

Biometrics and Standards

ITU-T Technology Watch Report
December 2009

Biometric recognition can be described as automated methods to accurately recognize individuals based on distinguishing physiological and/or behavioral traits. The report spotlights biometric recognition as a key form of authentication, one which is increasingly used in a wide range of applications made possible by advanced pattern recognition algorithms applied through powerful ICT.

ITU-T Technology Watch Reports are intended to provide an up-to-date assessment of promising new technologies in a format that is accessible to non-specialists, with a view to:

- Identifying candidate technologies for standardization work within ITU.
- Assessing their implications for the ITU Membership, especially developing countries.

Previous Reports in the series include:

- #1 [Intelligent Transport System and CALM](#)
- #2 [Telepresence: High-Performance Video-Conferencing](#)
- #3 [ICTs and Climate Change](#)
- #4 [Ubiquitous Sensor Networks](#)
- #5 [Remote Collaboration Tools](#)
- #6 [Technical Aspects of Lawful Interception](#)
- #7 [NGNs and Energy Efficiency](#)
- #8 [Intelligent Transport Systems](#)
- #9 [Distributed Computing: Clouds and Grids](#)
- #10 [Future Internet](#)
- #11 [ICTs and Food Security](#)

Acknowledgements

This report was prepared by Martin Adolph. It has benefitted from the comments and advice provided by Rapporteurs of ITU-T Study Group 17, Question 9 on Telebiometrics.

The opinions expressed in this report are those of the authors and do not necessarily reflect the views of the International Telecommunication Union or its membership.

This report, along with other Technology Watch Reports can be found at www.itu.int/ITU-T/techwatch.

Please send your comments to tsbtechwatch@itu.int or join the Technology Watch Correspondence Group, which provides a platform to share views, ideas and requirements on new/emerging technologies and to comment on the Reports.

The Technology Watch function is managed by the ITU-T Standardization Policy Division.

Biometrics and Standards

I. Introduction

As modern society increasingly depends on systems to provide secure environments and services to people, it becomes paramount to ensure the security of a system through means to identify the validity of an individual requesting access to it. This is usually established by extracting some form of information from the individual to check against information held by the system about valid users.

This ITU-T Technology Watch Report spotlights biometric recognition as a key form of authentication, one which is increasingly used in a wide range of applications made possible by advanced pattern recognition algorithms applied through powerful information and communication technologies (ICT).

Biometric recognition can be described as automated methods to accurately recognize individuals based on distinguishing physiological and/or behavioral traits. It is a subset of the broader field of the science of human identification. Technologies used in biometrics include recognition of fingerprints, faces, vein patterns, irises, voices and keystroke patterns (See Figure 1). In the subfield of telebiometrics, these recognition methods are applied to telecommunications.

In a non-automated way and on a smaller scale, parts of the human body and aspects of human behavior have been used ever since the dawn of mankind as a means of interpersonal recognition and authentication. For example, face recognition has been used for a long time in (non-automated) security and access applications, e.g., as a method to verify that the owner of a passport and the person showing the passport are the same, by comparing the person's face and the passport photo.

The Digital Revolution added ICT as a means to fulfill recognition and authentication processes, often through PCs and computerized telecommunication devices, such as cash dispensers. Users authenticate themselves to the machine by entering a secret knowledge-based authenticator, such as a PIN or passphrase, or by the possession of a token, like a bank card or key, and sometimes authentication requires a combination of knowledge and possession.

The 1960s also saw the first automated biometric recognition applications. However, the biometric industry did not take off at that time, due to high cost, low recognition accuracy and the lack of standards and testing benchmarks with which the different approaches could be compared and quality ensured.

To further the use of biometric systems, issues of security and privacy will need to be carefully addressed, as well as the high levels of expectation in accuracy, reliability, performance, adaptability, and cost of biometric technologies for a wide variety of applications.

Figure 1: Overview of some biometrics



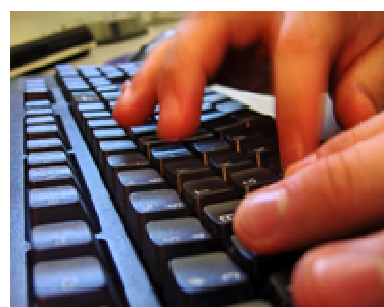
(1) Fingerprint



(2) Iris



(3) DNA



(4) Keystroke pattern

Images uploaded to Flickr by (1) [Fazen](#), (2) [Sarah Cartwright](#), (3) [ynse](#), (4) [Ben Harris-Roxas](#).

Safety, quality and technical compatibility of biometric technologies can be promoted through standards and standardization activities. Standards are essential for the deployment of biometric technologies on large-scale national and international applications.

This Report discusses the advantages of biometric authenticators over their knowledge- and possession-based counterparts, describes different physiology- and behavior-related human traits and how they are used in biometric systems. A choice of biometric recognition applications is highlighted, and an overview of standardization work in the field of biometrics is given.

II. Possess, know, be – Authentication methods

Fundamentally, authentication mechanisms that exist today use one or more of the following authenticators (factors):

- Knowledge-based – an authenticator only the individual knows, which usually refers to PIN, passphrase or an answer to a secret/security question.
- Possession-based – an authenticator only the individual possesses, which usually refers to keys, smart cards and tokens.
- Physiology-based or behavior-based – an authenticator only the individual is or can do, referring to biometrics.

Knowledge- and possession-based authentication mechanisms imply that users –in order to be granted access to a system, building, service– need to carry or remember the authenticator. When it comes to comparisons of these traditional authenticators and authentication through biometrics, it is often argued that keys could be lost, stolen or easily duplicated and passphrases could be forgotten. A critical drawback is that the link between the legitimate individual and the authenticator is weak, and the authentication system has no means to distinguish between a designated owner of the authenticator and a thief, impostor or guesser. On the other hand, the general view is that biometric traits have an advantage in that they cannot be stolen, easily guessed or forgotten.

III. Fingerprint, face, voice – Biometric traits

Biometrics are commonly categorized as either physiological or behavioral trait. Physiological traits (sometimes called passive traits) refer to fixed or stable human characteristics, such as fingerprints, shape and geometry of face, hands, fingers or ears, the pattern of veins, irises, teeth, as well as samples of DNA. Physiological traits are generally existent on every individual and are distinctive and permanent, unless accidents, illnesses, genetic defects, or aging have altered or destroyed them. Behavioral traits (active traits) measure human characteristics represented by skills or functions performed by an individual. These include gait, voice, key-stroke and signature dynamics.

The following paragraphs describe traits of both categories, which are sometimes evaluated based on such characteristics as:

- Universality – Each individual should have the biometric trait.
- Distinctiveness – Any two individuals should be different regarding the trait.
- Permanence – The biometric should be sufficiently invariant over a certain period of time.
- Collectibility – The biometric should be quantitatively measurable.

It is argued by some that none of the human biometric traits meets all the above requirements. Although each biometric trait has its strengths and drawbacks; no biometric is “optimal”.¹

III.1 Physiological traits

a) Fingerprint

Fingerprint biometrics is largely regarded as an accurate biometric recognition method. Today, fingerprint scanners are available at low cost and increasingly integrated in laptops and other portable ICT devices.

Most fingerprint recognition systems analyze the unique pattern of ridges and valleys, and the arrangement of small unique marks on the fingerprint, which are known as minutiae. They can be recognized and distinguished by their type, by x- and y-coordinates, and by their direction.

Fingerprint scanners can operate with touch-based or touchless optical systems. The former is to be found in laptops and works in a similar way to digital cameras by capturing a digital image of the fingertip using visible light. While this type of sensor provides a cheap and simple solution, it comes with some drawbacks: when a finger touches or rolls on the scanner surface, the elastic skin deforms.² The quality of the captured image strongly depends on amount and direction of pressure applied by the user and the fingerprint may appear different in every capture. In addition, when used in large-scale applications such as an immigration desk, special hygienic care needs to be exercised to avoid dirt being carried from one finger to the other.

