National Science and Technology Council (NSTC)

Committee on Technology

Committee on Homeland and National Security

Subcommittee on Biometrics

Biometrics Glossary

Introduction

This set of terms was developed by the National Science & Technology Council's (NSTC) Subcommittee on Biometrics with the full understanding that national (INCITS/M1) and international (ISO/IEC JTC1 SC37) standards bodies are working to develop standard references. The subcommittee will review this Glossary for consistency as standards are passed. The subcommittee recognizes the impact of ongoing challenge problems, technical evaluations, and technology advancements. The Glossary will be updated accordingly to reflect these changes. The statements herein are intended to further the understanding of a general audience and are not intended to replace or compete with sources that may be more technically descriptive/prescriptive.

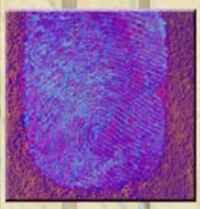
Glossary Terms

Accuracy

A catch-all phrase for describing how well a biometric system performs. The actual statistic for performance will vary by task (verification, open-set identification (watchlist), and closed-set identification). See www.biometricscatalog.org/biometrics/biometrics_101.pdf for further explanation. *See also d prime, detection error trade-off (DET), detect and identification rate, equal error rate, false acceptance rate (FAR), false alarm rate (FAR), false match rate, false non-match rate, false reject rate, identification rate, performance, verification rate.*

Algorithm

A limited sequence of instructions or steps that tells a computer system how to solve a particular problem. A biometric system will have multiple algorithms, for example: image processing, template generation, comparisons, etc.



National Science and Technology Council (NSTC)

Committee on Technology

Committee on Homeland and National Security

Subcommittee on Biometrics

ANSI - American National Standards Institute

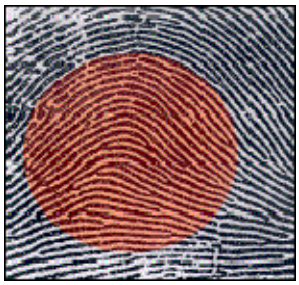
A private, non-profit organization that administers and coordinates the U.S. voluntary standardization and conformity assessment system. The mission of ANSI is to enhance both the global competitiveness of U.S. business and the U.S. quality of life by promoting and facilitating voluntary consensus standards and conformity assessment systems, and safeguarding their integrity. For more information visit www.ansi.org. *See also INCITS, ISO, NIST.*

Application Programming Interface (API)

Formatting instructions or tools used by an application developer to link and build hardware or software applications.

Arch

A fingerprint pattern in which the friction ridges enter from one side, make a rise in the center, and exit on the opposite side. The pattern will contain no true delta point. *See also delta point, loop, whorl.*

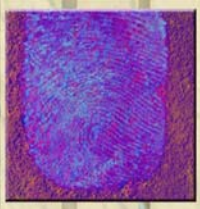


Attempt

The submission of a single set of biometric sample to a biometric system for identification or verification. Some biometric systems permit more than one attempt to identify or verify an individual. *See also biometric sample, identification, verification.*

Authentication

1. The process of establishing confidence in the truth of some claim. The claim could be any declarative statement for example: “This individual’s name is ‘Joseph K.’ ” or “This child is more than 5 feet tall.”
2. In biometrics, “authentication” is sometimes used as a generic synonym for verification. *See also verification.*



National Science and Technology Council (NSTC)

Committee on Technology

Committee on Homeland and National Security

Subcommittee on Biometrics

Automated Biometric Identification System (ABIS)

1. Department of Defense (DOD) system implemented to improve the U.S. government's ability to track and identify national security threats. The system includes mandatory collection of ten rolled fingerprints, a minimum of five mug shots from varying angles, and an oral swab to collect DNA.
2. Generic term sometimes used in the biometrics community to discuss a biometric system. *See also AFIS.*

Automated Fingerprint Identification System (AFIS)

A highly specialized biometric system that compares a submitted fingerprint record (usually of multiple fingers) to a database of records, to determine the identity of an individual. AFIS is predominantly used for law enforcement, but is also being used for civil applications (e.g. background checks for soccer coaches, etc). *See also IAFIS.*

Behavioral Biometric Characteristic

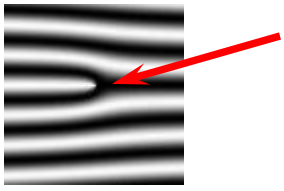
A biometric characteristic that is learned and acquired over time rather than one based primarily on biology. All biometric characteristics depend somewhat upon both behavioral and biological characteristic. Examples of biometric modalities for which behavioral characteristics may dominate include signature recognition and keystroke dynamics. *See also biological biometric characteristic.*

Benchmarking

The process of comparing measured performance against a standard, openly available, reference.

Bifurcation

The point in a fingerprint where a friction ridge divides or splits to form two ridges, as illustrated below. *See also friction ridge, minutia(e) point, ridge ending.*



Binning

Process of parsing (examining) or classifying data in order to accelerate and/or improve biometric matching.

BioAPI – Biometrics Application Programming Interface

Defines the application programming interface and service provider interface for a standard biometric technology interface. The BioAPI enables biometric devices to be easily installed, integrated or swapped within the overall system architecture.

