European
Commission

The Application of Biometrics in Critical Infrastructures Operations: Guidance for Security Managers

ERNCIP Thematic Group

Applied Biometrics for CIP

Deliverable: Guidance for Security Managers

Task 2

Marek Rejman-Greene, CAST, UK
Krzysztof Brzozowski, Government Centre for Security, PL
Tony Mansfield, NPL, UK
Raul Sanchez-Reillo, University Carlos III, Madrid, ES
Peter Waggett, IBM, UK
Geoff Whitaker, CAST, UK

March 2015

The research leading to these results has received funding from the European Union as part of the European Reference Network for Critical Infrastructure Protection project.

Report EUR 27191 EN

Joint
Research
Centre

European Commission
Joint Research Centre
Institute for the Protection and Security of the Citizen

Contact information
Georgios Giannopoulos
Address: Joint Research Centre, Via Enrico Fermi 2749, TP 721, 21027 Ispra (VA), Italy
E-mail: erncip-office@jrc.ec.europa.eu
Tel.: +39 0332 78 6211
Fax: +39 0332 78 5469

http://ipsc.jrc.ec.europa.eu/
http://www.jrc.ec.europa.eu/

Legal Notice
Neither the European Commission nor any person acting on behalf of the Commission
is responsible for the use which might be made of this publication.

JRC95453

EUR 27191 EN

ISBN 978-92-79-47446-0

ISSN 1831-9424

doi:10.2788/761739

Luxembourg: Publications Office of the European Union, 2015

Printed in Italy

The Application of Biometrics in Critical Infrastructures Operations:

Table of Contents

Table of Figures

Abstract

Biometric technologies have advanced considerably over the past decade, and have paved the way for more widespread use by governments, commercial enterprises and, more recently, by the consumer through the introduction of sensors and apps on mobile phones.

This report provides introductory information about the application of these technologies to achieve secure recognition of individuals by organisations which form part of critical infrastructures in the EU. As a specific example, it offers guidance about the implementation of physical access control systems using biometric technologies.

It is principally addressed at managers and security officers within these organisations. With the information in this report, managers and officers should be in a better position to discuss their specific requirements with technology suppliers, specialist systems integrators and consultants – and therefore lead to applications which are more secure without compromising on their usability.

The report emphasises the importance of considering the effectiveness of the entire application – and not just focussing on the performance of the biometric subsystem.

Note that the representation of specific devices does not imply any recommendation by the authors or the European Commission.

1 FOREWORD

This report has been compiled by the ERNCIP thematic group on Applied Biometrics.

It provides introductory information about the application of biometric technologies to achieve secure recognition of individuals by organisations which are responsible for parts of critical infrastructures in the EU.

Many security systems, such as access control or CCTV surveillance, could be improved by the use of biometrics. However, the proper implementation of a system which uses biometrics is crucial if the system is to prove effective. Every step of implementation of a system (from collecting requirements, to design, installation, training, service, etc.) requires careful attention.

This guidance is designed to help all involved in the implementation of a biometric system such as the security officers, managers and operational teams.

As a specific example, it offers guidance to operators on the implementation of physical access control systems using these technologies.

2 INTRODUCTION

ISO[1], the International Organization for Standardization, defines biometrics as

> 'automated recognition of individuals based on their biological and behavioural characteristics'.

Some biometric characteristics (e.g., the ridge-pattern on a finger imaged by a fingerprint sensor) are predominantly biological, and are relatively unaffected by conscious efforts of the individual. Other characteristics (e.g., the speech being recorded by a speaker recognition system), where the individual has to engage more actively in the process, may be predominantly behavioural.

Often, the focus in critical infrastructure applications will be on the use of biometrics in computerised applications, where the system incorporating the biometric function is designed to operate with only limited human intervention.

There will be times when the automated system is unable to recognise the individual; for example an individual may have injured their finger, have the fingerprints abraded through repeated contact with brick dust or be missing a finger. For these cases, there needs to be a fall-back process to check whether or not the person is who they claim to be. An assessment should be made early on to determine the number and types of problem cases in the target population of users.

Hence, the biometric component is almost always a part of a larger system which is designed to deliver specified benefits to the organisation (see Section 5 for more detail).

In understanding the accountability for the successful implementation and use of biometric applications, it is important to identify the principal roles and responsibilities of key organisations.

- The **Operator** of the application, typically with responsibilities for
    - Definition of the business requirements
    - Clarification of the appetite for risk by the organisation
    - Management of the legal contexts, such as health and safety, accessibility issues and management of personal data and biometric data
    - Operation of the enrolment and user deletion processes
    - Assurance that security and logging/audit services are maintained to the required level
    - Consideration of a fall-back system in case valid users are unable to be recognised
    - Effective management of communications with those affected by the introduction and use of biometrics

- The **Systems Integrator** typically with responsibilities for
    - Design and delivery of the application (which may include fall-back systems)
    - Provision of advice on legal implications of the use of a specific modality
    - Development of approaches to system security, health and safety and usability that address the business objectives of the operator
    - Development of the testing programme, ensuring that the significance of the results of testing are communicated in an appropriate way to the operator

[1] More specifically, it is the subcommittee of the ISO/IEC international standardisation group which addresses biometrics and their applications (JTC1 SC37)

  - Advice on whether aspects of the biometric subsystem should be designed or operated in accordance with international standards
  - Undertaking the programme to train users of the system, either by outsourcing to a specialist company or engaging with the supplier of the biometric subsystem to develop and deliver this directly to the operator's organisation.

- The **Supplier** of the biometric subsystem should
  - Provide the hardware and software to the integrator together with details of interfaces to other systems and services
  - Supply information about the impact of changes in any of the user-definable parameters in the software, and data on the interfaces to externally delivered security functionality
  - Offer information on training users and systems administrators, and on maintenance procedures for hardware and software.

In some applications, the human aspects of the system are included as an explicit part of the application, for example, in resolving the alerts which are raised when a facial recognition system operates on video footage from a specifically designed CCTV system.

Many types of biometric system have been described in research papers, but for today's practical applications by operators of critical infrastructure systems, two aspects are of particular significance.

