TECHNICAL REPORT

ISO/IEC TR 24741

Second edition
2018-02

Information technology — Biometrics — Overview and application

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

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

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

Contents

Page

Foreword

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

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

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

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

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

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

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

- terminology is revised to align with that of ISO/IEC 2382-37;
- clauses on “Overview of biometric technologies” and “Example applications” have been updated to reflect state of art;
- clauses on “Biometrics and information security” and “Biometrics and privacy” have been considerably expanded.

Introduction

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

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

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

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

Information technology — Biometrics — Overview and application

1 Scope

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

2 Normative references

There are no normative references in this document.

3 Terms and definitions

No terms and definitions are listed in this document.

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

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

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

4 Introduction and fundamental concepts

4.1 What are biometric technologies?

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

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

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

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

The perfect biometric characteristic for all applications would be:

— *Distinctive*: different across all subjects;

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

— *Accessible:* easily presented to a sensor (for example, camera or fingerprint scanner 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 must 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 in the mind of the subject. Consequently, the challenge of biometric deployment is to develop robust systems to deal with the vagaries and variations of human beings.

4.2 What biometric systems do

It has been recognized since 1970 that for some applications there are three pillars of automated personal recognition (IBM 1970[25]):

a) something known or memorized;

b) something carried;

c) a personal physical characteristic.

The original context for this concept was secure access control to computer data. The underlying assumptions were that persons authorized to access secure data would cooperatively make positive claims (e.g. "I am authorized to access data on the system") and could be counted on to protect their Personal Identification Numbers (PINs) and passwords. In such applications, biometric technologies do indeed compete with PINs, passwords and tokens, but have received less acceptance. 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 logically meet the security requirements. For example, PINs, passwords and tokens cannot logically be used in applications where enrolled individuals have little motivation to protect their accounts against use by others, such as with amusement parks. Similarly, in applications where the claim is negative (e.g. "I am not enrolled in the system as Pat") PINs, passwords and tokens cannot logically meet the requirements of demonstrating the truth of the claim.

Biometric systems recognize persons 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" persons, they can link bodies to records of attributes, which we will call "identities". Consequently, biometric recognition can become part of an identity management system.

Biometric recognition is used in two main classes of applications: 1) those that use biometric comparison to verify a biometric "claim of identity"; and 2) those that search a database of the biometric characteristics of known individuals to find and return the identifier attributable to a single individual. The former applications are called "biometric verification" and the latter, "biometric identification". Biometric systems can also be used to "cluster" characteristics, labelling together those that come from the same bodily source, 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 person presenting a biometric sample (e.g. "*I am the source of a biometric data record in the database*") or the claim can be made about the source by another actor in the system *("She is the source of a biometric data record in the database"*). The claims can be positive ("*I am the source of a biometric record in the database*"; *"These two samples came from the same bodily source*") or negative *("I am not the source of a biometric record in the database"*). Claims can be specific ("*I am the source of biometric record A in the database*") or unspecific *("I am not the source of any biometric record in the database"*). Any combination of specific or unspecific, positive or negative, first-person or third-person is possible in a claim.

To introduce the terminology of 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". We can look for a "match" between the biometric probe of an individual and an identified biometric reference stored in the database, or we can 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, we have to set thresholds for how close the comparison has to be before we can consider the biometric probe and the biometric reference 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. We talk about the proportion of such errors over the total number of comparisons, the "false match rate" (FMR) and the "false non-match rate" (FNMR) for a given technology and a given population in a given application environment.

Systems requiring a positive claim to a specific enrolled reference treat the biometric reference as an attribute of the enrolment record. These systems "verify" that the biometric reference in the claimed enrolment record matches the probe sample submitted by the subject. Some systems, such as those for social service and driver licensing, verify negative claims of no biometric data record already in the database by treating the biometric reference as a record identifier or pointer. These systems search the database of biometric pointers to find one matching the submitted biometric probe (and the process is one of biometric identification). However, the act of finding an identifier (or pointer) in a list of identifiers also verifies an unspecific 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.

In the simplest systems, "verification" of a positive claim to a specific enrolment record might require the comparison of submitted biometric probe to only the biometric reference in the single claimed record.

For example, a subject might claim to be the source of the fingerprint biometric reference stored on an immigration card. To prove the claim, the subject would insert the card into a card reader which reads the reference record, then place their finger on the fingerprint reading device. The system compares the biometric characteristics of the fingerprint on the reader with those of reference recorded on the card. The system may conclude, in accordance with defined thresholds, that the subject is indeed the source of the reference on the card, and therefore should be 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 that recorded on the card.)

Simple "identification" might 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 might be searched against the entire database of enrolled benefit recipients to verify that there are no matching fingerprints already in the system, or perhaps just the part of the database corresponding to subjects of the same sex as the applicant. If matching fingerprints are found, the enrolment record pointed to by those fingerprints is returned to the system administrator to confirm the rejection of the applicant's claim of no previous enrolment.