By emitting light on or through the finger and capturing the reflected or transmitted signals, fingerprints can be taken without contact between skin and scanner. To avoid fake-finger attacks, some systems employ so-called liveness detection technology, which takes advantage of the sweat activity of human bodies. High-magnification lenses and special illumination technologies capture the finger's perspiration and pronounce the finger dead or alive.

Application planners need to take into account that fingerprints of a small part of the population cannot be utilized for biometric recognition. This can be due to age (thin skin or senile atrophy of friction skin), accidents, genetic reasons, environmental or occupational reasons (e.g., construction workers may have worn fingerprints or a large number of cuts and bruises on their fingerprints that keep changing).

b) Face

Humans distinguish and recognize faces based on location, size and shape of facial features, such as eyes, eyebrows, lips, nose, cheekbones, chin and jaw. The corresponding automated approaches to face recognition are summarized as geometry feature-based methods. Other approaches are based on image templates and compute the correlation between a locally captured face and one or more model templates to estimate similarity.

Most vendors of automated face recognition systems use proprietary algorithms to generate biometric templates. The algorithms are kept secret and cannot be reverse-engineered to create a recognizable facial image from the template. Consequently, face recognition templates are not interoperable between vendors and therefore the original captured photograph has to be kept, instead of a ready-to-use template. In the case of machine-readable passports, the original captured photograph is stored on the RFID (radio-frequency identification) chip. When passing a border or immigration desk, the receiving state uses its own vendor algorithm to compare the passport bearer's facial image captured in real time with the data read from the chip. To be recognized accurately at many borders, it is important that the template image on the chip makes visible a number of facial features and is taken under certain light and contrast conditions.

Face recognition is a non-intrusive method and can be performed with digital cameras or in combination with closed-circuit television (CCTV), incorporating remote video surveillance cameras. However, today's technology may recognize accurately from full front faces or from images taken in small angles, with simple background and special illumination, but not from different viewing angles, under poor light conditions, or if hair, sunglasses, or hats cover the

person's face.³ These limitations became apparent in larger field tests at airports and train stations.⁴

c) Iris patterns

The idea of recognizing an individual by using iris patterns was proposed by an ophthalmologist in 1936. Later, the idea appeared in some action movies, including 1983's James Bond "Never Say Never Again", but at that time it remained science fiction. In 1994, the first automated iris pattern recognition algorithms were developed by physicist and computer-vision expert John Daugman and patented, and continue to be the basis of all current iris recognition systems and products.

Before extracting and analyzing an iris pattern, the iris has to be located within an image. Landmark features, such as the outer iris boundaries and the pupil in the center of the eye help to mark the iris' borders. Once located, the iris is captured with the help of a high quality camera, which in many cases emits infrared light to illuminate the eye without causing harm to the eye or discomfort.⁵ A digital representation of the iris features (orientation, spatial frequency, position) is computed (the IrisCode), stored and –in the application– compared.

It is extremely difficult to surgically tamper the texture of the iris, and spoof attacks (e.g., with prepared contact lenses) are detectable rather easily.⁶ On the downside, iris recognition is difficult to perform from distances further than a meter and it requires active user participation.

d) DNA

At present, there exists no technology to allow for instant and automated recognition of DNA samples. DNA analysis and profiling (genetic fingerprinting) requires a lab environment and at least several hours. However, significant R&D efforts are underway to develop this technology, and also to enable governments to better use the millions of DNA profiles collected and archived in DNA databases.

III.II Behavioral traits

a) Voice print

Behavioral traits can be learned or acquired, but also include physiological elements. For instance, the human voice is influenced by the physiological characteristics of lungs, tongue, throat, etc. and its behavioral features evolve and change over time. They can be influenced by factors such as age, illnesses, mood, conversational partner or surrounding noise.

Individuals (speakers) can be recognized by their voice print, the set of measurable characteristics of a human voice. Speaker recognition and speech recognition –a similar technology that focuses on the content of the spoken input rather than on who is speaking– rely on resource-intensive algorithms, including frequency estimation, vector quantization and hidden Markov models.⁷ These are applied in text-dependent, text-prompted or text-independent speaker recognition systems, as explained below:

- Text-dependent systems: The user is requested to speak a word or phrase, which was saved earlier during the enrollment process. The spoken input is represented by a sequence of feature vectors and compared with previously recorded input vectors, to calculate the degree of similarity.
- Text-prompted systems: The user is prompted to repeat or read a word or phrase from a pre-recorded vocabulary displayed by the system (e.g., "Please say the numbers 8 2 2 1!").
- Text-independent systems: These systems have no initial knowledge/vocabulary, but need to be trained by the user to recognize accurately. In the training phase, reference templates are generated for different phonetic sounds of the human voice, rather than samples for certain words. In operation mode, the system matches the acquired pho-

netic templates and those from arbitrary input text. Text-independent systems are more difficult to design, but offer higher protection against impostors and fraud.⁸

Speaker recognition systems are a useful choice for telephone-based applications. Individuals are used to speaking on the telephone and recognition systems can be easily integrated into telephone networks.

b) Signature dynamics

Biometric signature recognition systems measure and analyze the physical activity of signing. Important characteristics include stroke order, the pressure applied, the pen-up movements, the angle the pen is held, the time taken to sign, the velocity and acceleration of the signature.⁹ Some systems additionally compare the visual image of signatures, though the focus in signature biometrics lies on writer-specific information rather than visual handwritten content. While it may appear trivial to copy the appearance of a signature, it is difficult to mimic the process and behavior of signing.

However, a person's signature changes over time as well as under physical and emotional influences. Therefore, signature recognition works most effectively when used regularly, and when the biometric template is regularly updated to reflect gradual changes.¹⁰

Since a signature is one of the most accepted means of asserting identity, main uses of signature biometrics include limiting access to restricted documents and contracts, delivery acknowledgement and banking/finance related applications.

Signature data can be captured via pens that incorporate sensors or through touch-sensitive surfaces which sense the unique signature characteristics. Touch-sensitive surfaces are increasingly being used on ICT devices such as screens, pads, mobile phones, laptops and tablet PCs.

c) Keystroke dynamics

The recognition of keystroke dynamics is the process of analyzing the way an individual types at a terminal by monitoring the keyboard inputs thousands of times per second in an attempt to recognize the individual based on habitual typing rhythm patterns.¹¹ Keystroke dynamics are described by speed (the time a key is pressed, the time between keys pressed), rhythm, precision, keys used (e.g., left Shift key or right Shift key, Caps Lock), and other typing characteristics.

Similar to other active traits, an individual's keystroke rhythm evolves over time, for instance by switching from two finger typing to touch typing. Subjects can become tired or distracted during the course of a work day, which in turn affects the typing rhythm. Recognition accuracy would be very limited if only a small number of variables were considered. The longer the text entered the more characteristics revealed and the more accurate recognition can be.¹² The ultimate aim is to be able to continually check the identity of an individual typing on a keyboard.¹³

The equipment requirements are minimal (keyboard) and give information about the huge field of possible applications. For instance, Psylock, a keystroke recognition system developed at University of Regensburg (Germany), uses a JavaScript function to capture the user's keystroke dynamics on the client side (using a web browser), transmits the data on an encrypted connection (SSL) to an authentication server, which replies to authentication requests.ⁱ The university successfully used the system to authenticate users for service desk tasks (password reset); it was also proposed as an alternative to transaction authentication numbers (TAN) in home-banking applications.

ⁱ More information available at <http://www.psylock.com/>.

IV. Capture, compare, decide – Biometric systems

In addition to selecting a feasible biometric for an application, its interplay with a biometric system is a crucial factor for deployment decisions. The following desired quality factors may influence the choice of a specific biometric for an application:

- Performance – The measurement of the biometric trait is robust, accurate, fast and efficient.
- Acceptability – The extent to which individuals are willing to accept the use of a particular biometric trait in an application.
- Circumvention and Reliability – Extent to which the system can be manipulated by using fraudulent methods.
- Cost.

