International Standard

ISO/IEC 24741

Information technology — Biometrics — Overview and application

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

Third edition
2024-06

Reference number
ISO/IEC 24741:2024(en)

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

Contents

Page

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.

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.

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

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.

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.

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

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

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.

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

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;

— 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.

A further advantage of signature biometric technologies is that the signature is one of the most accepted means of asserting identity. It is also used in a number of situations to legally bind an individual, such as the signing of a contract. These factors have taken signature biometrics to a number of diverse markets and applications, ranging from checking welfare entitlement to document management and pen-based computing.

ISO/IEC 19794-7 specifies data interchange formats for signature and sign behavioural data captured in the form of a multiple time-series, using devices such as digitizing tablets or advanced pen systems while ISO/IEC 19794-11 specifies a data interchange format for processed dynamic data extracted from the time-series.

6.5 Vascular recognition

The blood vessels (veins) that exist in the subcutaneous areas of the human body form a distinctive pattern for each individual. Furthermore, as blood vessels are within a human body, their vascular pattern cannot be easily obtained by other individuals through the use of normal photography. The underlying vascular pattern can be captured using IR illumination either directed onto the region to be photographed or transmitted through the body part being imaged. The blood vessels absorb IR light more than the surrounding tissue and appear darker in the acquired image. The vascular pattern can then be extracted and encoded for reference or comparison by the biometric system.

In actual products, the parts of body chosen (such as the palm, fingers, wrist and the back of the hands) are the parts where a user can easily present the blood vessel pattern to the sensor.

ISO/IEC 19794-9 and ISO/IEC 39794-9 specify image interchange formats for biometric vascular images for use in exchange and comparison of vascular image data.

6.6 Hand geometry recognition

Hand geometry recognition has been widely used in access control applications since the 1980s. The most common commercial approach takes one or more, two-dimensional silhouette images of the hand and processes those images using a proprietary algorithm to develop a 9-byte code.

A subject places a hand on a reflective platen, aligning fingers with specially positioned guides. The platen is illuminated with IR light and returns a reflection only where the hand is not covering the platen, thus producing a silhouette image of the hand. A mirror reflects light horizontally across the top of the hand, supplying a second two-dimensional silhouette of the side of the hand.

ISO/IEC 19794-10 specifies a data interchange format that can be used for recording, storing and transmitting the information obtained from a hand silhouette.

6.7 Voice recognition

Speaker recognition is a biometric technology based on the sound of the voice. Speaker recognition should not be confused with the related non-biometric technology of speech recognition, which is used to recognize words for dictation or automate instructions given over the telephone.

The sound of a human voice is mainly caused by resonance in the vocal tract. The length of the vocal tract, the shapes of the mouth and nasal cavities are all important. Sound is measured as affected by these specific characteristics. The technique of measuring the voice can use either text-independent or text-dependent methods. In other words, the voice can be captured with the subject uttering a specifically designated response to a challenge, combining phrases, words or numbers (text-dependent) or by speaking any form of phrase, words or numbers without a specific challenge (text-independent).

Speaker recognition technologies are particularly useful for telephone-based applications. Biometric systems can be easily incorporated into private or public telephone networks. However, environmental background noise and interference over these networks can affect the performance of speaker recognition systems.

Subjects speak into a microphone and utter a previously selected (text-dependent) or unguided (text-independent) phrase. The process is usually repeated a number of times during enrolment to build a

sufficient model of the voice generally based on biometric features such as “cepstral coefficients” which capture the resonance characteristics of the vocal tract.

ISO/IEC 19794-13 specifies a data interchange format for storing, recording, and transmitting digitized human voice data assumed to be from a single speaker recorded in a single session. This format is designed specifically to support both text-dependent and text-independent speaker identification and verification applications.

6.8 DNA recognition

There are many types of semi-automated DNA analysis, some taking as little as fifteen minutes to implement. Given a sufficient number of loci, DNA analysis can not only identify individuals, it can also identify heredity relationships. Because DNA requires some form of tissue, blood or other physical biological sample, it is likely to remain exclusively a forensic technique, as opposed to a significant contender in the access control market.

ISO/IEC 19794-14 specifies a data interchange format. This data interchange format is for non-coding DNA data only, i.e., not providing information about specific genetic traits of an individual.

6.9 Full body recognition

There are a number of applications in which recognition can be based on analysis of traits of the full body, in addition to the face or other biometrics. Analyses of the full body can be considered in, for example:

— forensic applications for law enforcement;

— video surveillance for gait analysis and tracking;

— for disaster victim identification.

Rather than considering separate body features in isolation, utilizing the body tree structure is more organized. Multimodal biometric human verification or identification can utilize face features, full body features, full body gait and head movement. Multimodal biometric fusion can combine recognition results at a feature level, comparison-score level or decision level.

ISO/IEC 39794-16 addresses standard poses, element structures and data formats to help the parsing of the body tree data into body part representations and landmarks.

6.10 Gait recognition

Gait is defined as the style or manner of walking. Gait recognition systems typically record a full body video of an individual walking. A partial gait signal can be recorded by other means, such as from accelerometer data of a mobile phone carried on the individual, or from floor sensors. For imaging, the whole electromagnetic spectrum is available, not only the visible bandwidth.

Appearance-based methods for gait recognition analyse distinctive features of the shape and dynamics of the silhouette. Model-based methods of gait recognition model the relative positions and dynamics of joints and limbs and fit features extracted from the gait sequence to that model.

ISO/IEC 39794-17 provides requirements and recommendations on the capture of gait image sequence data to support automated gait-based verification and identification.

6.11 Retina recognition

The retina is the light-sensitive layer of nerves and blood vessels on the inner surface of the eye. During the 1980s and 1990s, retinal recognition systems that mapped the vein patterns on the retina were commercially available. Such systems did not develop images of the vein patterns, but rather scanned an IR light beam in a circular pattern over the retina and recorded the intensity of the returned light. This resulted in a one-dimensional pattern with high values of reflected light over portions of the circle for which no blood vessel was encountered and low values of reflected light where blood vessels absorbed the IR beam. Despite rumours to the contrary, no health information was known to exist in these patterns and no laser light was

ever used. Because of the requirement to shine the imperceptible IR light onto the back surface of the eye, data subjects were required to look into the capture device at a very close proximity, in near contact with the device. Today, retinal recognition devices are no longer commercially available.

6.12 Keystroke recognition

Keystroke dynamics analyse typing rhythm. An individual's keystroke dynamics evolve over time as they learn to type and develop their own distinctive typing habits. The algorithms will potentially need to cope with subjects becoming distracted or tired during the course of the day.

6.13 Scent and odour recognition

Recognition of individuals through personal odour has long been suggested based on the proven ability of dogs in this regard. Although no devices have ever been commercially marketed, some have been under development. For example, a "sniffing" device to draw the odour onto an electronic sensor with receptor proteins that react to specific odour molecules. The variations in the proportions of the various molecules can be distinctive enough to enable recognition.

6.14 Cardiogram recognition

Physical differences between heart muscles and circulatory systems give rise to distinctiveness in the fine details in cardiac rhythm as displayed in electrical signals or by blood flow. There have been many research projects in this area, some resulting in commercial products.

6.15 Multimodal biometrics

Multimodal biometrics is the combination of different modalities. This combination can be used to either increase accuracy or improve flexibility, or both. The modalities are typically used in the same context, with the application deciding how to best combine the results to make the best decision given the context of the solution.

ISO/IEC TR 24722 provides a reference on the methods for combining different modalities. ISO/IEC 29159-1 specifies a fusion information format that characterizes the statistics of comparison score input to optimize a fusion process.

7 General biometric system

7.1 Conceptual representation of general biometric system

Given the variety of applications and technologies, it can seem difficult to draw any generalizations about biometric systems. All such systems, however, have many elements in common. Biometric samples are acquired from a subject by a biometric capture device and are submitted to a processor that extracts the distinctive but repeatable measures of each sample (the biometric features), discarding all other components. The resulting features can be stored in the biometric enrolment database as a biometric reference. In other cases, the sample itself (without feature extraction) can be stored as the reference. A subsequent query or probe biometric sample can be compared to a specific reference, to many references, or to all references already in the database to determine if there is a match. A decision regarding the biometric claim is made based upon the similarities or dissimilarities between the features of the biometric probe and those of the reference or references compared.

Figure 1 illustrates the information flow within a general biometric system consisting of data capture, signal processing, data storage, comparison and decision subsystems. This diagram illustrates both enrolment and the operation of verification and identification systems.

