Association for Biometrics (AfB) and
International Computer Security Association (ICSA)

1999 Glossary of Biometric Terms

The following is a revision of the AfB and ICSA 1998 biometric glossary. This 1999 version has been compiled by Tony Mansfield of the National Physical Laboratory and the AfB and Gary Roethenbaugh of ICSA. Both would like to thank the biometric community for its help in making this effort possible.

The 1999 glossary organises terms into two categories:
1. General Biometric Terms
2. Terms Related to Specific Biometric Techniques

Part 1. General Biometric Terms

Active Impostor Acceptance

When an impostor submits a modified, simulated or reproduced biometric sample, intentionally attempting to relate it to another person who is an enrolee, and he/she is incorrectly identified or verified by a biometric system as being that enrolee. Compare with 'Passive Impostor Acceptance'.

Algorithm

A sequence of instructions that tell a biometric system how to solve a particular problem. An algorithm will have a finite number of steps and is typically used by the biometric engine to compute whether a biometric sample and template are a match. See also 'Artificial Neural Network'.

API (Application Program Interface)

A set of services or instructions used to standardise an application. An API is computer code used by an application developer. Any biometric system that is compatible with the API can be added or interchanged by the application developer. APIs are often described by the degree to which they are high level or low level. High level means that the interface is close to the application and low level means that the interface is close to the device.

Application Developer

An individual entrusted with developing and implementing a biometric application.

ASIC (Application Specific Integrated Circuit)

An integrated circuit (silicon chip) that is specially produced for a biometric system to improve performance.

Attempt

The submission of a biometric sample to a biometric system for identification or verification. A biometric system may allow more than one attempt to identify or verify.

Authentication

Alternative term for 'Verification'.

Automatic ID/Auto ID

An umbrella term for any biometric system or other security technology that uses automatic means to check identity. This applies to both one-to-one verification and one-to-many identification.

Behavioural Biometric

A biometric which is characterised by a behavioural trait that is learnt and acquired over time rather than a physiological characteristic. However, physiological elements may influence the monitored behaviour. See Part 2 Terms Related to Specific Biometric Techniques for 'Keystroke Dynamics', 'Signature Verification' and 'Speaker Verification'. Contrast with 'Physical/Physiological Biometric'.

Binning

Binning is the process of classifying biometric data. This allows a database of biometric data to be pre-sorted in order to speed up the process of matching captured biometric data with comparison data. This term is particularly used in conjunction with Automated Fingerprint Identification Systems. See Part 2, 'AFIS', 'Binning'.

Biometric

A measurable, physical characteristic or personal behavioural trait used to recognise the identity, or verify the claimed identity, of an enrolee.

Biometric Application

The use to which a biometric system is put. See also 'Application Developer'.

Biometric Data

The information extracted from the biometric sample and used either to build a reference template (template data) or to compare against a previously created reference template (comparison data).

Biometric Engine

The software element of the biometric system which processes biometric data during the stages of enrolment and capture, extraction, comparison and matching.

Biometric Device

The part of a biometric system containing the sensor that captures a biometric sample from an individual.

Biometric Sample

Raw data representing a biometric characteristic of an end-user as captured by a biometric system (for example the image of a fingerprint).

Biometric System

An automated system capable of:

1. capturing a biometric sample from an end user;
2. extracting biometric data from that sample;
3. comparing the biometric data with that contained in one or more reference templates;
4. deciding how well they match; and
5. indicating whether or not an identification or verification of identity has been achieved.

Biometric Taxonomy

A method of classifying biometrics. For example, San Jose State University's (SJSU) biometric taxonomy uses partitions to classify the role of biometrics within a given biometric application. Thus an application may be classified as:

- Co-operative vs. Non-Co-operative User
- Overt vs. Covert Biometric System
- Habituated vs. Non-Habituated User
- Supervised vs. Unsupervised User
- Standard Environment vs. Non Standard Environment

Co-operative refers to a willing end user participating in a biometric application. Overt refers to an undisguised and candid use of a biometric system. Habituated means that an end user is familiar with

the workings of the biometric system and application. Supervised means that trained personnel guide an end user through the biometric application. Standard environment refers to unchanging and non-volatile surroundings and climate.