It is obvious that some of these factors are intangible and may depend on the perception of each user. For instance, the question of whether a biometric application is acceptable or not may be linked to the user's cultural background, attitude to privacy and to technology, etc. Accuracy and performance, however, can be quantified and compared. This section describes biometric systems, its components, operation modes and rates that measure its performance.

A biometric system is a pattern recognition system that operates by acquiring biometric data from an individual, extracting a feature set from the data acquired, and comparing this sample against an earlier registered template. Depending on the type of application the template may be stored in the system's database or on a token, such as a smart card.¹⁴

All biometric systems use common main functional components, which include:

- Storage entity with the biometric data samples (templates) of the enrolled individuals that is linked or integrated in a database with the identity information of the corresponding individuals.
- Biometric sensor device and pre-processing capacities to capture the biometric sample data from an individual as input data.
- Comparison process evaluating the similarity between reference template and captured data sample, and then calculating a matching score.
- Decision function that decides if the data sample matches the reference template.

In addition, the communications channels between these components are of great importance. In telebiometrics, these can include wired or wireless telecommunication environments, and private or public networks, including the Internet.

The matching decision is a fundamental element of the biometric system. It is made on the basis of the matching score and a threshold value. The matching score is typically a single number on a scale from low to high, measuring the success that a biometric probe record (the individual being searched for) matches a particular gallery record (a previously enrolled individual). The threshold value is a benchmark score above which the match between the stored biometric and the individual is considered acceptable or below which it is considered unacceptable.

In contrast to a key (which fits or not) or a password (which is correct or not) a biometric match is never a complete match, but only a statistical probability. The matching probability in biometric systems is always below 100 per cent, which results from intra-class variability, inter-class similarity, noisy sensor input, and template variations. Intra-class variability can be observed in biometrics of one individual, for instance the face, due to change in pose, expression, lighting and eye glasses. Inter-class similarity can be observed in the face pattern of members of the same family. Template variations can be caused by the human aging process, by an injury or disease, or simply by a visit to the barber.

These limitations need to be considered by manufacturers and operators of biometric systems. Two rates are used to describe the ability of a biometric system to authenticate its users.

1. False match rate (FMR) describes the probability that a biometric system will incorrectly authenticate an individual or will fail to reject an impostor. It measures the percentage of invalid matches.
2. False non-match rate (FNMR) specifies the probability that a biometric system incorrectly declares failure of match between input sample and matching template. It measures the percentage of valid inputs being rejected.

The achievable characteristic rates vary for the different biometric traits described in the previous section. For instance, some organizations that tested iris recognition in large-scale tests involving millions of iris pairings have reported a FMR of 0.¹⁵ However, to design national-scale and international-scale deployments as inclusive as possible much greater demands are also being placed on the FNMR, because it is considered unacceptable to exclude members of outlier populations who, for various reasons, may have a nonstandard eye appearance or who simply have difficulty presenting to the camera. Ideally, both error rates would equal zero.

Advancements in processing power, sensor design and algorithms have led to considerable improvement in the accuracy of biometric systems. For face recognition systems operating at a defined FMR of 0.1 per cent (1 invalid match in 1,000 attempts), the FNMR was reduced from 79 per cent in 1993 to 1 per cent in 2006 (controlled illumination conditions, high-resolution images). Uncontrolled illumination conditions, moving objects, and recognition at a distance remain major challenges for research in biometrics.¹⁶

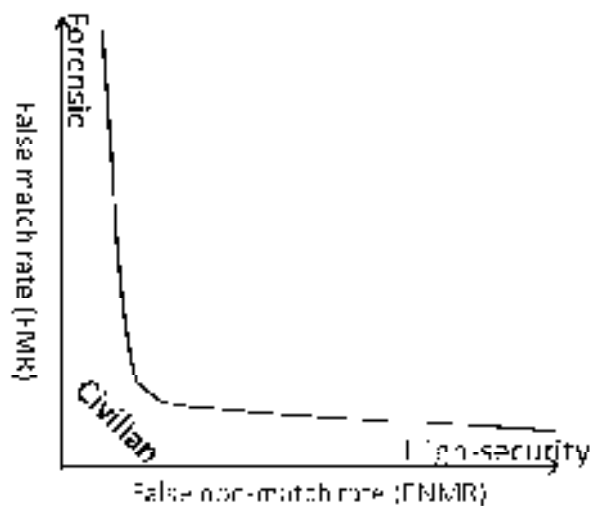
FMR and FNMR are typically traded off against each other, usually to increase either security or convenience/inclusiveness. Both are functions of the threshold value, which can be raised to a system-dependent level to make the biometric system more secure by reducing the number of false matches. However, at the same time the number of false non-matches increases and more valid users are rejected. The other way around, more impostors may gain access, if the threshold value is chosen at a lower level to make the application more convenient to users. This trade-off between security and convenience, FMR and FNMR, is illustrated in the receiver operating characteristic (ROC) curve in Figure 2, and the requirements of different types of applications (forensic, civilian and high security) are positioned.

High-security applications may require a very high threshold value, to keep the risk of granting access to impostors as low as possible. The operator might even accept a higher rate of valid users being rejected, only to be sure no access is granted to invalid users. Forensic applications, such as the identification of an individual from a huge population rather apply a lower threshold to avoid that the sought-after is wrongly excluded from the matches. In this case, the forensic examiner might accept to manually inspect a greater number of incorrect matches. The threshold used in civilian applications is found somewhere in the middle, depending on the application, closer to security or comfort.

Although used in many different kinds of applications, biometric recognition systems operate in two fundamental modes:

In verification mode an identity claim made by an individual is verified or refuted

Figure 2: Exemplary receiver operating characteristic (ROC) curve of a biometric system.



by the biometric system by comparing a 'freshly' given biometric sample with a previously enrolled sample of the claimed identity. The individual who desires to be recognized claims an identity by entering a name, password, PIN or by presenting a token such as an ID card. A possible claim could be: "I am holding the key card which is issued to me and I am entitled to enter the high-security computer center." This claim could be verified by comparing the biometric template of the individual's fingerprint stored on the key card with the fingerprint captured in situ at the entrance of the computer center. The authentication process is strengthened by something the individual 'is' (biometric fingerprint) in addition to something it 'possesses' (card). Verification is typically used for positive recognition in order to prevent multiple individuals using the same identity (e.g., unauthorized individuals using a key card to access the computer center).

In identification mode the biometric system recognizes an individual from the entire enrolled population. Therefore, it searches all templates stored in a database for a match based solely on the biometric trait held by the individual. Identification mode is used without any additional claims. Instead, all records in the database are compared with the captured sample, and a list of records with the closest match scores is returned. The question "Who is this individual?" is answered by "Person A" or "Person B" or by "This person is not in the database". Identification, a form of negative recognition, is used in order to prevent one individual from using multiple identities. While knowledge and possession-based authentication methods only allow for positive recognition, biometrics are the only authenticators allowing for negative recognition (an individual's identity cannot be determined based on a PIN or a key, but with a fingerprint sample and a database of fingerprints).

Enrollment, verification and identification are illustrated in the block diagrams in Figure 3.

In some applications of biometric identification, the process of capturing a sample of an individual may function from a distance and without the explicit participation, involvement or knowledge of the individual. However, in order to achieve accurate recognition results, today's biometric systems require active and intentional participation.

V. Applications

Advances in ICT, increased performance and availability of equipment at lower cost have smoothed the way for automated biometric recognition.