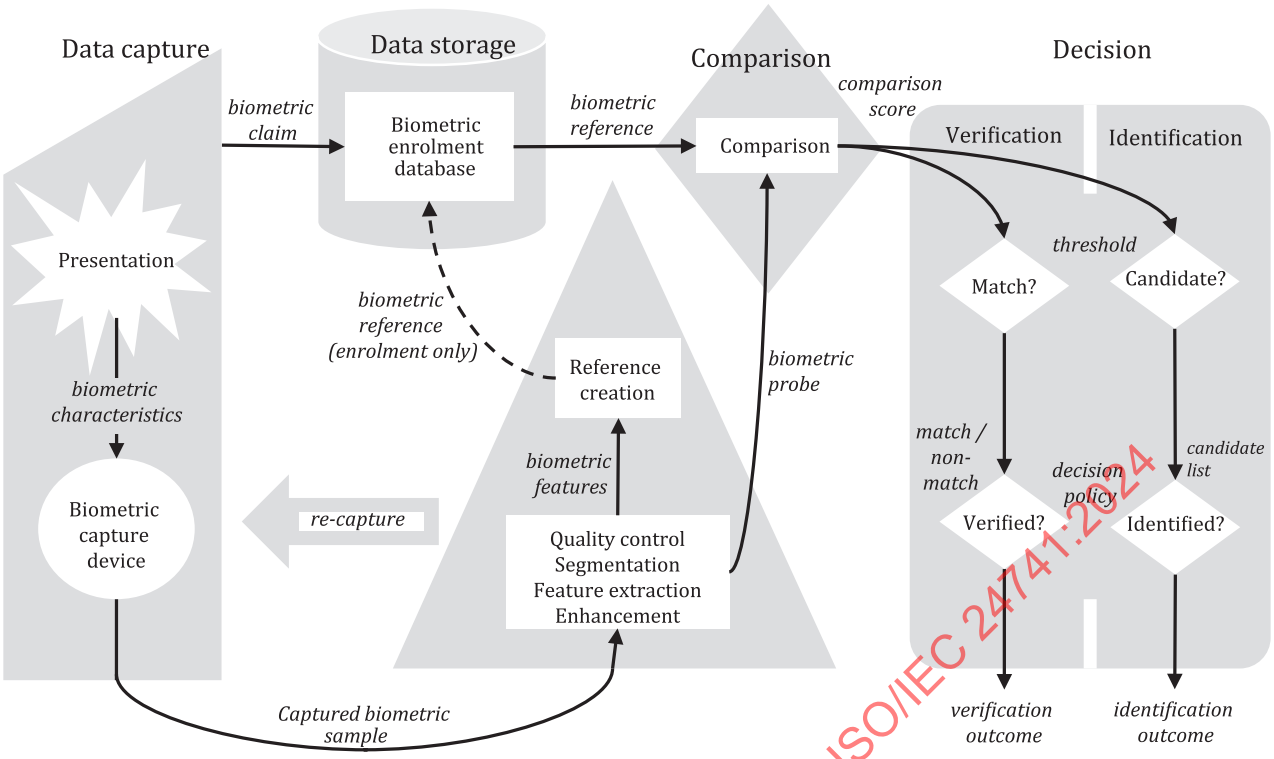

Figure 1 — Components of a general biometric system

Subclauses 7.2 to 7.3 describe each of these components in more detail. However, it should be noted that in any implemented system, some of these conceptual components can be absent, or possibly not have a direct correspondence with a physical or software entity.

7.2 Conceptual components of a general biometric system

7.2.1 Data capture

Data capture collects an image or signal of a subject's biometric characteristics presented to the biometric capture device, and outputs this image or signal as a captured biometric sample.

7.2.2 Transmission

Biometric data, samples, features, probes, references, comparison scores and outcomes are usually transmitted between different subsystems. Sometimes this can be via a manual submission process. The captured biometric sample can either be compressed or encrypted, or both, before transmission and either expanded or decrypted, or both, before use. A captured biometric sample can be altered in transmission due to noise in the transmission channel as well as losses in the compression and expansion processes. Data can be transmitted using standard biometric data interchange formats, and cryptographic techniques can be used to protect the authenticity, integrity, and confidentiality of stored and transmitted biometric data.

7.2.3 Signal processing

Signal processing includes processes such as:

— enhancement, i.e. improving the quality and clarity of the captured biometric sample;

— segmentation, i.e. locating the signal of the subject's biometric characteristics within the captured biometric sample;

— feature extraction, i.e. deriving the subject's repeatable and distinctive measures from the captured biometric sample;

— quality control, i.e. assessing the suitability of samples, features, references, etc. and possibly affecting other processes, such as returning control to the data capture subsystem to collect further samples (recapture), or modifying parameters for segmentation, feature extraction, or comparison. Quality can also be used in biometric fusion where the comparison scores are combined with a consideration of the associated quality values of the samples used for each comparison.

In the case of enrolment, signal processing creates a biometric reference. Sometimes the enrolment process requires features from several presentations of the individual's biometric characteristics. Sometimes the reference comprises just the features, in which case the reference can be called a "template". Sometimes the reference comprises just the sample, in which case feature extraction from the reference occurs immediately before comparison.

In the case of verification and identification, the signal processing creates a biometric probe.

Sequencing and iteration of the above-mentioned processes are determined by the specifics of each system.

7.2.4 Data storage

References are stored within an enrolment database. Each reference can be associated with some details of the enrolled subject or the enrolment process. It should be noted that prior to being stored in the enrolment database, references can be reformatted into a biometric data interchange format. References can be stored within a biometric capture device, on a portable medium such as a smart card, locally such as on a personal computer or local server, in a central database, or in the cloud.

7.2.5 Comparison

Probes are compared against one or more references and comparison scores are passed to the decision process. The comparison scores indicate the similarities or dissimilarities between the probe(s) and reference(s) compared. For verification, a single specific biometric claim would lead to a single comparison score. For identification, many or all references can be compared with the probes and output a comparison score for each comparison.

7.2.6 Decision

The comparison scores generated from one or more biometric comparisons are used to provide the decision outcome for a verification or identification transaction.

In the case of verification, the probes are considered to match a compared reference when (assuming that higher scores correspond to greater similarity) the comparison score exceeds a specified threshold. A biometric claim can then be verified on the basis of the decision policy, which can allow or require multiple attempts.

In the case of identification, the enrolee reference is a potential candidate for the subject either when (assuming that higher scores correspond to greater similarity) the comparison score exceeds a specified threshold or when the comparison score is among the predetermined number of ranked values generated during comparisons across the entire database, or both. The decision policy can allow or require multiple attempts before making an identification decision.

NOTE 1 In the context of a biometric application, the automated biometric decision policy can be a result of human oversight and organizational aspects.

NOTE 2 Conceptually, it is possible to treat multibiometric systems in the same manner as unibiometric systems, by treating the combined captured biometric samples, references or scores as if they were a single sample, reference or score and allowing the decision subsystem to operate score fusion or decision fusion as, and if, appropriate. See ISO/IEC TR 24722 for further information.

7.2.7 Administration

Administration governs the overall policy, implementation, configuration and operation of the biometric system. Illustrative examples include:

a) interacting with the subject, including providing guidance feedback to the subject either during or after data capture or both, and requesting additional information from the subject;

b) storing and formatting of either the biometric references or biometric interchange data, or both;

c) providing final arbitration on output from either decision or score, or both;

d) setting threshold values;

e) setting biometric system capture settings;

f) controlling the operational environment and non-biometric data storage;

g) providing appropriate safeguards for subject privacy and subject data security;

h) interacting with the application that utilizes the biometric system;

i) providing automated or ad-hoc reports to system users.

NOTE The administration subsystem is not portrayed in Figure 1.

7.2.8 Interface to external application

The biometric system will possibly not interface to an external application or system via a web services interface, an application programming interface (API), a hardware interface or a protocol interface.

NOTE The interface to the external application is not portrayed in Figure 1.

7.3 Functions of general biometric system

7.3.1 Enrolment

In enrolment, a transaction by a capture subject is processed by the system in order to generate and store an enrolment reference for that individual.

Enrolment typically involves:

a) sample capture;

b) sample optimization or enhancement;

c) segmentation;

d) feature extraction;

e) quality checks, which may reject either the sample or the features, or both, as being unsuitable for creating a reference, and require capture of further samples. Sample quality scores may also be stored with the biometric reference for subsequent use in biometric comparison;

f) presentation attack detection checks, which may reject either the sample or the features, or both, as being ineligible for use as an enrolment reference;

g) where system policy so requires, comparison against existing biometric references in order to ensure the subject is not already enrolled;

h) reference creation, which can require features from multiple samples, and possibly generation of a database index;

i) storage of the biometric reference data record, possibly after conversion to a biometric reference data interchange format;

j) test verification or identification attempts by the capture subject to ensure that the resulting biometric reference is usable;

k) allowing repeat enrolment attempts, if the initial enrolment is deemed unsatisfactory (dependent on the enrolment policy).

7.3.2 Verification of a positive biometric claim

In applications such as access control, a transaction by a subject can be processed by the system in order to verify a positive specific claim about the subject's enrolment (e.g. "I am enrolled as subject X"). Some biometric systems allow a single subject to enrol more than one instance of a biometric characteristic (for example, an iris system can allow subjects to enrol both iris images, while a fingerprint system can require enrolment of additional fingers for fall-back in case a primary finger is damaged).