The first aspect is the **type of application**; examples of which include

- verification of a claimed identity in an access control system to a building, perhaps using a fingerprint biometric system and

- identification of an individual seen on a CCTV camera and included in a 'watch list' of people of interest.

The second aspect relates to **biometric modality**[2]; i.e. the specific type of biological or behavioural characteristic which is employed.

Of the many modalities which have been researched, the following have been commercialised and are likely to be of interest to operators of CI systems:

- Fingerprints
- Facial features
- Iris patterns
- Hand geometry
- Pattern of veins in a finger, or within the palm of a hand.

Further information about some of these modalities is provided in the context of an access control application in Section 4.

[2] Biometric modalities are different types of biological or behavioural characteristic which can be utilised in automated recognition.

3 POTENTIAL BIOMETRIC APPLICATIONS FOR USE IN CRITICAL INFRASTRUCTURES

Biometric technologies can be applied in a number of ways, many of which are relevant to the requirements of operators of critical infrastructures who need to maintain the appropriate level of security. Among these applications are:

a. physical access control, to a site or to internal areas within a site (see more information below);

b. logical access control, to computers and mobile devices;

c. 'on-the-spot' verification of identity, challenging the identity of an individual in a specified zone using mobile biometric devices;

d. verifying the identity of individuals either entering or leaving a country through the use of Automated Border Control (ABC) gates and systems;

e. verification of identity against biometrically secured identity documents at places other than at the national border, e.g. on the first day at a workplace or prior to allowing access to computing facilities;

f. surveillance systems to identify unknown individuals, e.g. individuals repeatedly being seen in the neighbourhood of critical facilities using biometric recognition in combination with video surveillance systems (see more information below);

g. vetting of new (or existing) employees and managers as part of a criminal record or counter terrorism check;

h. authorisation and audit of key/critical actions in operation of facilities, to ensure that only authorised personnel are able to initiate specific functions;

i. confirmation of specialised training and qualifications, e.g. in a decentralised organisation with branches in different regions and countries, to allow managers to confirm that certificates of competency have not been tampered with;

j. to ensure integrity of critical components in critical infrastructure networks/facilities, through sign-off of by competent and identifiable individuals (the specific component or tests results can be individually marked with a digitally signed biometric identifier);

k. maintenance of the integrity of documents with a digital signature which includes biometric data of the author.

The ERNCIP Thematic Group on Applied Biometrics has proposed standards for two applications:

1. **Physical access control**
   This is a well-established application with many biometric reader units available. A European (CEN) standard is in development which is based on an existing UK national specification for access to high security areas.

Other applications, such as biometric Automated Border Control (ABC) gates share similarities with physical access control.

2. **Surveillance systems using automated facial recognition**
This application compares faces found in the field of view of one or more video surveillance system cameras with reference images of people of interest.

Work on a three part ISO standard is underway under the following projects:

- ISO/IEC 30137 Use of biometrics in video surveillance systems Part 1: Design and specification;
- ISO/IEC 30137 Use of biometrics in video surveillance systems Part 2: Performance testing and reporting;
- ISO/IEC 30137 Use of biometrics in video surveillance systems Part 3: Data Formats.

4 BIOMETRIC MODALITIES

4.1 Fingerprints

Fingerprint sensors are to be found in the widest range of biometric physical access control subsystems. Fingerprint sensors may use

- Optical sensors (Often these use illuminated glass platens, the platen forming part of a prism and camera arrangement such that frustrated total internal reflection highlights the finger ridges in contact with the platen) or
- Solid state sensors, imaging the fingerprint electronically.

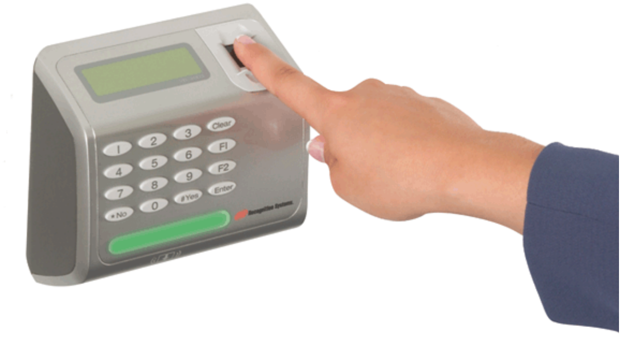

Figure 1: Fingerprint Reader

For verification systems, such as access control, fingerprint sensors that image a single finger are generally used. For identification in large populations, much larger format 'slap sensors' are also available, capable of simultaneously imaging four fingers from the one hand. When necessary, many sensors can be configured to deliver images in conformance to international standards, thereby facilitating cross-checking against law enforcement databases.

It is usual to enrol two fingers from each user, as this provides resilience should one finger be damaged or unusable for other reasons.

It is important to observe the guidance from the supplier of equipment on positioning of the reader. For example, systems can be affected by direct sunlight. There may also be difficulties in obtaining sufficient fingerprint detail in very low or very high humidity environments or in cold weather conditions.

Usability can be affected by the height at which the fingerprint reader is placed, and even the angle at which the sensor is mounted. Ignoring such usability considerations may result in poorer performance of the biometric subsystem. Even if users adjust their behaviour, it may impact on their satisfaction with the operation of the unit.

For evaluation of the software used in fingerprint systems, NIST, the National Institute of Standards and Technology in the USA, runs tests under the Proprietary Fingerprint Template Test Phase II programme (PFTII) to measure the performance of matching software using the vendor's proprietary fingerprint templates[3].

Many systems use variants of the minutiae approach (Fig 6) as a starting point for creating templates.

In some countries and cultures there may be an association in the minds of the user population between the use of fingerprint biometric systems for automated recognition and fingerprint forensic systems used in police work. The extent of such an association - and the impact this may have on the willingness to use biometric systems - may need to be ascertained through consultation, surveys and focus groups.