Biological Biometric Characteristic

A biometric characteristic based primarily on an anatomical or physiological characteristic, rather than a learned behavior. All biometric characteristics depend somewhat upon both behavioral and biological characteristic. Examples of biometric modalities for which biological characteristics may dominate include fingerprint and hand geometry. *See also behavioral biometric characteristic*.

Biometrics

A general term used alternatively to describe a characteristic or a process.

As a characteristic:

> A measurable biological (anatomical and physiological) and behavioral characteristic that can be used for automated recognition.

As a process:

> Automated methods of recognizing an individual based on measurable biological (anatomical and physiological) and behavioral characteristics.

Biometric Consortium (BC)

An open forum to share information throughout government, industry, and academia. For more information visit www.biometrics.org.

Biometric Data

A catch-all phrase for computer data created during a biometric process. It encompasses raw sensor observations, biometric samples, models, templates and/or similarity scores. Biometric data is used to describe the information collected during an enrollment, verification, or identification process, but does not apply to end user information such as user name, demographic information and authorizations.

Biometric Sample

Information or computer data obtained from a biometric sensor device. Examples are images of a face or fingerprint.

Biometric System

Multiple individual components (such as sensor, matching algorithm, and result display) that combine to make a fully operational system. A biometric system is an automated system capable of:

1. Capturing a biometric sample from an end user
2. Extracting and processing the biometric data from that sample
3. Storing the extracted information in a database
4. Comparing the biometric data with data contained in one or more reference references
5. Deciding how well they match and indicating whether or not an identification or verification of identity has been achieved.

A biometric system may be a component of a larger system.

Capture

The process of collecting a biometric sample from an individual via a sensor. *See also submission.*

CBEFF - Common Biometric Exchange Formats Framework

A standard that provides the ability for a system to identify, and interface with, multiple biometric systems, and to exchange data between system components.

Challenge Response

A method used to confirm the presence of a person by eliciting direct responses from the individual. Responses can be either voluntary or involuntary. In a voluntary response, the end user will consciously react to something that the system presents. In an involuntary response, the end user's body automatically responds to a stimulus. A challenge response can be used to protect the system against attacks. *See also liveness detection.*

Claim of identity

A statement that a person is or is not the source of a reference in a database. Claims can be positive (I am in the database), negative (I am not in the database) or specific (I am end user 123 in the database).

Closed-set Identification

A biometric task where an unidentified individual is known to be in the database and the system attempts to determine his/her identity. Performance is measured by the frequency with which the individual appears in the system's top rank (or top 5, 10, etc.). *See also identification, open-set identification.*

Comparison

Process of comparing a biometric reference with a previously stored reference or references in order to make an identification or verification decision. *See also match.*

Cooperative User

An individual that willingly provides his/her biometric to the biometric system for capture. Example: A worker submits his/her

biometric to clock in and out of work. *See also indifferent user, non-cooperative user, uncooperative user.*

Core Point

The "center(s)" of a fingerprint. In a whorl pattern, the core point is found in the middle of the spiral/circles. In a loop pattern, the core point is found in the top region of the innermost loop. More technically, a core point is defined as the topmost point on the innermost upwardly curving friction ridgeline. A fingerprint may have multiple cores or no cores. *See also arch, delta point, friction ridge, loop, whorl.*

Covert

An instance in which biometric samples are being collected at a location that is not known to bystanders. An example of a covert environment might involve an airport checkpoint where face images of passengers are captured and compared to a watchlist without their knowledge. *See also non-cooperative user, overt.*

Crossover Error Rate (CER)

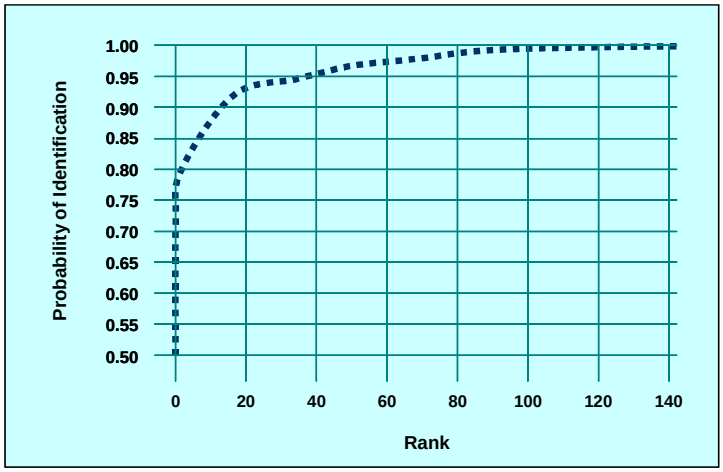
See equal error rate (EER).

Cumulative Match Characteristic (CMC)

A method of showing measured accuracy performance of a biometric system operating in the closed-set identification task.

Templates are compared and ranked based on their similarity. The CMC shows how often the individual's template appears in the ranks (1, 5, 10, 100, etc.), based on the match rate. A CMC compares the rank (1, 5, 10, 100, etc.) versus identification rate as illustrated below.

Cumulative Match Characteristic



D-Prime (D')

A statistical measure of how well a system can discriminate between a signal and a non-signal.

Database

A collection of one or more computer files. For biometric systems, these files could consist of biometric sensor readings, templates, match results, related end user information, etc. *See also gallery.*

Decision

The resultant action taken (either automated or manual) based on a comparison of a similarity score (or similar measure) and the system's threshold. *See also comparison, similarity score, threshold.*

Degrees of Freedom

A statistical measure of how unique biometric data is. Technically, it is the number of statistically independent features (parameters) contained in biometric data.

