The IBIA Glossary of Biometric Terms

International **Biometrics+Identity** Association

Dear Readers,

I'd like to introduce you to the International Biometrics + Identity Association's (IBIA) comprehensive Glossary of Biometric Terms. The genesis of the work represented here was the realization by our members that many terms in our industry are misunderstood, improperly used, misrepresented, or conflated with other terms. When we looked at potential sources of authoritative definitions, like ISO SC37, NIST and the classic 2007 National Science and Technology Council (NSTC) definitions, we found that some are still correct, some are no longer relevant or have been deprecated, others needed some updating, and still other modern terms were missing altogether. So, we began what would be a significant months-long undertaking — to create a Glossary that honors the past but is updated for present needs.

The Glossary you will see is the result of considerable volunteer work by our members and others in our ecosystem, and we are all grateful to them all for their contributions. We started with the original IBIA Glossary, which was mostly composed of the NSTC terms, and added other authoritative sources. To this base, we inserted additional missing terms from other authoritative sources, and supplemented these with terms and definitions provided by IBIA members when there weren't any other credible or understandable definitions for the new terms. The idea was to provide definitions acceptable to practitioners of the art, but also usable by the public, members of the media, and lawmakers.

The 312 terms in the Glossary are listed in alphabetical order, each the term name, the definition, and the source citation. Among the new definitions are ones for "bias", "demographic differentials", "face analytics", "face detection", "face recognition" and "face verification". However, so there isn't another years-long gap in major updates to the terms, we intend this to be a "living" document, and we solicit suggestions for changes or new terms by writing to info@IBIA.org.

We hope you find this Glossary informative and useful!
Regards,

John Mears
Chairman of the Board
International Biometrics + Identity Association
www.ibia.org

Index

Introduction to the First Edition

Dear Readers,

Welcome to the first edition of the IBIA Glossary of Biometric Terms. We are pleased to share this Glossary with you with the hope that it will serve as an enlightening tool and an educational resource.

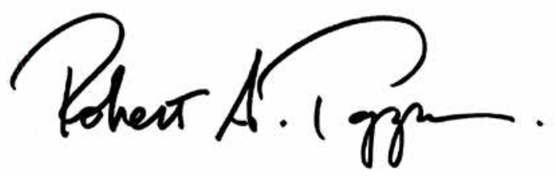
Given the highly technical nature of the science and technology that underpins the many aspects of biometrics, the terminology is often confusing and sometimes quite granular. Our intent in publishing this Glossary not was to aggregate the most important terms used in biometrics and present them in an easily-accessible and easy-to-understand guide.

We hope this Glossary will serve as a resource for everyone who is curious or who wants to know more about biometrics, and identity technologies we mean everyone — whether you are a student, a journalist, or even lawmaker — anyone who finds themselves having to quickly get up-to-speed and understand biometric terms, and who for accuracy and elucidation about this subject.

This Glossary is a collaborative work, gathered from a fount of different sources — some from the federal government and its attendant agencies, some from academia, as well as from the private sector — and curated by a number of individuals who are steeped in this discipline by virtue of their many years and far-reaching experience in biometrics and identity technologies. We are grateful to all who have contributed to this effort.

We hope you'll find this Glossary useful and helpful. We intend to update it and add new terms in succeeding editions. Any input or suggestions from you, the Reader, are most welcome.

Sincerely,



Robert Tappan
Managing Director
International Biometrics + Identity Association
Washington, DC
Initial Release: October 2023

Index

About the International Biometrics + Identity Association (IBIA)

The IBIA is the leading international trade organization representing the biometrics and identification technology industry. Recognizing the vital role that identity plays in a globally-connected world, IBIA brings stakeholders into a single organization that provides its members with: access to decisionmakers and policymakers; the latest in information and research about biometric technologies and industry trends; advocacy before lawmakers and legislative bodies; and thought-leadership regarding the ethical and responsible use of biometric and identity technologies.