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

5 History

In a non-automated way, biometric characteristics have been used for centuries. Parts of our bodies and aspects of our behaviour have historically been used, and continue to be used, as a means of identification. The use of fingerprinting dates back to ancient China; we often remember and identify a person by their face or by the sound of their voice; and a signature is the established method of authentication in banking, for legal contracts and many other walks 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 (Bertillon 1889[4]). The Bertillon system involved multiple measurements, including height, weight, the length and width of the head, width of the cheeks, and the lengths of the trunk, feet, ears, forearms, and middle and little fingers. Categorization of iris colour and pattern was also included in the system. By the 1880s, the Bertillon system was in use in France to identify repeat criminal offenders. Use of the system in the United States 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 known in the western world until the 1880s (Faulds, 1880[15]; Herschel, 1880[23]) when it was popularized scientifically by Sir Francis Galton (1888[18]) and in literature by Mark Twain (1893[71]). Galton's work also included the identification of persons 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). Research on new methods of human identification continued, however, in the scientific world. Handwriting analysis was recognized by 1929 (Osborne, 1929[57]) and retinal identification was suggested in 1935 (Simon and Goldstein, 1935[67]). 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 (Potter, Kopp and Green, 1947[61]) and early 1950s (Chang, Pihl, and Essignmann, 1951[13]). With the computer revolution picking up speed in the 1960s, speaker (Pruzansky, 1963[62]) and fingerprint (Trauring, 1963a[69]) 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" (Trauring, 1963b[70]). Computerized facial recognition research followed (Bledsoe 1966 [6]; Goldstein, Harmon, and Lesk, 1971[19]). In the 1970s, the first operational fingerprint and hand geometry systems were fielded (for example, the Identimat system), results from formal biometric system tests were reported (Wegstein, 1970[77]), measures from multiple biometric devices were being combined (Messner, Cleciwa, Kibbler, and Parlee, 1974[52]; Fejfar, 1978[16]) and government testing guidelines were published (Meissner, 1977[51]).

Running parallel to the development of hand technology, fingerprint recognition was making progress in the 1960s and 1970s. During this time a number of companies were involved in automated identification of fingerprints to assist law enforcers. The manual process of matching prints against criminal records was laborious and used up far too much manpower. Various fingerprint identification systems developed for the FBI in the 1960s and 1970s increased the level of automation, but these were ultimately based on fingerprint comparisons by trained examiners. Automated Fingerprint Identification Systems (AFIS) were first implemented in the late 1970s, most notably by the Royal Canadian Mounted Police AFIS in 1977. The role of biometrics in law enforcement has mushroomed since then and AFIS are used by a significant number of police forces throughout the globe. Building on this early success, fingerprinting is now exploring a range of civilian markets.

In the 1980s, fingerprint scanners and speaker recognition systems were being connected to personal computers to control access to stored information. Based on a concept patented in the 1980s (Flom and Safir, 1987[17]), iris recognition systems became available in the mid-1990s (Daugman, 1993[14]). Today there are close to a dozen approaches used in commercially-available systems, utilizing hand and finger geometry, iris and fingerprint patterns, face images, voice and signature dynamics, computer keystroke, and hand/finger vein patterns.

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

6 Overview of biometric technologies

6.1 Eye technologies

6.1.1 Iris recognition

Iris recognition technology is now available from a variety of commercial sources and has been used successfully in border crossing, benefit programs and access control environments. Iris recognition has been successfully used in access control applications without the need for any form of identification or claim of identity by the data subject. The data subject can be verified as allowed system access by searching through the entire database of enrolled persons. 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 persons walking through a portal.

In most implementations, a grayscale image of the iris is acquired in the near-infrared (IR) spectrum to maximize detail in eyes of all colours. To ensure pupil constriction to maximize the area of the iris, acquisition 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 these 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 ⅔ of the 0s and 1s coincide, the patterns are assumed to be from the same eye. This value of ⅔ represents a threshold that can be varied to aid in balancing the false negatives and false positives.

6.1.2 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 scanner at a very close proximity, in near contact with the device. Today, retinal recognition devices are no longer commercially available.

6.2 Face technologies

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 facial recognition systems that use digital photographs or video to capture images in visible, near IR or far IR (thermal) wavelengths. Facial 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 (generally a mouth placed under a nose placed below and between two eyes).

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 much for each person from image to image) and distinctive (varying greatly between persons).

At the current level of development, facial recognition technology can work quite 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.

Three-dimensional maps of the face can be created through various means, such as through laser ranging, the projection of a grid on to the face to observe grid distortion owing to facial structure, merging of multiple images, or using shading information in a single image.

Thermal imaging analyses heat 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 infrared 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 facial recognition systems based on this technology have not been commercially available since the 1990s.

6.3 Finger and palm ridge technologies

6.3.1 Fingerprint imaging

Most fingerprint systems analyse small friction ridge features on the finger which are known as minutiae. These are defined as fingerprint ridge endings, or bifurcations (branching of fingerprint ridges). Finger image density, or the distance between ridges, may also be analysed.

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. Today, inked prints are obsolete, with fingerprints being collected electronically by placing a finger into contact with a glass surface, called a "platen". Very recently, contactless systems 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 may vary from instance to instance for many reasons. For example, finger moisture, angle of placement, pressure and ridge damage will all change the images captured. The way a subject interacts with a finger scanner is of upmost importance. This includes the height and angle of the fingerprint scanner in relationship to the data subject. Vendors are addressing these problems so that scanners are ergonomically designed 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 the 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 scanner 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”. Two “slaps” (one from each hand) are taken, 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” as described above. Law enforcement AFIS systems, also known as booking stations, capture all ten fingerprints and generally do so now electronically as described above. A civil AFIS, however, need not capture all fingerprints and can operate effectively using as few as two.

