Access Control
Biometrics
User Guide

October 2016

For other information please contact:

British Security Industry Association
t: 0845 389 3889
e: info@bsia.co.uk
www.bsia.co.uk

Contents

1. Introduction

Biometrics is the name given to a variety of methods used to recognize humans based on individual physical properties or behavioural traits. Whilst analysis of behaviour might be used for surveillance purposes, when considered as a method of identifying individuals for control of systems or granting permission the physical methods are currently more appropriate. For security systems, biometrics can be used to allow restricted access to control of equipment. Frequently this can permit users to gain entry to all or part of a building via an Access Control system.

2. Scope

This guide provides an overview of the biometric technologies currently available that are typically used within an Access Control or Integrated Security System.

3. Terms, Definitions and abbreviations

3.1. Definitions and abbreviations

Enrolment: Enrolment is the process whereby the user's biometric template is captured and stored within the system for comparison at a later date during normal operation.

Templates: A template is a data representation of the biometric being measured and is stored as a series of 1s and 0s. The template can be stored in a number of places depending upon the design of the system and the customer's requirements. Biometric templates vary in size from a few hundred bytes to a few kilobytes depending upon the characteristic being captured. It is not possible to identify an individual using the limited data stored in the template. For multiple biometric reading devices templates are often combined using a suitable algorithm such that each individual template cannot be recovered.

Matching: In order to confirm the identity the biometric of the characteristic captured by the device is matched against a stored template that was taken when the user enrolled onto the system. There are two methods by which biometric data is confirmed against a pre-enrolled stored template, verification and identification.

Verification: "One to One" (1:1) technology is where the user's biometric sample is compared to a single template stored by the biometric system. The term used to describe this method is verification because the user is verifying a known template. The user identifies themselves to the system (e.g. via a keypad, smartcard, etc.), and then a biometric feature is scanned. This method is usually quick because the biometric system does not need to search through all records stored to find the user's template.

Identification: "One to Many" (1:N) technology is where the recorded biometric feature is compared to all biometric data saved in a system. This method is referred to as identification due to the user being unknown to the system prior to providing a biometric sample. If there is a match, the identification is successful, and the corresponding user name or user ID may be processed subsequently. The speed of identification can deteriorate proportionally with the greater number of users enrolled.

FRR: False Reject Rate is defined as the percentage of instances where a false rejection of the biometric occurs.

FAR: False Acceptance Rate is defined as the percentage of instances where a false acceptance of a biometric occurs.

Authentication

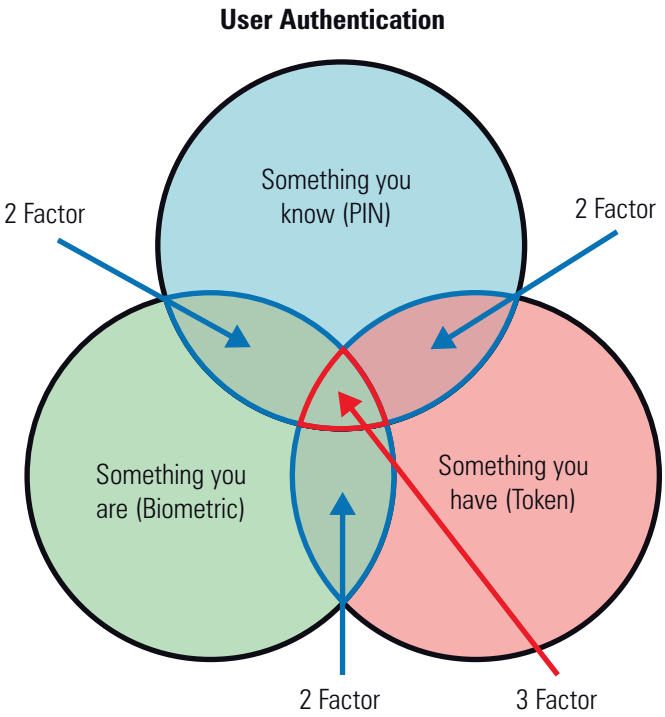


Figure 1 – User Authentication

Single Factor: Single factor authentication is where the user is identified against one element, i.e. something you are, such as a biometric.

2 factor: 2 factor authentication is where the user's credentials are checked against two elements, i.e. something the user is and something the user knows (biometric + PIN).

