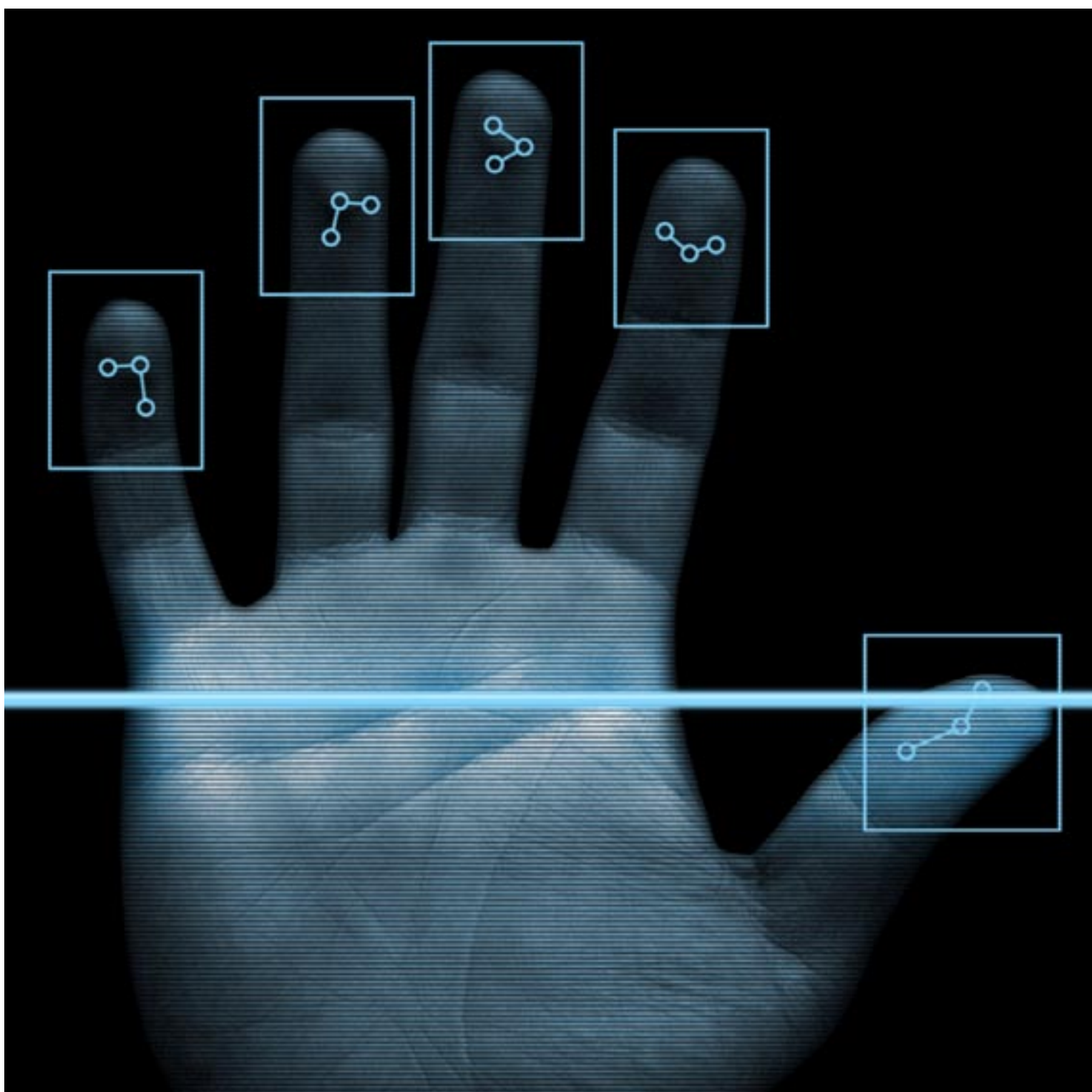


# Biometrics technology in global security



## Table of Contents

Introduction	3
Automated Fingerprint Identification System (AFIS)	4
Facial Recognition	5
Iris Recognition	6
Mobile Biometrics	
Biometrics in practise	
Multi-modal biometrics	7
Summary	

As governments engage in the fight to combat fraud, organised crime and illegal immigration, the demand for the further development and application of biometric technologies is increasing. Today, public officials tasked with immigration, border control, criminal justice and law enforcement, have a range of sophisticated options at their disposal – including mobile biometrics, facial/iris recognition, fingerprint matching, and multi-modal biometric solutions.



A biometric system can comprise an extensive array of biometrics identification subsystems, utilities, workstations and software development kits (SDKs). Essentially, a reader or scanning device is used for the capture of a biometric (e.g., fingerprint or facial image), which is converted into a digital format for storage and comparison against other records held in a database. During the conversion process, software identifies specific characteristics (or patterns) of the gathered information as match points, which are then processed using an algorithm into a value that can be compared against other biometric information in the database.

