TECHNICAL REPORT

# ISO/IEC TR 24741

Second edition
2018-02

# Information technology — Biometrics — Overview and application

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

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

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

## Contents

# Foreword

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

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

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

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

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

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

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

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

# Introduction

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

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

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

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

# Information technology — Biometrics — Overview and application

## 1 Scope

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

## 2 Normative references

There are no normative references in this document.

## 3 Terms and definitions

No terms and definitions are listed in this document.

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

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

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

## 4 Introduction and fundamental concepts

### 4.1 What are biometric technologies?

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

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

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

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

The perfect biometric characteristic for all applications would be:

— *Distinctive*: different across all subjects;

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

— *Accessible:* easily presented to a sensor (for example, camera or fingerprint scanner or finger-geometry measurement device);

— *Universal*: observable on all people;

— *Acceptable:* the subject is prepared to use the biometric characteristic in the given application.

Unfortunately, no biometric characteristic has all of the above properties, and practical biometric technologies must compromise on every point: there are great similarities among different individuals; biometric characteristics change over time; some physical limitations prevent presentation; not all people have all characteristics; “acceptability” is in the mind of the subject. Consequently, the challenge of biometric deployment is to develop robust systems to deal with the vagaries and variations of human beings.

## 4.2 What biometric systems do

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

a) something known or memorized;

b) something carried;

c) a personal physical characteristic.

The original context for this concept was secure access control to computer data. The underlying assumptions were that persons authorized to access secure data would cooperatively make positive claims (e.g. “I am authorized to access data on the system”) and could be counted on to protect their Personal Identification Numbers (PINs) and passwords. In such applications, biometric technologies do indeed compete with PINs, passwords and tokens, but have received less acceptance. For example, most web-based access control requires a User ID and an associated password, not biometrics. Passwords have been more widespread than biometrics in such applications because they are easily replaced, can vary across applications, require no specialized acquisition hardware, can be created with different levels of security and are exactly repeatable under conscious control.

However, in many applications, PINs, passwords and tokens cannot logically meet the security requirements. For example, PINs, passwords and tokens cannot logically be used in applications where enrolled individuals have little motivation to protect their accounts against use by others, such as with amusement parks. Similarly, in applications where the claim is negative (e.g. “I am not enrolled in the system as Pat”) PINs, passwords and tokens cannot logically meet the requirements of demonstrating the truth of the claim.

Biometric systems recognize persons by observing physical and behavioural characteristics of their bodies. Biometric characteristics are not as easy to transfer, forget or steal as PINs, passwords and tokens, so they can be used in applications for which these other authentication methods are inappropriate. Biometrics can be combined with PINs and tokens into “multifactor” systems for added security.

Although biometric technologies cannot directly “identify” persons, they can link bodies to records of attributes, which we will call “identities”. Consequently, biometric recognition can become part of an identity management system.

Biometric recognition is used in two main classes of applications: 1) those that use biometric comparison to verify a biometric “claim of identity”; and 2) those that search a database of the biometric characteristics of known individuals to find and return the identifier attributable to a single individual. The former applications are called “biometric verification” and the latter, “biometric identification”. Biometric systems can also be used to “cluster” characteristics, labelling together those that come from the same bodily source, even when the bodily source cannot be attributed to any known individual. Such types of systems are gaining application in law enforcement.

Biometric verification systems verify claims (test hypotheses) regarding the source of a biometric data record in a database. The claim can be made by the person presenting a biometric sample (e.g. "*I am the source of a biometric data record in the database*") or the claim can be made about the source by another actor in the system *("She is the source of a biometric data record in the database"*). The claims can be positive ("*I am the source of a biometric record in the database*"; "*These two samples came from the same bodily source*") or negative *("I am not the source of a biometric record in the database"*). Claims can be specific ("*I am the source of biometric record A in the database*") or unspecific *("I am not the source of any biometric record in the database"*). Any combination of specific or unspecific, positive or negative, first-person or third-person is possible in a claim.

To introduce the terminology of ISO/IEC 2382-37, an individual's biometric data record in a database is referred to as a "biometric reference" and the biometric sample used for comparison with the stored biometric reference is referred to as a "biometric probe". We can look for a "match" between the biometric probe of an individual and an identified biometric reference stored in the database, or we can search a population of biometric references in a database for a match with the supplied biometric probe and return an identifier for any reference that matches. In both cases, we have to set thresholds for how close the comparison has to be before we can consider the biometric probe and the biometric reference to have come from the same bodily source (a "match"). Of course, errors can be made: either by a "false non-match", failing to correctly declare a "match" when the probe and reference are indeed from the same bodily source, or by a "false match", incorrectly declaring a match when the probe and reference are from different bodily sources. We talk about the proportion of such errors over the total number of comparisons, the "false match rate" (FMR) and the "false non-match rate" (FNMR) for a given technology and a given population in a given application environment.