Delta Point

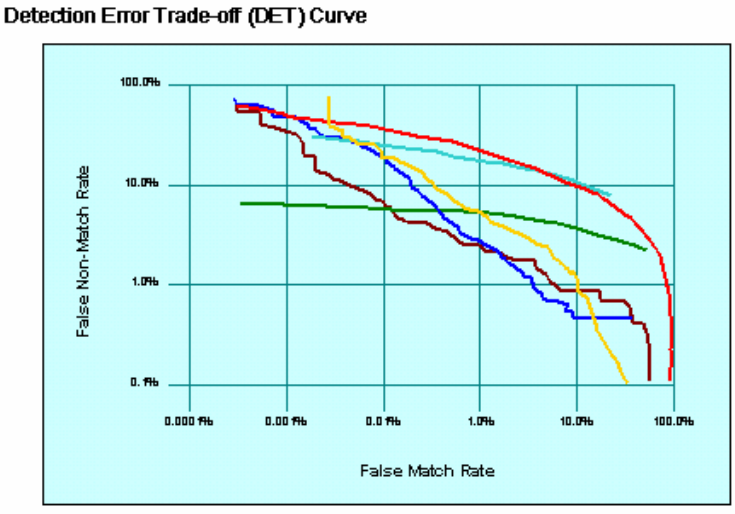
Part of a fingerprint pattern that looks similar to the Greek letter delta (▫), as illustrated below. Technically, it is the point on a friction ridge at or nearest to the point of divergence of two type lines, and located at or directly in front of the point of divergence. *See also core point, friction ridge.*

Detection and Identification Rate

The rate at which individuals, who are in a database, are properly identified in an open-set identification (watchlist) application. *See also open-set identification, watchlist.*

Detection Error Trade-off (DET) Curve

A graphical plot of measured error rates, as illustrated below. DET curves typically plot matching error rates (false non-match rate vs. false match rate) or decision error rates (false reject rate vs. false accept rate). *See also Receiver Operating Characteristics.*



Difference Score

A value returned by a biometric algorithm that indicates the degree of difference between a biometric sample and a reference. *See also hamming distance, similarity score.*

Eavesdropping

Surreptitiously obtaining data from an unknowing end user who is performing a legitimate function. An example involves having a hidden sensor co-located with the legitimate sensor. *See also skimming.*

EFTS - Electronic Fingerprint Transmission Specification

A document that specifies requirements to which agencies must adhere to communicate electronically with the Federal Bureau of Investigation's Integrated Automated Fingerprint Identification System (IAFIS). This specification facilitates information sharing and eliminates the delays associated with fingerprint cards. *See also Integrated Automated Fingerprint Identification System (IAFIS).*

Encryption

The act of transforming data into an unintelligible form so that it cannot be read by unauthorized individuals. A key or a password is used to decrypt (decode) the encrypted data.

End User

The individual who will interact with the system to enroll, to verify, or to identify. *See also cooperative user, indifferent user, non-cooperative user, uncooperative user, user.*

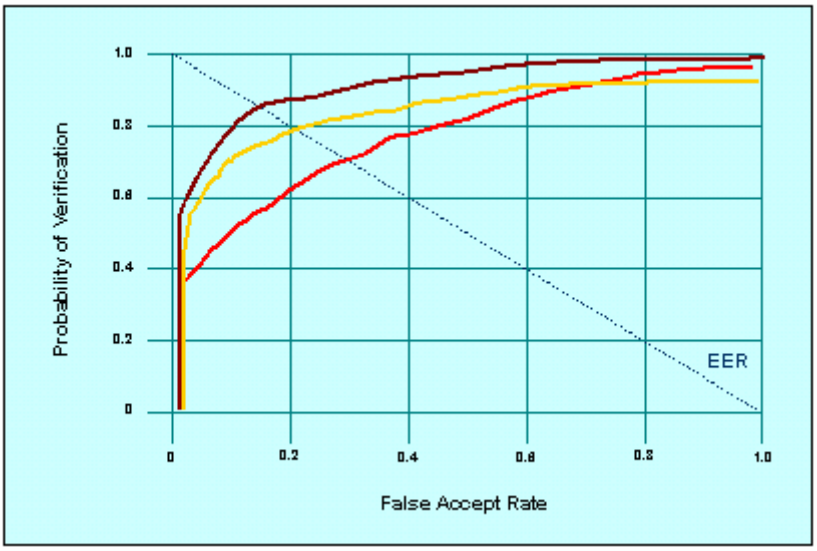
Enrollment

The process of collecting a biometric sample from an end user, converting it into a biometric reference, and storing it in the biometric system's database for later comparison.

Equal Error Rate (EER)

A statistic used to show biometric performance, typically when operating in the verification task. The EER is the location on a ROC or DET curve where the false accept rate and false reject rate (or one minus the verification rate {1-VR}) are equal, as illustrated below. In general, the lower the equal error rate value, the higher the accuracy of the biometric system. Note, however, that most operational systems are not set to operate at the "equal error rate" so the measure's true usefulness is limited to comparing biometric system performance. The EER is sometimes referred to as the "Crossover Error Rate." *See also Detection Error Trade-off (DET) curve, false accept rate, false reject rate, Receiver Operating Characteristics (ROC).*

Receiver Operating Characteristic (ROC) Curves with Equal Error Rate



Extraction

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

Face Recognition

A biometric modality that uses an image of the visible physical structure of an individual's face for recognition purposes.