Verification of a specific positive claim typically involves:

a) sample capture;

b) sample optimization or enhancement;

c) segmentation;

d) feature extraction;

e) quality checks, which may reject either the sample or the features, or both, as being unsuitable for comparison, and require capture of further samples (the sample quality may also be considered at biometric comparison);

f) presentation attack detection checks, which may reject either the sample or the features, or both, as being ineligible for use;

g) probe creation, which can require features from multiple samples possible conversion into a biometric data interchange format;

h) comparison of the probe and the reference for a biometric claim producing a comparison score;

i) determination of whether the biometric features of the probe match those of the reference based on whether the comparison score exceeds a threshold (in cases where higher scores correspond to greater similarity);

j) decision to verify a claim based on the comparison result of one or more attempts as dictated by the decision policy.

The verification function either accepts or rejects the specific positive claim. The verification decision outcome is considered to be erroneous if either a false claim is accepted (false accept) or a true claim is rejected (false reject). In this application, a false acceptance occurs if the submitted sample is wrongly matched to a stored reference not created by the data subject. A false rejection occurs if the submitted sample is not matched to a reference actually created by the data subject.

NOTE Verification of an unspecific positive claim is also possible with a biometric system. Such applications are referred to as "PIN-less verification" because no PIN or other identifier was necessary to establish that the data subject was indeed enrolled in the database. For verification of an unspecific positive claim, the process is as specified in 7.3.2 a) to g). However, steps h) to j) are different when the claim is unspecific:

h) comparison of the probe against all the references producing a score for each comparison;

i) determination of whether the biometric features of the probe match those of any reference based on whether the comparison score exceeds a threshold (in cases where higher scores correspond to greater similarity);

j) decision to verify a claim based on the comparison results of one or more attempts as dictated by the decision policy.

7.3.3 Identification

In identification, biometric samples from a capture subject are processed to generate a probe, and the enrolment database is searched to return identifiers of references similar to that probe. Identification provides a candidate list of identifiers containing zero, one, or more identifiers. Identification is considered correct when the subject is enrolled and an identifier for their enrolment is in the candidate list. The identification is considered to be erroneous if either an enrolled subject's identifier is not in the resulting candidate list (false-negative identification error), or if a transaction by a non-enrolled subject produces a non-empty candidate list (false-positive identification error).

Identification typically involves:

a) sample capture;

b) sample optimization or enhancement;

c) segmentation;

d) feature extraction;

e) quality checks, which may reject either the sample or the features, or both, as being unsuitable for comparison, and require capture of further samples, the sample quality may also be considered at biometric comparison;

f) presentation attack detection checks, which may reject either the sample or the features, or both, as being ineligible for use;

g) probe creation, which may require features from multiple samples, and possible conversion into a biometric data interchange format;

h) comparison against some or all references in the enrolment database, producing a score for each comparison;

i) determination of whether each compared reference is a potential candidate identifier for the capture subject, based on whether the comparison score either exceeds a threshold or is among the highest ranked scores returned, or both, producing a candidate list (higher scores correspond to greater similarity);

j) an identification decision based on the candidate lists from one or more attempts, as dictated by the decision policy.

NOTE In the context of a biometric application, the automated biometric decision policy can be a result of human oversight and organizational aspects.

8 Example applications

8.1 General

Applications of biometric technologies are extremely diverse and occur in a broad range of government, commercial and personal applications and therefore are difficult to distinctly categorize. This clause is organized by function of the application (e.g. "time and attendance", automated payments) as opposed to the implementing sector (e.g. banking, healthcare), while recognizing that a single biometric application can be used in multiple sectors.

8.2 Physical access control

Some of the earliest applications of automated human recognition were for opening doors. These applications continue at health clubs, theme parks and workplaces to allow members and employees to pass through portals with minimal staff supervision. In the 1990s and early 2000s, hand geometry was the primary biometric modality used for low to moderate security applications, but recently fingerprint recognition has become dominant. In the 1980s and 1990s, some high security applications for both government and business

were built around retinal recognition, but since then, iris recognition and multi-finger fingerprinting has come to dominate.

Disney World in Orlando, Florida in the US, began using finger geometry (a form of hand geometry) in the mid-1990s as a multi-factor access control solution for season pass holders. By the mid-2000s, the system transitioned to fingerprinting and was applied to all holders of any access pass to Disney World to prevent transference of passes.

8.3 Logical access control

The use of biometrics to control access to computer records was strongly advocated in the 1970s. By the late 1980s, many commercial fingerprint, retinal, and voice systems were being marketed. By the late 1990s, fingerprint capture devices were being built into computer keyboards and cell phones, but uptake was slow. On-card biometric comparison (also known as "match on card") technology became available by the late 2000s. This technology stores the reference and does all calculations required for recognition on a smart card controlled by the data subject. This solution is a privacy protective technology. Although the data subject is required to present a biometric sample to an external biometric capture device, that sample is not stored but is passed immediately to the smart card for comparison with the stored reference.

The rapid uptake of smart phones in the 2010s allowed extension of the "match on card" concept to the cell phone, but now with all aspects, e.g. biometric data collection, storage and comparison, under complete control of the biometric data subject. Apps for voice, face, sclera-vein and fingerprints became readily available for unlocking the phone and other apps on the phone, with no transfer of biometric data out of the direct possession of the data subject. Specially secured hardware within the smartphone (i.e. the trusted execution environment) is used to protect the biometric reference data and to carry out the biometric comparison operations.

Based on the specifications of the FIDO Alliance,[18] users can authenticate themselves securely and conveniently on the Internet with the help of cryptographic protocols running on a mobile device under their control. Access to the private key is secured by biometric methods (such as fingerprint, face, or iris verification) or PIN based verification

8.4 Time and attendance

Biometric systems for recording the entry and exit of employees from work sites date at least to the early 1990s, with current use extending to small business, industry and government. A variety of devices are available based on fingerprint, hand geometry and iris recognition. In addition to tracking time for payroll purposes, the systems can give supervisors immediate access to data about which employees are at the job site at any time, information which is useful in the event of an emergency.

8.5 Accountability

Biometric recognition can be used in applications requiring accountability and non-repudiation. Some hospitals and pharmacies use biometrics as a requirement for access to narcotics. The collection of a biometric characteristic assures that the dispensing of each dosage can be attributed to a registered individual in a way that cannot be later repudiated.

8.6 Electronic authorizations

A number of banks have released smart phone applications using biometric characteristics to authorize purchases and transfers of funds. Bank customers can be given a choice of biometrics, such as fingerprint, face or voice, or can choose to not use biometrics at all.

8.7 Government and citizen services

eGovernment services in a number of countries recognize citizens and residents using biometrics. The largest such application is the Unique Identification Authority India. Indian residents apply for an "Aadhaar" number at any of thousands of enrolment sites, supplying two iris images, ten fingerprints and a face image. The iris and fingerprint images are used for "de-duplication", meaning a search of the entire database to

avoid issuance of multiple Aadhaar numbers to a single individual. The issued number can be used with one of the biometric characteristics (generally fingerprint) for multifactor recognition for the dispensing of government benefits and services. The original purpose of the system was to promote economic participation, including the creation of bank accounts, for individuals who otherwise have no identity documents or government identity records.

The use of biometrics in voting has presented multiple challenges. The Mexican government has used facial images, along with biographic information, to de-duplicate voter registrations on a precinct-by-precinct basis. Use of biometrics at a national level on election day to connect voters with registrations has proven problematic because of the throughput and bandwidth requirements and the need for exception handling mechanisms for those not recognized.

The Australian Department of Human Services uses speaker recognition to verify the identity of phone callers to the Centrelink benefits offices. Speaker reference models are indexed by telephone number, so that an incoming call from a recognized phone number needs only be compared to a very few speaker models to verify the identity of the caller. This system operates in both text-dependent and text-independent modes.

8.8 Border protection

8.8.1 ePassports and machine-readable travel documents

In the 1990s, the International Civil Aviation Organization (ICAO), which is responsible for specifying international passport standards, began an initiative for the creation of machine-readable travel documents" (MRTDs) and in 2003, established face images supplemented as necessary with fingerprint and iris images as the preferred biometric reference for use on MRTDs. Since around 2006, many nations have issued ePassports which contain a computer chip compliant with ICAO MRTD specifications. The face image is stored on the computer chip. This has enabled the use of ePassports with biometric automated border control (ABC) systems, allowing passengers to transit through systems on which they have not been previously enrolled. Some countries have augmented this data with the inclusion of fingerprint image data.

8.8.2 Automated border control (ABC) systems

By the year 2022, 33 nations had implemented ABC systems for some international travellers, replacing primary line inspection with a biometric gate. The ABC system verifies the connection of the traveller to the travel document (generally a passport) by capturing the biometric characteristic presented by the traveller and comparing it with that encoded in the MRTD (either with the face image or, on some passports, with fingerprints) or with an enrolment reference previously created specifically for this ABC system and linked to the identity document. In the case of a traveller not being recognized against the reference image, the traveller is referred for processing by a border control officer.

Typically, ABC systems include other border control processing as required by a border control authority, such as a check on the currency and authenticity of the travel document, and the name or document number against a watchlist. ABC systems are not intended to replace all manual or human border control policies and procedures and are generally supported by human oversight.