4.2 Hand geometry

Hand geometry devices similar to the type shown in Fig 2 have been used extensively for over 30 years for access control as well as for time-and-attendance applications. The reflection of ambient light illuminating the reflective base plate and collected by sensors on the underside of the number pad is modified by the presence of the fingers and palm of the right hand. Reproducible operation is realised by ensuring that users position their fingers against the four posts on the base plate.

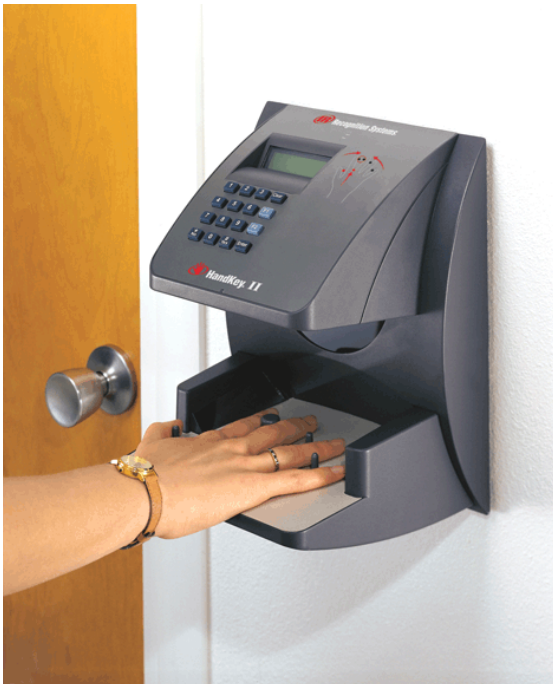

Figure 2: Hand geometry device

4.3 Iris patterns

This biometric modality makes use of the considerable amount of detail in the coloured part of the visible eye. In the 1990's, Iridian patented the approach and a very powerful comparison and matching algorithm. Since the expiry of the patents, other algorithms have been developed and a number of suppliers offer access control systems.

[3] http://www.nist.gov/itl/iad/ig/pftii.cfm and results page at http://www.nist.gov/itl/iad/ig/pftii_results.cfm

In normal operation, the eyes are illuminated by near infrared light to ensure that detail from both light and dark coloured irises is captured optimally.

Systems are now available which collect images of either one or both irises at a distance of up to two metres. In contrast, the earliest devices required considerable co-operation by the users to position their eyes at exactly the correct distance from the camera.

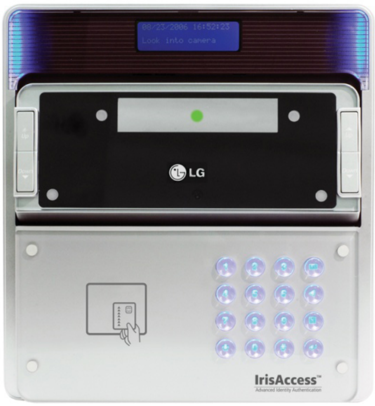

Figure 3: An iris recognition access control device

4.4 Facial images

The very simplicity of an access control system consisting of a camera and software has intrigued developers of access control systems. Though software for comparison of facial templates remains sensitive to change of pose of the head between enrolment and recognition, to uneven illumination of the face and to variable expressions by the user, the experiences gained by early adopters of the e-passport gates at airports has resulted in operationally robust systems with performance adequate to satisfy the risk appetite of the immigration authorities from a number of countries.

More compact systems have been sold extensively, for example for access control at construction sites, with some suppliers using near infrared illumination to counter the effects of uneven ambient lighting.

4.5 Finger and hand vein imaging

Devices have been developed for access control systems using the veins in the hand. In the design patented by Fujitsu, veins beneath the surface of the palm are imaged using infrared illumination. The Hitachi system images the veins of a finger using infrared illumination transmitted through the finger.

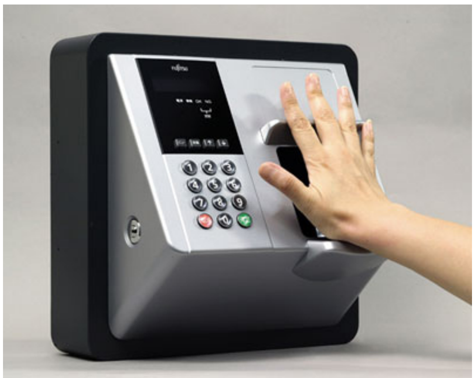

Figure 4: Hand Vein Device (courtesy of Fujitsu)

4.6 Future directions

New systems are being introduced which require that the user satisfies the requirement of two (or more) modalities before being recognised. One supplier offers a reader that incorporates sensors for both fingerprint and vein.

There is also a trend for reader units with sensors which do not require contact (e.g. some novel devices using fingerprints) and even to cater for recognition of people on the move (e.g. some iris recognition systems), while new mobile readers using smartphones are increasingly becoming available.

5 OPERATION OF A BIOMETRIC COMPONENT IN AN APPLICATION

Biometric components are usually integrated as a part of a larger, overall system that serves an application, with the latter providing one or more benefits to an operator (e.g. offering a more secure way of gaining access to a room or building). See Fig 5.

In this section we describe how the core biometric components need to be considered as part of a wider system in order to deliver those benefits. In applications where biometrics is used in the protection of critical infrastructures, it will be important to ensure that systems operate securely, but still remain usable to all who use the application.

Suppliers of biometric subsystem will rarely discuss this wider context. The basic technology as demonstrated at an exhibition, or tested in the supplier's own company, will often appear to work very well indeed. However, when integrated into the operator's environment, and with a wider range of users, the deployed system is very likely to work less well than under the idealised conditions. It is only through discussions with other operators of similar systems, and after running tests in operational applications that the true performance can be ascertained.

Biometric subsystems may include components such as:

- A tamper-resistant or tamper-evident reader through which the biometric data is collected from the user
- Computing hardware and a protected interface to deliver the result of the biometric processing
- A data store which holds biometric reference data relating to those people permitted to enter the building
- Biometric software for
    - Assessment of whether the quality of the data is sufficient for subsequent recognition – or whether the user should be asked to re-present their (for example) finger to the reader
    - Comparison of the biometric data collected from the user with one or more sets of reference data in the data store
    - Confirming whether the biometric data has indeed come from a living person and is not, for example, a plastic replica of a fingerprint
    - Communication to the overall system of the results of biometrics processing.