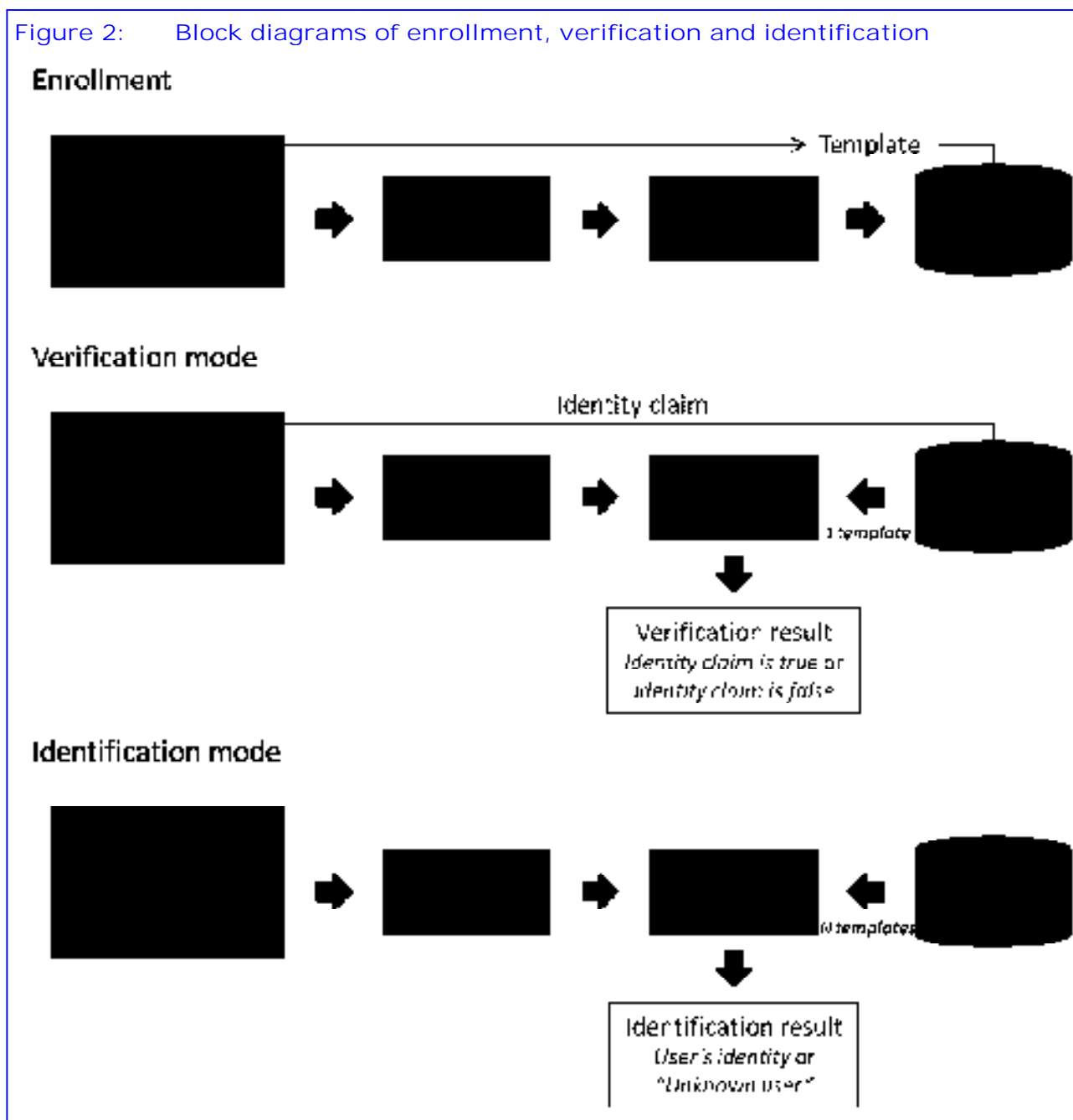
Biometric applications may be categorized into three main groups:

1. Forensic applications, in criminal investigations, e.g., for corpse identification, parenthood determination, etc.
2. Government applications, including personal documents, such as passports, ID cards and driver's licenses; border and immigration control; social security and welfare-disbursement; voter registration and control during elections; e-Government.
3. Commercial applications, including physical access control; network logins; e-Commerce; ATMs; credit cards; device access to computers, mobile phones, PDAs; facial recognition software; e-Health.

This order generally reflects the emergence and use over time of biometric recognition systems. Initially found mainly in the field of criminology and forensics, biometrics underwent a market breakthrough when governments started to integrate biometric access control mechanisms in personal documents. While access control and authentication have remained the primary purpose, other fields of application are taking off.

Google's photo organizer software Picasa and social-networking site Facebook have integrated face recognition algorithms to make it easier to search and display all photos featuring a certain person. Picasa is available as an application for several operating systems, while its photo sharing web site (Picasa Web Albums) and Facebook provide face recognition online. Biometric

Figure 2: Block diagrams of enrollment, verification and identification



systems embedded in cars of a vehicle fleet can help to identify the driver, adjust seat, rear mirrors, and steering wheel to meet individual preferences. A number of other applications are presented in Box 1.

Commercial and government applications are likely to overlap in some fields. Future e-commerce, e-health and e-government services may require authentication with the help of biometric personal documents issued by governments, as soon as they are used by a large enough part of the population. Some developing countries have used biometrics for voter registration in the run-up to elections in order to avoid out-dated voter lists and election fraud.

Market forecasts on biometric spending are generally optimistic. Growth is expected especially in commercial and government applications, where the biometrics industry and the related smart card chip industry benefit from government decisions toward the adoption of electronic

Box 1: Applications in biometrics

Electronic passports

An electronic passport (ePass, ePassport, sometimes referred to as a biometric passport) is a machine-readable travel document (MRTD) containing a contactless integrated circuit chip within which is stored data from the MRTD data page, a biometric measure of the passport holder and a security object to protect the data with Public Key Infrastructure (PKI) cryptographic technology.

The International Civil Aviation Organization (ICAO) has studied biometrics and their potential to enhance identity confirmation with passports and other travel documents since 1998, and subsequently developed technical standards for the incorporation of biometric recognition in MRTDs. In 2002, the face was recommended as the primary biometric, mandatory for global interoperability in passport inspection systems, while fingerprint and iris were recommended as secondary biometrics to be used at the discretion of the passport-issuing state. The selection of face recognition as the first choice technique raised questions and met with some criticism, due to some poor face recognition accuracy at that time. In addition, a number of security flaws were identified that allowed impostors to access, eavesdrop or modify the biometric and other personal data of the passport holder stored on the RFID chip. Most of these flaws were fixed in subsequent versions of electronic passports, for instance by strengthening basic access control (BAC) through extended access control (EAC) mechanisms, by implementing chip authentication to prevent cloning of the chip, and by establishing strongly secured communication channels between passport and reader terminals. At present, more than 60 countries—including developing and developed ones—have started issuing electronic passports.

Vascular recognition in ATMs

Japanese vendors have developed systems that verify identity claims made by individuals based on the unique pattern of veins in their palms and fingers. In order to obtain clear vein images, only specific blood flow patterns (vessels carrying oxygen-free blood to the heart) are considered.

Since 2004, this technology has been deployed in 66,463 ATMs of 289 Japanese bank groups to secure the access to more than two million accounts. Fraudulent withdrawals with fake / stolen ATM cards have decreased since 2005, when 89 per cent of fraudulent withdrawals were made with stolen cards. To authorize a transaction, the customer is required to present to the ATM a banking card, the corresponding PIN and the vascular pattern of palm or finger, which corresponds to a three-factor authentication scheme of possession, knowledge and biometric. The third factor could be used to authorize withdrawals of higher amounts. Vascular patterns are regarded as secure and tamper-proof biometric traits, as they are inside the human body. This large-scale deployment of biometrics in a commercial application proved to be successful and other banks started to equip their ATMs with biometric recognition capabilities.