To learn more about the International Biometrics + Identity Association, please visit us at: **www.ibia.org**

Terms Index

Terms Index

Terms Index

Terms Index

Terms Index

Terms Index

Terms Index

Terms Index

Terms Index

Terms Index

H

Terms Index

Terms Index

Terms Index

Terms Index

Terms Index

Terms Index

Terms Index

Terms Index

Terms Index

Terms Index

Terms Index

Terms Index

Terms Index

Acceptable Biometric Capture Attempt

Capture attempt that fulfils the requirements of a biometric capture process.

Source

International Organization for Standardization. (2017). Information technology - Vocabulary - Part 37: Biometrics. https://www.iso.org/standard/66693.html

Next Terms Alphabetically

Accuracy

Acquire

Algorithm

Accuracy

The true match rate of a biometric algorithm, determined by testing over many samples. The rate is the number of samples correctly matched or identified divided by the total number of samples presented. The resulting number is between 0 and 1, often represented as a percentage. It can also be represented by 1 minus the sum of the error rates (fraction of false matches plus fraction of false non-matches in the same test). Since the number can vary based on the match threshold setting for the algorithm, it is often quoted for a threshold setting that yields a particular false match rate, like 1 in 1000 or 0.001.

Source

IBIA

Next Terms Alphabetically

Acquire

Algorithm

American National Standards...

Acquire

Successfully complete a biometric acquisition process.

Source

International Organization for Standardization. (2017). Information technology - Vocabulary - Part 37: Biometrics. https://www.iso.org/standard/66693.html

Next Terms Alphabetically

Algorithm

American National Standards...

Analysis

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, and maintenance.

Source

IBIA

Next Terms Alphabetically

American National Standards...

Analysis

Analytics

American National Standards Institute (ANSI)

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.

Source

National Science & Technology Council (NSTC), 14 September 2007

Next Terms Alphabetically

Analysis

Analytics

Anonymized Biometric Data Record

Analysis

Refers to the process that converts data into actionable information and recommendations as applicable to increase situational awareness and better understand possible courses of action.

Source

Derived from Capstone Concept of Operations for DoD Biometrics in Support of Identity Superiority, November 2007

Next Terms Alphabetically

Analytics

Anonymized Biometric Data Record

Anthropometry

Analytics

A process in which a computer examines information using mathematical methods to find useful patterns. The term can apply to the algorithm that performs the process. Examples: facial analytics; video analytics.

Source

https://dictionary.cambridge.org/us/dictionary/english/analytics

Next Terms Alphabetically

Anonymized Biometric Data Record

Anthropometry

Arch

Anonymized Biometric Data Record

Biometric data record purposely disassociated from individual metadata.
Note 1 to entry: The biometric data within the biometric data record ultimately remains attributable to an individual.

Source

International Organization for Standardization. (2017). Information technology - Vocabulary - Part 37: Biometrics. https://www.iso.org/standard/66693.html

Next Terms Alphabetically

Anthropometry

Arch

Associated Information

Anthropometry

Anthropometric measurements are noninvasive quantitative measurements of the body. Anthropometry is a form of biometrics. Measurements such as height, weight, and build are useful in describing criminal suspects by witnesses. In medicine, they are important indicators of health, particularly for children, when compared to normal growth patterns.

Source

https://www.ncbi.nlm.nih.gov/books/NBK537315

Next Terms Alphabetically

Arch

Associated Information

Attempt

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.

Source

National Science & Technology Council (NSTC), 14 September 2007

Next Terms Alphabetically

Associated Information

Attempt

Authentication

Associated Information

Nonbiometric information about a person. For example, a person's name, personal habits, age, current and past addresses, current and past employers, telephone number, email address, place of birth, family names, nationality, education level, group affiliations, and history, including such characteristics as nationality, educational achievements, employer, security clearances, financial and credit history.

Source

Capstone Concept of Operations for DoD Biometrics in Support of Identity Superiority, November 2007

Next Terms Alphabetically

Attempt

Authentication

Authentication

Attempt

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

Source

National Science & Technology Council (NSTC), 14 September 2007

Next Terms Alphabetically

Authentication

Authentication

Auto-correlation

Authentication

Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to a system's resources.