8.8.3 Entry/exit systems

Some countries introduce entry-exit systems for electronically recording the time and place of entry and exit of third-country nationals with and without visas, in order to monitor compliance with the permitted length of stay. In addition to information about the travel document used, fingerprints and face images of travellers are also stored and compared.

8.8.4 Visas

Most countries require travellers from some countries to acquire visas from local consulates prior to entry. Some visa issuance processes collect face and fingerprint images for comparison to those of individuals previously denied visas and for comparison to the traveller upon arrival to prevent transference of the visa.

8.8.5 EURODAC

EURODAC is a European Union (EU) fingerprint database of asylum seekers which has been operational since 2003. The fingerprints of all EU asylum seekers over 14 years of age are compared to fingerprints of previous EU asylum seekers, then stored in the EURODAC central system for 10 years. The purpose of this system is to detect individuals applying multiple times for asylum within the EU within this 10-year period.

8.9 Law enforcement

The law enforcement community uses many of the world's largest biometric systems. The two main biometric functions in law enforcement agencies involve identification of arrestees (usually through sets of fingerprints but also in some applications through facial images), and identification of forensic evidence (often through latent fingerprints, surveillance camera footage or DNA left at crime scenes). In the US, fingerprints are searched against the FBI's NGI system, which currently contains fingerprint sets from over 70 million individuals. Police forces throughout the world use AFIS or ABIS technology to identify the source of fingerprints from crime scenes and to identify arrestees. Law enforcement databases will also frequently hold the fingerprints of individuals not associated with any criminal activity, such as those in law enforcement, the military, or government positions of trust.

8.10 Civil background checks

Many types of government and private employment require background checks on the criminal history of applicants. These checks are usually implemented by searching applicant fingerprints against the fingerprints held in the criminal portion of law enforcement databases.

8.11 Clustering

Biometrics has traditionally been associated with "identification" and "verification", but other applications follow from the definition of biometrics as "automated methods of recognizing individuals". Biometric systems can be used to "cluster" biometric samples (for example, face images), grouping samples likely to have come from the same individual without requirement for "enrolment" or knowledge of the individual being recognized.

Social media has begun to cluster and mark faces of single individuals. Those individuals can then be linked to clusters of other individuals appearing in the same images, allowing mappings of social networks.

In the same way, an audio recording containing the voices of multiple individuals can be segmented and clustered into the speech segments associated with each individual, even if the individuals are otherwise unknown.

9 Performance testing

9.1 General

Biometric devices and systems can be tested in many different ways. Types of testing include:

a) functional capability;

b) technical performance (in terms of error rates and throughput rates);

c) reliability, availability and maintainability;

d) vulnerability;

e) security;

f) user acceptance;

g) human factors;

h) cost/benefit;

i) legislative compliance, including that relating to privacy and transparency of the biometric data recorded for an individual.

Technical performance tests are generally conducted with the goal of predicting system performance with a target population in a target environment, but historically, extrapolation of results from a test environment to the "real world" has been difficult. To make test results more predictive of real-world performance, testing standards have been developed (the ISO/IEC 19795 series).

Technical tests can be either "closed-set" or "open-set". In closed-set testing, all test subjects are enrolled in the system. Closed-set tests cannot measure performance of the system when used by people who are not enrolled. A closed-set test returns the rank of the true comparison when an input sample is compared to all of the enrolled references. Closed-set tests measure the probability that the true pattern was found at rank *k*, or better, in the search against the database of size *N*. In any test, the rank *k* probability is dependent upon the database size, decreasing as the database size increases.

An "open-set" test does not require that all input samples be represented by a reference in the enrolled database, and measures all comparison scores against a score threshold. An open-set test returns, as a function of the threshold, the following probabilities:

1) declaring a non-match for a mated comparison of probe and reference from the same instance (i.e. the same finger) from the same subject (the false non-match rate);

2) declaring a match for a non-mated comparison of probe and reference from different individuals (the false match rate).

Examples of both open-set and closed-set tests are found in the literature, but as most applications have to acknowledge the potential for impostors, open-set results are of the greater practical value to the system designer or analyst.

Metrics generally collected in open-set technical tests include:

— failure-to-enrol;

— failure-to-acquire;

— false accept;

— false reject;

— throughput rates.

The failure-to-enrol rate is determined as the proportion of enrolment transactions in which the enrolment cannot be completed because of system or human failure. The failure-to-acquire rate is determined as the proportion of capture processes by all enrolled subject that are not acknowledged by the system. The false reject rate is the proportion of all verification transactions with true biometric claims erroneously rejected by the system. The false accept rate is the proportion of verification transactions with untrue biometric claims erroneously accepted by the system. Because false accept rate and false reject rate (or false match rate and false non-match rate) are competing measures, they can be displayed together on a detection error trade-off (DET) curve. The throughput rate is the number of individuals processed by the system per minute and includes both the human-machine interaction time and the computational processing time of the system.

9.2 Types of technical tests

Three types of technical tests are described in Reference [46]:

— Technology test: The goal of a technology test is to compare competing algorithms from a single technology, such as fingerprinting, against a standardized database collected with a sensor compliant with a stated standard (a "universal" sensor). There are comparative technology tests in:

  — speaker verification (see Reference [41]);

  - face recognition (see References [42], [5], [47], [48], [23], [24] and [25]);
  - fingerprinting (see References [34], [35], [11], [12], [10], [54], [63], and [22]);
  - iris (see References [29] and [48]).

- Scenario test: While the goal of technology testing is to assess the algorithm, the goal of scenario testing is to assess the performance of the subjects as they interact with the complete system in an environment that models a real-world application. Each system tested has its own capture sensor and so receives slightly different data. Scenario testing has been performed by a number of groups, but few results have been published openly (see References [53], [7] and [36]).
- Operational test: The goal of operational testing is to determine the performance of a target population in a specific application environment with a complete biometric system. In general, operational test results are not repeatable because of unknown and uncontrolled differences of operational environments. Further, "ground truth" (i.e. who is actually presenting a "good faith" biometric characteristic) is difficult to ascertain. Because of the sensitivity of information regarding error rates of operational systems, few results have been reported in the open literature (see Reference [52]).

All biometric recognition techniques require human interaction with a data collection device. Technology testing generally attempts to limit the effect of human interaction, while scenario and operational testing accounts for and attempts to measure these effects. Comparison error rates, failure-to-enrol, failure-to-acquire rates and throughput rates are determined by human interaction, which in turn depends upon the specifics of the collection environment. Human factors of biometric collection are an emerging discipline.

Results of technical performance tests can vary depending on:

- the type of test (technology, scenario, or operational);
- the composition of the corpus of test data and controls on data quality (see ISO/IEC 29794-1);
- application environment (which can affect the relative difference between mated probe and reference, making these harder to match (see ISO/IEC TR 29198);
- decision policy of the application (e.g. how many retries are permitted).

These issues can make comparison of test results and prediction of real-world performance difficult.

10 Biometric technical interfaces

10.1 Biometric data blocks (BDBs) and biometric information record (BIRs)

There are two key concepts in International Standards for biometrics technical interfaces.

The first is that of a biometric data block (BDB). A biometric data block is a block of data with a defined format that contains one or more biometric samples or biometric templates such as a fingerprint image, a record of "finger minutiae" (ridge and valley merging or bifurcation), an iris image, etc.

There are biometric data interchange format standards (ISO/IEC 19794 and ISO/IEC 39794) for various biometric technologies, each specifying one or more BDB formats (e.g. compact smart card formats as well as normal formats). Each BDB format has a BDB format identifier that enables the format to be interpreted and processed by any system that has knowledge of that format.

The second is that of a biometric information record (BIR). A BIR is a BDB with added metadata, e.g. when it was captured, its expiry date, the equipment capturing it, whether it is encrypted. A number of different BIR formats are defined by ISO/IEC 19785-3 as part of ongoing work in this area, based both on the amount of information included in the BIR and on the compactness of the encoding scheme used. BIR formats have an identifier, called a "Common Biometric Exchange Formats Framework (CBEFF) patron format identifier".

The BIR is the unit used in most International Standards for the storage and movement between software modules and computer systems, for example, using biometrics identity assurance services (BIAS) and the BioAPI interfaces (within a system) or the Biometric Interworking Protocol (BIP) (between systems).

The BIAS, BioAPI and BIP architectures are important for any work involving the movement of biometric information (BDBs, BIRs) within a system or between systems.

The ISO/IEC 19785 series for CBEFF promotes interoperability of biometric-based applications and systems by specifying standard structures for BIRs (BDBs plus metadata) and a set of abstract data elements and values that can be used to create the header part of a CBEFF-compliant BIR.

A BIR is an encoding in accordance with a CBEFF patron format (as specified within 10.1). It is a unit of biometric data for storage in a database or for interchange between systems or parts of systems. A BIR always has at least two parts: a standard biometric header (SBH) and at least one BDB. It can also have a third part called the security block (SB). CBEFF places no requirements on the content and encoding of a BDB, except that its length needs to be an integral number of octets. The ISO/IEC 19794 series specifies standardized BDB formats for a number of biometric types.

