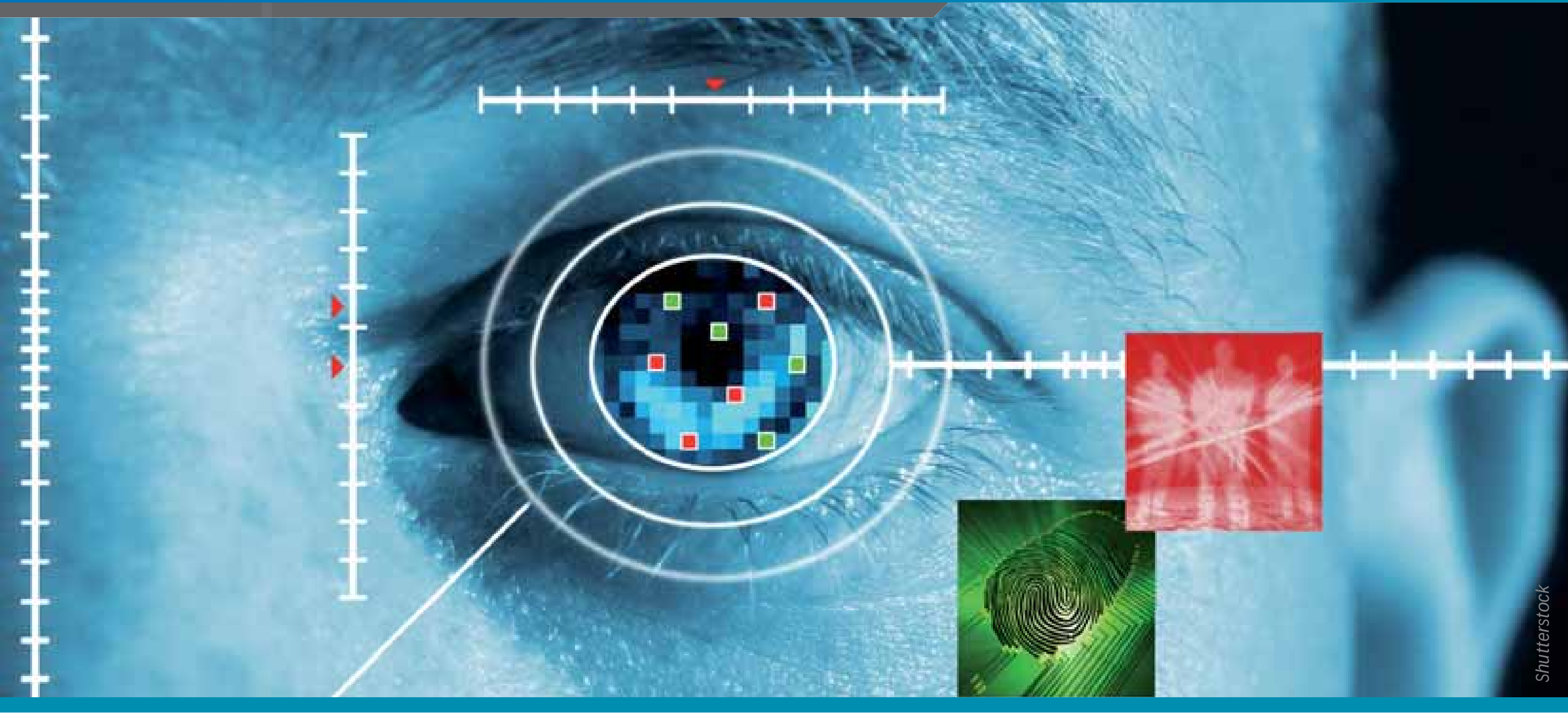

Shutterstock

Biometrics and standards

Usually, we recognize people we know by looking at their faces, sometimes by their voices or handwriting, or by the way they move. In times past, human scrutiny was the only way of checking the identity of travellers moving from one country to another, visitors seeking to enter private areas, or traders withdrawing cash from banks. This is no longer realistic, given the growth of international travel, the need for security in workplaces, and the spread of electronic banking, among many other changes in our daily lives. Nowadays, there is a new way of checking identity, using automated methods and information and communication technologies (ICT) to recognize individuals based on physical or behavioural traits — a field known as biometrics. This is the topic of a new Technology Watch report from ITU on "Biometrics and Standards"*.

Biometrics are now applied in electronic passports, as well as for finger-vein recognition in automatic teller machines (ATM) in banks, and even to prevent vending machines from selling cigarettes to children. In each case, some combination of inherent characteristics is measured and automatically compared with templates stored on a token or in a database to find a match. The measured characteristics are often physical but may also be behavioural, such as a pattern of keystrokes in entering a word or phrase. With the wide acceptance of biometrics for

⏩

* *This article is based on the Technology Watch Report "Biometrics and Standards" issued by ITU's Telecommunication Standardization Sector (ITU–T) in December 2009. Technology Watch reports are prepared by the ITU–T Policy & Technology Watch Division. They evaluate emerging technologies to assess their implications for the ITU membership, especially developing countries, and to identify candidates for standardization work. The reports can be viewed and downloaded at www.itu.int/ITU-T/techwatch.*

identity verification, especially in an open network environment, the challenges of privacy, reliability and the security of biometric data become more complicated and demanding.

