

# An introduction to biometrics

## **CONTENTS**

- 3 Executive Summary
- 4 Biometrics: A brief history
- 6 Current Biometric Information Systems (BIS)
- 7 Emerging BIS
- 8 Why biometrics is important
- 9 Biometrics in the European Union
- 10 Big Brother Fears
- 11 Glossary of Terms

# Executive Summary

## **“Are you who you claim to be?”**

This is a question that is increasingly being asked of individuals by governments and business organisations in their bid to fight fraud, organised crime and terrorism, as well as to combat illegal immigration. Biometrics technology using advanced computer techniques is now widely adopted as a front-line security measure for both identity verification and crime detection, and also offers an effective crime deterrent. A term derived from ancient Greek: ‘bios’ meaning ‘life’ and ‘metric’, ‘to measure’ – biometrics embraces a range of techniques such as fingerprinting and handwriting recognition for identity verification using physical data and/or behavioural patterns.

## Biometrics: A brief history

Measurement of physical features such as height, eye colour, scars, etc, as a method of personal identity is known to date back to the ancient Egyptians. Archaeological evidence of fingerprints being used to at least associate a person with some event or transaction is also said to date back to ancient China, Babylonia and Assyria. But it was not until the end of the 19th century that the study of biometrics entered the realm of crime detection. Alphonse Bertillon, a French police clerk and anthropologist, pioneered a method of recording multiple body (anthropometric) measurements for criminal identification purposes. Known as 'Bertillonage' it was adopted by many police authorities worldwide during the 1890s, but soon became obsolete once it was recognised that people could indeed share the same physical measurements.

Meanwhile, the quest for a physical identifier that was unique to each individual gained significant ground when British anthropologist, Sir Francis Galton, worked on the principle that fingerprints were permanent throughout life, and that no two people had identical fingerprints. Galton calculated the odds of prints from two people being identical to be 1 in 64 billion and also identified characteristics – known as 'minutiae' – that are still used today to demonstrate that two impressions made by the same finger match. Minutiae are points of interest formed by the endings or forking of the friction skin ridges on each finger and are defined as one of the following:

- Ridge ending – the point at which a ridge terminates
- Bifurcation – the point at which a single ridge splits into two ridges

It is the arrangement of all the minutiae in terms of their location, orientation of ridge flow and type (i.e. ridge ending or bifurcation) that make an individual's fingerprints unique.

The flow of the friction skin ridges also form the patterns – the whorl, arch and loop of each finger

It is the arrangement of all the minutiae in terms of their location, orientation of ridge flow and type (i.e. ridge ending or bifurcation) that make an individual's fingerprints unique. The flow of the friction skin ridges also form the patterns – the whorl, arch and loop of each finger – that were identified by Galton.

Galton's patterns provided the basis of the first fingerprint file established in 1891 by Juan Vucetich, an Argentine police officer, who became the first to use a bloody fingerprint to prove the identity of a murderer during a criminal investigation. In 1897, Sir Edward Henry, a British police officer serving as Inspector General of the Bengal Police in India, also developed an interest in the use of fingerprints for identifying criminals, even though the Bengal Police was at that time using Bertillonage. Based on Galton's observations, Henry and colleagues established a modified classification system allowing fingerprints captured on paper forms using an ink pad to be classified, filed and referenced for comparison against thousands of others. By 1901, Henry's fingerprinting system had been adopted in the UK by Scotland Yard and its use then spread through most of the world (the exception being South America, where the Vucetich system was used) to become a standard method of identity detection and verification in criminal investigations.

With the advent of computers and digital technology in the 1970s, fingerprinting took on a new dimension. As a result, the UK's fingerprint service now records 120,000 sets of fingerprints each year – a volume of records that was simply untenable before computerisation. Within a century, biometrics had evolved from tape measure, ink and pad techniques requiring vast manual filing and archiving resources, to an automated biometric digital scanning process using computerised storage, automated search and find/match techniques, plus extensive archiving and access systems with worldwide links. Such technology now provides for the capture and processing of biometrics information and has transformed fingerprinting techniques and procedures.

In the mid-1960s, the Royal Canadian Mounted Police (RCMP) adopted an automated video tape-based filing system allowing identification officers to make fingerprint comparisons on-screen. A similar 'Videofile System' was installed at New Scotland Yard in 1977. Around the same time, the USA's Federal Bureau of Investigation (FBI) was working with industry to build the first automated fingerprint card reader, which was implemented in 1974. Over the next five years, the FBI and other organisations in Canada, Japan and the UK, developed further core technologies including fingerprint matching hardware, plus automated classification software and hardware. By the early 1980s, this culminated in the automatic fingerprint identification system (AFIS), which allowed the automatic matching of one or many unknown fingerprints against an electronic database of known prints; another major forward step in the world of crime detection and international security. Such systems have since reduced the manual capture, store, search and match processes for fingerprints from weeks and months, to hours and minutes, and have led to AFIS being deployed by law enforcement agencies in Europe and world-wide.