The primary purpose of CBEFF is to define abstract data elements (data elements with a set of defined abstract values, with their semantics) that are expected to be of general utility as parts of the SBH in BIRs.

A CBEFF patron format is defined for a particular domain of use. A CBEFF patron format is a full bit-level specification of encodings that can carry some or all of the abstract values of the CBEFF data elements defined in ISO/IEC 19785 (possibly with additional abstract values determined by the CBEFF patron), together with one or more BDBs containing biometric data.

The ISO/IEC 19785 series consists of four parts. ISO/IEC 19785-1 specifies a full set of (metadata) data elements and their abstract values (without determining any particular encoding). ISO/IEC 19785-2, defines procedures for the operation of the Biometric Registration Authority. ISO/IEC 19785-3 defines a number of useful patron formats that vary from minimal to maximal metadata and include both binary and XML encodings of the metadata. ISO/IEC 19785-4 defines the SB to provide for both integrity and encryption of the biometric data.

10.2 Management of information on source of biometric data

The source of biometric data can have a significant impact on the appearance and characteristics of a biometric sample. This dataset bias caused by different capture techniques or modes can be challenging for processes like biometric feature extraction. For example, samples acquired from a live face image differ from those from a stored digital photo, while fingerprint images from a contactless capture device differ from those of a contact-based capture device. Instead of using sample normalization or general-purpose processing, better results can be obtained using specialized processing. In order to dispatch the samples to specialized processes, it is necessary to obtain the biometric source information and make the classification.

There are standardized data interchange formats, which provide meta information about capture mode and technique, e.g. the ISO/IEC 39794 defined biometric data formats. But biometric samples do not always come with such information about their origin, or the information is not reliable. This lack of information is possibly unintentional, e.g. when processing legacy data in a system in which the samples have various data origins. Estimating the data origin of biometric samples can be done using a CNN.[56]

10.3 Service architectures

Service-oriented architecture (SOA) is a software design pattern based on discrete pieces of software called services. Services are independent software programs designed to fulfil a specific function and comprise a set of capabilities to realize that function. The service is typically expressed in service contracts, which are technical service descriptions designed for runtime consumption (for example, a Web Services Description Language (WSDL) definition and an XML schema definition). Services are akin to APIs. The SOA design pattern provides for services to be aggregated through service compositions, the effect of which is to provide automated support to any business process that requires the functionality of the service composition.

Biometric software services are designed to provide a generic set of biometric and identity-related functions and associated data definitions to facilitate the collection, storage, use and disclosure of biographic and biometric data in a variety of business contexts and domains. These services typically do not contain logic that is specific and unique to a particular business operation. As such, logic is more appropriately contained within the application logic layer. Rather, the services contain the logic required to enable biometric services to be applied agnostic to the operating environment.

Biometric services include:

a) WS biometric devices (WS-BD), described in Reference [40], which define a number of primitive and aggregate services for the integration of biometric sensor devices into biometric systems that have a biometric capture component.

b) Biometric identity assurance services, described in ISO/IEC 30108. In essence, these services provide for the storage and retrieval of biographic and biometric data collected from an individual where the biometric data is collected via a biometric sensor of some sort.

10.4 The BioAPI application programming interface

BioAPI provides an implementation architecture that supports biometric applications using software (and hardware) modules from multiple vendors (see ISO/IEC 19784 for further information).

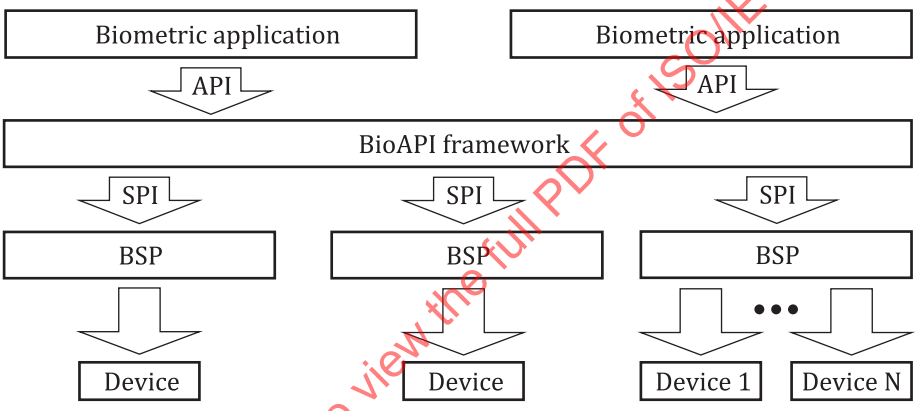

Figure 2 — BioAPI architecture

The basic concept is of applications (from multiple vendors) interacting with a BioAPI framework (from a single vendor, but with defined interfaces), which in turn interacts with biometric service providers (BSPs) (from multiple vendors) to perform the biometric functions. The BioAPI architecture is shown in Figure 2.

Interaction between these various components is by passing a BIR.

BSPs can perform capture, comparison, archiving, or processing of a BIR.

In a recent addition to the BioAPI architecture, the BSP can consist of code from one vendor interacting with a BioAPI unit provided by a different vendor (typically a hardware device and its driver, thus minimizing the work needed by hardware suppliers to become part of a biometric system).

10.5 The BioAPI interworking protocol (BIP)

The BIP provides bits-on-the-line communication to enable an application in one BioAPI system to interact with BSPs in a remote BioAPI system. This extension of the BioAPI architecture forms part of the transmission subsystem described in 7.2.2 (see Figure 3) (see ISO/IEC 24708 for further information).

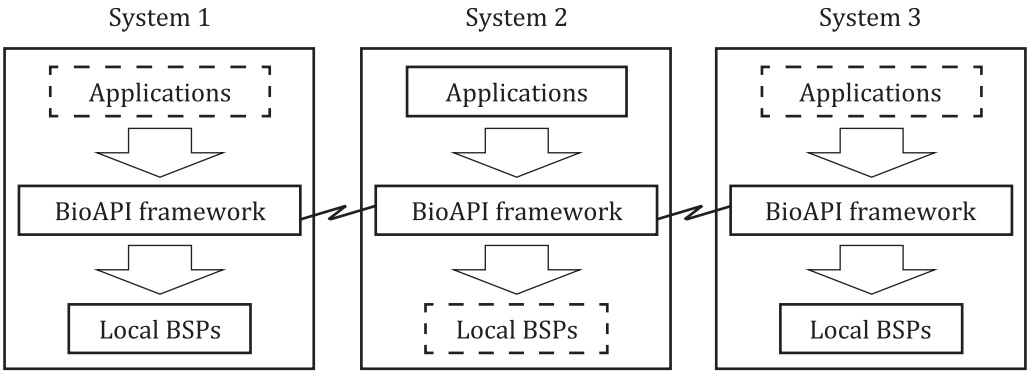

Figure 3 — Use of the BIP for communication between systems

11 Biometrics and information security

11.1 General

Biometrics can have an important role in information security, as it is much more closely linked to a subject and more difficult to forget, give away or lose than a token, a PIN or password. Use of biometrics can provide additional evidence that a credential belongs to the individual to whom it was issued. However, biometric technologies are not a panacea, eliminating the need for PINs, passwords, and tokens.

In architecting a system for verifying a positive biometric claim, a decision needs to be made regarding whether:

— each individuals' biometric reference will be carried by the individual themselves on a token, and if so, whether the reference will be stored in processed form as a template or in the same form as acquired, such as an image;

— whether the reference will be stored centrally in a database linked to the point of service by a communications system (see 10.5).

The first approach has positive implications for privacy (see Reference [30]), but if biometric references are stored centrally, several different questions arise.

a) Will the acquired biometric sample be sent to the central system or will the central system pass the reference to the point of service for processing? In either case, some strong form of encryption is required to protect the data during transmission.

b) If the biometric sample is sent from the point of service to the central site, will it be in raw form or as biometric features? If the latter, computational power and knowledge of the feature extraction algorithm is required at each point of service, but the demand for transmission bandwidth is reduced.

c) How will the encrypted data be unencrypted when necessary for comparison?

d) How will the individual trust the point of service to be legitimate and not to be storing the biometric data after transmission?

Although these issues are not insurmountable, they demonstrate that the use of biometrics does not eliminate the usual security issues.

11.2 Security of biometric data

An individual's captured biometric data (and other personal data attached at the time of collection), including facial appearance, should be confidential and not subject to unauthorized access, use and modification, or disclosed to unauthorized entities. Ideally, the encryption of the biometric data should occur immediately

upon creation of the biometric file as this is an important consideration for both the transmission and storage of biometric data.

The integrity of the biometric data across the various processing subsystems in the biometric system is critical. For example, if the integrity of the data is compromised resulting in an untrustworthy biometric reference, subsequent verification and identification processing results are also untrustworthy.

If an individual's biometric reference is subject to identity theft and compromised by a successful presentation attack or replay attack, the persistence of the biometric characteristics from which the reference is derived means that it is very difficult to revoke the stolen reference and enrol a new one. Therefore, methods for mitigating the risk of compromised biometric references include presentation attack detection and provisions for revocable and renewable biometric references (RBRs).