Failure to Acquire (FTA)

Failure of a biometric system to capture and/or extract usable information from a biometric sample.

Failure to Enroll (FTE)

Failure of a biometric system to form a proper enrollment reference for an end user. Common failures include end users who are not properly trained to provide their biometrics, the sensor not capturing information correctly, or captured sensor data of insufficient quality to develop a template.

False Acceptance Rate (FAR)

A statistic used to measure biometric performance when operating in the verification task. The percentage of times a system produces a false accept, which occurs when an individual is incorrectly matched to another individual's existing biometric. Example: Frank claims to be John and the system verifies the claim. *See also false match rate, type II error.*

False Alarm Rate

A statistic used to measure biometric performance when operating in the open-set identification (sometimes referred to as watchlist) task. This is the percentage of times an alarm is incorrectly sounded on an individual who is not in the biometric system's database (the system alarms on Frank when Frank isn't in the database), or an alarm is sounded but the wrong person is identified (the system alarms on John when John is in the database, but the system thinks John is Steve).

False Match Rate

A statistic used to measure biometric performance when. Similar to the False Acceptance Rate (FAR).

False Non-Match Rate

A statistic used to measure biometric performance. Similar to the False Reject Rate (FRR), except the FRR includes the Failure To Acquire error rate and the False Non-Match Rate does not.

False Rejection Rate (FRR)

A statistic used to measure biometric performance when operating in the verification task. The percentage of times the system produces a false reject. A false reject occurs when an individual is not matched to his/her own existing biometric template. Example: John claims to be John, but the system incorrectly denies the claim. *See also false non-match rate, type I error.*

Feature(s)

Distinctive mathematical characteristic(s) derived from a biometric sample; used to generate a reference. *See also extraction, template.*

Feature Extraction

See extraction.

FERET - FacE REcognition Technology program

A face recognition development and evaluation program sponsored by the U.S. Government from 1993 through 1997. For more information visit www.frvt.org/FERET/default.htm. *See also FRGC, FRVT.*

Fingerprint Recognition

A biometric modality that uses the physical structure of an individual's fingerprint for recognition purposes. Important features used in most fingerprint recognition systems are minutiae points that include bifurcations and ridge endings. *See also bifurcation, core point, delta point, minutia(e) point.*

FpVTE - Fingerprint Vendor Technology Evaluation (2003)

An independently administered technology evaluation of commercial fingerprint matching algorithms. For more information visit fpvte.nist.gov.

FRGC - Face Recognition Grand Challenge

A face recognition development program sponsored by the U.S. Government from 2003-2005. For more information visit www.frvt.org/FRGC. *See also FERET, FRVT.*

Friction Ridge

The ridges present on the skin of the fingers and toes, and on the palms and soles of the feet, which make contact with an incident surface under normal touch. On the fingers, the distinctive patterns formed by the friction ridges that make up the fingerprints. *See also minutia(e) point.*

FRVT - Face Recognition Vendor Test

A series of large-scale independent technology evaluations of face recognition systems. The evaluations have occurred in 2000, 2002, and 2005. For more information visit www.frvt.org/FRVT2005/default.aspx. *See also FRGC, FERET.*

Gallery

The biometric system's database, or set of known individuals, for a specific implementation or evaluation experiment. *See also database, probe.*

Gait

An individual's manner of walking. This behavioral characteristic is in the research and development stage of automation.

Hamming Distance

The number of non-corresponding digits in a string of binary digits; used to measure dissimilarity. Hamming distances are used in many Daugman iris recognition algorithms. *See also difference score, similarity score.*

Hand Geometry Recognition

A biometric modality that uses the physical structure of an individual's hand for recognition purposes.

ICE - Iris Challenge Evaluation

A large-scale development and independent technology evaluation activity for iris recognition systems sponsored by the U.S. Government in 2005. .For more information visit iris.nist.gov/ICE.

Identification

A task where the biometric system searches a database for a reference matching a submitted biometric sample, and if found, returns a corresponding identity. A biometric is collected and compared to all the references in a database. Identification is "closed-set" if the person is known to exist in the database. In "open-set" identification, sometimes referred to as a "watchlist," the person is not guaranteed to exist in the database. The system must determine whether the person is in the database, then return the identity. *See also closed-set identification, open-set identification, verification, watchlist.*

Identification Rate

The rate at which an individual in a database is correctly identified.

Identity Governance

The combination of policies and actions taken to ensure enterprise-wide consistency, privacy protection and appropriate interoperability between individual identity management systems.

Identity Management

The combination of systems, rules and procedures that defines an agreement between an individual and organization(s) regarding ownership, utilization and safeguard of personal identity information.