3 factor: 3 factor authentication is where a user's credentials are checked against something the user knows (PIN), has (Card) and are (biometric).

4. Understanding Technology / Biometric systems

4.1. What is Biometrics?

Biometrics is measurement and analysis of the unique physical or behavioural characteristics used to recognise humans. It works by unobtrusively matching patterns of live individuals' data in real time, against enrolled records.

Biometric data is initially read with an 'enrolment' reader and the data is then 'encoded' into a template which is usually stored in an access control database or on a smartcard for later use. The encoding process ensures that the data cannot be reproduced from the template, only compared against a recently read sample for a pass/fail result.

Biometric sensors are either contact (i.e. the user needs to touch the sensor) or contactless (i.e. the user does not touch the sensor) technologies.

4.2. Types of Biometrics

4.2.1. Finger

Fingerprint identification has been used by police agencies around the world since the late nineteenth century to identify both suspected criminals as well as the victims of crime. The technique relies on the identification of the unique pattern of ridges and furrows on the surface of the finger.

Type	Advantages	Disadvantages
Contact	Speed of recognition Easily understood Relatively inexpensive Improving accuracy	Damaged / dirty fingers Sensor needs cleaning

4.2.2. Vein

A vein scanner can use contact or contactless technology with an infra-red light source which excites the haemoglobin in the blood thereby identifying the pattern of veins in the individual's hand, palm or finger. Unlike other biometrics the vein pattern of a human is set pre-birth and never changes.

At present there are three main vein matching systems on the market:

1. Palm Vein
2. Finger Vein
3. Reverse of hand

Type	Advantages	Disadvantages
Contact or contactless	As the veins are internal this is a difficult technology to forge and thus has a higher security than finger prints.	The cost of the readers are still high due to the technology required to capture the information.

4.2.3. Combined Fingerprint and Vein

A multi-format biometric reader can read both a fingerprint and/or a vein thereby providing increased security and resilience from damaged fingers.

4.2.4. Iris

Iris recognition uses contactless camera technology to identify the unique patterns of the 'irides' in an individual's eyes. As the information is taken from a photograph of the eye, this is a less intrusive method than older retinal scanners.

Iris recognition is rarely impeded by glasses or contact lenses, and it has the smallest outlier (those who cannot use/enrol) group of all biometric technologies. Iris recognition is well-suited for "one-to-many" identification as, barring trauma, a single enrolment can last a lifetime.

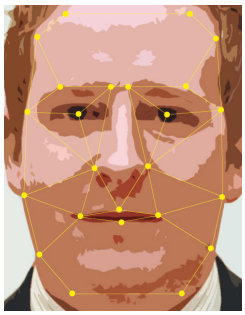
Type	Advantages	Disadvantages
Contactless	Accuracy Security	Price Fear of use

4.2.5. Facial

Facial recognition uses camera(s) to extract features from the subject's face, such as the relative position, size, and/or shape of the eyes, nose, cheekbones, and jaw.

A newly emerging trend is three-dimensional face recognition to improve the quality of the information about the shape of a face. This information is then used to identify distinctive features on the surface of a face, such as the contour of the eye sockets, nose, and chin. This technique is not affected by changes in lighting, and can identify a face from a range of viewing angles, including a profile view.

Type	Advantages	Disadvantages
Contactless	Non-intrusive Multi-disciplined usage Hands free	Price (slightly) Camera positioning

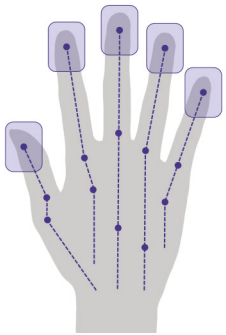


4.2.6. Hand geometry

Hand geometry identifies a user by the shape of their hands. Hand geometry readers use contact technology to measure a user's hand along many dimensions and compare them to previously recorded measurements.

As the human hand is not unique to an individual, hand geometry is not suitable for 'one-to-many' applications, in which a user is identified purely from the biometric, but it is suitable for one-to-one for verification of a user's identity.

Type	Advantages	Disadvantages
Contactless	Quicker enrolment Speed of use	Contact Sunlight Physical size (aesthetics)



4.2.7. Other techniques

Other technologies include: voice; retina scanning; and gait recognition.