Systems requiring a positive claim to a specific enrolled reference treat the biometric reference as an attribute of the enrolment record. These systems "verify" that the biometric reference in the claimed enrolment record matches the probe sample submitted by the subject. Some systems, such as those for social service and driver licensing, verify negative claims of no biometric data record already in the database by treating the biometric reference as a record identifier or pointer. These systems search the database of biometric pointers to find one matching the submitted biometric probe (and the process is one of biometric identification). However, the act of finding an identifier (or pointer) in a list of identifiers also verifies an unspecific claim of enrolment in the database, and not finding a pointer verifies a negative claim of enrolment. Consequently, the differentiation between "identification" and "verification" systems is not always clear and these terms are not mutually exclusive.

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

For example, a subject might claim to be the source of the fingerprint biometric reference stored on an immigration card. To prove the claim, the subject would insert the card into a card reader which reads the reference record, then place their finger on the fingerprint reading device. The system compares the biometric characteristics of the fingerprint on the reader with those of reference recorded on the card. The system may conclude, in accordance with defined thresholds, that the subject is indeed the source of the reference on the card, and therefore should be afforded the rights and privileges associated with the card. (This does, of course, assume that the card has not been forged. All that the biometric verification achieves is to determine that the human being has presented biometric characteristics that are a close match to that recorded on the card.)

Simple "identification" might require the comparison of the submitted biometric sample with all of the biometric references stored in the database. The State of California requires applicants for social service benefits to verify the negative claim of no previously enrolled identity in the system by submitting fingerprints from both index fingers. Depending upon the specific automated search strategy, these fingerprints might be searched against the entire database of enrolled benefit recipients to verify that there are no matching fingerprints already in the system, or perhaps just the part of the database corresponding to subjects of the same sex as the applicant. If matching fingerprints are found, the enrolment record pointed to by those fingerprints is returned to the system administrator to confirm the rejection of the applicant's claim of no previous enrolment.

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

## 5 History

In a non-automated way, biometric characteristics have been used for centuries. Parts of our bodies and aspects of our behaviour have historically been used, and continue to be used, as a means of identification. The use of fingerprinting dates back to ancient China; we often remember and identify a person by their face or by the sound of their voice; and a signature is the established method of authentication in banking, for legal contracts and many other walks of life.

The modern science of recognizing people based on physical measurements owes much to the French police clerk, Alphonse Bertillon, who began his work in the late 1870s (Bertillon 1889[4]). The Bertillon system involved multiple measurements, including height, weight, the length and width of the head, width of the cheeks, and the lengths of the trunk, feet, ears, forearms, and middle and little fingers. Categorization of iris colour and pattern was also included in the system. By the 1880s, the Bertillon system was in use in France to identify repeat criminal offenders. Use of the system in the United States for the identification of prisoners began shortly thereafter and continued into the 1920s.

Although research on fingerprinting began in the late 1850s, knowledge of the technique did not become known in the western world until the 1880s (Faulds, 1880[15]; Herschel, 1880[23]) when it was popularized scientifically by Sir Francis Galton (1888[18]) and in literature by Mark Twain (1893[71]). Galton’s work also included the identification of persons from profile facial measurements.

By the mid-1920s, fingerprinting had completely replaced the Bertillon system within the U.S. Bureau of Investigation (later to become the Federal Bureau of Investigation). Research on new methods of human identification continued, however, in the scientific world. Handwriting analysis was recognized by 1929 (Osborne, 1929[57]) and retinal identification was suggested in 1935 (Simon and Goldstein, 1935[67]). However, at this time none of these techniques were automated.