The overall system may, in addition to the biometric subsystem, include components such as

- A proximity card reader and associated software, which requires presentation of a valid card as well as satisfying the biometric comparison. This should strengthen the security of the recognition by requiring the user to prove their identity by both something they have (card) as well as something they are (biometrics)
- Recognition system software which i) aggregates the results from the biometric subsystem interface (match/non-match) and other non-biometric subsystems such as the proximity card subsystem, and ii) if the user is correctly recognised, to send the message to door actuation system
- Hardware to operate the door to the secured room or building, upon receipt of a message from the recognition system confirming identity
- Security functionality to protect the system (e.g. to stop repeated failed attempts or to prevent unauthorised change of the threshold for a biometric match)
- System management (such as logging of failed and successful transactions).

The organisation wishing to implement the application (e.g. secure physical access control into a room or building) will also need to consider **non-functional aspects such as**:

- An **enrolment process** for registering users' biometric references into the system. In a formal enrolment (see Section 6.1) the user's credentials (e.g. a passport) should first be checked to confirm that they are authorised to be enrolled into the system, thereby precluding unauthorised individuals from being registered. Well-designed and operated processes are needed to ensure that the best possible biometric data is captured. In some cases, there may be a need to repeat the enrolment periodically for those users whose characteristics have changed since the initial enrolment (e.g. due to aging), and which now cause difficulties in operation.
- A **fall-back solution** for cases when a correctly enrolled person fails to be matched to their reference. Fall-back solutions will also be required when individuals cannot be enrolled in the first place, e.g. due to disability – whether temporary or permanent in nature.
- A **testing policy** for the operation of the overall system to demonstrate that the operational system and/or application delivers the benefits required by the operator
- A **security policy** specifying the practices and controls for the secure operation and maintenance of the biometric system
- A **privacy policy** (and, perhaps, a Privacy Impact Assessment) to declare how personal data (including the biometric data) will be protected, and - for some systems and in some countries - to demonstrate the legal basis for processing.

It is advisable to consider all of these issues as early as possible in the design process; the later these functions are added, the more expensive and less effective these will be.

The relationship of these components is shown in Fig 5 below, which is adapted from an international standard currently under development, ISO/IEC 30124, Code of practice for the implementation of a biometric system. This standard should be consulted for further information about the design, planning and operation of applications using biometrics.

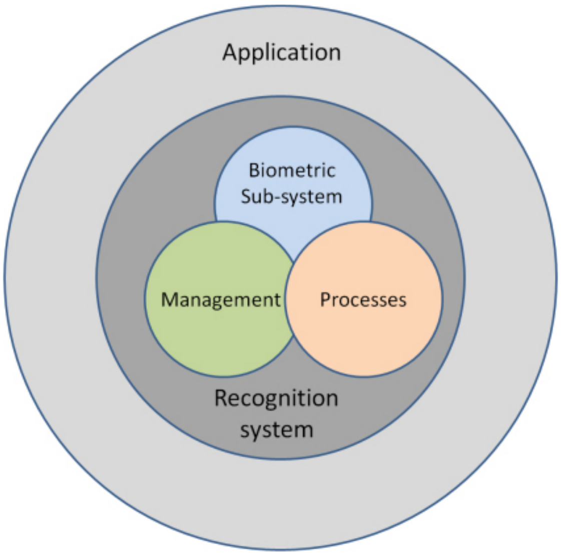

Figure 5: Relationship between a biometric sub-system, the overall system and the application

It should be noted that at the present time, many commercial biometric systems do not offer resistance to spoofing through measures such as liveness detection. This functionality will vary according to the specific modality and even the way in which the modality is implemented. For example, for iris recognition systems, the response of the iris to changes in illumination or the monitoring of the involuntary movements of the eye may provide evidence of a live iris – and that the presentation to the system is not a photograph or video clip.

System operators should also be aware that someone may intentionally present an artefact such as a glass eye while pretending to be an authorised individual (e.g. by keying in a reference number) with the aim of locking out the legitimate individual.

Adding software to counter such attacks may impact adversely on the performance of systems, through changes in the system error rates such as FAR and FRR (See Section 6). Users should insist that for systems that are required to have liveness detection, the specification and testing of systems should always relate to operation with the liveness detection functionality switched on. In case there is a need to know the contribution of a liveness detection to overall error rates, a separate testing of the biometric algorithm and the liveness detection algorithm is needed.

6 BIOMETRIC PROCESSES

At the core of the biometric component, there is hardware and software which collects the image, checks that it is of an adequate quality and then extracts features that can be used for comparison with earlier or later attempts at recognition.

Feature extraction software is designed such that the resulting digital biometric code (reference or probe) for a specific individual satisfies two criteria:

- to be as individually discriminating of a person as possible against codes for everyone else, while

- being stable against everyday changes. Changes can be **environmental** (e.g. in the level of ambient lighting which expands or contracts the iris), or **personal**, as in the impact of a common cold which changes the sound of a voice, or an emotional expression which changes the appearance of a face.

The extracted features are then encoded into a biometric probe or a biometric reference - a short piece of digital/electronic data. (Typical sizes of biometric probes and references range from 10 bytes to 25 kilobytes).

The supplier of biometric software will keep secret aspects of the biometric process such as

- the features which are selected from the output of the sensor
- the way the features are transformed into a reference or probe
- the details of the comparison process which measures the similarity between a reference (produced at enrolment) and probe (produced for recognition).

The biometric recognition process consists of a digital comparison between a biometric probe and biometric reference(s). The comparison score is then used to determine whether or not the probe and reference are from the same person.

Fig 6 demonstrates some 'everyday' changes between key features in a fingerprint taken at two times. In this simple case, the 'minutiae' – at points where the ridge of a fingerprint either ends or splits into two – will not directly superimpose on each other due to differences in finger pressure on the sensor surface. A supplier's proprietary template for this fingerprint may include the number of ridges crossed by a line between pairs of minutiae, the angle of this line when compared with lines linking other pairs of minutiae, etc.

