TECHNICAL REPORT

ISO/IEC TR 24741

First edition
2007-09-15

Information technology — Biometrics tutorial

Technologies de l'information — Tutoriel biométrique

Reference number
ISO/IEC TR 24741:2007(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

Foreword

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

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

In exceptional circumstances, the joint technical committee may propose the publication of a Technical Report of one of the following types:

— type 1, when the required support cannot be obtained for the publication of an International Standard, despite repeated efforts;

— type 2, when the subject is still under technical development or where for any other reason there is the future but not immediate possibility of an agreement on an International Standard;

— type 3, when the joint technical committee has collected data of a different kind from that which is normally published as an International Standard ("state of the art", for example).

Technical Reports of types 1 and 2 are subject to review within three years of publication, to decide whether they can be transformed into International Standards. Technical Reports of type 3 do not necessarily have to be reviewed until the data they provide are considered to be no longer valid or useful.

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.

ISO/IEC TR 24741, which is a Technical Report of type 3, was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 37, *Biometrics.*

Introduction

"Biometric authentication" is the automatic recognition of individual persons based on distinguishing biological and behavioural traits. The field is a subset of the broader field of human identification science. Example technologies include fingerprinting, face recognition, hand geometry, speaker recognition and iris recognition.

At the current level of technology, DNA analysis is a laboratory technique not fully automated and requiring human processing, so it is not considered "biometric authentication" under this definition (it is not currently automatic and fast, but may become so in the near future).

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

Biometric authentication 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 tutorial

1 Scope

This Technical Report provides a tutorial on biometrics.

It contains a description of the architecture of biometric processes and of the processes themselves.

An annex provides further details of International Standards' activity in the field of biometrics.

A further annex provides terms and definitions that are in use in these International Standards.

2 Introduction and general history

2.1 What are biometric technologies?

The all-encompassing term ‘biometrics’ refers to the quantification or statistical analysis of biological characteristics. In this context, we are concerned with technologies that analyze human characteristics for recognition security purposes. The statistical science of biometrics, usually used in biomedical contexts, is a separate discipline. A broadly accepted definition of biometrics for recognition states that:

A biometric is a unique, measurable characteristic or trait for automatically recognizing or verifying the identity of a human being.

The agreed SC37 definition comes in two parts, and broadly agrees with the above. It is recommended that the word biometric be normally used only as an adjective, and not where the fuller term biometric characteristic (as above) would be more appropriate. We have for adjectival use:

biometric
of or having to do with biometrics

and for noun use:

biometrics
automated recognition of individuals based on their behavioural and biological characteristics

So, biometric technologies are concerned with the physical parts of the human body or the personal traits of human beings, and the recognition of individuals based on either or both of those parts or traits. It is important to note the term ‘automatic’ in the above definition. This essentially means that a biometric technology must recognize or verify a human characteristic quickly and automatically, in real time. (A fuller explanation of the various biometric technologies is given in clause 3.) In summary the most common *physical biometric characteristics* are the eye, face, fingerprints, hand and voice; while signature, typing rhythm and gait are the most common *behavioural biometric characteristics*. Use of DNA is excluded today, as it is not yet a fast automated process, although that is likely to change in the next few years.

2.2 History

In a non-sophisticated 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 study 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 (Beavan, 2001 [3]; Cole, 2001 [11]). 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 by a British colonial magistrate in India, William Herschel, began in the late 1850s, knowledge of the technique did not become known in the western world until the 1880s (Faulds, 1880 [13]; Herschel, 1880 [18]) when it was popularized scientifically by Sir Francis Galton (1888) [16] and in literature by Mark Twain [47] (1893). 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 [36]) and retinal identification was suggested in 1935 (Simon and Goldstein, 1935 [44])

None of these techniques was "automatic", however, so none meets the definition of "biometric authentication" being used in this Technical Report. Automatic techniques require automatic computation (and are expected to be fast). Work in automatic speaker recognition can be traced directly to experiments with analogue filters done in the 1940s (Potter, Kopp and Green, 1947 [38]) and early 1950s (Chang, Pihl, and Essignmann, 1951 [10]). With the computer revolution picking up speed in the 1960s, speaker (Pruzansky, 1963 [39]) and fingerprint (Trauring, 1963 [46]) pattern recognition were among the very first applications in automatic signal processing. By 1963, a "wide, diverse market" for automatic fingerprint recognition was identified, with potential applications in "credit systems", "industrial and military security systems" and for "personal locks". Computerized facial recognition research followed (Bledsoe, 1966 [6]; Goldstein, Harmon, and Lesk, 1971 [17]). In the 1970's, 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 [52] ;), measures from multiple biometric devices were being combined (Messner, Cleciwa, Kibbler, and Parlee, 1974 [27]; Fejfar, 1978 [14]) and government testing guidelines were published (NBS, 1977 [28]).

