can be extracted for the purpose of biometric recognition~~" (ISO/IEC 2382-37:2022, 37.01.02).".~~ 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~~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~~" is more appropriate.

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

— — Distinctive: differentDifferent across all subjects;.

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

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

— — Universal: observableObservable on all people;.

— — Acceptable: theThe 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 mustinevitably compromise on every point: there.

— There are great similarities among different individuals; biometric.

— Biometric characteristics change over time; some.

— Some physical limitations prevent presentation; not.

— Not all people have all characteristics; "acceptability.

— "Acceptability" is in the mind of the subject. subjective.

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

3.24.2 What biometricBiometric systems do

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

a) a) something known or memorized;

b) b) something carried;

c) c) a personal physical or behavioralbehavioural characteristic.

The underlying assumptions wereare that individuals authorized to access secure data wouldwill cooperatively make positive claims (e.g. "I am authorized to access data on the system") and couldcan be counted on to protect their Personal Identification Numberspersonal identification numbers (PINs) and passwords. In such applications, biometric technologies do indeed compete with PINs, passwords and tokens. For example, most web-based access control requires a Useruser 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 logically 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.

Biometric recognition is used in two main classes of applications:.

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

2) 2) biometricBiometric 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"; "These two samples came from the same bodily source"*) 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.

To introduce the terminology ofAccording 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 it is possible 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" (FMR) and the "false non-match rate" (FNMR) 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 (and thethis process is one of biometric identification). However, the act of finding an identifier (or pointer) in a list of identifiers also verifies an unspecificunspecified 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.

~~Often usernames~~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 ~~would insert~~inserts the card into a card reader which reads the reference record, then ~~place~~places their finger on the fingerprint capture device. The system compares the biometric characteristics of the fingerprint on the reader with those of reference recorded on the card. The system ~~may~~can conclude, in accordance with defined thresholds, that the subject is indeed the source of the reference on the card, and therefore ~~should be~~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~~state of California requires applicants for social service benefits to verify the negative claim of no previously enrolled identity in the system by submitting fingerprints from both index fingers. Depending upon the specific automated search strategy, these fingerprints ~~might~~can be searched against the entire database of enrolled benefit recipients ~~to verify that there are no matching fingerprints already in the system, or perhaps~~, 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) ~~will~~ 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.

45 History

~~In a non-automated way, biometric~~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~~; we often remember~~, individuals are remembered and ~~identify an individual~~identified by their face or by the sound of their voice~~;~~, and ~~a signature is~~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] (Bertillon 1889[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] (Faulds, 1880[16]; Herschel, 1880[26])) when it was popularized scientifically by Sir Francis Galton[20] (1888[20])) and in literature by Mark Twain.[60] (1893[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). ResearchHowever, research on new methods of human identification continued, however, in the scientific world. Handwriting analysis was recognized by 1929[45] (Osborne, 1929[45])) and retinal identification was suggested in 1935.[55] (Simon and Goldstein, 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] (Potter, Kopp and Green, 1947[49])) and early 1950s.[13] (Chang, Pihl, and Essignmann, 1951[13]).) With the computer revolution picking up speed in the 1960s, speaker[50] (Pruzansky, 1963[50])) and fingerprint[58] (Trauring, 1963a[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]" (Trauring, 1963b[59]).) Computerized face recognition research followed.[6][21] (Bledsoe, 1966[6]; Goldstein, Harmon, and Lesk, 1971[21]).) In the 1970s, the first operational fingerprint and hand geometry recognition systems were fielded (for example, the Identimat system), results from formal biometric system tests were reported,[44] (Wegstein, 1970[44]),) measures from multiple biometric devices were being combined[39][17] (Messner, Cleciwa, Kibbler, and Parlee, 1974[39]; Fejfar, 1978[17])) and government testing guidelines were published.[38] (Meissner, 1977[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 automatedautomating the identification of fingerprints to assist law enforcers. The manual process of comparing fingerprints against criminal records was laborious and used up far 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 Systemsfingerprint identification systems (AFIS) were first implemented in the late 1970s, most notably by the Royal Canadian Mounted Police AFIS in 1977. The role of biometrics in law enforcement has mushroomedgrown exponentially since then and AFIS are used by a significant number of police forces throughoutacross 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 being connected to personal computers to control access to stored information. Based on a concept patented in the 1980s,[19] (Flom and Safir, 1987[19]),) iris recognition systems became available in the mid-1990s.[14] (Daugman, 1993[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 hard partchallenge is bringing a product to market and proving its operational performance. It does taketakes time for any laboratory technology to migrate to a fully operational system. However, such systems are nowcurrently in place and are proving themselveseffective across a range of diverse applications.