Regardless of the fingerprint imaging technology employed, the fingerprint scanner develops a matrix of numbers, each corresponding to a pixel, representing the fingerprint. The standard resolution for fingerprint images is 500 pixels per inch. The numbers in the matrix generally range from 0 (dark) to 255 (light), but some non-optical scanners may output only a matrix of 0s and 1s.

6.3.2 Fingerprint comparison

There are many ways to compare fingerprints computationally (the word “computationally” is added here to indicate exclusion of optical comparison methods developed in the 1960s and 1970s, which will not be covered in this document). The major computational approaches are: 1) transform-based; 2) local correlation; 3) minutiae-based. All three have been used in commercial systems, but minutiae-based systems are by far the most popular.

We start with the premise that 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. We will never be in a position of comparing two identical fingerprints even from the same finger. The variation of fingerprints from the same finger is called “within-class” variability and has many causes: 1) the ridge pattern has changed through injury or skin degradation; 2) the moisture level of the finger has changed; 3) different pressure was applied to the platen; 4) different finger orientation on the platen along any of the three axes; 5) changes in the imaging device.

So how can we compare fingerprints under such circumstances? Transform-based methods are generally based on two-dimensional Fourier transforms and Hough transforms applied to the matrix of pixels representing the fingerprint. 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. ISO/IEC 19794-3[33] was developed as a standard for transform-based fingerprint transmission and storage.

Correlation based methods recognize that fingerprints, and their representative matrices from the scanner, cannot simply be overlaid owing to all the variation. However, small areas of two fingerprints, when overlaid, might 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, maybe the images are of the same finger friction ridges.

Minutiae methods seek to crudely emulate what forensic examiners do. In this context, a ridge “minutiae” can be of two types: a bifurcation, or an ending. Minutiae also have a direction associated with the ridge at the point they occur. The mathematical algorithm moves over the image looking for ridges and where they split or end and make a minutiae map. To compare two fingerprints, we lay their minutiae maps on top of each other and spin/slide them around. If we can get some number of minutiae to overlay in position and direction, we call it a “match”.

6.3.3 Palm technologies

Palm biometrics can be closely aligned with finger-scanning, and in particular AFIS 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 equally as useful in criminal investigation as latent fingerprints. Other palm biometrics based not on the friction ridge structures but on the palm creases have been developed in laboratory programs.

Palm biometric characteristics are predominantly used for one-to-many identification and the capture process is essentially the same as the optical technique described for fingerprinting. A palm print system captures prints when a hand is placed on a scanner. Latent or ink palm prints can also be scanned into the system in the same way as an AFIS.

6.4 Hand geometry technologies

Hand geometry techniques have 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 infrared 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.

6.5 Dynamic signature technologies

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 sensitive 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 characteristics 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.

6.6 Speaker recognition technologies

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 may use either text-independent or text-dependent methods. In other words, the voice may 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. We are all used to speaking on the telephone and 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.

6.7 Vascular patterns

The blood vessels (veins) that exist in the subcutaneous areas of the human body form a distinctive pattern for each person. Furthermore, as blood vessels are within a human body, their vascular pattern cannot be easily obtained by other persons through use of normal photography. The underlying vascular pattern can be captured using infra-red illumination either directed onto the region to be photographed, or transmitted through the body part being imaged. The blood vessels absorb infra-red 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.

6.8 Keystroke dynamics

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 may need to cope with subjects becoming distracted or tired during the course of the day.

6.9 Scent/Odour

Recognition of persons through personal odour has long been suggested based on the proven ability of dogs in this area. Although no devices have ever been commercially marketed, they have been under development. A “sniffing” device will 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 may be distinctive enough to enable recognition.

6.10 DNA

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 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.

6.11 Cardiogram

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.

6.12 Gait and full body recognition

Gait is defined as the style or manner of walking. Gait recognition systems record video of a person walking and analyse distinctive features of the shape and dynamics of the silhouette, and/or relative positions and dynamics of joints and limbs.

7 Example applications

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 may be used in multiple sectors.

7.1 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 work places for allowing 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, 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.

7.2 Logical access control

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 readers were being built into computer keyboards and cell phones, but uptake was slow. "Match on Card" technology was available by the late 2000s. This technology stored the reference (generally, a fingerprint) and did all computer calculations required for recognition on a smart card controlled by the data subject. This solution was thought to be a privacy protective technology. Although the data subject was required to submit a biometric sample to a host computer, that sample was not stored, but was 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 matching, 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.

7.3 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 useful in the event of an emergency.

7.4 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 person in a way that cannot be later repudiated.

7.5 Electronic authorizations

A number of banks have released smart phone apps 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 may choose to not use biometrics at all.

7.6 Government/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 (UIDAI). 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 may 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 persons 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.

7.7 Border protection

7.7.1 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 characteristic for use on MRTDs. Since the around 2006, nearly all developed nations have been issuing ePassports which contain a computer chip compliant with ICAO MRTD specifications. The face image is stored on the computer chip as a JPEG file. Some countries have augmented this data with the inclusion of fingerprint minutiae templates. This has enabled use of ePassports with biometric Automated Border Crossing (ABC) systems, allowing passengers to transit through systems on which they have not been previously enrolled.