Anyone who has queued at a check-in point at an airport will appreciate the importance of speed and accuracy in reading an electronic passport. Similarly, when you draw money from an ATM, you expect to be the only person able to gain access to your account. These uses of biometrics grew out of the development of measures to meet the need for accurate identification in the fields of criminology and forensics — the fingerprints and DNA samples that feature so prominently in crime stories. There are now three main categories of biometric applications: forensic, governmental (passports, identity cards, voter registration, and so on), and commercial (for example, network login systems, ATM, credit-card processing, and face recognition in photographic software).

To ensure that biometric identification systems are reliable, secure, interoperable and easy to use, there is an evident need for the development of international standards. Governmental authorities, in particular, are unlikely to accept a non-standardized system offered by a single manufacturer. There has to be general agreement on what biometric traits to measure, and confidence that the chosen metrics will distinguish between any two individuals. Standards are also needed to protect biometric data, both to maintain personal privacy and to prevent attacks that would open the way for fraud or impersonation. The underlying objectives in standardization are to make biometric systems easier to install, cheaper to run and more reliable to use.

Standards-setting organizations

Although the earliest biometric standards were created by governments and law-enforcement agencies in the 1980s to exchange fingerprint data, the current accelerated pace of standards development did not begin until 2002. Now, several national and international players are developing these standards. They include the International Organization for Standardization (ISO), the International Electrotechnical Commission (IEC), and ITU's Telecommunication Standardization Sector (ITU–T). Industry consortia also develop standards that support the objectives of their membership, while United Nations specialized agencies, such as the International Civil Aviation Organization (ICAO) and the International Labour Organization (ILO), develop standards within their specific domains that might not have been addressed by other organizations. In particular, ICAO is responsible for the standardization of machine-readable travel documents, including electronic passports, while ILO has provided guidelines on biometric identity documents for seafarers.

Over 30 international standards on biometrics have been developed by the ISO/IEC Joint Technical Committee 1 (JTC 1) since the establishment of its Subcommittee 37 on Biometrics in June 2002. The work of JTC 1 on biometric standards is also carried out in its Subcommittee 27 on IT Security Techniques (which covers template protection, algorithm security, and security evaluation), and in Subcommittee 17 on Cards and Personal Identification.

Within ITU–T, work on biometrics began in 2001, led by ITU–T Study Group 17 which coordinates this work across all study groups. In particular, ITU–T Study Group 17 is responsible for looking at identity management; that is, technical methods for identifying individuals and protecting those identities.

Work is intensifying to meet current challenges for more secure network infrastructure, services and applications. Clearly, telecommunication applications using mobile terminals and Internet services call for authentication methods that not only provide high security, but are also convenient for users. More than 70 ITU–T Recommendations on security have been published.

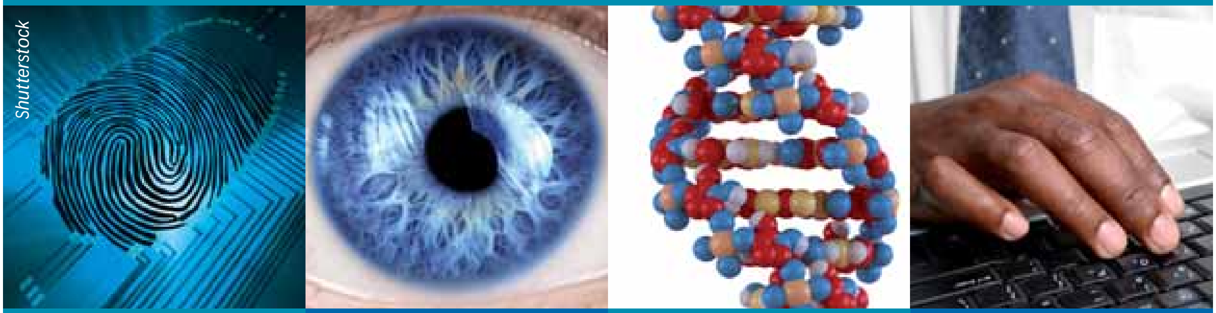
Biometric systems

All biometric systems have a storage component containing biometric data samples of individuals linked to information on their identity. There is also a sensor to capture the person's biometric data. The captured data sample is compared with a reference template, and a decision is taken on whether it matches. In telebiometrics, the communication channels between these components of a biometric system may be wired or wireless telecommunications, or private or public networks, including the Internet. Whether the biometric trait is physical (such as DNA) or behavioural (such as a keystroke pattern), each individual should have that trait uniquely. Also, the biometric trait should be invariant over a certain period of time, and should be measurable.

Recommendation ITU–T X.1081 "The telebiometric multimodal model — A framework for the specification of security and safety aspects of biometrics" is the first biometric standard to be published. It provides a model that can be used as a framework for identifying and specifying safety aspects of telebiometrics, and for classifying biometric technologies used for identification. The multimodal model covers both the physical and behavioural interactions between a person and the environment, providing a taxonomy of over 1600 combinations of measurement units, modalities and fields of study. The model is based on earlier theoretical work dealing with the way humans interact with their environment, and on the ISO/IEC 80000 series of international standards, specifying the quantities and units for all known forms of measurement of the magnitude of interactions between individuals and their environment.