Biometric Technology

A classification of a biometric system by the type of biometric. See Part 2.

Capture

The method of taking a biometric sample from the end user.

CCD (Charge-Coupled Device)

A CCD is a semiconductor device that records images electronically.

Certification

The process of testing a biometric system to ensure that it meets certain performance criteria. Systems that meet the testing criteria are said to have passed and are certified by the testing organisation.

CMOS (Complementary Metal Oxide Semiconductor)

A type of integrated circuit used by some biometric systems because of its low power consumption.

Comparison

The process of comparing a biometric sample with a previously stored reference template or templates. See also 'One-To-Many' and 'One-To-One'.

Claim of Identity

When a biometric sample is submitted to a biometric system to verify a claimed identity.

Claimant

A person submitting a biometric sample for verification or identification whilst claiming a legitimate or false identity.

Closed-Set Identification

When an unidentified end-user is known to be enrolled in the biometric system. Opposite of 'Open-Set Identification'.

Crossover Error Rate

Synonym for 'Equal Error Rate'.

Database

Any storage of biometric templates and related end user information. Even if only one biometric template or record is stored, the database will simply be "a database of one". Generally speaking, however, a database will contain a number of biometric records.

D Prime

A statistical measure of how well a biometric system can discriminate between different individuals. The larger the D Prime value, the better a biometric system is at discriminating between individuals.

Degrees of Freedom

The number of statistically independent features in biometric data.

Discriminant Training

A means of refining the extraction algorithm so that biometric data from different individuals are as

distinct as possible.

End User

A person who interacts with a biometric system to enrol or have his/her identity checked.

End User Adaptation

The process of adjustment whereby a participant in a test becomes familiar with what is required and alters their responses accordingly.

Encryption

The act of converting biometric data into a code so that people will be unable to read it. A key or a password is used to decrypt (decode) the encrypted biometric data.

Enrolee

A person who has a biometric reference template on file.

Enrolment

The process of collecting biometric samples from a person and the subsequent preparation and storage of biometric reference templates representing that person's identity.

Enrolment Time

The time period a person must spend to have his/her biometric reference template successfully created.

Equal Error Rate

The error rate occurring when the decision threshold of a system is set so that the proportion of false rejections will be approximately equal to the proportion of false acceptances.

Extraction

The process of converting a captured biometric sample into biometric data so that it can be compared to a reference template.

Failure to Acquire

Failure of a biometric system to capture and extract biometric data (comparison data).

Failure to Acquire Rate

The frequency of a failure to acquire.

Failure to Enrol

Failure of the biometric system to form a proper enrolment template for an end-user. The failure may be due to failure to capture the biometric sample or failure to extract template data (of sufficient quality).

Failure to Enrol Rate

The proportion of the population of end-users failing to complete enrolment

False Acceptance

When a biometric system incorrectly identifies an individual or incorrectly verifies an impostor against a claimed identity.

False Acceptance Rate/FAR

The probability that a biometric system will incorrectly identify an individual or will fail to reject an impostor. The rate given normally assumes passive impostor attempts. The False Accept Rate may be estimated as

$$FAR = NFA / NIIA$$

or

$$FAR = NFA / NIVA$$

where

FAR is the false acceptance rate
NFA is the number of false acceptances
NIIA is the number of impostor identification attempts
NIVA is the number of impostor verification attempts

False Match Rate

Alternative to 'False Acceptance Rate'. Used to avoid confusion in applications that reject the claimant if their biometric data matches that of an enrolee. In such applications, the concepts of acceptance and rejection are reversed, thus reversing the meaning of 'False Acceptance' and 'False Rejection'. See also 'False Non-Match Rate'.

False Non-Match Rate

Alternative to 'False Rejection Rate'. Used to avoid confusion in applications that reject the claimant if their biometric data matches that of an enrolee. In such applications, the concepts of acceptance and rejection are reversed, thus reversing the meaning of 'False Acceptance' and 'False Rejection'. See also 'False Match Rate'.

False Rejection

When a biometric system fails to identify an enrolee or fails to verify the legitimate claimed identity of an enrolee.