Impostor

A person who submits a biometric sample in either an intentional or inadvertent attempt to claim the identity of another person to a biometric system. *See also attempt.*

INCITS - International Committee for Information Technology Standards

Organization that promotes the effective use of information and communication technology through standardization in a way that balances the interests of all stakeholders and increases the global competitiveness of the member organizations. For more information visit www.INCITS.org. *See also ANSI, ISO, NIST.*

Indifferent User

An individual who knows his/her biometric sample is being collected and does not attempt to help or hinder the collection of the sample. For example, an individual, aware that a camera is being used for face recognition, looks in the general direction of the sensor, neither avoiding nor directly looking at it. *See also cooperative user, non-cooperative user, uncooperative user.*

Infrared

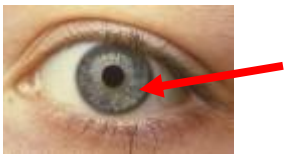
Light that lies outside the human visible spectrum at its red (low frequency) end.

Integrated Automated Fingerprint Identification System (IAFIS)

The FBI's large-scale ten fingerprint (open-set) identification system that is used for criminal history background checks and identification of latent prints discovered at crime scenes. This system provides automated and latent search capabilities,

electronic image storage, and electronic exchange of fingerprints and responses. *See also AFIS.*

Iris Recognition



A biometric modality that uses an image of the physical structure of an individual's iris for recognition purposes, as illustrated below. The iris muscle is the colored portion of the eye surrounding the pupil.

IrisCode©

A biometric feature format used in the Daugman iris recognition system.

ISO - International Organization for Standardization

A non-governmental network of the national standards institutes from 151 countries. The ISO acts as a bridging organization in which a consensus can be reached on solutions that meet both the requirements of business and the broader needs of society, such as the needs of stakeholder groups like consumers and users. For more information visit www.iso.org. *See also ANSI, INCITS, NIST.*

Keystroke Dynamics

A biometric modality that uses the cadence of an individual's typing pattern for recognition.

Latent Fingerprint

A fingerprint "image" left on a surface that was touched by an individual. The transferred impression is left by the surface contact with the friction ridges, usually caused by the oily residues produced by the sweat glands in the finger. *See also friction ridge.*

Live Capture

Typically refers to a fingerprint capture device that electronically captures fingerprint images using a sensor (rather than scanning ink-based fingerprint images on a card or lifting a latent fingerprint from a surface). *See also sensor.*

Liveness Detection

A technique used to ensure that the biometric sample submitted is from an end user. A liveness detection method can help protect the system against some types of spoofing attacks. *See also challenge response, mimic, spoofing.*

Loop

A fingerprint pattern in which the friction ridges enter from either side, curve sharply and pass out near the same side they entered as illustrated below. This pattern will contain one core and one delta. *See also arch, core point, delta point, friction ridge, whorl.*

Match

A decision that a biometric sample and a stored template comes from the same human source, based on their high level of similarity (difference or hamming distance). *See also false match rate, false non-match rate.*

Matching

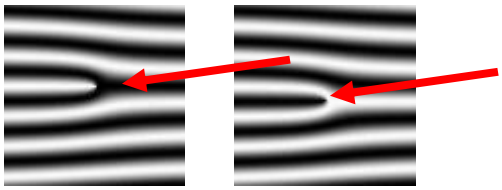
The process of comparing a biometric sample against a previously stored template and scoring the level of similarity (difference or hamming distance). Systems then make decisions based on this score and its relationship (above or below) a predetermined threshold. *See also comparison, difference score, threshold.*

Mimic

The presentation of a live biometric measure in an attempt to fraudulently impersonate someone other than the submitter. *See also challenge response, liveness detection, spoofing.*

Minutia(e) Point

Friction ridge characteristics that are used to individualize a fingerprint image, see illustration below. Minutiae are the points where friction ridges begin, terminate, or split into two or more ridges. In many fingerprint systems, the minutiae (as opposed to the images) are compared for recognition purposes. *See also friction ridge, ridge ending.*



Modality

A type or class of biometric system. For example: face recognition, fingerprint recognition, iris recognition, etc.

Model

A representation used to characterize an individual. Behavioral-based biometric systems, because of the inherently dynamic characteristics, use models rather than static templates. *See also template.*

Multimodal Biometric System

A biometric system in which two or more of the modality components (biometric characteristic, sensor type or feature extraction algorithm) occurs in multiple.

Neural Net/Neural Network

A type of algorithm that learns from past experience to make decisions. *See also algorithm.*

NIST - National Institute of Standards and Technology

A non-regulatory federal agency within the U.S. Department of Commerce that develops and promotes measurement, standards, and technology to enhance productivity, facilitate trade, and improve the quality of life. NIST's measurement and standards work promotes the well-being of the nation and helps improve, among many others things, the nation's homeland security. For more information visit www.nist.gov. *See also ANSI, INCITS, ISO.*

Noise

Unwanted components in a signal that degrade the quality of data or interfere with the desired signals processed by a system.

Non-cooperative User

An individual who is not aware that his/her biometric sample is being collected. Example: A traveler passing through a security line at an airport is unaware that a camera is capturing his/her face image. *See also cooperative user, indifferent user, uncooperative user.*

One-to-many

A phrase used in the biometrics community to describe a system that compares one reference to many enrolled references to make a decision. The phrase typically refers to the identification or watchlist tasks.

One-to-one

A phrase used in the biometrics community to describe a system that compares one reference to one enrolled reference to make a decision. The phrase typically refers to the verification task (though not all verification tasks are truly one-to-one) and the identification task can be accomplished by a series of one-to-one comparisons.