7.7.2 Automated border crossing (ABC) systems

By the mid-2010s, at least 15 countries have 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 the face image or on some passports, 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/human border control policies and procedures, and are generally supported by human oversight.

7.7.3 Visas

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

7.7.4 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 persons applying multiple times for asylum within the EU within this 10 year period.

7.8 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 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 technology to identify the source of fingerprints from crime scenes and to identify arrestees. Law enforcement databases will also frequently hold the fingerprints of persons not associated with any criminal activity, such as those in law enforcement, the military, or government positions of trust.

7.9 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.

7.10 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 person without requirement for "enrolment" or knowledge of the person 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.

8 General biometric system

8.1 Conceptual representation of general biometric system

Given the variety of applications and technologies, it might seem difficult to draw any generalizations about biometric systems. All such systems, however, have many elements in common. *Captured biometric samples* are acquired from a subject by a sensor. The sensor output is sent to a processor that extracts the distinctive but repeatable measures of the 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) may 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.

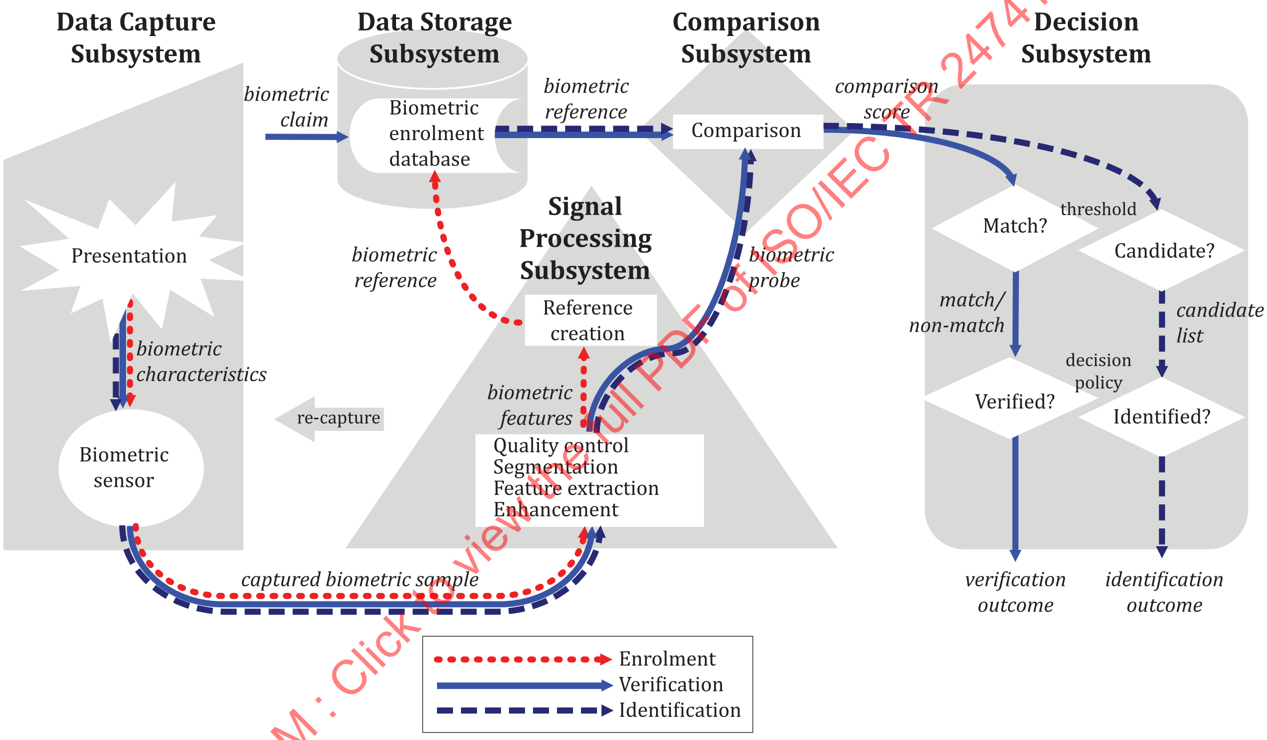

Figure 1 — Components of a general biometric system

Figure 1 illustrates the information flow within a general biometric system, showing 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. The following sub-clauses describe each of these subsystems in more detail. However, it should be noted that in any implemented system, some of these conceptual components may be absent, or may not have a direct correspondence with a physical or software entity.

8.2 Conceptual components of a general biometric system

8.2.1 Data capture subsystem

The data capture subsystem collects an image or signal of a subject's *biometric characteristics* presented to the *biometric sensor*, and outputs this image/signal as a *captured biometric sample*.

8.2.2 Transmission subsystem

The transmission subsystem (not always present or visibly present in a biometric system) will transmit *samples, features, probes* and *references* between different subsystems. The captured biometric sample may be compressed and/or encrypted before transmission, and expanded and/or decrypted before use. A captured biometric sample may be altered in transmission due to noise in the transmission channel as well as losses in the compression/expansion process. Data may be transmitted using standard biometric data interchange formats, and cryptographic techniques may be used to protect the authenticity, integrity, and confidentiality of stored and transmitted biometric data.

8.2.3 Signal processing subsystem

Signal processing may include 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; or modifying parameters for segmentation, feature extraction, or comparison.