The primary objective of such systems is the positive identification of an individual, and there are three key elements to this process:

**i.** Enrolment – the capture of a biometric sample, which is then extracted and encoded as a biometric template and stored in a database, or on a document, together with other information (e.g., demographic data, signature etc.)

**ii.** Identification, or one-to-many (1:N) recognition – determines a person's identity by performing matches against multiple biometric templates. Positive biometric identification answers the question: "Who is this person?" or "Is this person already in my records under a different identity?"

**iii.** Verification/authentication, or one-to-one (1:1) matching – the process of establishing the validity of a claimed identity by comparing a verification template to an enrolment template. Verification answers the question: "Am I who I claim to be?"

## Automated Fingerprint Identification System (AFIS)

Proven to provide one of the highest levels of security amongst all types of biometrics to date, Automated Fingerprint Identification Systems (AFIS) allow the automatic matching of one or many unknown fingerprints against electronic databases of prints stored previously. Finger-printing is the capture of an image of an individual's fingerprints – generally either two or all ten-prints (depending on the application) – to record characteristics such as whorls, arches, loops and minutiae. Fingerprints can be captured manually on paper forms/cards using ink, or scanned directly into an AFIS using devices that sample the fingerprint area at 500 or 1,000 pixels per inch (ppi). Finger impressions left at crime scenes (latents) can be imaged directly at the scene, or 'lifted' using adhesive tape and imaged later. New-generation AFIS solutions can now process palm-prints too.

Once captured, the image of the finger/palm-print is converted into a biometric template, whereby distinctive features are extracted, enhanced and classified for comparison against other print records. Many millions of possible candidates can be compared rapidly and ranked by their likelihood of being a match. When there is a requirement for positive verification by a print technician (i.e. during criminal investigations), the AFIS assembles a collection of possible candidates as ordered by the search and matching process, and delivers these candidate images to a display station for review/verification by the fingerprint operator.

### A typical AFIS will comprise the following:

- Data Server – a central repository (e.g., an Oracle database) for storage and near-immediate retrieval of all ten-print, palm-print and latent images for each unique print record, together with associated features and textual data (known as 'descriptor' data)
- Work stations – equipped with a camera and scanner to enable the capture, encoding and submission of finger/palm-print images, slap (also called 'plan' or 'flat') impressions, rolled fingerprint images, photographs, signatures and demographic information. A large viewing area and a variety of image enhancement tools, such as 3D viewers, might also be incorporated to help the operator to see more unique print information in detail (e.g., pores) and improve placement/matching of minutiae
- Review stations – designed for the dedicated review and verification of ten-prints, latent images and palm-print search results. Match analysis, quality control, reports and system administration can also be conducted
- Live verification stations – for the identification of individuals when the subject is present at the time of processing. This is achieved by acquiring his/her biometrics (using any one or multiple capture devices) and verifying them against a biometrics database or secured credential containing biometrics – i.e. 2D barcode, contact or contactless smartcard
- Optional peripherals – portable and single-finger scanning devices, cameras, two/ten-print card printers, automated case management systems, web servers, application servers, mobile gateways, descriptor import/export modules
- Interfaces to external systems – e.g., other national databases, or international systems such as Interpol or EURODAC – that facilitate the electronic transmission of fingerprints from the local agency to the destination fingerprint system(s)

In many parts of the world, it is common practice for fingerprints to be taken for civil identification purposes – when obtaining an identity card, driving license or registering to vote, for example. There are also implementations of AFIS to control the abuse of welfare benefit systems and to tighten border security. Future applications might also include personal access protection, banking security and business-to-business transactions.

## Facial Recognition

Facial recognition is the automated or semi-automated process of matching facial images. Captured via a camera/scanner, the image of the face is analysed in order to obtain a biometric template. Individuals are identified by the sections of the face that are less susceptible to alteration, e.g., the upper outlines of the eye sockets, the areas around the cheekbones and the sides of the mouth. Facial recognition requires only minimal cooperation or awareness from the subject and is suitable for non-intrusive security checks at high-risk public sites (i.e., airports, borders) and for passive identification and monitoring of known suspects. It can also be used to compare static images, such as digitised passport photographs.