False Rejection Rate/FRR

The probability that a biometric system will fail to identify an enrolee, or verify the legitimate claimed identity of an enrolee. The False Rejection Rate may be estimated as follows:

$$FRR = NFR / NEIA$$

or

$$FRR = NFR / NEVA$$

where

FRR is the false rejection rate
NFR is the number of false rejections
NEIA is the number of enrolee identification attempts
NEVA is the number of enrolee verification attempts

This estimate assumes that the enrolee identification/verification attempts are representative of those for the whole population of end-users. The False Rejection Rate normally excludes 'Failure to Acquire' errors

Field Test / Field Trial

A trial of a biometric application in 'real world' as opposed to laboratory conditions.

Filtering

The process of classifying biometric data according to information that is unrelated to the biometric data itself. This may involve filtering by sex, age, hair colour or other distinguishing factors, and including this information in an end user's database record. This term is particularly used in conjunction with Automated Fingerprint Identification Systems. See Part 2, 'AFIS', 'Filtering'.

Goats

Biometric system end users whose pattern of activity when interfacing with the system varies beyond the specified range allowed by the system, and who consequently may be falsely rejected by the system.

Genetic Penetrance

The degree to which characteristics are passed from generation to generation.

Hamming Distance

The number of disagreeing bits between two binary vectors. Used as measure of dissimilarity.

Identification/Identify

The one-to-many process of comparing a submitted biometric sample against all of the biometric reference templates on file to determine whether it matches any of the templates and, if so, the identity of the enrolee whose template was matched. The biometric system using the one-to-many approach is seeking to find an identity amongst a database rather than verify a claimed identity. Contrast with 'Verification'.

Impostor

A person who submits a biometric sample in either an intentional or inadvertent attempt to pass him/herself off as another person who is an enrolee.

In-House Test

A test carried out entirely within the environs of the biometric developer, which may or may not involve external user participation.

Live Capture

The process of capturing a biometric sample by an interaction between an end user and a biometric system.

Match/Matching

The process of comparing a biometric sample against a previously stored template and scoring the level of similarity. An accept or reject decision is then based upon whether this score exceeds the given threshold.

Multiple Biometric

A biometric system that includes more than one biometric system or biometric technology.

Neural Net/Neural Network

One particular type of algorithm. An artificial neural network uses artificial intelligence to learn by past experience and compute whether a biometric sample and template are a match.

OEM (Original Equipment Manufacturer)

A biometric organisation (Manufacturer) which assembles a complete biometric system from parts.

OEM (Original Equipment /Module)

A biometric module for integration into a complete biometric system.

One-to-a-Few

A hybrid of one-to-many identification and one-to-one verification. Typically the one-to-a-few process involves comparing a submitted biometric sample against a small number of biometric reference templates on file.

One-to-Many

Synonym for 'Identification'.

One-to-One

Synonym for 'Verification'.

Open-Set Identification

Identification, when it is possible that the individual is not enrolled in the biometric system. Opposite of 'Closed-Set Identification'.

Out of Set

In open-set identification, when the individual is not enrolled in the biometric system.

Passive Impostor Acceptance

When an impostor submits his/her own biometric sample and claiming the identity of another person (either intentionally or inadvertently) he/she is incorrectly identified or verified by a biometric system. Compare with 'Active Impostor Acceptance'.

Performance Criteria

Pre-determined criteria established to evaluate the performance of the biometric system under test.

Physical/Physiological Biometric

A biometric which is characterised by a physical characteristic rather than a behavioural trait. However, behavioural elements may influence the biometric sample captured. See Part 2 Terms Related to Specific Biometric Techniques for 'Body Odour', 'Ear Shape', 'Face Recognition', 'Finger Geometry', 'Finger Image', 'Hand Geometry', 'Iris Recognition', 'Palm', 'Retina', 'Speaker Verification' and 'Veincheck'. Contrast with 'Behavioural Biometric'.

PIN (Personal Identification Number)

A security method whereby a (usually) four digit number is entered by an individual to gain access to a particular system or area.

Population

The set of end-users for the application.

Receiver Operating Curves (ROC)

A graph showing how the false rejection rate and false acceptance rate vary according to the threshold.