Source

NIST SP800-63-3, Appendix A, Definitions and Abbreviations

Next Terms Alphabetically

Authentication

Auto-correlation

Automated Biometric Identification...

Authentication

The act of proving or showing to be of undisputed origin or veracity.
Note 1 to entry: Use of this term as a synonym for biometric verification or biometric identification is deprecated; the term biometric recognition is preferred.

Source

International Organization for Standardization. (2017). Information technology - Vocabulary - Part 37: Biometrics. https://www.iso.org/standard/66693.html

Next Terms Alphabetically

Auto-correlation

Automated Biometric Identification...

Automated Fingerprint Identification...

Auto-correlation

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

Source

International Association for Biometrics (iAfB) and International Computer Security Association (ICSA), 1999 Glossary of Biometric Terms

Next Terms Alphabetically

Automated Biometric Identification...

Automated Fingerprint Identification...

Behavioral Biometric Characteristic

Automated Biometric Identification System (ABIS)

ABIS is a central, multimodal biometrics data repository that is the enterprise-level authoritative data source for all DOD biometrics. DOD ABIS can transmit, store, manage, share, retrieve and display biometric data in support of identity superiority operations. DOD ABIS includes multimodal (fingerprint, palm, iris and face) storage and matching, watch-list capability and sharing with interagency repositories. It is based on adaptations of Commercial Off-The-Shelf products, using open architecture to minimize development and speed deployment.

Source

https://asc.army.mil/web/portfolio-item/biometric-enabling-capability-bec

Next Terms Alphabetically

Automated Fingerprint Identification...

Behavioral Biometric Characteristic

Bias

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).

Source

National Science & Technology Council (NSTC), 14 September 2006

Next Terms Alphabetically

Behavioral Biometric Characteristic

Bias

Bifurcation

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.

Source

National Science & Technology Council (NSTC), 14 September 2006

Next Terms Alphabetically

Bias

Bifurcation

Binning

Bias

Bias is a prejudice in favor of or against one thing, person, or group compared with another, usually in a way considered to be unfair. [Bias is often used by opponents of biometrics as a pejorative term for demographic differentials in face recognition systems.]

Source

Oxford Dictionary

[IBIA]

Next Terms Alphabetically

Bifurcation

Binning

Biographic Data

Bifurcation

The point in a fingerprint where a friction ridge divides or splits to form two ridges.

Source

National Science & Technology Council (NSTC), 14 September 2007

Next Terms Alphabetically

Binning

Biographic Data

Biological Biometric Characteristic

Binning

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

Source

IBIA

Next Terms Alphabetically

Biographic Data

Biological Biometric Characteristic

Biometric (Adjective)

Index

Biographic Data

Data that describes physical and nonphysical attributes of a biometric subject from whom biometric sample data has been collected. For example, full name, age, height, weight, address, employers, telephone number, email address, birthplace, nationality, education level, group affiliations, also data such as employer, security clearances financial and credit history.

Source

Derived from USCENTCOM Biometric Identification System for Access (BISA) CONOPS

Next Terms Alphabetically

Biological Biometric Characteristic

Biometric (Adjective)

Biometric Acquisition Process

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 characteristics. Examples of biometric modalities for which biological characteristics may dominate include fingerprint and hand geometry.

Source

National Science & Technology Council (NSTC), 14 September 2007

Next Terms Alphabetically

Biometric (Adjective)

Biometric Acquisition Process

Biometric Applicant

Biometric (Adjective)

Of or having to do with biometrics.

Note 1 to entry: The use of biometric as a noun, to mean for example, biometric characteristic (3.1.2), is deprecated.

Note 2 to entry: Since the late 19th century, the designations 'biometrics' and 'biometry' have been used with the general meaning of counting, measuring and statistical analysis of any kind of data in the biological sciences including the relevant medical sciences.