So far, much work has been focused on facial recognition techniques using two dimensional images (2D facial recognition) although more recently, advances in techniques for recognition with three dimensional facial images (3D facial recognition) show promise in improving match accuracy:

- 2D facial recognition – uses information from a two-dimensional image of a face, such as a photograph, to compare relative positions of facial features. For practical applications, the ability of the algorithm to cope with the relative aspect of the comparison is particularly important because image scale (actual size of the face) and orientation of the face are generally unknown and are frequently different between the file image and comparison image. A typical 2D facial recognition system will comprise:
  - Work station – automated management system incorporating a camera/scanner for the capture of photographs, or 'mugshots', for rapid search against a biometric database,

as well as other shared records repositories

- Data entry station – for the entry of descriptor data (names, supplementary text information) and collection of images (mugshots, scars, marks, tattoos, etc.) via an automated photo imaging application
- Optional modules – facial composition, facial recognition, wristband and ID card, etc.

- 3D facial recognition – the capture of a three dimensional image of a face that includes information on depth, so that the image can be viewed and analysed from a range of orientations. This means that although the scale of the face in the image is a variable, the orientation of the face is accommodated more readily. A key component of a 3D recognition solution is an Enrolment Station, which is equipped with a special projector and digital camera and uses advanced optical technology (structured light in near-infrared range,) and algorithms to produce both a 3D biometric template and a standard 2D colour image of the subject. This process entails the following:

- Face Capture – a camera projects an invisible structured light pattern onto the face. The light pattern is distorted by the surface geometry of the face, enabling the camera to precisely record the pattern distortion
- 3D Reconstruction Process – the distorted pattern is input into a 3D reconstruction algorithm and a 3D mesh of the face is created in real-time by means of triangulation
- Feature Extraction and Matching – a biometric template is extracted from the 3D facial geometry (e.g., skull curvature) and is based on the unique rigid tissues of the skull, which are unchanging over time. The resulting

numeric template is stored in an ordinary database, with identification performed by matching the biometric template against the enrolment database

- Verification – performed by matching the biometric template against a template stored on portable media (smartcards or documents)

Currently, standards are being developed to include 3D face in e-Passports. There is also technology available to integrate 2D and 3D technologies such that current investments can be protected and the benefits of the new technology used fully.



## Iris Recognition

It is estimated that an iris – the coloured ring around the pupil – has approximately 250 distinctive characteristics and that the odds of two people having the same pattern are 1 in 7 billion. One approach to Iris recognition is to use these distinctive characteristics to define the boundaries of the iris, establish a coordinate system over the iris and then define the zones for analysis within the coordinate system. Typically, Iris recognition entails the following:

- Iris scan – a photograph of the iris is taken under near-infrared illumination using a camera which, typically, captures images over narrow-angles. The subject must therefore position their eyes accurately in the camera's field of view. The resulting photograph is analysed using algorithms to locate the iris and extract feature information to create a biometric template known as an 'IrisCode'
- Feature extraction – firstly, the iris, pupil and both eyelid boundaries must be localised to determine the location of the iris in the picture. An IrisCode is then created using proprietary algorithms and stored in a template, either in a local or centralised database, or portable media (smartcards, tokens)
- Comparing templates – both verification (1:1) or identification (1:N) modes involve taking a live photograph of the iris to be matched, and comparing the resultant IrisCode against the stored template (1:1 for verification) or with N IrisCodes registered in a database (1:N identification)
- Matching – As with all biometric systems, this process produces a score that is then forwarded to the decision process, which compares the specific score to a decision threshold that may be adjusted as required

Some of the major applications of iris recognition currently include: immigration control/border crossing (using verification, identification or watch-lists), aviation security, controlling access to restricted areas/buildings/homes and database/login access. There is also a registered traveller (fast pass) solution operating at airports throughout London, UK.

## Mobile Biometrics

Mobile Biometrics systems provide public officials with remote access to fingerprints, facial/iris images and data records, across agency, jurisdictional and country boundaries. Biometrics captured out in the field can be transmitted via secure radio or telephony networks to local and nationwide databases, allowing queries of travel/visa records, identity cards and criminal justice information. Queries are processed by a central database and responses returned. If desired, the transaction can take place in the handheld unit carried by the public official. Optional hardware includes peripheral devices such as cameras and printers.

### Mobile Biometrics delivers four key capabilities:

- 1:N local identification – the ability to capture and search one or more fingerprint(s) against a portable database stored on a handheld device in situations where communications may be limited
- 1:N remote identification – the capability to perform searches against designated segments of remote databases using records transmitted via wireless technology from a handheld biometric capture device
- 1:1 local verification – the means to match one fingerprint against another fingerprint to verify that the two are the same. This requires the use of a smart card or other machine-readable

embedded biometric solution. The person responsible for performing the authentication would be equipped with a hand-held device able to acquire the reference print from the credential, together with any other appropriate identification and/or photo image information and match that information to the person holding the card

- 1:1 remote verification – the ability to match one fingerprint against another fingerprint stored at a remote location to verify identity and establish that the record is maintained in the database

Mobile biometrics is already proving essential in helping European governments to strengthen immigration control and ensure effective identity management. One of the key objectives of any biometric system is to facilitate the free and easy movement of persons across borders. Travellers in particular, cannot wait for hours at border control points. Mobile biometrics is therefore an easy way to add security without slowing the traveller down, since public officials have the necessary tools at their disposal to identify those individuals that have already entered the country but are subsequently found to be without valid visas or identification documents.