Open-set Identification

Biometric task that more closely follows operational biometric system conditions to 1) determine if someone is in a database and 2) find the record of the individual in the database. This is sometimes referred to as the "watchlist" task to differentiate it from the more commonly referenced closed-set identification. *See also closed-set identification, identification.*

Operational Evaluation

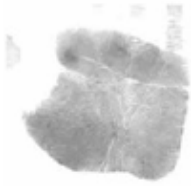
One of the three types of performance evaluations. The primary goal of an operational evaluation is to determine the workflow impact seen by the addition of a biometric system. *See also technology evaluation, scenario evaluation.*

Overt

Biometric sample collection where end users know they are being collected and at what location. An example of an overt environment is the US-VISIT program where non-U.S. citizens entering the United States submit their fingerprint data. *See also covert.*

Palm Print Recognition

A biometric modality that uses the physical structure of an individual's palm print for recognition purposes, as illustrated below.



Performance

A catch-all phrase for describing a measurement of the characteristics, such as accuracy or speed, of a biometric algorithm or system. *See also accuracy, crossover error rate, cumulative match characteristics, d-prime, detection error trade-off, equal error rate, false accept rate, false alarm rate, false match rate, false reject rate, identification rate, operational evaluation, receiver operating characteristics, scenario evaluation, technology evaluation, true accept rate, true reject rate, verification rate.*

PIN - Personal Identification Number

A security method used to show "what you know." Depending on the system, a PIN could be used to either claim or verify a claimed identity.

Pixel

A picture element. This is the smallest element of a display that can be assigned a color value. *See also pixels per inch (PPI), resolution.*

Pixels Per Inch (PPI)

A measure of the resolution of a digital image. The higher the PPI, the more information is included in the image, and the larger the file size. *See also pixel, resolution.*

Population

The set of potential end users for an application.

Probe

The biometric sample that is submitted to the biometric system to compare against one or more references in the gallery. *See also gallery.*

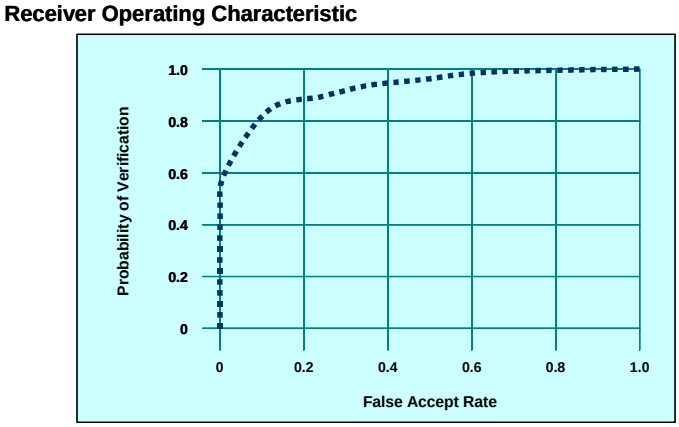
Radio Frequency Identification (RFID)

Technology that uses low-powered radio transmitters to read data stored in a transponder (tag). RFID tags can be used to track assets, manage inventory, authorize payments, and serve as electronic keys. RFID is not a biometric.

Receiver Operating Characteristics (ROC)

A method of showing measured accuracy performance of a biometric system. A verification ROC compares false accept rate

vs. verification rate. An open-set identification (watchlist) ROC compares false alarm rates vs. detection and identification rate.



Recognition

A generic term used in the description of biometric systems (e.g. face recognition or iris recognition) relating to their fundamental function. The term "recognition" does not inherently imply verification, closed-set identification or open-set identification (watchlist).

Record

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

Reference

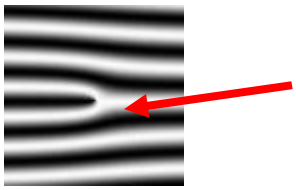
The biometric data stored for an individual for use in future recognition. A reference can be one or more templates, models or raw images. *See also template.*

Resolution

The number of pixels per unit distance in the image. Describes the sharpness and clarity of an image. *See also pixel, pixels per inch (PPI).*

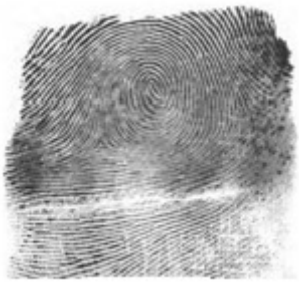
Ridge Ending

A minutiae point at the ending of a friction ridge, as illustrated below. *See also bifurcation, friction ridge.*



Rolled Fingerprints

An image that includes fingerprint data from nail to nail, obtained by "rolling" the finger across a sensor, as illustrated below.



Scenario Evaluation

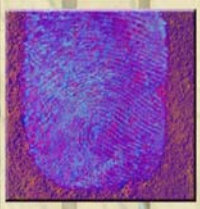
One of the three types of performance evaluations. The primary goal of a scenario evaluation is to measure performance of a biometric system operating in a specific application. *See also technology evaluation, operational evaluation.*

Segmentation

The process of parsing the biometric signal of interest from the entire acquired data system. For example, finding individual finger images from a slap impression, as illustrated below.

Sensor

Hardware found on a biometric device that converts biometric input into a digital signal and conveys this information to the processing device.



National Science and Technology Council (NSTC)

Committee on Technology

Committee on Homeland and National Security

Subcommittee on Biometrics

Sensor Aging

The gradual degradation in performance of a sensor over time.