4.2.8. Comparison of FAR/FRR

If you are choosing a biometric system then reference should be made to the manufacturers' data sheets to identify the suitable FAR and FRR figures applicable to your application.

4.3. System Architecture

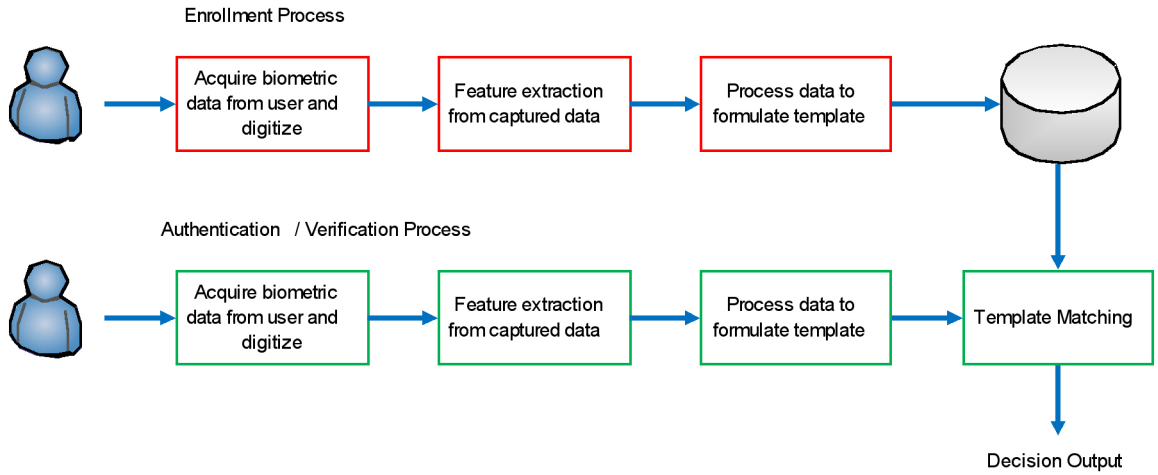


Figure 2 – Enrolment/Authentication/Verification Block Diagram

4.4. Advantages/disadvantages

There are many advantageous to using biometric technology:

Biometric technology provides a number of advantages over traditional card and/or PIN based systems:

- Increased security level over card or PIN based systems;
- Biometric information cannot be passed to another person in the same way a card or PIN can be;
- Reduces identification fraud at borders and at work (clocking in);
- Eliminates security threats that lost or borrowed cards and PINs create;
- System administration cost savings, by removing the management of lost, stolen and forgotten cards or PINs;
- Replaces hard to remember passwords (which risk being shared or observed);
- Identifies Who, Where and When without any doubt.

The disadvantages of biometrics vary depending upon the technology:

Biometric readers rarely suit an external or exposed location. In extreme cases finger print readers can fail to identify users with damaged, dirty or worn fingerprints. Not everyone can use fingerprints and certain tasks, such as construction, can affect the user's fingerprint.

Some biometric readers can take slightly longer to identify users than card-based systems take to allow entry, due to the user normally having to stop and present themselves to the biometric readers and how the biometric information is verified. Users can perceive biometrics as less convenient and/or more intrusive than card based systems.

There are significant cost savings associated with the running and management of biometric systems, though the initial design and installation costs can be higher than card or PIN based systems. Correct management of the system is critical to ensure user data protection concerns are alleviated.

4.5. Factors to be considered

4.5.1. Speed of operation

Speed of recognition (authentication) consists of two phases. The capture phase and the authentication phase. The speed of capture depends upon the technology used and the number of points being sampled. The authentication phase depends upon the matching method. For one to many (1:N) matching the time to match will depend upon the size of the database and the search algorithm being used with increasing size corresponding to increased matching time.

4.5.2. Level of security

The level of security offered by biometrics is dependent upon the type being used and its configuration. The amount of data stored within the template for matching will have an impact of the FAR/FRR figures for the product and consideration should be given as to which of these is more important from an operational perspective.

Most systems can be configured in terms of template quality to increase or decrease the FAR/FRR figures depending upon usage requirements. For example, a system that only has 10 people enrolled will typically accept a higher FRR, whereas a system that has 500 people will typically want a lower FRR.

When defining the system requirements, as well as the FAR/FRR figures consideration should also be given to the type of authentication required to meet the security risk, i.e. 1-factor, 2-factor or 3-factor. By combining multiple technologies the FAR/FRR figures can be increased, however this could reduce the throughput at the reader.