## Biometrics in practise

After 30 years of development, implementation and operational use of fingerprints for criminal identification, and at least 25 years of more limited application for access control, particularly in high security environments, the biometrics industry is ready for broader civil applications. Today, border control is one of the fastest growing applications for biometrics. The Swiss National Police (Fedpol) for example, implemented a centralised AFIS in 1984 and now maintains three national databases: Demographics, DNA Profiles and Fingerprints. These records can be cross-referenced to provide more information

on an individual when a match, or 'hit' is found – for civil identity-management purposes, as well as during police investigations.

Fedpol upgraded its AFIS recently and deployed mobile biometrics at its border control points and at embassies throughout the country. Border Guards use two-finger 'scanning sticks' to capture the thumbprints of suspicious individuals attempting to cross the border. The prints are downloaded via USB to a ruggedised PC or laptop running an AFIS client and transmitted to Fedpol's central database. The prints are then searched and any hits verified, with the individual's information sent back to the AFIS web server, ready for download by the Border Guard. In 2005, more than 13,000 prints were captured by the Border Guard and amongst other 'AFIS hits' an individual travelling on false documents was apprehended and subsequently identified as a murder suspect using a two-fingerprint check.

Similar systems to that of Fedpol are being deployed in a number of European countries, including Cyprus and Sweden. In Belgium, the Refugee Bureau is already an established user of AFIS and has implemented mobile biometrics to check an asylum claimant's identity, and the identity of those suspected of being in the country illegally, against both its national database of fingerprints and that of EURODAC.

Naturally, fingerprint identification of criminals in law enforcement continues to be a major application for AFIS. The introduction of palm-print identification is a major advancement however, and has been a key requirement in a number of recent biometric system upgrades implemented by police forces in Europe. Switzerland's Fedpol for example, expects to produce up to 25% more hits during crime scene investigations using palm-print identification.

## Multi-modal biometrics

Based around a core AFIS, the latest-generation Biometric Identification Systems (BIS) offer full biometric integration – with the inclusion of fingerprints, palm-prints, facial images, descriptive data, signatures and documents. Known as 'multi-modal biometrics', BIS delivers a comprehensive solution for investigation, identification and verification in both criminal and civil markets. Multi-modal biometrics – or 'fusion' technology as it is otherwise known – optimises the results, consequently achieving more accurate responses.

At the present time, the Serbian Ministry of Interior is deploying a nation-wide, integrated identification system, using BIS to meet four objectives:

- Enable biometric identification for civilian purposes and to supply governmental agencies with the biometric data of criminals
- Provide the integrated biometric component to the National Civil Identification solution
- The deployment of civil devices throughout the country that allow officials to conduct 2-finger searches and facial matching
- Provide state-of-the-art latent matching capabilities to forensics

The Serbian Mol's BIS includes AFIS, facial/photo image capture, fingerprint and palm-print scanning technologies, and is part of a larger project undertaken for the management of all identification – such as passports, driving licenses and other government-issued identification documents. The success of this multi-faceted biometrics solution will undoubtedly drive forward future deployments of integrated biometric solutions.

## Summary

In a world where freedom, security and justice is recognised as paramount to peace and prosperity, biometrics is able to offer a filter that can enhance the freedom of the individual whilst ensuring the security and well being of citizens from all nations. In the EU, the goal of achieving such aims without internal borders relies heavily on the effectiveness of government agencies and the success of biometrics technology such as electronic travel documents, the EURODAC initiative, the future second generation of the Schengen Information System (SIS II), the visa information system (VIS) and cooperation between Member States.

Today, biometric technology is capable of providing accurate answers to the question, "Are you who you say you are?" The adoption of open-standards will further enhance the scope and capability of this technology to provide a more unified international approach to verifying an individual's identity in the interests of national and global security and justice. In the civil market too, a variety of future biometric applications promise to enhance the personal security of individuals on a daily basis. Biometrics can provide an effective measure against fraud and identity theft in applications as diverse as personal access (to buildings or computers for example), banking security; business-to-business transactions and e-commerce.





MOTOROLA and the Stylized M Logo are registered in the U.S. Patent & Trademark Office.

All other product or service names are the property of their respective owners.

© Motorola, Inc. 2006.

[www.motorola.com](http://www.motorola.com)