Running parallel to the development of hand technology, fingerprint biometrics were making progress in the 60s and 70s. During this time a number of companies were involved in automatic 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 systems developed for the FBI in the 1960s and 70s increased the level of automation, but these were ultimately based on human fingerprint comparisons. Automated Fingerprint Identification Systems (AFIS) were first implemented in the late 70s, most notably the Royal Canadian Mounted Police AFIS in 1977. The role of biometrics in law enforcement has mushroomed since then and Automated Fingerprint Identification Systems (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 [15]), iris recognition systems became available in the mid-1990s (Daugman, 1993 [12]). 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 vein patterns.

Today's speaker verification systems have their roots in technological achievements of the 1970s, while biometric technologies such as signature verification and facial recognition are relative newcomers to the industry. The migration from R&D towards commercialization continues today. 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 a system to become fully operational. However, such systems are now in place and proving themselves across a range of diverse applications.

3 Technology overview

Biometric systems now come in many shapes and sizes. This can range from hardware, software, OEMs, software development kits or complete solutions. Systems may be marketed and sold by vendors directly or through various distribution channels, such as systems integrators, strategic partners or value added resellers. All biometric systems have the principles of capture, extraction, and comparison in common. Yet, biometric technologies focus on different parts of the human make-up, so the workings of each technology and each vendor's specific system will differ. This clause looks at the operation of each biometric technology within the four stages of capture, extraction, comparison and decision.

3.1 Eye technologies

Biometric technologies that analyze the eye are generally thought to offer the highest levels of accuracy at present, and differ even between identical twins. They can be divided into two specific technologies: iris biometric characteristics and retina biometric characteristics.

3.1.1 Iris characteristics

The iris is the coloured ring of textured tissue that surrounds the pupil of the eye. Each iris is a unique structure, featuring a complex pattern. This can be a combination of specific characteristics known as corona, crypts, filaments, freckles, pits, radial furrows and striations. It is claimed that artificial duplication of the iris is virtually impossible because of its unique properties and that no two irises are alike. The iris is closely connected to the human brain and is thought to be one of the first parts of the body to be rendered unusable for biometric recognition after death. It is therefore very unlikely that an artificial iris could be recreated or that a dead iris could be used to fraudulently by-pass the biometric system. (Equally, this means that identification of a dead body using recorded iris data is unlikely to work as well as DNA, which survives death very well under most conditions - heat and salt-water excluded.)

In most implementations, a grayscale image of the iris is acquired in the near-IR spectrum to maximize detail in dark-colored eyes; some implementations capture irises in color. This should be done in a well-lit environment. Non-patterned contact lenses do not interfere with image capture. Sunglasses and glasses, however, should not be worn as these can affect the capture process.

Unique features of the iris are extracted from the captured sample by the biometric engine. These features are then converted into a unique mathematical code and stored as a template (a biometric reference) for that individual.

3.1.2 Retina characteristics

The retina is the layer of blood vessels situated at the back of the eye. As with the iris, the retina forms a unique pattern and is thought to be one of the first parts of the body to be rendered unusable for biometric recognition after death. A precise enrolment procedure is necessary, which involves lining up the eye to achieve an optimum reading.

The eye is positioned in front of the system, The eye is positioned in front of the system, at a capture distance ranging from 8 cm to one metre.. The subject must look at a series of markers, viewed through the eyepiece,

and line them up. When this is done, the eye is sufficiently focused for the scanner to capture the retina pattern. The retina is scanned and the unique pattern of the blood vessels is captured.

The biometric engine maps out the position of the blood vessels; a unique mathematical representation is extracted and stored as a template (a biometric reference) for that individual.

3.2 Face technologies

The face is a key component in determining the way human beings remember and recognize each other. Automatically identifying an individual by analyzing a face is a complex process which can require sophisticated artificial intelligence and machine learning techniques. A number of biometric vendors and research institutions have developed facial recognition systems, using either standard video or thermal imaging to capture facial images. Because people change over time, and facial hair, glasses and the position of the head can affect the way a biometric system can match one face with another, machine learning is important in order to adapt to changes and accurately compare new samples with previously recorded templates.