Age recognition cigarette vending machines

A different approach to biometric recognition is embedded in cigarette vending machines to ensure that buyers are not underage. Facial features of the smoker, such as wrinkles surrounding the eyes, facial bone structure and skin sags, are studied by the vendor and compared to the facial data of more than 100,000 people enrolled in a database to estimate the age. The functioning is similar to the identification mode of biometric systems described above. The system may operate in favor of minors looking older than they are (the legal smoking age in Japan is 20), and to the disadvantage of “baby-faced” adults that may have to verify their age differently. In a test with 500 people ranging in age from their teens to their 60s, this software was able to identify adults with 90 per cent accuracy.



(1) Electronic passport (Germany)



(2) Finger-vein recognition in ATM



(3) Age recognition in cigarette vending machine

personal documents and biometrics. From an estimated US\$ 3 billion spent on biometric technologies in 2008, market researchers forecast investment of US\$ 7.3 billion by 2013.¹⁷

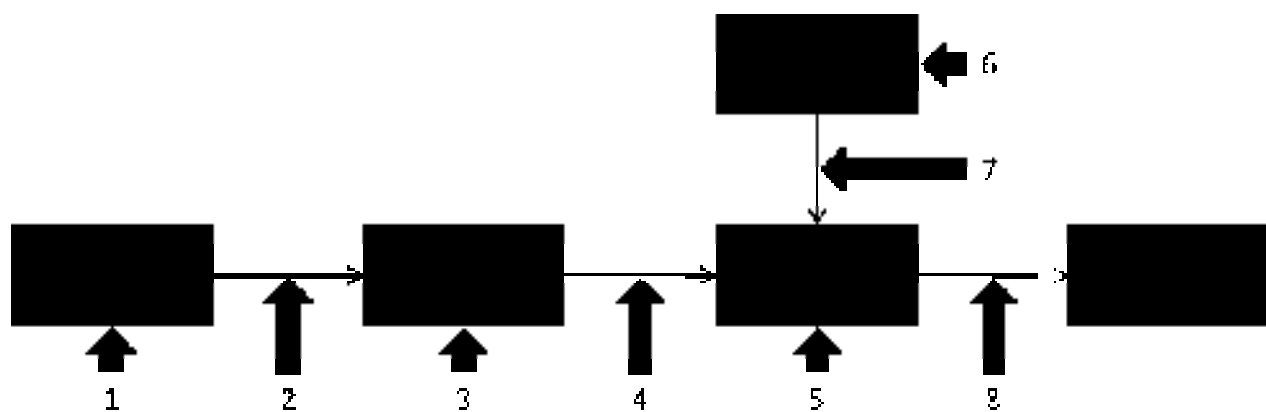
Alongside fingerprints, which will remain the dominant biometric traits, face, iris, hand and speech recognition systems are expected to emerge and be widely adopted in biometric applications.

VI. Security and privacy

Biometrics can play an important role in authentication applications, since they are strongly linked to the holder, and difficult to forget, lose or give away. It is important that biometric systems be designed to withstand attacks when employed in security-critical applications, especially in unattended remote applications such as e-commerce.

In an often-cited paper published in the IBM Systems Journal in 2001 the authors identify eight vulnerable points in biometric systems (illustrated and described in Box 2), which are also critical for local and remote (tele-) biometric applications.

Box 2: Illustration and description of possible attacks and vulnerabilities in biometric systems



- 1 Attack on the biometric sensor with mockups or dummies. A reproduction of a biometric trait is presented as input to the system.
- 2 Replay attack. A recorded signal (containing a previously intercepted signal) is replayed to the system, bypassing the biometric sensor.
- 3 Attack on the feature extractor. The feature extractor is forced, e.g., by Trojan horse, to oppress single features of a biometric trait, or to produce altered values than those read by the biometric sensor.
- 4 Tampered feature representation. Features extracted from the sensor input are replaced by a different (fraudulent) feature set. The stages of feature extraction and matching are often inseparable, and the attack is complex. However, if the extracted feature set is sent to a remote matcher, e.g., over the Internet, the threat is real.
- 5 Attack on the matcher. The matcher is forced, e.g., by Trojan horse, to produce high or low matching score, in order to allow or deny access to an individual.
- 6 Attack on stored biometric templates. Templates stored in a biometric database (local, remote, distributed) are added, modified or deleted.
- 7 Tampered template representation. See 4.
- 8 Attack on the decision end point. If the final matching decision is manipulated by the attacker, the authentication system is disabled. By overriding the final matching decision, the biometric system is rendered useless and the biometric data irrelevant.

The strong link between biometrics and the holder also guarantees that the characteristics cannot be influenced or altered by its holder, without harm. It appears to be difficult to deny or hide one's biometrics. Privacy concerns exist wherever uniquely identifiable data relating to an individual are collected, stored or processed. Some argue that the ubiquitous use of biometrics in large-scale commercial applications, the ease to create biometric templates and the accumulation of biometric profiles in huge databases could devalue classic forensic applications.¹⁸

A number of provisions and techniques have been proposed to safeguard security and privacy in biometrics.

a) Multimodal biometric systems

It is now recognized that biometric recognition can be better performed when multiple measurements are involved—an approach described as multimodal, multibiometric or biometric fusion. The five different operational scenarios of the multimodal approach are described in Box 3. This approach addresses the issue of non-inclusiveness due to non-universality of certain biometric traits, since sufficient population coverage can be ensured using multiple traits.¹⁹

b) Template-on-token

Storing biometric authenticator and identity data of an individual on a token, such as a smart card, represents a two factor authentication with the following security-/ privacy-enhancing features:

- Avoidance of knowledge-based authenticators;
- Avoidance of a centralized database storing biometrics or other personal information;
- Two authenticators, biometric and token, are required for successful authentication;
- Prevention of unauthorized read-out or manipulation of the content stored on the token through access control mechanisms possible.

In this approach, the user retains control over its biometrics, and would be able to hand them out only to trustworthy services and devices. However, once a communication partner is deemed trustworthy, the personal information leaves the token and the controlled area of the user.

c) Match-on-token

This approach extends template-on-token to the extent that only the final matching decision leaves the token, or activates it. In addition to the biometric template being stored, the token integrates a biometric sensor and a comparator with sufficient processing power.

d) Data-hiding techniques

In telebiometric applications, digital representations of biometrics are transmitted in a compressed format over the communication network. For instance, the Wavelet Scalar Quantization (WSQ) image compression scheme proposed by the American FBI is the de facto standard used for compressing fingerprint images, because its low image distortion characteristics even at a high compression ratio have advantages over other formats including JPEG.²⁰ However, being an open format, WSQ-compressed fingerprint bitstreams can be intercepted and decrypted, saved and fraudulently used, for instance in replay attacks.

Data-hiding techniques embed additional information in fingerprint images—an approach similar to hiding digital watermarks in image or audio data to ensure data integrity. If the embedding algorithm remains secret, a service provider (e.g., e-commerce) can investigate the received fingerprint image for the expected standard watermark to ensure it has been sent from a trusted sensor. One-time templates are generated by embedding a different verification string provided by the service provider into the fingerprint image, and are only valid for one transaction.