Work in automated speaker recognition can be traced directly to experiments with analogue filters done in the 1940s (Potter, Kopp and Green, 1947[61]) and early 1950s (Chang, Pihl, and Essignmann, 1951[13]). With the computer revolution picking up speed in the 1960s, speaker (Pruzansky, 1963[62]) and fingerprint (Trauring, 1963a[69]) pattern recognition were among the very first applications in automated signal processing. By 1963, a “wide, diverse market” for automated fingerprint recognition was identified, with potential applications in “credit systems”, “industrial and military security systems” and for “personal locks” (Trauring, 1963b[70]). Computerized facial recognition research followed (Bledsoe, 1966 [6]; Goldstein, Harmon, and Lesk, 1971[19]). In the 1970s, the first operational fingerprint and hand geometry systems were fielded (for example, the Identimat system), results from formal biometric system tests were reported (Wegstein, 1970[77]), measures from multiple biometric devices were being combined (Messner, Cleciwa, Kibbler, and Parlee, 1974[52]; Fejfar, 1978[16]) and government testing guidelines were published (Meissner, 1977[51]).

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

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

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

## 6 Overview of biometric technologies

### 6.1 Eye technologies

#### 6.1.1 Iris recognition

Iris recognition technology is now available from a variety of commercial sources and has been used successfully in border crossing, benefit programs and access control environments. Iris recognition has been successfully used in access control applications without the need for any form of identification or claim of identity by the data subject. The data subject can be verified as allowed system access by searching through the entire database of enrolled persons. Technologies vary by vendor, with some systems collecting images from a single eye and some systems collecting images of both eyes simultaneously. Technologies are now available that can collect iris images from distances of over a metre or from persons walking through a portal.

In most implementations, a grayscale image of the iris is acquired in the near-infrared (IR) spectrum to maximize detail in eyes of all colours. To ensure pupil constriction to maximize the area of the iris, acquisition should be done in a well-lit environment. Non-patterned contact lenses and glasses do not interfere significantly with image capture. Sunglasses, however, should not be worn as these can affect the capture process. The computer algorithms unwrap these images to form a rectangular matrix of pixels over which a smaller filter is placed in multiple locations. The filter represents a smooth wave with a frequency and direction. At every filter placement, the phase of the same frequency and direction in iris image is observed relative to the filter and used to create a pattern of 0s and 1s. These 0s and 1s are the iris "features" and do not directly represent any of the visible patterns on the iris such as crypts, filaments and freckles. Features of two iris patterns are compared by counting the percentage of 0s and 1s that coincide over the length of this binary vector, a function that can be performed by a computer at the bit level with extreme efficiency. If over about ⅔ of the 0s and 1s coincide, the patterns are assumed to be from the same eye. This value of ⅔ represents a threshold that can be varied to aid in balancing the false negatives and false positives.

#### 6.1.2 Retina recognition

The retina is the light-sensitive layer of nerves and blood vessels on the inner surface of the eye. During the 1980s and 1990s, retinal recognition systems that mapped the vein patterns on the retina were commercially available. Such systems did not develop images of the vein patterns, but rather scanned an IR light beam in a circular pattern over the retina and recorded the intensity of the returned light. This resulted in a one-dimensional pattern with high values of reflected light over portions of the circle for which no blood vessel was encountered and low values of reflected light where blood vessels absorbed the IR beam. Despite rumours to the contrary, no health information was known to exist in these patterns and no laser light was ever used. Because of the requirement to shine the imperceptible IR light onto the back surface of the eye, data subjects were required to look into the scanner at a very close proximity, in near contact with the device. Today, retinal recognition devices are no longer commercially available.

## 6.2 Face technologies

Automatically identifying an individual by analysing a face is a complex process for which there are a variety of algorithmic approaches. A number of biometric vendors and research institutions have developed facial recognition systems that use digital photographs or video to capture images in visible, near IR or far IR (thermal) wavelengths. Facial recognition is made difficult by changes in images of the same face owing to pose angle, lighting, facial expression or adornment, and by the basic structural similarity of all faces (generally a mouth placed under a nose placed below and between two eyes).

Algorithms often start the identification process with image enhancement and normalization: finding eye centres, reposing the facial image to a full-frontal orientation, and adjusting for shadows etc. On the normalized image, a variety of image processing techniques are available to extract abstract measures from the image by the placement of filters over all or parts of the face. The extracted “facial features” are abstract measures not related directly to distances between “landmarks” on the face, such as nose, mouth and ears. Such measures, however, need to be both stable (not changing much for each person from image to image) and distinctive (varying greatly between persons).

At the current level of development, facial recognition technology can work quite accurately with high resolution (more than 100 pixels between the eye centres), full frontal images in good lighting. However performance degrades as resolution reduces or pose angle increases. Lighting variations also cause a decrease in accuracy.