In the case of enrolment, the signal processing subsystem 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 may 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 subsystem creates a biometric probe.

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

8.2.4 Data storage subsystem

References are stored within an *enrolment database* held in the data storage subsystem. Each reference might 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* may be reformatted into a biometric data interchange format. *References* may 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, or in a central database.

8.2.5 Comparison subsystem

In the comparison subsystem, *probes* are compared against one or more *references* and *comparison scores* are passed to the decision subsystem. The *comparison scores* indicate the similarities or dissimilarities between the *probe(s)* and *reference(s)* compared.

For verification, a single specific claim of subject enrolment would lead to a single *comparison score*. For identification, many or all *references* may be compared with the *probes*, and output a *comparison score* for each comparison.

8.2.6 Decision subsystem

The decision subsystem uses the *comparison scores* generated from one or more comparison attempts 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 may allow or require multiple attempts.

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

NOTE Conceptually, it is possible to treat multibiometric systems in the same manner as unibiometric systems, by treating the combined captured biometric *samples/references/scores* as if they were a single *sample/reference/score* and allowing the decision subsystem to operate score fusion or decision fusion as and if appropriate. (See also ISO/IEC TR 24722:2007 Multimodal and other multibiometric fusion[37].)

8.2.7 Administration subsystem

The administration subsystem governs the overall policy, implementation, configuration and usage of the biometric system, in accordance with the relevant legal, jurisdictional and societal constraints and requirements. Illustrative examples include:

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

b) storing and formatting of the biometric references and/or biometric interchange data;

c) providing final arbitration on output from decision and/or scores;

d) setting threshold values;

e) setting biometric system acquisition 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.

8.2.8 Interface

The biometric system may or may not interface to an external application or system via a Web Services Interface, an Application Programming Interface, a Hardware Interface or a Protocol Interface.

8.3 Functions of general biometric system

8.3.1 Enrolment

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

Enrolment typically involves:

a) sample acquisition;

b) sample restoration or enhancement;

c) segmentation;

d) feature extraction;

e) quality checks (which may reject the sample/features as being unsuitable for creating a reference, and require acquisition of further samples);

f) (where system policy requires it) comparison against existing biometric references to ensure the subject is not already enrolled;

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

h) storage;

i) test verification or identification attempts to ensure that the resulting enrolment is usable;

j) allowing repeat enrolment attempts, should the initial enrolment be deemed unsatisfactory (dependent on the enrolment policy).

8.3.2 Verification of a positive biometric claim

In applications such as access control, a transaction by a subject may 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"). Note that some biometric systems will allow a single subject to enrol more than one instance of a biometric characteristic (for example, an iris system may allow subjects to enrol both iris images, while a fingerprint system may require enrolment of additional fingers for fallback in case a primary finger is damaged).

Verification of a specific positive claim typically involves:

a) sample acquisition;

b) sample restoration or enhancement;

c) segmentation;

d) feature extraction;

e) quality checks (which may reject the sample/features as being unsuitable for comparison, and require acquisition of further samples);

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

g) comparison of the probe against the reference for the claimed identity producing a comparison score;

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

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

EXAMPLE In a verification system allowing up to three recognition attempts, a false rejection will result with any combination of failures during the acquisition process, or false non-matches in the comparison process, over three attempts. A false acceptance will result if a sample is acquired and falsely matched to the enrolled reference for the claimed identity on any of three attempts.

The verification function will either accept or reject 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 is the submitted sample is not matched to a reference actually created by the data subject.

Verification of an unspecific positive claim is also quite possible with a biometric system. In the 1990s, such applications were called "PIN-less verification" because no PIN or other identifier was necessary to establish that the data subject was indeed enrolled in the database. Since the late 1990s, iris recognition systems have been used in this fashion for access control. The process is as above through steps a) to f). However, steps g) to i) are somewhat different when the claim is unspecific.

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

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

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

8.3.3 Identification

In identification, a transaction by a subject is processed by the system and the enrolment database is searched to return identifiers of similar references. Identification provides a candidate list of identifiers that will contain 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 acquisition;

b) sample restoration or enhancement;

c) segmentation;

d) feature extraction;

e) quality checks (which may reject the sample/features as being unsuitable for comparison, and require acquisition of further samples);

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

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

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

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

9 Performance testing

9.1 General

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

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

b) reliability, availability and maintainability;

c) vulnerability;

d) security;

e) user acceptance;

f) human factors;

g) cost/benefit;

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

Technical performance has been the most common form of testing in the last three decades. Technical 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 (ISO/IEC 19795[34]).

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 probabilities of (i) declaring a non-match for a mated comparison of probe and reference from the same subject (the false non-match rate) and (ii) 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 must 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 are: failure-to-enrol, failure-to-acquire, false acceptance, false rejection and throughput rates. The failure-to-enrol rate is determined as the proportion of enrolment transactions in which the enrolment could not be completed because of system or human failure. The failure-to-acquire rate is determined as the proportion of acquisition processes by all enrolled subject that are not acknowledged by the system. The false rejection rate is the proportion of all verification transactions with true biometric claims erroneously rejected by the system. The false acceptance rate is the proportion of verification transactions with untrue biometric claims erroneously accepted by the system. Because false acceptance rate and false rejection 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 persons 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: Technology, Scenario, and Operational (Philips, Martin, Wilson and Przybocki, 2000[58]).