Box 3: Operational scenarios of the multibiometrics

Biometric fusion is used to increase accuracy and accessibility of a biometric system. It can be designed in five ways:

- 1 Multiple sensors: Combination of the recognition results for the same biometric trait from different sensors. For instance, in face recognition, the results of two-dimensional and three-dimensional recognition technologies can be combined to increase overall recognition accuracy.
- 2 Multiple biometrics: Combination of the recognition results for different biometric traits. This design can improve recognition accuracy in verification scenarios and speed in identification applications. For instance, face recognition is typically fast, but not the most accurate biometric recognition method. It can be applied to quickly sort out a number of outliers. Afterwards, fingerprint recognition (slower, but more accurate) is applied to make the final identification decision.
- 3 Multiple units of same type of biometric. For instance, the combination of the recognition results for two or more fingers, or irises of both eyes.
- 4 Multiple snapshots of the same biometric: Combination of the recognition results for two or more instances of the same biometric, e.g., multiple prints of the same finger, multiple images of the face, etc.
- 5 Multiple representations and matching algorithms for the same biometric. Combination of the recognition results obtained using different approaches to feature extraction and matching of the same biometric trait.

e) Cancelable biometrics

One advantage of knowledge- and possession-based authenticators over biometrics is that they can be re-issued. If a token or a password is lost or stolen, it can be cancelled and replaced by a newer version, an option not readily available for biometrics. Cancelable biometrics perform an intentional and repeatable distortion of the original biometric signal by applying a chosen noninvertible transform, which is applied in the same way during the enrollment and authentication process. Every biometric application may use a different transform to render cross-matching of biometrics impossible. If one variant of transformed biometric is compromised, this representation can be “canceled” and replaced by a biometric generated with a new transform. The original biometric remains secret and cannot be reconstructed from compromised representations.²¹

VII. Standards in biometrics

As biometric recognition becomes an increasingly critical component in the protection of infrastructure and personal identity, the continued development of comprehensive biometric standards is essential to ensure reliability, security, interoperability, usability and scalability. An underlying goal in developing standards in biometrics is to make these systems easier, cheaper and more reliable to deploy and maintain.²²

The deployment of a range of national and international biometric-based identity documents, including electronic passports, ID cards and visas, provided a great incentive to the development of international standards. The development of new standards for these documents has made them more robust. Government authorities deploying cross-border applications are not likely to accept proprietary, non-standardized solutions of a single manufacturer.²³

Although the earliest biometric standards were created by governments and law enforcement agencies beginning in the mid to late 80s to exchange fingerprint data²⁴, the current accelerated pace of standards development did not begin until 2002. There are several national and international players developing biometric standards:

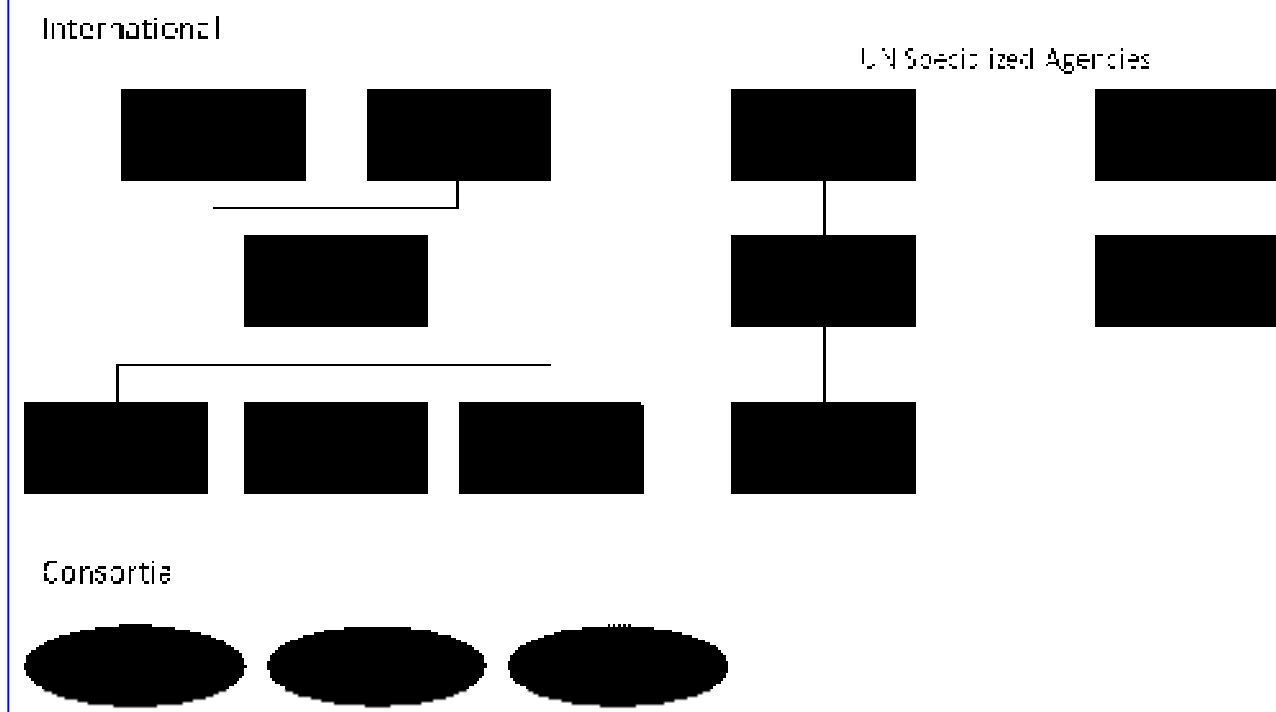
- Standards development organizations (SDO): including ISO/IEC, ITU-T, CEN, ANSI
- Industry consortia: including BioAPI Consortium, Biometric Consortium, OASIS
- Other organizations: including ICAO, ILO

Members of the first category try to develop standards in accordance with their respective mandates, for example to achieve the overall economic benefit that results from standardization or to fulfill specific legislative mandates. Industry consortia develop standards that support the objectives of their membership, which generally is intended to align and complement with the overall goal of enhancing standardization. Members of the third category develop very specific standards related to particular applications within their domain, which may have not been addressed by the other organizations. An overview of the biometric standardization landscape is given in Figure 4.

A major part of the international biometric standards work has been taking place in ISO/IEC Joint Technical Committee 1 (JTC 1), particularly in its Subcommittee 37 (SC 37) on 'Biometrics' established in June 2002. To date, more than 30 International Standards related to biometrics have been published under the direct responsibility of this group.ⁱⁱ The areas of template protection, algorithm security and security evaluation are addressed outside SC 37, in SC 27 on 'IT Security techniques', and SC 17 deals with biometrics in 'Cards and personal identification'.

ITU-T standardization work in biometrics began in 2001 in its lead study group on telecommunications security (SG 17).ⁱⁱⁱ It was noticed that the spread of biometric authentication in many different applications represents challenges related to security, reliability and privacy of biometric data, and that these challenges would become more complicated and demanding when

Figure 4: Overview of standardization landscape in biometrics: International bodies and consortia.



ⁱⁱ More information on JTC 1 SC 37 available at http://www.iso.org/iso/iso_technical_committee.html?commid=313770.

ⁱⁱⁱ More information on ITU-T SG 17 available at <http://www.itu.int/ITU-T/studygroups/com17/>.

conducted in open network environments. ITU-T Recommendations in the field of telebiometrics ensure high security, reliability, and interoperability for biometric systems, as well as safety and convenience of use. The first biometric standard published, ITU-T Recommendation X.1081, defines a multimodal model to assist in the standardization of telebiometrics. Its scope is outlined in Box 4. Recommendations X.1084 and X.1085 specify nine authentication protocols for telebiometrics, which may include a client, a server and a trusted third party, and describe protection profiles for each of the protocols, to allow for secure authentication. Vulnerabilities of telebiometric systems (corresponding to these outlined in Box 2) and a general guideline for countermeasures to establish a safe environment and privacy when using telebiometrics are standardized in ITU-T X.1086.

Procedures to protect (multimodal) biometric data against interception, modification and replacement are specified in ITU-T X.1087 and include encryption, watermarking and non-invertible transformation highlighted in the previous section. Two other Recommendations describe a framework for biometric digital key generation and protection (X.1088) and an implementation of biometric authentication with certificate issuance, management, usage and revocation (X.1089). Other items currently under study in SG 17 are dealing with biometric template protection, reflecting the research on one-time templates and cancelable biometrics described above.

Biometric applications, in particular those operating over networks, embrace SG 16 work on multimedia coding and ubiquitous systems. For instance, the digital photo is usually stored on the electronic passport's chip in JPEG (ITU-T T.81) or JPEG2000 (ITU-T T.800) format. The same is true for most applications involving analysis and compression of audio, still and moving images.