Over 50 countries issue their citizens with machine-readable passports, which store biometric data that can be used to verify identity at the border.

Overview of some biometric methods



Fingerprints *Iris recognition* *DNA* *Keystroke pattern*

A facial image, and perhaps a digital representation of fingerprints or the iris, is stored on a tiny radio-frequency identification (RFID) chip, and this can be compared with information in a biometric database. The Joint Photographic Experts Group (JPEG), a Working Group of ISO/IEC and ITU, is responsible for the JPEG, JPEG2000, JPSearch and JPEG XR families of imaging standards. These are methods of image compression, and such methods are usually used to store a digital photograph on the chip in an electronic passport. The standards for the JPEG or JPEG2000 format are given respectively in Recommendations ITU–T T.81 and T.800, developed by ITU–T Study Group 16. JPEG XR (ISO/IEC 29199-2) is now an international standard, reflected in Recommendation ITU–T T.832. It specifies a coded image format, designed primarily for storage and interchange of continuous-tone photographic content.

Shutterstock

More than 50 countries now issue passports with stored biometric data

Keeping data secure

A key can be lost, stolen or duplicated. A password can be forgotten. It is generally considered that biometric traits have the advantage of being virtually impossible to steal or forget, and difficult to guess. Yet biometric systems are vulnerable to attack. Any element of the biometric system could be the target: the sensor, the feature extractor, the matcher, the stored biometric templates or the decision endpoint. An attack could also take place by bypassing the biometric sensor, or by tampering with the feature extractor or template.

Biometrics are increasingly used to complement or replace traditional authentication schemes such as personal identification numbers (PIN) or passwords. But biometric data cannot be kept secret. Photographs of faces, recordings of voices and copies of signatures, for instance, are all easily made. Biometrics rely on highly sensitive personal information, but the security of an authentication system cannot rely on the secrecy of biometric data. A system must ensure the integrity and authenticity of biometric data in order to be operationally effective, and additional protective measures are needed to safeguard privacy.

To allow for secure authentication, Recommendations ITU–T X.1084 and X.1085 specify nine authentication protocols for telebiometrics and describe protection profiles, while Recommendation ITU–T X.1086 provides guidance on countermeasures to establish a safe environment and privacy. Recommendation ITU–T X.1087 sets out procedures to protect multimodal biometric data against attempts to intercept, modify or replace the data. The procedures include encrypting, watermarking and transforming data. Recommendations ITU–T X.1088 and X.1089 provide respectively a framework for generating and protecting biometric digital keys, and a way of managing biometric authentication.

Commercial and government applications to drive growth

Advances in ICT, increased performance and availability of equipment at lower cost have smoothed the way for automated biometric recognition. Future e-commerce, e-health and e-government services may require authentication with the help of biometric personal documents issued by governments. For example, some developing countries have already started using biometrics for voter registration in the run-up to elections in order to avoid outdated voter lists and election fraud.

Market forecasts on biometric spending are generally positive. Growth is expected to come mainly from commercial and government applications, where the biometrics and smart card chip industries will benefit from government decisions to adopt electronic personal documents and biometrics. From an estimated USD 3 billion spent on biometric technologies in 2008, market researchers now forecast investment of USD 7.3 billion by 2013.

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

What next?

Standards allow for the effective development of biometric systems by establishing common criteria and setting guidelines for the protection of privacy. Agreements on data formats and application software interfaces will help to reduce the cost of developing systems. Furthermore, the development of standards for applying biometrics and for testing accuracy contributes to clarifying vulnerabilities and guides the search for countermeasures to attacks.

As well as being universal and unique, biometric characteristics should be reasonably permanent and easy to collect and measure. A biometric system should deliver accurate results under varied environmental circumstances, and should be difficult to deceive. Perhaps the most crucial aspect of a biometric system is its acceptance by the general public. For obvious reasons, non-intrusive methods are more acceptable than intrusive techniques. Although DNA is considered the ultimate biometric for identifying a person (other than an identical twin), DNA matching is too intrusive for extensive use in authenticating identity. Facial thermography, which detects the heat patterns created by blood vessels and emitted from the skin, is non-intrusive but too costly. Among the biometrics currently being considered for future deployment are blood pulse, body odour, skin composition, nail-bed pattern, gait and ear shape. More research is needed to see whether any of these will emerge as the biometric of choice.

Whatever system is used, it must be secure, ensure privacy and produce accurate results. A system that is insecure, unreliable or invasive will undermine public trust and may lead to a general lack of acceptance of biometric recognition techniques. The development of international standards is a key strategy in guaranteeing the appropriate choice and use of biometric methods. In less than a decade, huge progress has been made in improving biometric sensors, algorithms and procedures, but there remain vulnerabilities that need to be addressed. The need to protect privacy and safeguard sensitive biometric data remains fundamental. ■