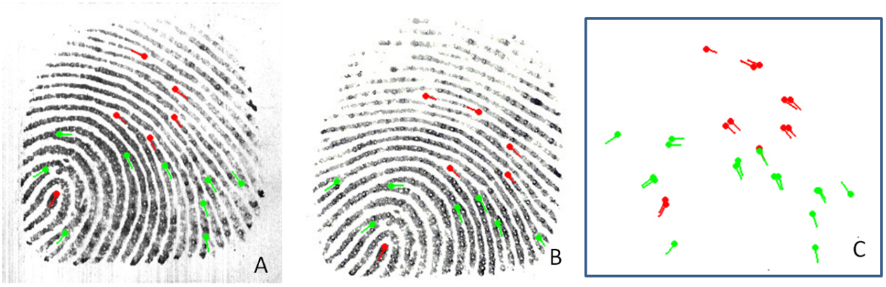

Figure 6: A and B are images of the same fingerprint taken at different times, highlighting the minutiae points (ridge endings in red, splits in ridges in green). Image C shows the overlap between the minutiae maps (after rotation, and offset).

Note that even with these transformations, some minutiae are not present in both A and B, and that some points do not precisely align, as a result of differences in pressure across the finger when it is pressed on to the sensor surface.

6.1 Stage 1: Enrolment process

In almost all applications, an individual is first enrolled into a system, in this way, 'becoming known to the system'. This provides the first of the two images or data streams which are subsequently compared in a biometric process of recognition of a person. Two types of enrolment are distinguished, depending on whether (or not) the user is present and aware of the process.

This enrolment can be **formal**, with

1. an official first checking the evidence of identity submitted by the person (e.g. birth certificate, passport, identity pass at work); this is often termed a 'registration' process

2. collection of a good quality sample of the biometric characteristic using the sensor

3. automated extraction of the relevant parts of the image and conversion into a reference

4. storage of the reference in a secure environment either on a card, inside a locally based biometric reader unit or in a centralised database.

Alternatively, the enrolment may be **informal**. For example, if an unknown individual is highlighted by the automated facial recognition system operated with CCTV surveillance cameras, the security policy for the system may require that a reference is created for the unknown individual together with a reference identifier.

In a very few cases of interest to operators of critical infrastructures, there may be no need for the collection and storage of any personal information about those enrolled. In this case, biometric systems could be used for anonymous recognition.

Lessons learnt from best practice

1. The complexity of a carefully supervised enrolment process, and the resources that must be allocated, must not be underestimated.

2. A good enrolment is key to the reliability of subsequent recognitions, and it is worth striving for the best possible image, voice sample, etc.

3. In the part of the process related to the collection of a good quality sample, it may be possible to use a 'quality assessment tool' to highlight whether the biometric sample (image or data stream) is of good enough quality to provide reliable matching when the person is required to be recognised in Stage 2. This type of software can prompt the user through information on the reader unit (or an associated display) to present the biometric characteristic for another time if the first attempt is not good enough. More sophisticated quality assessment tools can assess the biometric sample itself in detail, helping the supervisor of the enrolment to focus on specific aspects or issues and to assist the user. For example, for facial images, the tool may note that the bridge of spectacle glasses has slipped a little down the nose, with the rim obscuring a part of the eye and/or causing reflections from the glass which will interfere with the creation of a good reference.

Further information is available in the soon-to-be published ISO/IEC TR 29196, Technical Report on Guidance for Biometric Enrolment.

6.2 Stage 2: recognizing the individual using biometric comparison

Having enrolled the person, a biometric system can work with the stored enrolment reference in one of three types of application:

- **Verification**

  Confirmation of a claim by an individual that (s)he is the enrolled person through a comparison of the biometric reference collected at enrolment and a biometric probe created at the time when recognition is required.

  Note that this is a one-to-one comparison of probe to a single reference either in the database or on a card.

  The application may use a PIN pad or card reader; the PIN or card presented by the individual points to the biometric reference against which recognition will take place.

- **Identification**

  Search of a biometric probe against a database of reference templates to find and return the identifying reference number of a matched reference.

  Note that this compares probes to references on a one-to-many basis, i.e. comparing the probe against many – or all – of the references in a database.

- **Duplicate biometric check**

  A check of a (new) biometric reference against a database of biometric references to determine whether the individual already been enrolled into the database.

Note that this also compares images on a one-to-many basis.

6.3 The biometric comparison process and biometric accuracy

In all three cases (verification, identification and duplicate biometric check), we are asking the biometric subsystem to compare biometric probes and references. For example, in applications using fingerprint verification for access control, the probe created from an attempt to gain access through placement of a finger on the reader's sensor will be compared directly against a corresponding reference. A comparison score will be generated by the supplier's software which indicates the degree of similarity between the probe and reference.

Earlier in this section we showed that even when the same individual uses a biometric system over a period of time, it is unlikely that there will ever be an exact match when they use the biometric to gain access to the room; indeed, there will be a range of different comparison scores against their single reference template.

In considering how to use a biometric subsystem, it is important to ascertain the range of scores which result from comparison of probes and references collected from different individuals. If individuals 'A' and 'B' have similar probes and references 'B' might be able to impersonate 'A'.

The operator, in discussion with the supplier of the biometric subsystem, has to decide how different the templates have to be for a range of people before the risk of an accidental match of templates from two different individuals becomes unacceptable. This chance of accidental match, expressed as a probability, is called the False Acceptance Rate (FAR).

Of course, on occasion, person 'A' will be less careful in the pressure she applies to the sensor (or there may be a change in the environmental conditions, the wrong finger is used, etc.) and the comparison score with her reference template is much lower – lower than the threshold score for declaring a match. She will be rejected on these occasions. Taken across all users of a system, the likelihood of rejection is expressed as a False Rejection Rate (FRR).