Confidentiality, integrity, renewability and revocability of biometric data are achieved through the application of classical cryptographic techniques and homomorphic cryptographic techniques (see ISO/IEC 24745).

Various forms of cryptographic encryption algorithms (ciphers) can be used for providing confidentiality of stored data. The encryption algorithms are applied to the biometric data to produce encrypted data and are designed such that the encrypted data yields no information about the biometric data. There is a corresponding decryption algorithm, which transforms the encrypted data into its original form. Ciphers work in association with keys. Where the key is the same for both encryption and decryption, the cipher is symmetric. Where they are different for encryption and decryption, the cipher is asymmetric. The public key infrastructure for encrypting biographic and biometric face image data on e-Passports uses asymmetric ciphers.

To safeguard the integrity of transmitted biometric data, message authentication code (MAC) algorithms are used to verify that biometric data has not been subject to unauthorized alteration. These algorithms provide integrity and authenticity assurances on a transmitted message by detecting message changes and also affirming the origin of the message. As a MAC does not provide non-repudiation, digital signature schemes are employed where this is required.

There are also methods available for processing data to provide both confidentiality and integrity protection. They typically involve either specific combination of encryption and a MAC computation or the use of an encryption algorithm in a special way. ISO/IEC 19772 specifies six methods for authenticated encryption with three key security objectives:

— Data confidentiality: Protection against unauthorized disclosure of data.

— Data integrity: Protection that enables the recipient of data to verify that it has not been modified.

— Data origin authentication: Protection that enables the recipient of data to verify the identity of the data originator.

All six methods require the originator and the recipient of the protected data to share a secret key.

Renewable and revocable biometric references are achieved through the concept of pseudonymous identifiers (PIs). PIs are anonymous and renewable biometric identity verification strings in a predefined context (see Reference [8]). A PI is derived from a data subject's biometric characteristics. Features extracted from a data subject's captured biometric sample are processed by a pseudonymous identified encoder, which generates a pseudonymous identifier and auxiliary data (AD), providing an RBR. Once this reference is generated, it can be stored and the captured biometric sample and extracted features discarded. For subsequent verification processes, features are extracted from a captured biometric sample and a PI re-coder is applied generating a probe PI based on the extracted features and the AD component of the RBR. The reference PI and probe PI are then compared. They will only match if the correct biometric characteristics are presented and the correct AD is used.

In addition to enabling the reference probe comparison, the AD component of the RBR can be used to serve a number of purposes, including:

— generation of multiple independent PIs from the same captured biometric sample to provide a sufficient number of diversifications for the biometric characteristics of an individual and, therefore, an RBR capability within the same application context;

— generation of independent PIs from the same captured biometric sample with minimal common information between the PIs to prevent biometric comparisons and linking across applications where they are used.

Depending on the security requirements for the biometric system, RBRs can either be used or not used. Where RBRs are not used, the generalized model for the biometric system at Figure 1 applies. Where RBRs are used, the generalized model is varied as shown in Figure 4 (adapted from ISO/IEC 24745):

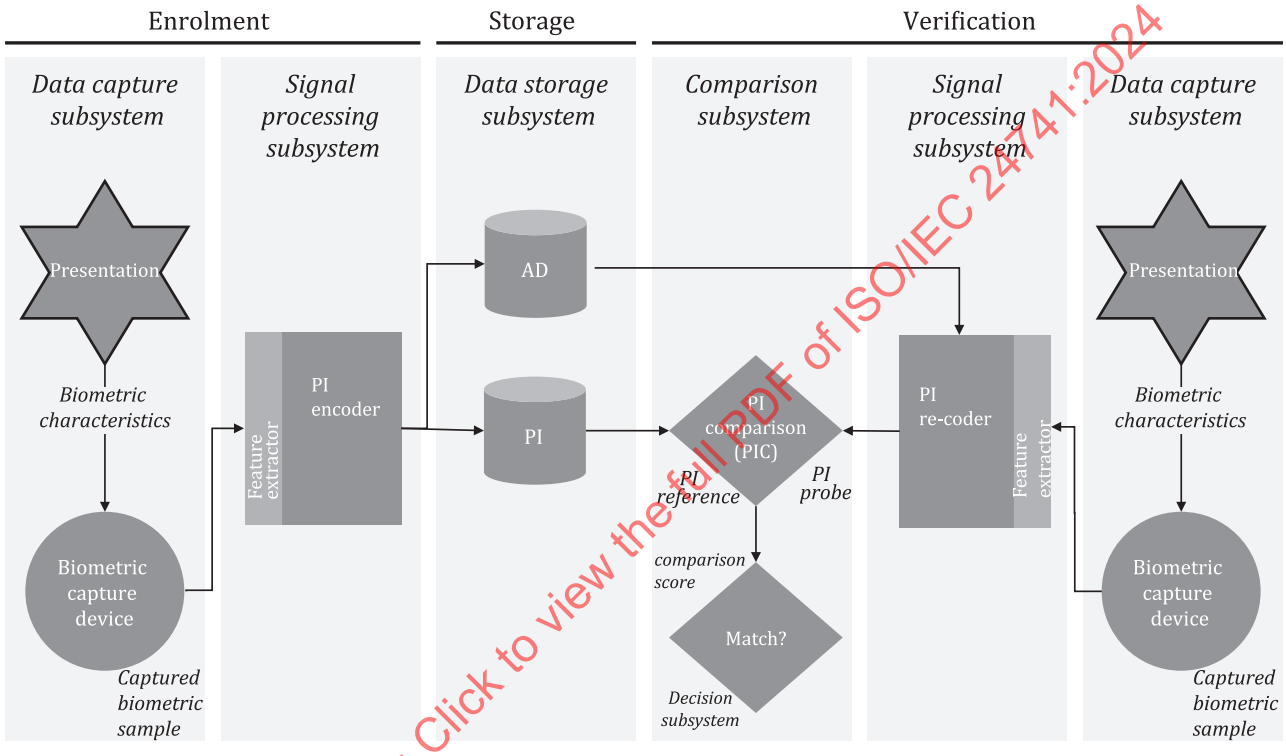

Figure 4 — Generalized model of biometric system using RBRs

The generalized model and RBR models can be implemented in various ways based on where the biometric reference is stored and where the comparison of the reference with the probe is made and, in the case where RBRs are implemented, where the PI and AD components are stored. In this context, possible topologies include:

— Model A: Store on server and compare on server;

— Model B: Store on token and compare on server;

— Model C: Store on server and compare on client;

— Model D: Store on client and compare on client;

— Model E: Store on token and compare on client;

— Model F: Store on token and compare on token;

— Model G: Store distributed on token and server, compare on server;

— Model H: Store distributed on token and client, compare on client.

Each model has its own security and privacy advantages and disadvantages. See ISO/IEC 24745 for a detailed description of these models.

11.3 Presentation attack (spoofing) detection

Notwithstanding the methods for biometric data protection, it has been well known since the 1970s that biometric devices can be fooled by forgeries.[33],[38],[51] "Spoofing" is a term that has been commonly used for presenting a forgery of another individual's biometric characteristics, in order to be recognized as that individual. ISO/IEC 30107-1, which focuses on biometric-based attacks on the biometric data capture subsystem, uses the term "presentation attack", which points to what can be done with a biometric presentation to subvert the intended operation of a biometric system.

Two basic types of presentation attacks are identified:

— where an individual intends to be recognized as an individual other than themselves;

— where an individual intends not to be recognized as any individual known to the system and so conceals their biometric characteristics.

In both cases, the individual is termed a subversive user.

To be recognized as another person by a biometric system, a subversive user can perform a biometric sensor attack by coercing another individual to present their biometric characteristics or through impersonation. In a coercive attack, the biometric data subject's biometric characteristics are presented to the sensor without their permission. This can be through force or some other means. In an impersonation attack, an individual changes their biological or physical characteristics (for example, their appearance) in an effort to match that of an enrolled data subject. An individual can also conceal or disguise their biometric characteristics to avoid recognition. For example, in a face recognition system, caps and sunglasses can be worn to conceal the face. An individual can also distort their biometric characteristics, for example by placing glue on their fingers or wearing artificial or patterned contact lenses. Forging the biometric characteristics of another individual is more difficult than disguising one's own characteristics, but is possible nonetheless.

Several studies[9],[37],[57],[61] discuss ways by which facial, fingerprint and iris biometrics can be forged. Presentation attack detection is possible for several biometric modes, for example:

— speaker recognition systems can request that the subject say numbers randomly chosen by a computer;

— iris systems can check for the presence of pupillary oscillation;

— fingerprint systems can check for blood flow.

However, it is difficult to conduct effective presentation attack detection without increasing the false reject rate. The likelihood of forgery can be reduced through the collection of multiple biometric instances or modes (e.g. ten fingers, or iris and face), along with trained operators. Coercive presentations can be difficult to detect. Some modalities enable measurement of coercion indicators, such as voice stress, extreme pulse rate or facial emotion.