These security-related standards belong to one layer of an 'Onion Diagram' (Figure 5) which is commonly used to show biometric standards as a series of layers, starting with standards at the heart that are of most direct relevance to biometric system developers and users. Standards of the next layer define interfaces between biometric components and the rest of an application, such as access control mechanisms, watch list identification, and financial applications. The outer two layers address privacy and legal issues and define a harmonized biometric vocabulary. Interoperability and conformance requirement and testing standards play an important role for each of these layers and for the entire onion model, giving it structure and support.²⁵

a) Logical data structure

The Common Biometrics Exchange Formats Framework (CBEFF) defines a data structure called Biometric Information Record (BIR) used to exchange biometric data within biometric systems. BIRs consist of three parts: biometric header, with metadata about data type and security options; biometric data block (BDB), containing the actual biometric data; and security block, pro-

Box 4: The telebiometric multimodal model

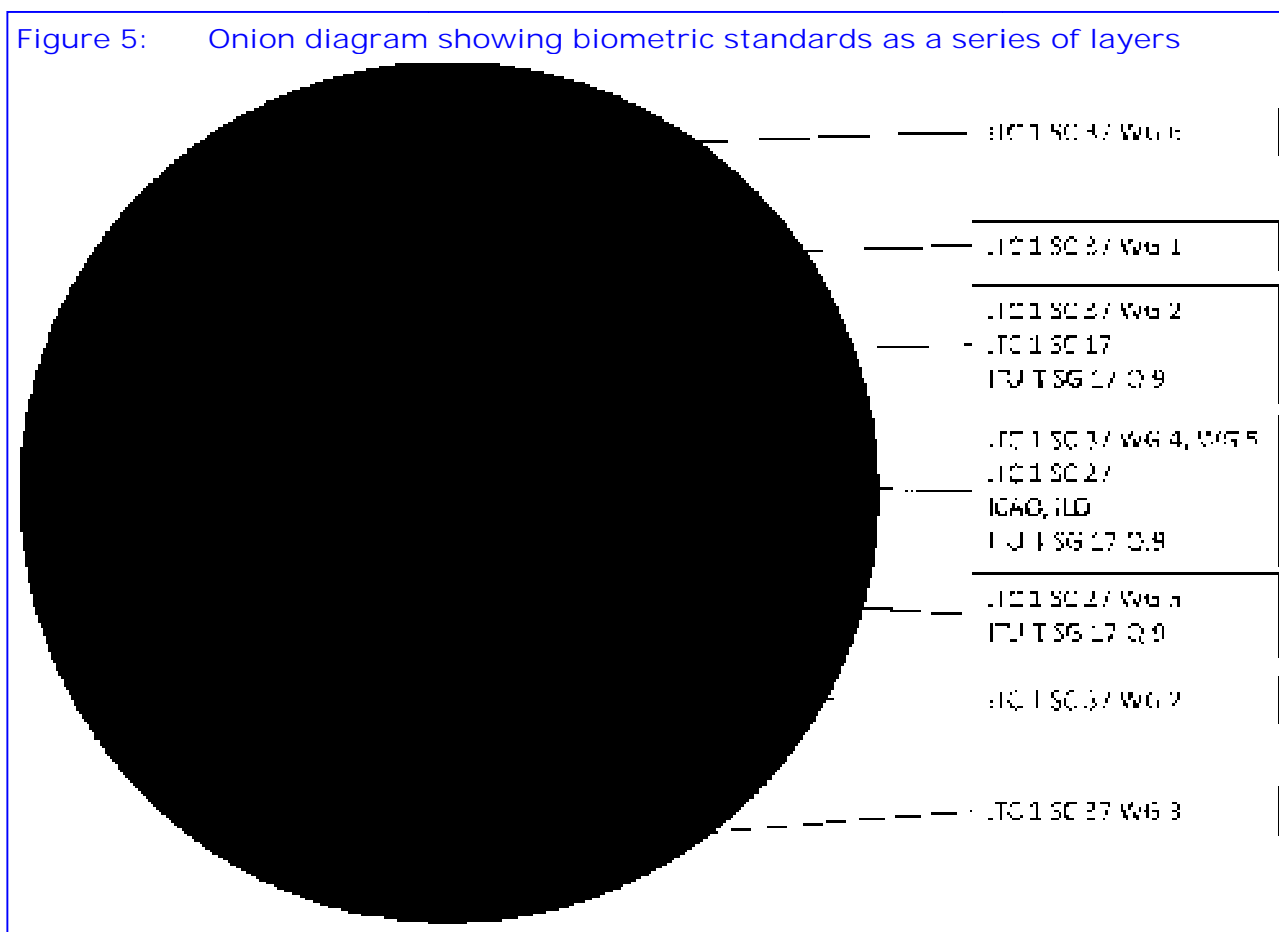
The first biometric standard published by ITU-T, ITU-T Recommendation X.1081, defines a telebiometric multimodal model that can be used as a framework for identifying and specifying safety aspects of telebiometrics, and for classifying biometric technologies used for identification (security aspects).

The model has been developed from two main sources that provide its foundation. The first relates to theoretical work on systems, scale proximity, hierarchies and modalities of interaction between a human being and the environment. The second is the specification of quantities and units for all known forms of measurement of the magnitude of physical interactions between a person and its environment (International Standards of the ISO/IEC 80000 series).

The telebiometric multimodal model is not limited to consideration of purely physical interactions, but also recognizes behavioral interactions. Such interactions are currently not quantified by standard units. The model itself consists of a specification of a number of dimensions related to interactions in a set of specified modalities, in both directions, at various intensities, using the complete range of quantities and units specified. This provides a taxonomy of all possible interactions, which contains more than 1,600 combinations of measurement units, modalities and fields of study.

ITU-T X.1081 is freely available at <http://www.itu.int/rec/T-REC-X.1081/en>.

Figure 5: Onion diagram showing biometric standards as a series of layers



viding detailed information about algorithms used to secure the record.

b) Biometric data interchange formats

JTC 1 SC 37 Working Group 3 is developing a multipart standard to define BDBs for each specific biometric trait in order to ensure interoperability at the level of digital images and/or extracted biometric features. Biometric samples may or may not be in a standardized format before being processed and converted to be a BDB. Current interchange formats exist for fingerprint, face, iris pattern, vascular pattern, hand geometry and signature biometrics. Formats describing voice and DNA data are currently under development.

c) Security

Most ITU-T Recommendations on telebiometrics developed in Study Group 17 belong to this layer. Other related standards are under the responsibility of JTC 1 SC 27 (mainly Working Group 5).

d) System properties

As highlighted in the previous sections, reliability and performance of biometric systems are crucial for deployment. Significant progress has been made in Working Groups 4 and 5 of SC 37 to develop performance testing and reporting standards and to define profiles for interoperability and data interchange. The International Civil Aviation Organization (ICAO) and the International Labour Organization (ILO) have developed specifications required for particular application domains. ICAO is responsible for the global standardization of machine-readable travel documents (MRTD) including electronic passports. ICAO Doc 9303—a multi-part document first published in 1980 under the title “A Passport with Machine Readable Capability”—requires

that biometrics stored in travel documents conform to the biometric data interchange formats for face, finger and iris data. The convention developed by ILO provides guidelines for biometric identity documents for seafarers.

e) Interfaces

BioAPI is an open systems common application programming interface that allows biometric technology modules and applications to communicate with each other. Initially developed by the BioAPI Consortium, the interface became first a national and later an international standard. The work has been taken up by ITU-T Study Group 17 in Recommendation X.1083, which defines Biometric Interworking Protocol (BIP) messages.

f) Vocabulary

A harmonized vocabulary is necessary to align the work within SC 37, but also to make easier cooperation with other SDOs, and to facilitate the understanding of biometric standards. Standards need to be understandable and unambiguous for the international community of standards' users. A draft vocabulary is maintained online, in English, French and German versions.^{iv}

g) Cross-jurisdictional and societal aspects

The terms of reference of SC 37 Working Group 6 include the design and implementation of biometric technologies with respect to accessibility, health and safety, support for legal requirements, and acknowledgement of other cross-jurisdictional and societal aspects related to personal information. Cooperation on an international level will be of particular importance for the deployment of large-scale cross-border applications of biometrics. To date, SC 37 has published a Technical Report which outlines general guidelines for privacy, accessibility and other societal and legal issues.