Standard video techniques use a facial image, or collection of images, captured by a video camera. The precise position of the subject's face and the surrounding lighting conditions may affect the system's performance. The complete facial image is usually captured and a number of points on the face can then be mapped out. For example, the position of the eyes, mouth and nostrils may be plotted so that a unique template is built. Three-dimensional maps of the face can be created through various means, such as the projection of an infrared grid ("structured light"), merging of multiple images, or using shading information in a single image.

Thermal imaging analyzes 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.

A proprietary algorithm or neural network within the biometric engine will convert the facial image sample into a pattern and then a unique mathematical code. This is stored as a template (a biometric reference) for that individual.

3.3 Finger ridge technologies

3.3.1 Finger scanning

Finger image biometrics are largely regarded as an accurate method of biometric identification and verification. Most one-to-many AFIS and one-to-one fingerprint systems analyze small unique marks on the fingerprint – which are known as minutiae. These may be defined as fingerprint ridge endings, or bifurcations (branches made by fingerprint ridges). Some fingerprinting systems also analyze tiny sweat pores on the finger which, in the same way as minutiae, are uniquely positioned to differentiate one person from another. Finger image density, or the distance between ridges, may also be analyzed.

Certain conditions may affect the prints of different individuals. For example, dirty, dry or cracked prints will all reduce the quality of image capture. Age, gender and ethnic background are also found to have an impact on the quality of finger images. The way a subject interacts with a finger scanner is another important consideration. By pressing too hard on the scanner surface, for example, an image can be distorted. Vendors are addressing these problems so that scanners are ergonomically designed to optimize the fingerprinting process.

A key difference between the various fingerprint technologies on the market is the means of capturing an image. One-to-one fingerprint verification systems use four main capture techniques: optical, thermal or tactile, capacitance and ultra-sound. Most one-to-many systems capture finger images using the optical technique or by electronically scanning images from paper.

3.3.2 Finger image verification

The optical image technique typically involves generating a light source, which is refracted through a prism. Subjects place a finger on a glass surface, known as a platen. Light shines on the fingerprint and the impression made by the print is captured.

Tactile or thermal techniques use sophisticated silicon chip technology to acquire fingerprint data. A subject places a finger on the chip sensor which senses heat or pressure from the finger. Fingerprint data is then captured.

Capacitance silicon sensors measure electrical charges and give an electrical signal when a finger is placed on the sensor surface. The core element of capacitance techniques, as with tactile and thermal methods, is the chip sensor. Using capacitance, the peaks and troughs of fingerprint ridges and valleys are analyzed. An electrical signal is given when fingerprint ridges contact the sensor. No signal is generated by the valleys. This variance in electrical charge produces an image of the fingerprint.

Ultra-sound image capture 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.

The biometric engine extracts fingerprint data contained in the print. A unique mathematical representation of the print is then stored as a template (a biometric reference) for that individual.

3.3.3 Finger image identification

For one-to-many identification, individuals are enrolled using the optical live-scan capture process described above for finger image verification. Law enforcement AFIS systems, also known as booking stations, capture all ten fingerprints. A civil AFIS, however, need not capture all fingerprints and can operate effectively using one or two. Latent prints, those taken from the scene of a crime, or inked images on paper can also be captured by the AFIS using a flatbed scanner.

For an AFIS, the process of binning fingerprints refines the extraction process. Minutiae data is extracted and is stored as a template (a biometric reference) for that individual.

A new sample, captured by either live-scan, latent or paper scanning techniques, is compared against the database of references. If binning has taken place the comparison will be against the bin that holds similar features as the newly presented print.

3.3.4 Palm technologies

Palm biometrics can be closely aligned with fingers-canning, and in particular AFIS technology. Ridges, valleys and minutiae data are found on the palm, as with fingerprints. These are usually analyzed using optical capture techniques. This area of the biometrics industry is particularly focused on the law enforcement community, as latent palm prints are equally as useful in crime detection as latent fingerprints. However, certain vendors are also looking at the access control market and hope to migrate to civil applications, following in the footsteps of fingerprinting.

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.

Minutiae data are extracted by the biometric engine and the palm print data is stored as a template (a biometric reference) on a database.

A newly captured print, by either live-scan, latent or paper scanning techniques, is compared against the database of reference templates.