Recognition

The preferred term is 'Identification'.

Record

The template and other information about the end-user (e.g. access permissions)

Response Time

The time period for a biometric system to return a decision on identification or verification of a biometric sample.

Score

The level of similarity from comparing a biometric sample against a previously stored template.

Template/Reference Template

Data, which represents the biometric measurement of an enrolee, used by a biometric system for comparison against subsequently submitted biometric samples.

Template Ageing

The degree to which biometric data evolves and changes over time, and the process by which templates account for this change.

Template Size

The amount of computer memory taken up by the biometric data.

Third Party Test

An objective test, independent of a biometric vendor, usually carried out entirely within a test laboratory in controlled environmental conditions.

Threshold/Decision Threshold

The acceptance or rejection of biometric data is dependent on the match score falling above or below the threshold. The threshold is adjustable so that the biometric system can be more or less strict, depending on the requirements of any given biometric application.

Throughput Rate

The number of end users that a biometric system can process within a stated time interval.

Type I Error

In statistics, the rejection of the null hypothesis (default assumption) when it is true. In a biometric system the usual default assumption is that the claimant is genuine, in which case this error corresponds to a 'False Rejection'.

Type II Error

In statistics, the acceptance of the null hypothesis (default assumption) when it is false. In a biometric system the usual default assumption is that the claimant is genuine, in which case this error corresponds to a 'False Acceptance'.

User

The client to any biometric vendor. The user must be differentiated from the end user and is responsible for managing and implementing the biometric application rather than actually interacting with the biometric system.

Validation

The process of demonstrating that the system under consideration meets in all respects the specification of that system.

Verification/Verify

The process of comparing a submitted biometric sample against the biometric reference template of a single enrolee whose identity is being claimed, to determine whether it matches the enrolee's template. Contrast with 'Identification'.

WSQ (Wavelet Transform/Scalar Quantisation)

A compression algorithm used to reduce the size of reference templates.

Zero Effort Forgery

Where an impostor uses his or her own biometric sample and claims the identity of a different enrolee.

Part 2. Terms Related To Specific Biometric Techniques

Terms relating to specific biometric technologies and techniques are grouped below.

2.1 AFIS (Automated Fingerprint Identification System)

A highly specialised biometric system that compares a single finger image with a database of finger images. AFIS is predominantly used for law enforcement, but is also being put to use in civil applications. For law enforcement, finger images are collected from crime scenes, known as latents, or are taken from criminal suspects when they are arrested. In civilian applications, finger images may be

captured by placing a finger on a scanner or by electronically scanning inked impressions on paper. See also Finger Image.

Binning

A specialised technique used by some AFIS vendors. Binning is the process of classifying finger images according to finger image patterns. This predominantly takes place in law enforcement applications. Here finger images are categorised by characteristics such as arches, loops and whorls and held in smaller, separate databases (or bins) according to their category. Searches can be made against particular bins, thus speeding up the response time and accuracy of the AFIS search.

Booking

The process of capturing inked finger images on paper, for subsequent processing by an AFIS.

Filtering

A specialised technique used by some AFIS vendors. Filtering is the process of classifying finger images according to data which is unrelated to the finger image itself. This may involve filtering by sex, age, hair colour or other distinguishing factors.

Latent

An impression of a finger image collected from a crime scene.

2. Body Odour

A physical biometric that analyses the unique chemical pattern made up by human body smell.

Volatiles

The chemical breakdown of body odour.

3. DNA

DNA is a unique, measurable human characteristic. However, current DNA technology is not automatic and cannot currently rank alongside other biometric technologies.

4. Ear Shape

A lesser-known physical biometric that is characterised by the shape of the outer ear, lobes and bone structure.

5. Face Recognition

A physical biometric that analyses facial features.

Eigenface

A method of representing a human face as a linear deviation from a mean or average face.

Eigenhead

The three dimensional version of Eigenface that also analyses the shape of the head.

Face Monitoring

A biometric application of face recognition technology where the biometric system monitors the attendance of an end user. This may be over or covert.

Facial Thermogram

A specialised face recognition technique that senses heat in the face caused by the flow of blood under the skin.