VIII. Conclusion

Within a fairly short period of time, biometric recognition technology has found its way into many areas of everyday life. Citizens of more than 50 countries hold machine-readable passports that store biometric data—a facial image and in most cases a digital representation of fingerprints—on a tiny RFID chip, to verify identity at the border. Law enforcement agencies have assembled biometric databases with fingerprints, voice and DNA samples, which make their work more efficient and manageable. Commercial applications use biometrics in local access control scenarios, but also increasingly in remote telebiometric deployments, such as e-commerce and online banking, and complement or replace traditional authentication schemes like PIN and passwords.

Biometrics-based authentication clearly has advantages over these mechanisms, but there are also vulnerabilities that need to be addressed. No biometric trait can be applied universally, it may be a good choice for a given application, but unfeasible in another.

Significant progress has been made recently in the capabilities of biometric sensors, algorithms and procedures. Due to the availability of ever-increasing processing power at low cost, the accuracy of biometric systems has improved to a degree which in some scenarios may exceed the recognition accuracy of humans. In addition, sensors have decreased in size, allowing biometric applications to increasingly appear on mobile devices, which could outsource the processing-intensive parts of biometric recognition to the cloud. Scientific and technical challenges remain in achieving accuracy in recognition under uncontrolled illumination and environment conditions and in the recognition of moving objects.

^{iv} See <http://www.3dface.org/media/vocabulary.html>.

Since biometrics rely on highly sensitive personal information, the handling of biometric information needs to be given special attention and protective measures need to be put in place to safeguard privacy and avoid compromise of biometric data.

Some approaches to improve security and ensure privacy when deploying biometric recognition have been described in this Report and are increasingly reflected in international biometric standards. Insecure biometric systems may not only have negative consequences for a specific application or its users, but may also result in loss of public trust and lack of acceptance of biometric recognition technologies as a whole.

The accelerated development of biometric standards in recent years has facilitated the enhancement and increasing use of biometric applications. As more international standards become available, it is likely that these systems will be used in an ever-widening range of applications.

Glossary of acronyms

ATM	Automated teller machine
BAC	Basic access control
BDB	Biometric data block
BioAPI	Biometric application programming interface
BIP	Biometric interworking protocol
BIR	Biometric information record
CBEFF	Common biometrics exchange formats framework
CCTV	Closed-circuit television
DNA	Deoxyribonucleic acid
EAC	Extended access control
FMR	False match rate
FNMR	False non-match rate
ICAO	International Civil Aviation Organization
ICT	Information and Communications Technologies
IEC	International Electrotechnical Commission
ILO	International Labour Organization
ISO	International Organization for Standardization
ISO/IEC JTC 1	ISO/IEC Joint Technical Committee 1
ITU	International Telecommunication Union
ITU-D	ITU Telecommunication Development Sector
ITU-R	ITU Radiocommunication Sector
ITU-T	ITU Telecommunication Standardization Sector
JPEG	Joint Photographic Experts Group (method of image compression)
MRTD	Machine-readable travel document
PDA	Personal digital assistant
PIN	Personal identification number
R&D	Research and development
RFID	Radio-frequency identification
ROC	Receiver operating characteristic
SDO	Standards development organization
SSL	Secure sockets layer (cryptographic communications protocol)
TAN	Transaction authentication number
WSQ	Wavelet scalar quantization (fingerprint image compression algorithm)

Notes, sources and further reading

- ¹ A.K. Jain, A. Ross, S. Prabhakar: An Introduction to biometric recognition. *IEEE Transactions on Circuits and Systems for Video Technology*, 14(1):4-20, 2004.
- ² G. Parziale: Touchless fingerprinting technology. *Advances in biometrics*, 25-48, 2008.
- ³ Y. Adini, Y. Moses, S. Ullman: Face recognition: the problem of compensating for changes in illumination direction. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 19(7):721-732, 1997.
- ⁴ See, for instance, S. Murphy, H. Bray: Face recognition devices failed in test at Logan. *The Boston Globe*, September 2003.
http://www.boston.com/news/local/articles/2003/09/03/face_recognition_devices_failed_in_test_at_logan/
- ⁵ National Science and Technology Council: Introduction to biometrics. 2007.
<http://www.biometrics.gov/documents/biofoundationdocs.pdf>
- ⁶ A.K. Jain, A. Ross, S. Prabhakar: Biometrics: a tool for information security. *IEEE Transactions on Information Forensics and Security*, 1(2):125-143, 2006.
- ⁷ J.P. Campbell: Speaker recognition: a tutorial. *Proceedings of the IEEE*, 85(9):1437-1462, 1997.
- ⁸ See Jain et al.: Biometrics: a tool for information security.
- ⁹ J. Ortega-Garcia, J. Bigun, D. Reynolds, J. Gonzalez-Rodriguez: Authentication gets personal with biometrics. *IEEE Signal Processing Magazine*, 21(2):50-62, 2004.
- ¹⁰ M. Gifford, N. Edwards: Trial of dynamic signature verification for a real-world identification solution. *BT Technology Journal*, 23(2):259-266, 2005.
- ¹¹ F. Monroe, A.D. Rubin: Keystroke dynamics as a biometric for authentication. *Future Generation Computer Systems*, 16(4):351-359, 2000.
- ¹² D. Bartmann: On the design of an authentication system based on keystroke dynamics using a predefined input text. *International Journal of Information Security and Privacy*, August 2006.
- ¹³ ISO/IEC: Information technology – Biometrics tutorial. *ISO/IEC TR 24741:2007(E)*. 2007.
- ¹⁴ See Jain et al.: An Introduction to biometric recognition.
- ¹⁵ J. Daugman: How iris recognition works. *IEEE Transactions on Circuits and Systems for Video Technology*, 14(1):21-30, 2004.
- ¹⁶ P.J. Phillips et al.: Face Recognition Vendor Tests 2006 and Iris Challenge Evaluation 2006: Large-scale results. 2007. <http://frvt.org/FRVT2006/docs/FRVT2006andICE2006LargeScaleReport.pdf>
- ¹⁷ Biometrics faces rosy future says pundits. *Biometric Technology Today*, 16(9):4-5, 2008.
- ¹⁸ A. Pfizmann: Biometrie: wie einsetzen und wie keinesfalls. *Informatik-Spektrum*, 29(5):353-356, 2006. (German)
- ¹⁹ See Jain et al.: An Introduction to biometric recognition.
- ²⁰ N.K. Ratha, J.H. Connell, R.M. Bolle: Enhancing security and privacy in biometrics-based authentication systems. *IBM Systems Journal*, 40(3):614-634, 2001.
- ²¹ N.K. Ratha, J.H. Connell, R.M. Bolle, S. Chikkerur: Cancelable biometrics: a case study in fingerprints. *ICPR '06: Proceedings of the 18th International Conference on Pattern Recognition*, 370-373, 2006.
- ²² R. Ryan: The importance of biometric standards. *Biometric Technology Today*, 17(7):7-10, 2009.
- ²³ F. Deravi: Biometrics standards. *Advances in biometrics*, 473-489, 2008.
- ²⁴ C. Tilton: Biometric standards – an overview. 2009. White paper available at <http://www.daon.com/>.
- ²⁵ See R. Ryan: The importance of biometric standards.