These two figures of merit, FRR and FAR, are closely related as shown in Fig 7 which plots them against the corresponding threshold value for comparison scores. At the threshold comparison score represented by the arrow marked '2', the False Acceptance Rate, FAR2, is low (2%), and is represented by a point on the blue curve. However, there is a rather high likelihood of a genuine person being rejected falsely as the comparison score fails to reach the threshold for declaring a match; the corresponding False Rejection Rate, FRR2 (9%), is represented by a point on the red curve.

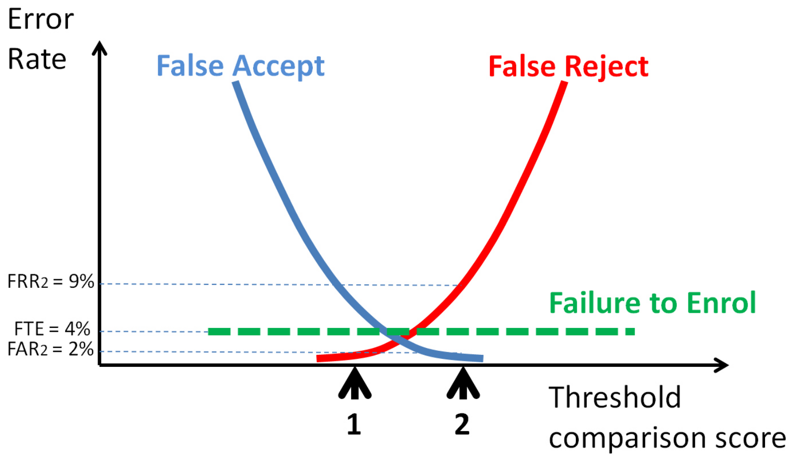

Figure 7: Simple representation of error rate curves for a biometric subsystem.
To note that, in general, the blue and red curves are not symmetrical.

If the threshold comparison score is reduced, say to point '1', we can follow the red curve to see that the FRR is now considerably lower, but that the FAR on the blue curve, the percentage chance of someone just happening to have a sufficiently similar template, is much higher.

The performance of the biometric subsystem (on its own) is therefore more secure when the threshold for comparison is set at score '2'. In contrast, setting the threshold for acceptance of an individual at score '1' will risk many more people being accidentally accepted (but at a much lower risk of the authorised person being rejected) – and hence corresponds to a more convenient and usable system.

Fig 7 also shows that some people cannot be enrolled. In this particular case, the Failure to Enrol Rate, FTE, is 4% which would be unacceptably high in many applications of interest to operators of critical national infrastructure systems, as a fall-back (non-biometric) system would need to be provided for at least 4% of the user population. However, it should be noted that suppliers of biometric subsystems rarely quote the FTE rate as this will depend on the types of individual in the test group, the design of the enrolment process, etc.

Suppliers of biometric subsystems should either produce data such as Fig 7, or provide at least a pair of FRR and FAR figures at a threshold which is sensible for the specific application of interest to the operator of a critical infrastructure facility. In the past, suppliers used to just supply one of the figures, e.g. an FAR value of 0.001%, to give the impression of a highly accurate system, a metric which is meaningless without the corresponding FRR.

There is one very important consideration. The performance quoted by suppliers or independent test houses is based on

- biometric data collected for a basic biometric subsystem,
- set up in a rather idealised environment, and
- using a group of readily available individuals (often students or employees) who may - or may not - be conscientious users trying to get the best from the system.

Once the biometric subsystem is integrated into an overall system, and operated in an application environment with a different group of users, both FRR and FAR error rates will, in general, increase above those obtained in the tests on just the biometric subsystem. It is therefore important to carry out operational tests once the application is in place, and that all security measures, such as those to protect against fake/spoof fingerprints are switched on.

Further information about error rates in physical access control systems is to be found in Section 8.2.

7 SYSTEM DESIGN AND SYSTEM INTEGRATION

7.1 Design Considerations

Looking more closely at the roles mentioned in the Introduction, we can identify the following entities that could be involved in the design of applications which include a biometric subsystem:

- vendors of the hardware readers and input devices (e.g. cameras or fingerprint sensors)
- suppliers of software for comparison of biometric features
- middleware suppliers that allow multiple biometric (multi-modal) approaches to be integrated,
- training companies
- specialist systems integrators (SIs) who draw together elements from a number of such vendors to offer a solution which meets the requirements of the organization planning to introduce a biometric-enabled access control system.

Not all system integrators have experience in the design, delivery and operation of biometric systems for the type of application envisaged by an operator. Those without experience may fail to appreciate the significance of issues which are discussed in this document. For example, the interpretation of the performance of a 'biometric system' may be different for the supplier of biometric components, the systems integrator and the operator (see Section 6.3 for the distinction between accuracy of biometric technology determined in tests of the subsystem and the performance of the overall system or application).

A "lesson learnt" in development of biometric applications is the complexity of the systems integration process, especially in contexts where biometric technologies have to be integrated with pre-existing information technology architectures and business processes. Choose your integrator carefully – you will be spending a lot of time with them! And, ask for evidence of examples of well-designed and well-performing systems which they have delivered previously to satisfied customers.

More detailed information about the systematic design of applications which include a biometric subsystem are to be found in the UK standards authority publication PAS 92:2011, Code of practice for the implementation of a biometric system[4] (from which Fig 8, the lifecycle for design and development, is extracted) and which will be superseded in due course by an ISO standard, ISO/IEC 30124, currently under development and with the same title. Operators of critical infrastructures intending to use biometric components in their applications are strongly encouraged to refer to these publications in their discussions with systems integrators.