Signature Dynamics

A behavioral biometric modality that analyzes dynamic characteristics of an individual's signature, such as shape of signature, speed of signing, pen pressure when signing, and pen-in-air movements, for recognition.

Similarity Score

A value returned by a biometric algorithm that indicates the degree of similarity or correlation between a biometric sample and a reference. *See also difference score, hamming distance.*

Skimming

The act of obtaining data from an unknowing end user who is not willingly submitting the sample at that time. An example could be secretly reading data while in close proximity to a user on a bus. *See also eavesdropping.*

Slap Fingerprint

Fingerprints taken by simultaneously pressing the four fingers of one hand onto a scanner or a fingerprint card, as illustrated below. Slaps are known as four finger simultaneous plain impressions.

Speaker Recognition

A biometric modality that uses an individual's speech, a feature influenced by both the physical structure of an individual's vocal tract and the behavioral characteristics of the individual, for recognition purposes. Sometimes referred to as "voice recognition." "Speech recognition" recognizes the words being said, and is not a biometric technology. *See also speech recognition, voice recognition.*

Speaker Recognition Evaluations

An ongoing series of evaluations of speaker recognition systems. For more information, visit www.nist.gov/speech/tests/spk/index.htm.

Speech Recognition

A technology that enables a machine to recognize spoken words. Speech recognition is not a biometric technology. *See also speaker recognition, voice recognition.*

Spoofing

The ability to fool a biometric sensor into recognizing an illegitimate user as a legitimate user (verification) or into missing an identification of someone that is in the database. *See also liveness detection, mimic.*

Submission

The process whereby an end user provides a biometric sample to a biometric system. *See also capture.*

Technology Evaluation

One of the three types of performance evaluations. The primary goal of a technology evaluation is to measure performance of biometric systems, typically only the recognition algorithm component, in general tasks. *See also operational evaluation, scenario evaluation.*

Template

A digital representation of an individual's distinct characteristics, representing information extracted from a biometric sample. Templates are used during biometric authentication as the basis for comparison. *See also extraction, feature, model.*

Threat

An intentional or unintentional potential event that could compromise the security and integrity of the system. *See also vulnerability.*

Threshold

A user setting for biometric systems operating in the verification or open-set identification (watchlist) tasks. 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. *See also comparison, match, matching.*

Throughput Rate

The number of biometric transactions that a biometric system processes within a stated time interval.

Token

A physical object that indicates the identity of its owner. For example, a smart card.

True Accept Rate

A statistic used to measure biometric performance when operating in the verification task. The percentage of times a system (correctly) verifies a true claim of identity. For example, Frank claims to be Frank and the system verifies the claim.

True Reject Rate

A statistic used to measure biometric performance when operating in the verification task. The percentage of times a system (correctly) rejects a false claim of identity. For example, Frank claims to be John and the system rejects the claim.

Type I Error

An error that occurs in a statistical test when a true claim is (incorrectly) rejected. For example, John claims to be John, but the system incorrectly denies the claim. *See also false reject rate (FRR).*

Type II Error

An error that occurs in a statistical test when a false claim is (incorrectly) not rejected. For example: Frank claims to be John and the system verifies the claim. *See also false accept rate (FAR).*

Uncooperative User

An individual who actively tries to deny the capture of his/her biometric data. Example: A detainee mutilates his/her finger upon capture to prevent the recognition of his/her identity via fingerprint. *See also cooperative user, indifferent user, non-cooperative user.*

User

A person, such as an administrator, who interacts with or controls end users' interactions with a biometric system. *See also cooperative user, end user, indifferent user, non-cooperative user, uncooperative user.*

US-VISIT - U.S. Visitor and Immigrant Status Indicator Technology

A continuum of security measures that begins overseas, at the Department of State's visa issuing posts, and continues through arrival and departure from the United States of America. Using biometric, such as digital, inkless fingerscans and digital photographs, the identity of visitors requiring a visa is now matched at each step to ensure that the person crossing the U.S. border is the same person who received the visa. For visa-waiver travelers, the capture of biometrics first occurs at the port of entry to the U.S. By checking the biometrics of a traveler against its databases, US-VISIT verifies whether the traveler has previously been determined inadmissible, is a know security risk

(including having outstanding wants and warrants), or has previously overstayed the terms of a visa. These entry and exit procedures address the U.S. critical need for tighter security and ongoing commitment to facilitate travel for the millions of legitimate visitors welcomed each year to conduct business, learn, see family, or tour the country.

Verification

A task where the biometric system attempts to confirm an individual's claimed identity by comparing a submitted sample to one or more previously enrolled templates. *See also identification, watchlist.*

Verification Rate

A statistic used to measure biometric performance when operating in the verification task. The rate at which legitimate end-users are correctly verified.

Voice Recognition

See speaker recognition.