11.4 Integrity of the enrolment process

The use of biometrics does not reduce the need to appropriately confirm applicants' identity information or authorizations. A biometric system can neither verify the external truth of the enrolled identity itself nor establish the link automatically to an external identity with complete certainty. Determining a subject's "true" identity, if required, is done at the time of enrolment through trusted external documents, such as a passport, birth certificate or (depending on national regulations) an identity card or driver's licence. The biometric characteristics link the subject to an enrolled identity and associated authorizations and affordances that are only as valid as the original determination process.

Not all systems, however, have a requirement to know a subject's "true" name or identity. Biometric characteristics can be used as pseudo-anonymous identifiers and, consequently, have potential for privacy enhancement of authorization systems.

All biometric characteristics can change over time, due to aging, injury or disease. Therefore, re-enrolment can be necessary. If continuity of identity is required, re-enrolment necessitates presentation of trusted external documentation or credentials. Enrolment template update mechanisms can also be employed to periodically update enrolment references from biometric samples acquired in transactions subsequent to enrolment. The aim of template updating is to automatically adapt a biometric reference over time. This takes into account the variation of the biometric data presented on each occasion, for example due to ageing, in order to minimize the impact of such variations on recognition performance.

12 Biometrics and privacy

12.1 General

Recognition by close observation of the body can cause privacy concerns for some people. Privacy is a legally and culturally determined concept which can directly affect the success of any biometric deployment.

Legal definitions of privacy vary from country to country and, in the US for example, even from state to state (see Reference [2]). A classic definition is the intrinsic "right to be let alone" (see Reference [62]), but modern definitions encompass informational privacy and the rights of individuals to establish appropriate boundaries that constrain communication of personal information. A third, more recent concern, is to protect the individual from having their identity stolen, or to be reliably and quickly informed after an accident or incident.

The increasing pervasiveness of web and mobile technologies means that more individuals are transacting electronically for social and economic reasons on the basis of personal information that they are required to provide, including biometric information. The safeguarding and the controls in place for the access, use, disclosure and discarding of that information are a concern for many.

Various national and international legal and normative instruments relating to the privacy of personal data are based on a set of transparency principles that inform individuals:

— when personal data will be collected;

— who is requesting the data and the reason for their request;

— potential third party disclosure and under what circumstances;

— how they can verify accuracy and request changes;

— how their data will be protected from unauthorized access, modification, use and disclosure;

— the parties to whom the data has been disclosed;

— how long the data provided will be stored in all of the places it is stored before it is required to be permanently deleted.

NOTE Some jurisdictions define biometric information as sensitive personal information, placing more stringent requirements on entities using biometrics. For example, in the EU, Regulation 2016/679 (General Data Protection Legislation)[15] and in Australia, the 2014 update to the Privacy Act 1988, both specifically identify biometric information as sensitive personal information.

The objectives of these various instruments are the protection of the personal rights of those whose data are processed and the protection of data subjects, not simply the protection of data. Using a biometric system means, in most cases, using personal data, which in turn means operating within the privacy governance regime generally established by national laws. Depending on how a system is deployed, use of biometrics can either threaten or protect a data subject's privacy. The possibility of protection is especially valid in view of the special properties of biometric characteristics, which are intrinsically linked to the subject, unlike PINs and passwords, which are only indirectly and weakly linked to an individual. Therefore, by using biometric technologies, other types of personal data can be better protected from theft and misuse than by traditional means. Biometrics can therefore be both an object to be safeguarded and a tool to enhance the safeguarding.

12.2 Privacy protections for biometric applications

The key privacy protections that are generally considered for the applications of biometrics are:

— the proportionality of the application of the biometric data collected;

— the acceptability in the subject population of the biometrics employed given cultural, religious and, therefore, privacy sensitivities;

— the confidentiality of the biometric data provided by the individual;

— the integrity of the biometric data provided by the individual;

— the irreversibility of the biometric data generated from the biometric samples provided by the individual;

— the unlinkability of the biometric data in contexts outside of permissions agreed to when the biometric samples were provided by the individual;

— the renewability of the biometric reference created from the biometric samples provided by the individual in case they are compromised;

— the prohibition of processing of biometric data except in exceptional cases;

— explicit consent from the data subject to the processing of data for one or more specific purposes;

— the data subject manifestly made those data public;

— the processing is a legal necessity.

In general terms, the implementations of these protections are guided by a number of general principles, which are considered privacy enhancing, including:

— limit the storing and use of personal data;

— use encryption if using personal data;

— destroy raw data as soon as possible;

— anonymize personal data wherever possible;

— do not use central databases where they are not required;

— give subjects control over their personal data;

— use a means of evaluation and certification to verify that an application delivers a guarantee of an appropriate level of trust.

See ISO/IEC 24714 for further information.

Biometrics can thus be used as a privacy enhancing technology (PET). The principle of PETs applies to biometrics from two standpoints. First, the implementation and application of biometrics has to follow a correct privacy regime in order to be privacy enhancing. Second, biometrics itself can be a privacy enhancing method. Whether or not identification is necessary for each of the processes of the conventional information system is the main question with regards to the concept of PETs, as well as in general in the application of biometrics, following the proportionality principle. In most cases, it is not necessary to know the data subject's identity in order to grant privileges. However, there are some situations in which the data subject's identity is necessary in order to allow verification.

12.3 Proportional application of biometrics

In all biometric applications, the principle of proportionality should be applied. That means that biometric data used should be adequate, relevant and non-excessive with regard to the purposes for which it is collected and further processed. In practice this means that a biometric application is used to link the biometric reference with the necessary and sufficient attributes of the identity of an individual to assign the rights or

authorizations that the specific individual is entitled to in the application context. Such assignment occurs upon verification of a biometric claim made by the individual concerned. However, there are applications, especially in the context of border protection, fraud and forensics, where individuals are subject by law to identification processes, and they are not always cooperative. Further, rights or authorizations can be denied if the identification process results in an assessment by an authority that there is an unacceptable risk to the community if the rights or authorizations are afforded. So, the notion of proportionality extends to the basic purpose of the identification process (see Reference [31]).

12.4 Biometric technology acceptability

The acceptability of biometric technology is deeply related to personal preferences, values and norms which are influenced by historical, societal and cultural backgrounds. Not surprisingly, there are differing preferences, values and norms across geographic areas and populations, resulting in differences between the acceptability of different biometric technologies.

Some biometric technologies require physical contact (for example, with a fingerprint capture device), which is no different from the use of a keypad to enter a PIN. Some require a light to shine into the eye (retina images). But many technologies are very non-intrusive, such as face recognition and iris scans. Nonetheless, there are some cultures where it is objectionable to display a face to a camera. Thus, a range of biometric technologies will need to be employed if all preferences, values and norms are to be accommodated.

It can be argued (see Reference [3]) that a physical body is not identical to the individual that inhabits it. Whereas PINs and passwords identify individuals, biometrics identifies the body. Biometric characteristics can allow linking of the various identities that each of us manifests in our separate dealings within our social structures. Biometrics, if universally collected without adequate controls, can help to link employment records to health history and to church membership, for example. Whilst the investigation of such linkages can be a valid research activity, this research typically anonymises the data used. Similar safeguards are needed when the use of biometric technologies becomes widespread.

12.5 Confidentiality of biometric data

Identity theft and identity fraud are serious, growing problems. There are many mechanisms in use today to ensure that no one individual can operate under many different identities, and to ensure that a person's privacy, rights, and privileges cannot be compromised by others masquerading under their identity. Therefore, it is essential for the privacy of biometric data stored as part of an individual's identity data record that these data be kept confidential.

Confidentiality of biometric data overlaps with security of biometric data (discussed in 11.2) and is typically achieved by:

— storing biometric references (or parts thereof) on a personal token or card instead of using centralized databases to prevent privacy threats resulting from a security breach of the centralized database (for example, when an adversary obtains illegitimate access to a centralized database and publishes its contents);

— encryption of biometric references using a key only known to either the operator of the application or the data subject, or both.

12.6 Integrity of biometric data

Given that rights and authorization can be afforded or denied an individual in decision making processes following the assessment of biometric comparison results, it is critical for the operator of the biometric system, decision makers and the individual concerned that the integrity of the biometric data is maintained at all times. Decisions based on untrustworthy biometric data have the potential to deny individuals' rights and authorizations and lead to unnecessary intrusions into their personal and private lives.

As discussed in 11.2, employing MAC algorithms or digital signature algorithms can achieve integrity of the biometric data.

12.7 Irreversibility of biometric data

It is possible that an observer of the biometric information, particularly raw biometric information as can be contained in a captured biometric sample, can interpret it to mean that an individual has certain medical conditions or that the individual is of a particular ethnicity or religion. This is generally considered personal and highly sensitive information.