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

Thermal imaging analyses heat caused by the flow of blood under the face. A thermal camera captures the hidden, heat-generated pattern of blood vessels underneath the skin. Because infrared cameras are used to capture facial images, lighting is not important, and systems can capture images in the dark. However, such cameras are significantly more expensive than standard video cameras and facial recognition systems based on this technology have not been commercially available since the 1990s.

## 6.3 Finger and palm ridge technologies

### 6.3.1 Fingerprint imaging

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

Historically, fingerprints were collected by placing inked fingers onto collection cards. In the early days of automated fingerprint recognition, those cards were then scanned into a computer. Today, inked prints are obsolete, with fingerprints being collected electronically by placing a finger into contact with a glass surface, called a “platen”. Very recently, contactless systems have been developed that use either laser or standard lighting that do not require the fingers to touch any surface.

Fingerprints derived from finger friction ridges may vary from instance to instance for many reasons. For example, finger moisture, angle of placement, pressure and ridge damage will all change the images captured. The way a subject interacts with a finger scanner is of upmost importance. This includes the height and angle of the fingerprint scanner in relationship to the data subject. Vendors are addressing these problems so that scanners are ergonomically designed to optimize the fingerprinting process.

A key difference between the various contact-based fingerprint technologies on the market is the means of capturing an image. Most large-scale systems capture finger images using the optical technique or by electronically scanning inked images from paper. Other capture techniques include capacitive, thermal and ultra-sonic devices.

In contact fingerprint systems, the optical image technique is based on the concept of "frustrated total internal reflection". A glass platen is illuminated from below at an angle of incidence just beyond the critical angle at which light becomes reflected. If nothing is touching the topside of the platen, all of the light is reflected into the camera sensor. But where a finger ridge is touching the platen, the internal reflection is "frustrated", i.e. the light rays are not reflected but pass through to the finger. Consequently, the resulting fingerprint image is dark where there are ridges and light where there are valleys, replicating the pattern obtained through traditional ink impressions.

With capacitive fingerprint sensors, the platen comprises an array of tiny cells, each smaller than the width of a fingerprint ridge. Measurement of capacitance over the cells in the array indicates where the finger ridges are in contact with the sensor, generating a fingerprint image.

Thermal techniques use silicon chip technology to acquire fingerprint data as the subject moves a finger across the sensor. Variation in temperature between the ridges and the valleys are sensed and converted into a black and white image.

Ultra-sonic imaging uses sound waves beyond the limit of human hearing. A finger is placed on a scanner and acoustic waves are used to measure the density of the fingerprint pattern.

Fingerprints can be imaged one at a time, or in combinations of two or four. An image of four fingers (index through little finger) is known as a "slap". Two "slaps" (one from each hand) are taken, followed by a single image of both the thumbs to create a "ten-print" image. In large-scale identification systems, individuals are enrolled using the optical live-scan capture process using multiple fingers, often taken as "slaps" as described above. Law enforcement AFIS systems, also known as booking stations, capture all ten fingerprints and generally do so now electronically as described above. A civil AFIS, however, need not capture all fingerprints and can operate effectively using as few as two.

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

### 6.3.2 Fingerprint comparison

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

We start with the premise that no two fingerprints are alike. That is, even the same finger placed twice on a fingerprint platen will produce two different images of the ridge structure. We will never be in a position of comparing two identical fingerprints even from the same finger. The variation of fingerprints from the same finger is called "within-class" variability and has many causes: 1) the ridge pattern has changed through injury or skin degradation; 2) the moisture level of the finger has changed; 3) different pressure was applied to the platen; 4) different finger orientation on the platen along any of the three axes; 5) changes in the imaging device.

So how can we compare fingerprints under such circumstances? Transform-based methods are generally based on two-dimensional Fourier transforms and Hough transforms applied to the matrix of pixels representing the fingerprint. The idea is to mathematically transform the image in some way, then compare coefficients of the transformed images. In this context, the fingerprints' "features" are the transform coefficients. ISO/IEC 19794-3[33] was developed as a standard for transform-based fingerprint transmission and storage.

Correlation based methods recognize that fingerprints, and their representative matrices from the scanner, cannot simply be overlaid owing to all the variation. However, small areas of two fingerprints, when overlaid, might be correlated. If the geometrical relationship between centres of the small areas remains about the same when overlaid to maximize correlation between the two images, maybe the images are of the same finger friction ridges.