- *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 competitive technology tests in:
  - speaker verification (NIST, 1996-2012[54]);
  - facial recognition (NIST FERET, 1993-1997[55] and NIST FRVT 2000-2013[5][59][60][21][22]);

 - fingerprinting (Fingerprint Verification Competition 2000-2006,[47][48][11][12] NIST FpVTE 2003-2012[79][75]; NIST, 2004-2006[74]; NIST MINEX, 2004-2006[20]),
 - and iris (International Biometric Group, 2005[26]; NIST ICE 2004-2006[60]).

- *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 will have its own acquisition sensor and so will receive slightly different data. Scenario testing has been performed by a number of groups, but few results have been published openly (Rodriguez, Bouchier and Ruehie, 1993[65]; Bouchier, Ahrens and Wells, 1996[7]; Mansfield, Kelly, Chandler and Kane, 2000[49]).
- *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 will not be repeatable because of unknown and uncontrolled differences of operational environments. Further, "ground truth" (i.e. who was actually presenting a "good faith" biometric characteristic) will be difficult to ascertain. Because of the sensitivity of information regarding error rates of operational systems, few results have been reported in the open literature (Wayman, 2000[76]).

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 must account for and may attempt to measure these effects. Match errors, failure-to-enrol/acquire and throughput rates are determined by human interaction, which in turn depends upon the specifics of the collection environment. Human factors of biometric collection is 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[39]);
- application environment (which can affect the relative difference between mated probe and reference, making these harder to match (see ISO/IEC TR 29198[40]);
- 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 BDBs and 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[32]) 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[31] 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. Again, BIR formats have an identifier, called in this case 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.

10.2 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 Application Programming Interfaces (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 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.

There are currently two standards of interest which specify biometric services:

a) WS Biometric Devices (WS-BD), described in NIST Special Publication 500-288[53], which defines a number of primitive and aggregate services for the integration of biometric sensor devices into biometric systems that have a biometric acquisition component;

b) Biometric Identity Assurance Services, described in ISO/IEC 30108[42], which defines a number of primitive and aggregate biometric identity assurance services. 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.

10.3 Common Biometric Exchange Formats Framework (CBEFF)

The International Standard for CBEFF (ISO/IEC 19785[30]) 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 (see below). 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 may 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 be an integral number of octets; the parts in the ISO/IEC 19794[32] series specify 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 standard biometric header (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 some or all of the

CBEFF data elements defined in this document (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, which defined procedures for the operation of the Biometric Registration Authority, was withdrawn in order to avoid conflicts with the contract established between ISO/IEC and 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 meta-data. ISO/IEC 19785-4 defines the security block (SB) to provide for both integrity and encryption of the biometric data.

10.4 The BioAPI International Standard

BioAPI (ISO/IEC 19784[29]) provides an implementation architecture that supports biometric applications using software (and hardware) modules from multiple vendors.

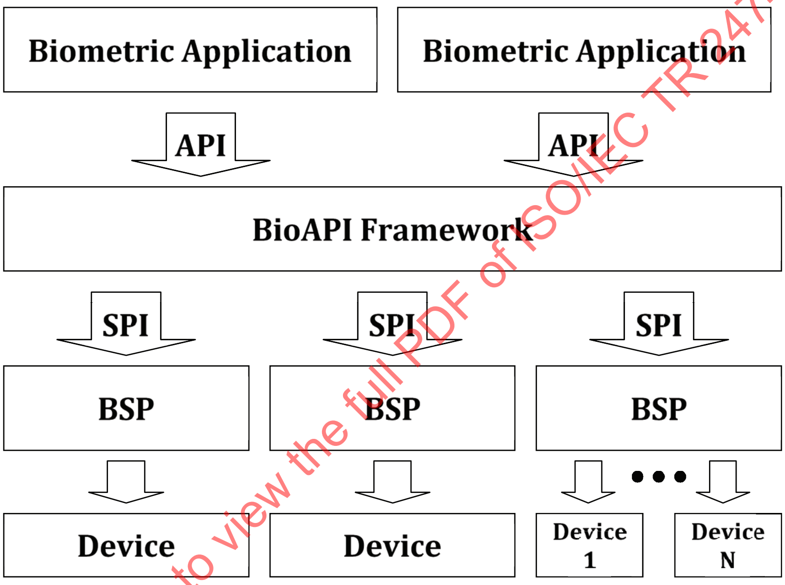

Figure 2 — BioAPI architecture

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 may 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 BIP International Standard

The BIP International Standard (ISO/IEC 24708[35]) 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 8.2.2 (see Figure 3 below).