[4] For a freely available description of the standard,, http://shop.bsigroup.com/upload/PASs/PAS92-2011leaflet.pdf

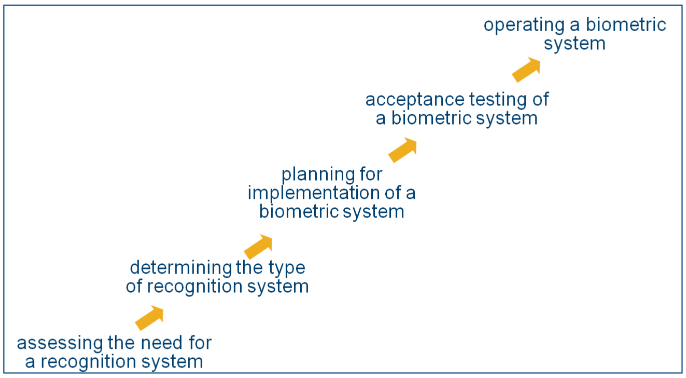
operating a biometric system
acceptance testing of a biometric system
planning for implementation of a biometric system
determining the type of recognition system
assessing the need for a recognition system

Figure 8: Life cycle model for design and development of a system using biometrics

In the design of a recognition system for operators of facilities in critical infrastructure sectors it is important to consider factors that may not be as explicitly highlighted in traditional IT systems. These include:

1. **Usability**, so that the overall system works as well as possible for almost everyone in the target population. This means that provision is made for those individuals who are less able to interface with the biometric reader, and a secure fall-back solution is included for those who cannot be recognised by the subsystem
2. **Acceptance** by the user population
3. **Legal compliance** with the provisions of the country of operation, in particular in respect of data protection and privacy legislation.

More information about these issues is to be found in a freely downloadable Technical Report from ISO[5].

In the initial phase of thinking about the introduction of a biometric subsystem, the operator should consider the business requirement in more detail. For example, the need for additional recognition functionality should be questioned. If the business case can indeed be validated, the requirement for a specific type of recognition system, e.g. a biometric subsystem, should be established. The information in this report offers guidance to help the operator in making this determination.

Once a decision has been made to work with a consultant or systems integrator, the requirements for certain non-functional aspects should be captured at an early stage, and addressed early in the design and development of the system. Experience shows that failure to consider these aspects – for example security, privacy and usability – from the start of a project can lead to more expensive and less satisfactory solutions.

In considering the specific biometric modalities, it should be noted that some will be found to be inappropriate due to environmental constraints, e.g. if gloves have to be worn to minimise cross-infection in hospital operating theatres, many simple fingerprint systems will not be usable.

Good practice in the development of systems using biometrics involves a continued focus throughout the design and development cycle on how to test the performance of the overall system

[5] ISO/IEC TR 24714-1:2008 Jurisdictional and societal considerations for commercial applications — Part 1: General guidance

once it is configured for the application. Guidance for testing in an operational context is available in two ISO standards[6]. A summary of lessons learnt in testing of larger scale systems with biometric components has been compiled by this ERNCIP Thematic Group[7].

7.2 Use of databases

Most biometric subsystems for multi-portal access control are networked in order to maintain a centralized record of transactions. Storage of the enrolment biometric data (templates), however, can be centralized or decentralized, depending upon the system. There are significant differences between these approaches that must be considered in the design of systems.

7.2.1 Decentralized storage of biometric data

Verification systems often store biometric data only on cards or tokens held by the users of the system. This approach has the advantage of allowing each person control over their own data and eliminates the need for the creation and maintenance of an accessible, but secure, centralized infrastructure.

The disadvantages are that losing an access control token or identity document will require the entire enrolment process to be repeated. In addition, without a centralized database, there can be no checking for multiple enrolments in the system. The cards and tokens themselves, and the reference biometric data on them, may need protection against counterfeiting and forgery, for example using a cryptographic digital signature.

Systems are available which allow for the comparison of reference and probe to be made directly on a card, and other systems are being trialled which include a biometric sensor on the card itself.

7.2.2 Centralized storage of biometric data

Other verification systems and all identification systems store all biometric data in a non-local database. This data can be:

- Held centrally for one-to-many identification
- Stored in a distributed database for one-to-many identification
- Held in a central database for one-to-one verification with a pointer to the specific record.

In verification systems, this has the advantage of allowing re-issue of lost tokens by checking that the stored biometric data refers to the person applying for re-issuance. Centralized databases are required in identification systems which are designed to prevent registration of multiple identities for a single individual. Otherwise (as an example) at the termination of employment only one of the identities might be removed, leaving the individual still registered under the duplicate identity.

The design of such databases, however, needs to address all the maintenance and security requirements of any large database holding personal information. They require a secure design with encryption during storage and transmission. The ease of access of records has to be balanced with

[6] ISO/IEC 19795-1:2006 Biometric performance testing and reporting — Part 1:Principles and framework and ISO/IEC 19795-6:2012 Biometric performance testing and reporting — Part 6: Testing methodologies for operational evaluation

[7] Peter Waggett, Experiences from Large Scale Testing of Systems using Biometric Technologies, ERNCIP publication (2015)

mechanisms to prevent unauthorised personnel from adding, modifying and deleting records – or to search for templates which are a close match.

8 EXAMPLE APPLICATION: PHYSICAL ACCESS CONTROL

8.1 Access Control Systems

By "physical access control", we refer to systems intended to restrict entry to physical spaces (such as rooms and buildings).

When combined with other technology elements, networks, security and privacy policies, biometric technologies can become part of an access control system designed to ensure that access to physical or virtual spaces is granted only to people with the appropriate access rights.

Since at least the 1970s both government and commercial organizations have implemented biometrics in access control applications. Some of these implementations have been successful, some less so. The purpose of this section is to provide a brief overview of how biometric technologies can address this type of application, and to outline some of the benefits and implementation complexities encountered in practice.

By recognizing people from bodily characteristics, rather than from PINs, passwords or tokens, biometric technologies are particularly useful for establishing a firm connection between a person and the record of their privileges of access.

Often, the biometric component can be combined with another identity credential to offer greater security or to make it more convenient for the individual. In this section, reference will be made to a draft CEN standard which mandates a physical token integrated with the application.

The benefits of using a biometric solution for physical access control are:

- Evidence of identity (and hence of privilege) are much harder to accidentally or deliberately transfer between persons than passwords or tokens.
- Biometric records can also leave a much stronger audit trail for access control events, with less room for repudiation.

Consequently, biometric technologies are most often thought of as appropriate primarily for access control to highly secure spaces or highly sensitive data.