Industry accepts that current iris and vein recognition systems are at the higher end of the security spectrum.

Reference should be made to the published FAR and FRR figures when selecting the level of security required.

4.5.3. Data Protection / Storage

The biggest issue with biometrics is the privacy argument about what and where the data is stored. Unlike the fingerprints used by the police where an image is stored, the data used for authentication is a series of 1s and 0s. It is not possible to identify an individual using the limited data stored in the template. However there are still concerns over the location and storage of this data, which can reside in a number of different locations as described below.

At one end of the scale all templates are stored on a central server and the reader will pass the scanned information back to the server for identification and verification.

Typically in access control systems the templates are stored in the reader and the reader makes the decision on the user's credential thus eliminating any traffic of the template across the network.

At the other end of the scale the user's template is stored on a smart card and a 1:1 match is performed, thereby eliminating any data protection worries.

The type of system used will be dependent upon the risk and concerns over privacy.

4.5.4. Security/encryption

As biometric template data is stored as a series of 1s and 0s no reference to the individual can be obtained from the data. In theory it could be possible to capture this data and then inject it onto a network in a centralised system, however the probability of this happening is low. For any centralised system the data transferred between the readers and the server could be encrypted to enhance the security and resilience of the system.

4.6. Choosing the right Biometric

Biometrics could be used for a single high security door on a system otherwise controlled by card or PIN. When choosing a biometric technology the first questions that should be asked are “why do we need biometrics?” and “what is our security risk?”.

Biometric technologies provide high security protection, though the reasons to choose biometrics may not just be to do with high security. The requirement may be for a solution that reduces the administration and management of Cards or PINs.

Do you want biometric only or a mix of traditional access readers and biometrics? Again this will depend upon what you are trying to protect. Most biometric readers will provide an output that will allow it to integrate with an access control system.

Systems need to be designed carefully considering how many users need to enter or exit at any time. The speed of the reader and entry point open/close time, will it cause backlogs?, will additional entry and exit routes be required?

For realistic operation the authentication process should typically take less than 3s, otherwise the usability will be questioned.

Considerations for any Access Control System:

- Volume of traffic
- Identification v verification
- Speed of operation
- Security Level Required
- Application Type – e.g. builders, office workers
- Disability Discrimination Act (DDA) and Equality Act
- Reader Locations
- Future Expansion
- Time and Attendance

5. Legal matters

Users of access control systems and biometric technologies should comply with all applicable discrimination legislation, The Data Protection Act (1998) and should apply the recommendations of the Information Commissioner’s “Employment Practices Code”.

This document was created by the Access and Asset Protection Section of the British Security Industry Association (BSIA).

The British Security Industry Association is the trade association for the private security industry in the UK. Our members provide over 70% of UK security products and services and adhere to strict quality standards.

The British Security Industry Association's Access and Asset Protection Section brings together companies involved in areas of security providing physical products to stop unwanted people from accessing property or valuables and the electronic measures that can, optionally, control them.

The section includes member companies involved in the manufacture, supply and installation of solutions that restrict, control and monitor the movement of people, assets or vehicles in, out and around a building or site. This includes physical protection methods, such as security doors, fencing, locks, barriers, safes and strong rooms, rising screens, etc and the electronic access control systems that control them and allow authorised persons in and keep undesired people out.

Access control products are subject to fast-moving technological development. The section aims to raise awareness amongst end-users and specifiers of the different types of equipment that are available, the applicable standards and the most appropriate environments for using them.

The Access and Asset Protection Section sits in a strong position when it comes to lobbying for consistent standards and regulations. Access control products are subject to fast-moving technological development. A major focus of the section is to raise awareness amongst end-users and specifiers of the different types of equipment that are available and the most appropriate environments for using them.

BSIA membership will raise your company profile and ensure that your business is at the heart of influencing the future of the security industry. You will become part of a unique group of high quality and professional companies which are well-respected and well-represented to government, end users, specifiers, standards and legislative bodies. For more information contact the BSIA.

BSIA Ltd
Kirkham House
John Comyn Drive
Worcester
WR3 7NS

t: 0845 389 3889
e: info@bsia.co.uk
www.bsia.co.uk

@thebsia

bsia
british security industry association