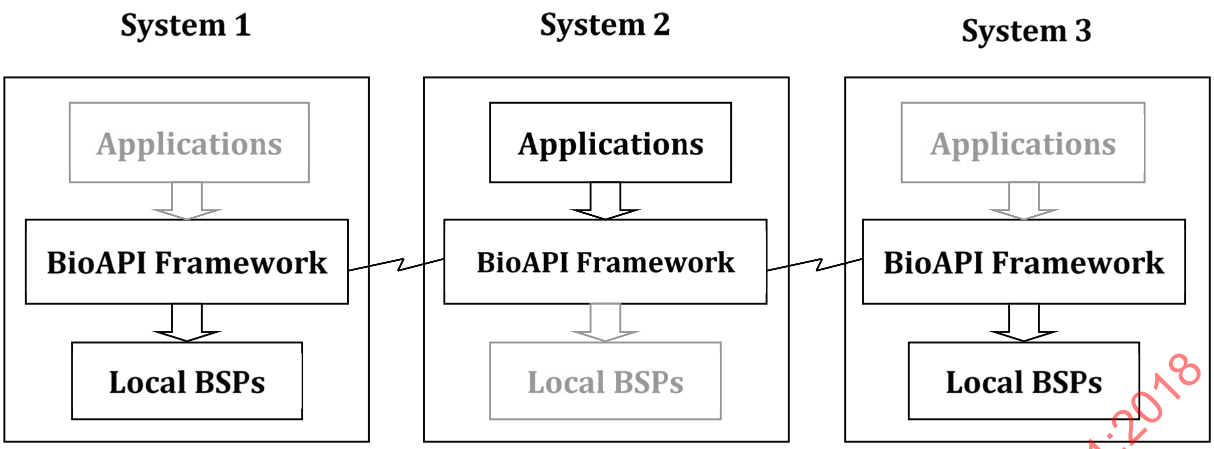

Figure 3 — Use of the BIP for communication between systems

11 Biometrics and information security

11.1 General

It should be clear by this point that biometrics can have an important role in information security, being much more closely linked to a subject and more difficult to forget, give away or lose than a token, a PIN or a password. Use of biometrics can provide additional evidence that a credential is being presented by the person to whom it was issued. However, biometric technologies do not represent a "silver bullet" eliminating PINS, passwords and tokens while resolving all security issues.

In architecting a system for verifying a positive biometric claim, we must decide whether each person's biometric reference will be carried by the person 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), or whether the reference will be stored centrally in a database linked to the point of service by a communications system (see 10.5). The former approach has positive implications for privacy (Kent and Millett, 2003[43]), 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 will be 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 will be required at each point of service but transmission bandwidth will be reduced.

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

d) How will the person 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 use of biometrics does not eliminate the usual security issues.

11.2 Security of biometric data

The requirements for the use of biometrics to verify the claim of an individual for authorizations are well documented.

Firstly, a person's biometric data should be confidential and not be subject to unauthorized access, use and modification or disclosed to unauthorized entities. This is an important consideration for both the transmission and storage of biometric data.

Secondly, the integrity of the biometric data across the various processing subsystems in the biometric system is also 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.

Thirdly, if an individual's biometric reference is the subject of an identity theft and therefore compromised, 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 including provisions for revocable/renewable biometric references are considered.

Confidentiality, integrity and renewability and revocability of biometric data are achieved through the application of cryptographic techniques (ISO/IEC 24745:2011[38] pages 13-14).

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, where this is required digital signature schemes are employed.

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[28] specifies six methods for authenticated encryption with the following 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 pseudo identities (PIs). PIs are anonymous and renewable biometric identity verification strings in a predefined context (Breebart et al, 2009[8] page 302). 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 a Renewable Biometric Reference (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 pseudo identity 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. All things being equal, 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 a renewable biometric reference 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 may or may not be employed. 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 below (adapted from ISO/IEC 24745[38] page 18):