8.2 Accuracy/performance rates in physical access control systems

All security systems can experience errors and biometric systems are no exception. Unlike other recognition technologies, such as PINs, passwords or tokens, the usage errors for biometric systems have been well studied in a variety of environments. Errors can be of three types:

- false positives (recognizing one individual as someone else, and hence allowing the possibility of someone else with a similar reference/template being accepted),
- false negatives (not recognizing an individual as herself and being denied access to the system)
- a 'Failure to Enrol', that is not being able to collect usable biometric images on an individual from the outset.

Laboratory and in situ testing can establish 'rates' for such errors with tested populations in tested environments. The accuracy rate relating to false positives in a verification system is FAR, and that for a false negative is FRR. (See Section 6.3 for more information.)

The requirement for a specific pair of rates (FAR and FRR) as measured in an operational application will vary greatly from application to application, depending upon the organisation's appetite for risk, the user population, the enrolment conditions and details of the usage environment.

The measured rates in a test do not take account of planned attacks on the system, but rather measure the impact of random processes. Note that the rates establish only the potential for an error, they do not alone allow us to predict how many such errors will be encountered in an operational system.

The operational system (including the fallback method) should be tested under realistic conditions, for example at peak throughput times, to determine its overall performance.

REFERENCES

Undated standards are still under development.

ISO/IEC 30124, Code of practice for the implementation of a biometric system

ISO/IEC 2382-37:2012, Biometric Vocabulary, available for public download from http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html

ISO/IEC TR 29196, Technical Report on Guidance for Biometric Enrolment

ISO/IEC 30137-1 Use of biometrics in video surveillance systems Part 1: Design and specification

ISO/IEC 30137-2 Use of biometrics in video surveillance systems Part 2: Performance testing and reporting

ISO/IEC 30137-3 Use of biometrics in video surveillance systems Part 3: Data Formats

ISO/IEC 19795-1:2006 Biometric performance testing and reporting — Part 1: Principles and framework

ISO/IEC 19795-6:2012 Biometric performance testing and reporting — Part 6: Testing methodologies for operational evaluation

ISO/IEC TR 24714-1:2008 Jurisdictional and societal considerations for commercial applications — Part 1: General guidance, available for public download from http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html

Peter Waggett, Experiences from Large Scale Testing of Systems using Biometric Technologies, ERNCIP publication (2015)

9 GLOSSARY

Access Control – function to determine whether to grant an individual access to resources, facilities, services or information based on pre-established rules and specific rights or authority associated with the requesting party

Application – set of interrelated components and processes to perform a specific function

Biometric reader – an electronic device for capturing a biometric feature from person, usually equipped with a sensor, processing software and feedback to the user

Biometric recognition – automated recognition of individuals based on their biological or behavioural characteristics

Biometric mode or modality – combination of a human biometric characteristic type (e.g. fingerprint) together with a sensor type (e.g. an infrared sensor) and a processing method

Biometric system - integrated set of components that perform biometric recognition

Enrolment – act of creating and storing a biometric enrolment data record in accordance with an enrolment policy

Failure to Enrol – failure to create and store a biometric enrolment data record for an eligible biometric capture subject in accordance with a biometric enrolment policy

False Acceptance Rate, FAR – number of false acceptances as a proportion of the total number of biometric claims that ought to have been rejected

False Rejection Rate, FRR – number of false rejections as a proportion of the total number of biometric claims that ought to have been accepted

Minutia – characteristic element of fingerprint image, as in a bifurcation or end of ridgeline

PIN – Personal Identification Number – secret number used as knowledge-based authentication for physical or logical access to a restricted domain

Probe – biometric sample or biometric feature set input into an algorithm for use as the subject of biometric comparison to a reference

Recognition system – system for the recognition of an individual using distinguishing data provided by the individual

Reference – one or more stored biometric samples, biometric templates or biometric models attributed to a biometric data subject and used as the object of biometric comparison

Spoofing attack - attack on a biometric system by an unauthorised person that uses artefacts to allow the perpetrator to masquerade as a specific authorised individual

Template – set of stored biometric features comparable directly to probe biometric features

Threshold – numerical value, or set of values, that define the boundary between a match or a non-match so that a decision can be made about whether a match or a non-match has been achieved

European Commission
EUR 27191 EN – Joint Research Centre – Institute for the Protection and Security of the Citizen

Title: The Application of Biometrics in Critical Infrastructures Operations: Guidance for Security Managers

Authors: Marek Rejman-Greene, CAST, UK
Krzysztof Brzozowski, Government Centre for Security, PL
Tony Mansfield, NPL, UK
Raul Sanchez-Reillo, University Carlos III, Madrid, ES
Peter Waggett, IBM, UK
Geoff Whitaker, CAST, UK

2015 – 34 pp. – 21.0 x 29.7 cm

EUR – Scientific and Technical Research series – ISSN 1831-9424

ISBN 978-92-79-47446-0

doi:10.2788/761739

Abstract

Biometric technologies have advanced considerably over the past decade, and have paved the way for more widespread use by governments, commercial enterprises and, more recently, by the consumer through the introduction of sensors and apps on mobile phones. This report provides introductory information about the application of these technologies to achieve secure recognition of individuals by organisations which form part of critical infrastructures in the EU. As a specific example, it offers guidance about the implementation of physical access control systems using biometric technologies. It is principally addressed at managers and security officers within these organisations. With the information in this report, managers and officers should be in a better position to discuss their specific requirements with technology suppliers, specialist systems integrators and consultants – and therefore lead to applications which are more secure without compromising on their usability. The report emphasises the importance of considering the effectiveness of the entire application – and not just focussing on the performance of the biometric subsystem. Note that the representation of specific devices does not imply any recommendation by the authors or the European Commission.

LB-NA-27191-EN-N

JRC Mission

As the Commission's in-house science service, the Joint Research Centre's mission is to provide EU policies with independent, evidence-based scientific and technical support throughout the whole policy cycle.

Working in close cooperation with policy Directorates-General, the JRC addresses key societal challenges while stimulating innovation through developing new methods, tools and standards, and sharing its know-how with the Member States, the scientific community and international partners.

Serving society
Stimulating innovation
Supporting legislation

doi:10.2788/761739

ISBN 978-92-79-47446-0

Publications Office