## Current Biometric Information Systems (BIS)

Biometrics is, essentially, based on the development of pattern recognition systems. Today, electronic or optical sensors such as cameras and scanning devices are used to capture images, recordings or measurements of a person's 'unique' characteristics. This digital data is then encoded and can be stored and searched on demand, via a computer. Such biometric search is not only very rapid (often taking place in real-time), it is also a process that is accepted globally in establishing forensic evidence in a law court. Consequently, there are numerous forms of biometrics now being built into technology platforms. The most widely applied methods include:

### FACIAL RECOGNITION TYPES

- **Type 1**  
Photo ID recognition
- **Type 2**  
High restriction live image
- **Type 3**  
Low restriction live image
- **Type 4**  
No restriction

**Fingerprints and palmprints** – uses impressions printed on paper or card with ink, or digital scans of an individual's fingers (or palms) to record their unique characteristics. The risk of a duplicate print/scan occurring is now estimated at being 10 to the 48th power: in other words, each finger print is as close to being 'unique' as you can get. Fingerprints therefore remain the most powerful and widely used biometric technology in forensics. A common statistic however, is that 30% of crime scenes include palmprints, which is why these are also captured and processed using the latest AFIS solutions.

**Facial recognition** – identifies people 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. 2D facial recognition, as the name suggests, uses information from a two dimensional image of a face –such as a photograph – and relies on the comparison of relative positions of facial features. Substantial work has been devoted to 2D facial recognition but, more recently, advances in techniques for 3D facial recognition (which includes information on depth and enables images to be viewed and analysed from a range of orientations) show promise in improving match accuracy. It should also be noted that facial recognition is the only viable recognition technology able to operate without the subject's cooperation, since facial characteristics can be captured from video cameras or closed-circuit television (CCTV). The accuracy of facial recognition however, is heavily dependent on the quality of the facial image and the consistency of its capture. As such, there are four types of facial recognition that vary in accuracy. The most accurate results are obtained from systems where the image capture is tightly controlled:

- **Type 1: Photo ID recognition** – whereby the picture image on an identification document is compared to the individual carrying the document. The picture image could also be compared to an image captured when the document was issued, to ensure that the document is not a forgery
- **Type 2: High restriction live image** – the individual places their chin on a certain spot while their picture is taken. This picture is then compared to the an original image stored on a computer
- **Type 3: Low restriction live image** – the individual is asked to stand in a marked area and look forward while their image is captured and then matched or rejected when compared to an original image stored on a computer
- **Type 4: No restriction** – the individual walks through a security area and their image is captured and compared to the original image

**Iris recognition** – uses a high-quality camera to capture a black-and-white, high-resolution image of the iris (the coloured ring surrounding the pupil). It has been estimated that with an average of approximately 250 distinctive characteristics in an iris, 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. The accuracy of Iris recognition however, is dependent on the cooperation of the subject. For example, criminals have been known to use eye drops to dilate their pupil to hide the majority of their Iris.

## Emerging BIS

Although fingerprints, facial images and iris recognition offer a proven methodology for mainstream applications, biometric alternatives are still being developed. Other physiological or behavioural characteristics have, and are, being researched – some of which are not yet viable, while others, although available commercially, are inappropriate for mass market application:

- **Hand geometry** – the capture of measurements encompassing the width, height and length of the fingers, distances between joints and shapes of the knuckles. While reasonably diverse, the geometry of an individual's hands is not necessarily unique.
- **Voice recognition** – focuses on differences resulting from the shape of vocal tracts and learned speaking habits. Operates best when there's no background noise.
- **Signature recognition** – analyses a series of movements that contain unique biometric data such as personal rhythm, acceleration and pressure flow. Since these movements can vary with each signing, differentiating between the consistent and the behavioural parts of a signature is difficult.
- **Keystroke recognition** – assesses the user's typing style, including how long each key is depressed (dwell time), time between key strokes (flight time) and typical typing errors. This is more suited as an internal security technology, such as providing computer access within an organisation.
- **Gait recognition** – captures a sequence of images for analysis of how an individual walks. Still in an early stage of research & development.



**Hand geometry** While reasonably diverse, is not necessarily unique.

# Verification answers the question: “Am I who I claim to be?”

## Why biometrics is important

The need to facilitate the increasing levels of international trade, migration and travel while combating organised crime and national security threats, has placed identity management high on the agenda of governments world-wide. The implementation of biometrics technology in ID-cards, passports and other travel documents is under consideration because biometrics combines two processes key to verifying the identity of an individual and establishing the validity of their documents:

- **Enrolment** – uses the capture of an individual’s unique characteristics to create a secure credential that ties their identity to the document. This then facilitates the next process of:
- **Identification and verification**
  - **Identification: one-to-many (1:N) recognition** – determines a person’s identity by searching against a biometric database. Positive identification answers the question: “Who is this person?” The response could be anything from a name or an employee’s ID number, to a criminal’s alias.
  - **Verification: one-to-one (1:1) matching or authentication** – establishes 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?”