When creating biometric templates from captured biometric samples for reference or comparison purposes, feature extraction algorithms perform data reduction and redundancy removal. This increases the difficulty of using the extracted features to obtain medical or racial data. These data minimization approaches seek to mitigate the risk of information leakage from the biometric data. However, at least until 2007, no systematic research has been carried out with respect to retaining additional information in templates and the extent to which information, such as medical history, can still be derived (see Reference [31]). It is known that the knowledge of a trained PCA eigenspace coupled with the PCA eigenvalues for an individual allows reconstruction of the individual's face (see Reference [1]). Fingerprint minutia information can also be reverse engineered from templates and used to create artificial fingerprints (see Reference [27]).

In recent times, significant research has been directed to methods which make it computationally harder to retrieve biometric features from the stored templates. Current methods to achieve this include:

— encryption using a key only known either by the operator of the system or by the data subject, or both, prevents external observers having access to the biometric data;

— using PIs and irreversible transforms to provide a means to prevent access to the biometric characteristics of the data subject.

12.8 Unlinkability of biometric information

Using biometric data for purposes other than that communicated to an individual at the time of collection presents various risks for that individual. For example, the biometric data can be used to identify links in information held by various organizations that are not within the scope of the purpose for which the data was originally collected. This can result in an individual being disadvantaged in some way. For example, being denied credit on the basis of credit information obtained from financial institution data holdings using the biometric data as the linking mechanism.

To mitigate risks to the individual from unauthorized linking attempts, various mechanisms can be employed, either separately or in combination, including (see ISO/IEC 24745):

— encryption of biometric references employing different, secret keys or mechanisms across applications;

— independent PIs created from a biometric reference (diversification);

— logical or physical separation of the enrolment data record and the corresponding biometric reference data record, or PI and AD components where RBRs are employed;

— the use of incompatible feature extraction algorithms or biometric data exchange formats across applications.

The strength of the unlinkability of biometric references that are derived from the same source can be quantized.[64]

13 Overview of biometric standardisation

13.1 Standards development organizations

There are a number of standards development organizations (SDOs) developing biometric standards. Most are private sector organizations. There are presently around 200 biometric standards published or under development. Almost all of these biometric standards have been developed, revised, amended, or corrected as a result of innovation, and feedback from testing and implementation over the last twenty years.

Details of technical committees (ISO/IEC or other) currently developing standards for biometrics are listed in Tables 1 to 10.

Clause 13.2 provides a representative snapshot of the types of biometric standards available and the SDOs involved. These standards are periodically reviewed and either reaffirmed, revised, or withdrawn. Moreover, amendments or corrections can occur at any time. Refer to the relevant SDOs for the latest status of these standards.

13.2 Types of biometric standards

13.2.1 Biometric data interchange format standards

The documents listed in Table 1 specify the common content, meaning, and representation of biometric data formats of biometric modalities (e.g. fingerprint, iris, face, DNA).

This list of standards is current at the time of the publication of this standard. Additionally, users are encouraged to utilize the online browsing platform (https://www.iso.org/obp/ui) for current information about ISO/IEC documents.

Table 1 — Example standards: Biometric and data interchange formats

Published and under development	SDO/Committee
ISO/IEC 19794, *Information technology — Biometric data interchange formats* *Part 1: Framework* *Part 2: Finger minutiae data* *Part 3: Finger pattern spectral data* *Part 4: Finger image data* *Part 5: Face image data* *Part 6: Iris image data* *Part 7: Signature/sign time series data* *Part 8: Finger pattern skeletal data* *Part 9: Vascular image data* *Part 10: Hand geometry silhouette data* *Part 11: Signature/sign processed dynamic data* *Part 13: Voice data* *Part 14: DNA data* *Part 15: Palm crease image data*	ISO/IEC (JTC 1/SC 37)
ISO/IEC 39794, *Information technology — Extensible biometric data interchange formats* *Part 1: Framework* *Part 2: Finger minutiae data* *Part 4: Finger image data* *Part 5: Face image data* *Part 6: Iris image data* *Part 9: Vascular image data* *Part 16: Full body image data* *Part 17: Gait image sequence data*	ISO/IEC (JTC 1/SC 37)
ANSI/NIST-ITL 1, *Data Format for the Interchange of Fingerprint, Facial & Other Biometric Information*	ANSI NIST (ITL)

The ISO/IEC 19794 series specifies the first and second generations of internationally standardized biometric data interchange formats. The first generation has been adopted widely, e.g. for biometric data stored in machine-readable travel documents. The ISO/IEC 39794 series specifies the third generation of standard biometric data interchange formats capable of being extended with additional data elements in a defined way.

The following documents remain valid until January 2040, along with the latest editions of these documents:

— ISO/IEC 19794-4:2005;

— ISO/IEC 19794-5:2005;

— ISO/IEC 19794-6:2005;

— ISO/IEC 19794-7:2007;

— ISO/IEC 19794-8:2006;

— ISO/IEC 19794-9:2007.

However, it is recommended that new fingerprint, face, iris and signature and vascular recognition deployments should follow the latest editions of these standards.

13.2.2 Biometric technical interface standards

The documents listed in Table 2 specify interfaces and interactions between biometric components and sub-systems, as well as the possible use of security mechanisms to protect stored data and data transferred between systems.

Using biometric data interchange format and biometric technical interface standards allows for data interchange and interoperability between biometric systems, which can include components of different design or manufacture.

Table 2 — Example standards: Biometric technical interfaces

Published and under development	SDO / Committee
ISO/IEC 19784, *Information technology — Biometric application programming interface* *Part 1: BioAPI specification* *Part 2: Biometric archive function provider interface* *Part 4: Biometric sensor function provider interface*	ISO/IEC (JTC 1/SC 37)
ISO/IEC 19785, *Information technology — Common biometric exchange formats framework* *Part 1: Data element specification* *Part 2: Biometric registration authority* *Part 3: Patron format specifications* *Part 4: Security block format specifications*	ISO/IEC (JTC 1/SC 37)
ISO/IEC 24708, *Information technology — Biometrics — BioAPI Interworking Protocol*	ISO/IEC (JTC 1/SC 37)
ISO/IEC 24709, *Information technology — Conformance testing for the biometric application programming interface (BioAPI)* *Part 1: Methods and procedures* *Part 2: Test assertions for biometric service providers* *Part 3: Test assertions for BioAPI frameworks*	ISO/IEC (JTC 1/SC 37)
ISO/IEC 29164, *Information technology — Biometrics — Embedded BioAPI*	ISO/IEC (JTC 1/SC 37)
ISO/IEC 30106, *Information technology — Object oriented BioAPI* *Part 1: Architecture* *Part 2: Java implementation* *Part 3: C# implementation* *Part 4: C++ implementation*	ISO/IEC (JTC 1/SC 37)

13.2.3 Biometric conformance testing standards

The documents listed in Table 3 specify the concepts, framework, test types, test methods, and criteria required to test biometric products claiming conformance to biometric data interchange records or biometric technical interfaces.

Table 3 — Example standards: Biometric conformance testing

Published and under development	SDO / Committee
ISO/IEC 18584, *Information Technology — Test methods for on-card biometric comparison applications*	ISO/IEC (JTC 1/SC 17)
ISO/IEC 24709, *Information Technology — Conformance testing for the biometric application programming interface (BioAPI)* *Part 1: Methods and procedures* *Part 2: Test assertions for biometric service providers* *Part 3: Test assertions for BioAPI frameworks*	ISO/IEC (JTC 1/SC 37)
ISO/IEC 29109,, *Information Technology — Conformance testing methodology for biometric data interchange formats defined in ISO/IEC 19794* *Part 1: Generalized conformance testing methodology* *Part 2: Finger minutiae data* *Part 4: Finger image data* *Part 5: Face image data* *Part 6: Iris image data* *Part 7: Signature/sign time series data* *Part 8: Finger pattern skeletal data* *Part 9: Vascular image data* *Part 10: Hand geometry silhouette data*	ISO/IEC (JTC 1/SC 37)

13.2.4 Biometric sample quality standards

The standards listed in Table 4 specify the use and testing of image quality metrics for a particular modality (e.g. face, iris), which impacts the accuracy of a biometric comparison. Quality metrics are useful for understanding and enhancing the performance of biometric recognition systems.

Table 4 — Example standards: Biometric sample quality

Published and under development	SDO / Committee
ISO/IEC 29794, *Information Technology — Biometric sample quality* *Part 1: Framework* *Part 4: Finger image data* *Part 5: Face image data* *Part 6: Iris image data*	ISO/IEC (JTC 1/SC 37)
ICAO TR, *Portrait Quality (Reference Facial Images for MRTD)* Significant parts of this ICAO TR are included in ISO/IEC 39794-5 as a normative annex.	ICAO TAG/MRTD NTWG and ISO/IEC (JTC 1/SC 17, & ISO/IEC JTC 1/SC 37)

13.2.5 Biometric application profile standards

The standards listed in Table 5 define conforming subsets or combinations of base standards used to provide specific functions (e.g. enrolment, verification, identification). Profiles facilitate implementations of the base standards (e.g. biometric data interchange format and biometric interface standards) for defined applications. These profile standards define the functions of an application (e.g. physical access control for employees at airports) and then specify use of options in the base standards to ensure biometric interoperability.