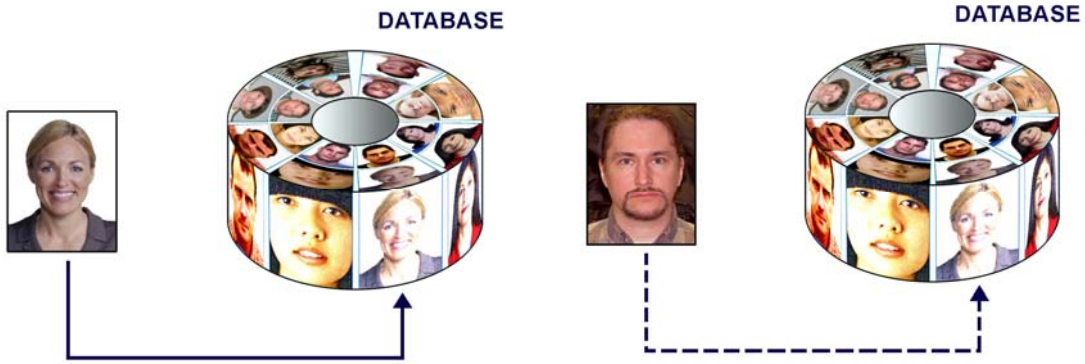
Vulnerability

The potential for the function of a biometric system to be compromised by intent (fraudulent activity); design flaw (including usage error); accident; hardware failure; or external environmental condition. *See also threat.*

Watchlist

A term sometimes referred to as open-set identification that describes one of the three tasks that biometric systems perform. Answers the questions: Is this person in the database? If so, who are they? The biometric system determines if the individual's biometric template matches a biometric template of someone on the watchlist, as illustrated below. The individual does not make

an identity claim, and in some cases does not personally interact with the system whatsoever. *See also closed-set identification, identification, open-set identification, verification.*



(This individual is in the watchlist) (This individual is not in the watchlist)

Wavelet Scalar Quantization (WSQ)

An FBI-specified compression standard algorithm that is used for the exchange of fingerprints within the criminal justice community. It is used to reduce the data size of images.

Whorl

A fingerprint pattern in which the ridges are circular or nearly circular, as illustrated below. The pattern will contain 2 or more deltas. *See also arch, delta point, loop, minutia(e) point.*

About the National Science and Technology Council

The National Science and Technology Council (NSTC) was established by Executive Order on November 23, 1993. This Cabinet-level Council is the principal means within the executive branch to coordinate science and technology policy across the diverse entities that make up the Federal research and development enterprise. Chaired by the President, the membership of the NSTC is made up of the Vice President, the Director of the Office of Science and Technology Policy, Cabinet

Secretaries and Agency Heads with significant science and technology responsibilities, and other White House officials.

A primary objective of the NSTC is the establishment of clear national goals for Federal science and technology investments in a broad array of areas spanning virtually all the mission areas of the executive branch. The Council prepares research and development strategies that are coordinated across Federal agencies to form investment packages aimed at accomplishing multiple national goals. The work of the NSTC is organized under four primary committees; Science, Technology, Environment and Natural Resources and Homeland and National Security. Each of these committees oversees a number of sub-committees and interagency working groups focused on different aspects of science and technology and working to coordinate the various agencies across the federal government. Additional information is available at www.ostp.gov/nstc.

About the Subcommittee on Biometrics

The NSTC Subcommittee on Biometrics serves as part of the internal deliberative process of the NSTC. Reporting to and directed by the Committee on Homeland & National Security and the Committee on Technology, the Subcommittee:

- Develops and implements multi-agency investment strategies that advance biometric sciences to meet public and private needs;
- Coordinates biometrics-related activities that are of interagency importance;
- Facilitates the inclusions of privacy-protecting principles in biometric system design;
- Ensures a consistent message about biometrics and government initiatives when agencies interact with Congress, the press and the public;
- Strengthen international and public sector partnerships to foster the advancement of biometric technologies.

Additional information on the Subcommittee is available at www.biometrics.gov.

Subcommittee on Biometrics

Co-chair: Duane Blackburn (OSTP)

Co-chair: Chris Miles (DOJ)

Co-chair: Brad Wing (DHS)

Executive Secretary: Kim Shepard (FBI Contractor)

Department Leads

Mr. Jon Atkins (DOS)

Dr. Sankar Basu (NSF)

Mr. Duane Blackburn (EOP)

Ms. Zaida Candelario (Treasury)

Dr. Joseph Guzman (DoD)

Dr. Martin Herman (DOC)

Ms. Usha Karne (SSA)

Dr. Michael King (IC)

Mr. Chris Miles (DOJ)

Mr. David Temoshok (GSA)

Mr. Brad Wing (DHS)

Mr. Jim Zok (DOT)

Communications ICP Team

Champion: Kimberly Weissman (DHS US-VISIT)

Members & Support Staff:

Mr. Richard Bailey (NSA Contractor)

Mr. Duane Blackburn (OSTP)

Mr. Jeffrey Dunn (NSA)

Ms. Valerie Lively (DHS S&T)

Mr. John Mayer-Splain (DHS US-VISIT Contractor)

Ms. Susan Sexton (FAA)

Ms. Kim Shepard (FBI Contractor)

Mr. Scott Swann (FBI)

Mr. Brad Wing (DHS US-VISIT)

Mr. David Young (FAA)

Mr. Jim Zok (DOT)

Special Acknowledgements

The Communications ICP Team wishes to thank the following external contributors for their assistance in developing this document:

- Kelly Smith, BRTRC, for performing background research and writing the first draft
- Donald Reynolds, Hirotaka Nakasone, Jim Wayman, and the Standards ICP Team for reviewing the document and providing numerous helpful comments

Document Source

This document, and others developed by the NSTC Subcommittee on Biometrics, can be found at www.biometrics.gov.