The International Civil Aviation Organization (ICAO) has already defined standards for machine readable passports that include a facial biometric as mandatory for global interoperability. Finger and iris are also recommended by ICAO as secondary biometrics to be included at the discretion of the passport issuing authority with fingerprints becoming mandatory in 2008. Wireless technologies such as TETRA, APCO-P25, GSM/GPRS or professional mobile radio (PMR), are also adding a further dimension. Mobile solutions for example, comprising ruggedised laptops, two-finger scanning devices and wireless connectivity to a central AFIS, have been implemented in a number of European countries for law enforcement and border control. Such systems ensure remote and timely access to valuable information, such as fingerprints, facial images, and relevant demographic records and documents.

## Biometrics in the European Union

Biometric technologies are being utilised across a variety of applications – from security, fraud prevention and border control, to public aid/social benefits, customs, immigration, passport and healthcare identity verification, as well as commercial enterprise use. The Serbian Ministry of Interior (Mol) has implemented a contract to issue both national and government IDs, as well as driving licences, that will use the latest smartcard and multi-modal biometrics technology (fingerprint and facial). In Switzerland, a national AFIS with fingerprint-enabled border checks has been deployed by the National Police. And in Belgium, the Mol's Refugee Bureau has created a national AFIS for immigration and asylum, which interfaces to EURODAC – the pan-European asylum fingerprint system operated by the European Commission (EC).

EURODAC enables all immigration authorities in the European Union, plus Norway and Iceland, to search an asylum applicant's fingerprints, or those of someone who is suspected of being an asylum seeker, against the existing stored data, to prove whether or not the individual has applied for asylum in another of these countries since January 2003. If the individual is identified as having applied for asylum first in another of these countries, he/she can then be returned without a lengthy and expensive expulsion process.

Biometrics technology has become an integral part of key, EC programmes that will facilitate free movement across borders, as set out in the Schengen Agreement. Such programmes include:

- **Development of a second-generation Schengen Information System (SIS II)** – the original SIS is at the heart of the Schengen mechanism. It was created to allow all border posts, police stations and consular agents from Schengen signatory States to access data on specific individuals, vehicles or objects that have been lost or stolen. The new SIS will include storage of biometrics data.
- **Introduction of a Visa Information System (VIS)** – a central database of demographic information, digitised photographs and fingerprints, supporting Common Visa Policy for the exchange of visa information (including biometrics) between Member States. By 2010, VIS could become the largest biometric database in the world, holding 70 million sets of fingerprints. This programme also calls for the creation of a Biometric Matching System (BMS).
- **United States Visitor and Immigrant Status Indicator Technology (US-VISIT) programme** – although outside of EU jurisdiction, the US-VISIT programme is important because it requires those travelling to the US to have computer-readable passports containing biometric identifiers that comply with ICAO standards (i.e. digital fingerprints and photos). This has prompted an EU mandate that all future passports issued by Member States contain biometric identifiers.

“Formulating a workable privacy framework.....will require leadership at all levels...”

## Big Brother Fears

Not everyone sees biometrics as a helpful tool. Objections may focus on cost, effectiveness or inconvenience, while others simply do not like the idea of biometrics. Some consider it physically intrusive to, for example, pause and position themselves in relation to a biometric capture device while presenting their biometric. Verifying one's identity via a hardware device rather than by human interaction is sometimes deemed as 'too impersonal'. Fingerprint systems, in particular, face opposition because of their association with criminal applications.

Hygiene may also be a concern. For example, people may object to hand geometry scanners because they do not like to place their palms on the same surface as others. There are even fears that devices that scan sensitive areas of the body, such as eyes, may cause physical damage. Such concerns are often an emotional response to biometrics, however, that doesn't mean they can be ignored.

The greatest barrier to widespread adoption stems from public concern that biometrics technology will be used to track not just the 'bad guys' but also law-abiding citizens – creating a 'Big Brother' scenario. The possibility that biometric information could be gathered without permission or for an explicitly defined purpose, and used for applications other than identity management, is known as 'function creep' and this raises key questions:

- **What** data should be included or linked to a biometric identification card or e-passport?
- **Who** should have access to such information, legitimately or otherwise?
- **How** can people who can access such data be controlled?

Clearly such questions call for a study of the type of public policies and legislation required, as well as directives based on international agreements on how biometric databases should be used. Formulating a workable privacy framework which extends existing data protection legislation and embraces the principles of protecting personal privacy whilst not compromising national security, will require leadership at all levels if the aims of better identity management via biometric technologies are to be realised.

## Glossary of Terms

AFIS	Automatic Fingerprint Identification System
BIS	Biometrics Information Systems
BMS	Biometric Matching System
CCTV	Closed-circuit television
CJIS	Criminal Justice Information Services Division
EC	European Commission
EU	European Union
FBI	Federal Bureau of Investigation
GSM	Global System for Mobile
GPRS	General Packet Radio Service
ICAO	International Civil Aviation Organization
PMR	Professional Mobile Radio
RCMP	Royal Canadian Mounted Police
SIS II	Second-generation Schengen Information System
TETRA	Terrestrial TRunked Radio
VIS	Visa Information System



**Motorola, Limited.**

Jays Close  
Viabes Industrial Estate  
Basingstoke  
Hampshire  
RG 22 4PG  
UNITED KINGDOM  
[www.motorola.com/Biometrics](http://www.motorola.com/Biometrics)