6. Finger Image

A physical biometric which looks at the patterns found in the tip of the finger.

Auto-correlation

A proprietary fingerscanning technique. Two identical finger images are overlaid in the auto-correlation process, so that light and dark areas, known as Moiré fringes, are created.

Bifurcation

A branch made by more than one finger image ridge.

Capacitance

A finger image capture technique that senses an electrical charge, from the contact of ridges, when a finger is placed on the surface of a sensor.

DPI (Dots Per Inch)

A measurement of resolution for finger image biometrics.

Fingerprint/Fingerprinting

Synonyms for 'Finger Image' and 'Fingerscanning'.

Fingerscanning

The process of finger image capture.

Live Scan

The term live scan is typically used in conjunction with finger image technology. Synonym for 'Live Capture'.

Minutiae

Small details found in finger images such as ridge endings or bifurcations.

Optical

A finger image capture technique that uses a light source, a prism and a platen to capture finger images.

Platen

The surface on which a finger is placed during optical finger image capture.

Ridge

The raised markings found across the fingertip. See also 'Valley'.

Ridge Ending

The point at which a finger image ridge ends.

Ultrasound

A technique for finger image capture that uses acoustic waves to measure the density of a finger image pattern.

Thermal

A finger image capture technique that uses a sensor to sense heat from the finger and thus capture a finger image pattern.

Valley

The corresponding marks found on either side of a finger image ridge.

7. Finger Geometry

A physical biometric that analyses the shape and dimensions of one or more fingers.

8. Hand Geometry/Hand Recognition

A physical biometric that involves analysing and measuring the shape of the hand.

9. Iris Recognition

A physical biometric that analyses iris features, found in the coloured ring of tissue that surrounds the pupil.

Iris Features

A number of features can be found in the iris. These are named corona, crypts, filaments, freckles, pits, radial furrows and striations.

IrisCode

The biometric data that is generated for each live iris presented. The code is a mathematical representation of the features of the iris.

10. Keystroke Dynamics

A behavioural biometric under development that analyses typing rhythm when an end user types onto a keyboard.

11. Palm

A physical biometric that analyses the palm of the hand. Typically this will involve an analysis of minutiae data.

12. Retina

A physical biometric that analyses the layer of blood vessels situated at the back of the eye.

13. Signature Verification

A behavioural biometric that analyses the way an end user signs his/her name. The signing features such as speed, velocity and pressure exerted by a hand holding a pen are as important as the static shape of the finished signature.

Acoustic Emission

A proprietary technique used in signature verification. As a user writes on a paper surface, the movement of the pen tip over the paper fibres generates acoustic emissions that are transmitted in the form of stress waves within the material of a writing block beneath the document being signed. The structure-borne elastic waves behave in materials in a similar way to sound waves in air and can be detected by a sensor attached to the writing block.

Dynamic Signature Verification (DSV)

Synonym for ‘Signature Verification’.

Static Signature Verification

Verification of signature based only on the shape of the resulting signature

14. Speaker verification

A part physical, part behavioural biometric that analyses patterns in speech.

Fixed-Text System

The preferred term is ‘Text Dependent System’.

Free-Text System.

The preferred term is ‘Text Independent System’.

Speaker-Dependent

A term sometimes used by speaker verification vendors to emphasise the fact their technology is designed to distinguish among voices.

Speaker Separation

A technology that separates overlapping voices from each other and other background noises.

Speech Recognition

This is not a biometric and should not be confused with speaker verification. Speech recognition involves recognising words as they are spoken and does not identify the speaker.

Text Dependent System

A system that requires a speaker to say a specific set of numbers or words.

Text-Independent System

A system that creates voiceprints from unconstrained speech and does not require a speaker to say a specific set of numbers or words.

Text-Prompted System

A speaker verification system that prompts the speaker to say randomly ordered numbers or words. The term ‘Challenge-Response’ is also used in a similar way to define text prompting.

Voice Verification

The preferred term is ‘Speaker Verification’.

Voice Print/Voiceprint

A representation of the acoustic information found in the voice of a speaker.

15. Veincheck/Vein Tree

A physical biometric that analyses the pattern of veins e.g. in the back of the hand.