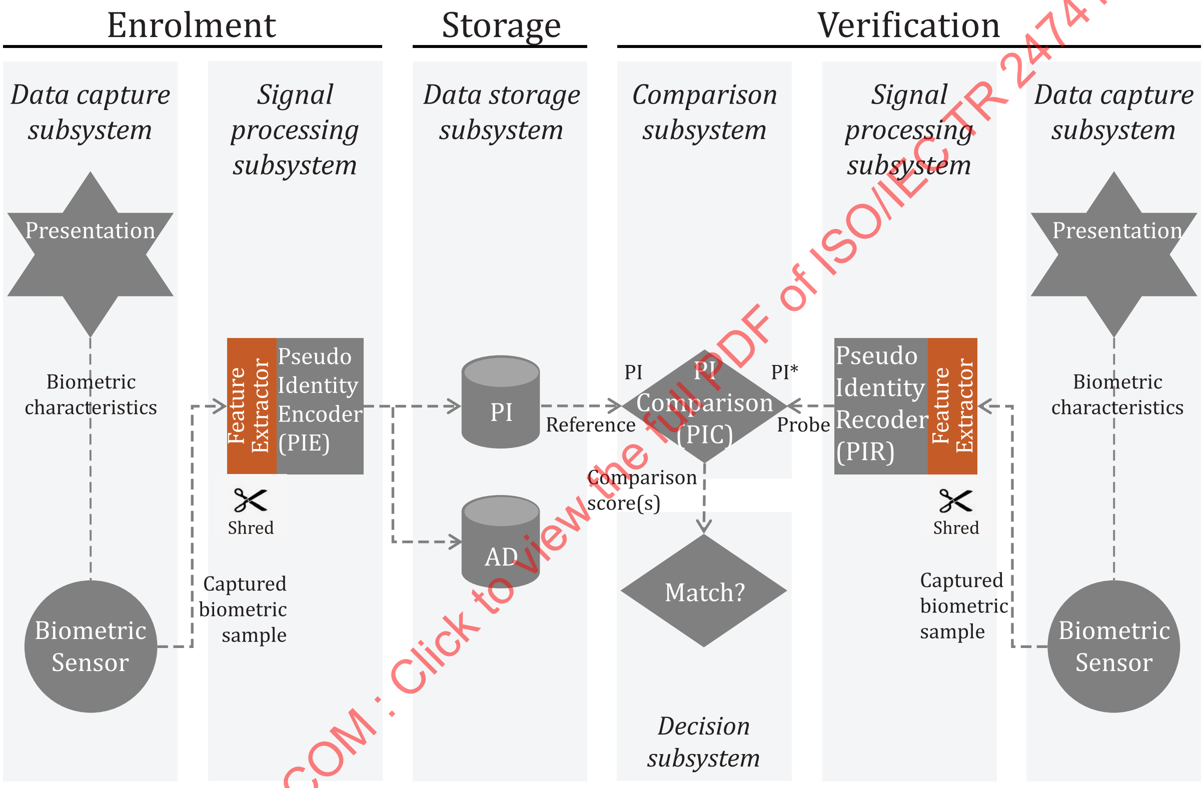

Figure 4 — Generalized model of biometric system using renewable biometric references

The generalized model and RBR models may 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 (ISO/IEC 24745:2011[38] pages 25-38):

— 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.

11.3 Presentation attacks (Spoofing)

Notwithstanding the methods for biometric data protection, it has been well known since the 1970s that biometric devices can be fooled by forgeries (Lummis and Rosenberg, 1972[46]; Raphael and Young, 1974[63]; Meissner, 1977[51]). "Spoofing" is a term that has been commonly used in literature for presenting a forgery of another person's biometric characteristics, in order to be recognized as that person. ISO/IEC 30107-1[41] 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 attack are identified:

— where a person intends to be recognized as an individual other than him/herself;

— where a person intends not to be recognized as any individual known to the system and so conceal their biometric characteristics

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

To be recognized as another person by a biometric system, a subversive user may perform a biometric sensor attack by coercing another person 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 may be through force or some other means. In an impersonation attack, a person changes their biological or physical characteristics, for example their appearance, in an effort to match that of an enrolled data subject. A person may also conceal or disguise their biometric characteristics to avoid recognition. For example, in a facial recognition system, concealment may be by the wearing of caps and sunglasses to conceal the face. A person may also distort their biometric characteristics, for example by placing glue on fingers or wearing artificial or patterned contact lenses. Forging the biometric characteristics of another person is more difficult than disguising one's own characteristics, but is quite possible nonetheless.

Several studies (Blackburn, et al 2001[5]; van der Putte and Keuning, 2000[72]; Matsumoto, Matsumoto, Yamada and Hoshino, 2002[50]; Thalheim, Krissler and Ziegler, 2002[68]; BSI, 2003[9] and BSI, 2005[10]) discuss ways by which facial, fingerprint and iris biometrics can be forged. Liveness testing (testing for forgeries) is possible for several biometric modes. For example, speaker recognition systems can make forgery difficult by requesting 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, liveness testing is a research area, and effective liveness testing without increasing false rejection rates is problematic. 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.

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 intriguing potential for privacy enhancement of authorization systems.

All biometric characteristics may change over time, due to aging of the body, injury or disease. Therefore, re-enrolment may be required. If "true" identity or continuity of identity is required by the system, re-enrolment must necessitate presentation of trusted external documentation. Both enrolment and reenrolment also require the physical presence of the enrolling person before the enrolling authority. Otherwise, there is no way to determine that the enrolled biometric characteristic came from the body of the person presenting it. Enrolment template update mechanisms might 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, including from ageing, to minimize the impact of such variations on recognition performance.

12 Biometrics and privacy

12.1 General

Recognition by close observation of the body causes discomfort in some people who may react by stating that "biometrics invades my privacy". Privacy is a legally and culturally determined concept which is extremely important and can directly affect the success of any biometric deployment.

Legal definitions of "privacy" vary from country to country and, in the United States, even from state to state (Alderman and Kennedy, 1995[2]). A classic definition is the intrinsic "right to be let alone" (Warren and Brandeis, 1890[73]), but more modern definitions include informational privacy: the right of individuals "to determine for themselves when, how and to what extent information about them is communicated to others" (Westin, 1967[78]) and the right of informational self-determination as the right to know who gets which information, when and for which purpose. A third, more recent, concern is to protect the individual from having their identity stolen, or to be reliably and quickly identified after an accident or incident.

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

Various national and international legal and normative instruments relating to the privacy of personal data are based on a set of principles including that individuals be informed (Robinson et al, 2009[64] page 1):

- when and for what purpose (scope) personal data is collected;
- who is requesting the data and the reason for their request to help them decide whether to provide and release control of all or part of such data;
- of the parties that the data they provide might be disclosed to and under what circumstances;
- how they can access data about themselves in order to verify its accuracy and request changes;
- how their data will be protected from unauthorized access, modification, use and disclosure;
- how long the data provided will be stored in all of the places is stored, including the parties to whom the data has been disclosed to, before it is required to be permanently deleted.

NOTE In some jurisdictions, biometric information is considered to be sensitive personal information, placing more stringent obligations on entities using biometrics. For example in the European Union, Directive 2016/680 on the processing of personal data, 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 is the protection of the personal rights of those whose data are processed, and the protection of data subjects and not simply the protection of data. Using a biometric system means in most cases using personal data, thus the privacy regime of national laws