Source

International Organization for Standardization. (2017). Information technology - Vocabulary - Part 37: Biometrics. https://www.iso.org/standard/66693.html

Next Terms Alphabetically

Biometric Acquisition Process

Biometric Applicant

Biometric Application Database

Index

Biometric Acquisition Process

Biometric capture process and additional processing to attempt to produce a suitable biometric sample(s) in accordance with the defined policy.

Source

International Organization for Standardization. (2017). Information technology - Vocabulary - Part 37: Biometrics. https://www.iso.org/standard/66693.html

Next Terms Alphabetically

Biometric Applicant

Biometric Application Database

Biometric Application Decision

Biometric Applicant

Individual seeking to be enrolled in a biometric enrollment database.

Source

International Organization for Standardization. (2017). Information technology - Vocabulary - Part 37: Biometrics. https://www.iso.org/standard/66693.html

Next Terms Alphabetically

Biometric Application Database

Biometric Application Decision

Biometric Attendant

Biometric Application Database

Database of biometric data and associated metadata developed from and supporting the operation of a biometric application.

Source

International Organization for Standardization. (2017). Information technology - Vocabulary - Part 37: Biometrics. https://www.iso.org/standard/66693.html

Next Terms Alphabetically

Biometric Application Decision

Biometric Attendant

Biometric Automated Toolset (BAT)

Biometric Application Decision

[1] A conclusion based on the application decision policy after consideration of one or more comparison decisions, comparison scores and possibly other nonbiometric data.

[2] Decision to perform an action at the application level based on the results of a biometric process.

Source

[1] JTC001-SC37-n-2263 Text of Standing Document 2(SD2) Version 8, Harmonized Biometric Vocabulary, November 2007

[2] ISO/IEC 2382-38

Next Terms Alphabetically

Biometric Attendant

Biometric Automated Toolset (BAT)

Biometric Candidate

Biometric Attendant

Agent of the biometric system operator who directly interacts with the biometric capture subject.

Source

International Organization for Standardization. (2017). Information technology - Vocabulary - Part 37: Biometrics. https://www.iso.org/standard/66693.html

Next Terms Alphabetically

Biometric Automated Toolset (BAT)

Biometric Candidate

Biometric Candidate List

Biometric Automated Toolset (BAT)

A multimodal biometric system that collects and compares fingerprints, iris images and facial photos. It is used to enroll, identify, and track persons of interest; build digital dossiers on the individuals that include interrogation reports, biographic information, relationships, etc. BAT has an internal biometric signature searching and matching capability.

Source

Capstone Concept of Operations for DoD Biometrics in Support of Identity Superiority, November 2007

Next Terms Alphabetically

Biometric Candidate

Biometric Candidate List

Biometric Candidate Score

Biometric Candidate

Biometric reference identifier of a biometric reference in the biometric reference database determined to be sufficiently similar to the biometric probe to warrant further analysis.

Source

International Organization for Standardization. (2017). Information technology - Vocabulary - Part 37: Biometrics. https://www.iso.org/standard/66693.html

Next Terms Alphabetically

Biometric Candidate List

Biometric Candidate Score

Biometric Capture Device

Biometric Candidate List

Set of zero, one or more biometric candidates that may be intermediate or final.

Source

International Organization for Standardization. (2017). Information technology - Vocabulary - Part 37: Biometrics. https://www.iso.org/standard/66693.html

Next Terms Alphabetically

Biometric Candidate Score

Biometric Capture Device

Biometric Capture Process

Biometric Candidate Score

Comparison score for a biometric candidate.

Source

International Organization for Standardization. (2017). Information technology - Vocabulary - Part 37: Biometrics. https://www.iso.org/standard/66693.html

Next Terms Alphabetically

Biometric Capture Device

Biometric Capture Process

Biometric Capture Subject

Index

Biometric Capture Device

A device that collects a signal from a biometric characteristic and converts it to a captured biometric sample.

Source

JTC001-SC37-n-2263 Text of Standing Document 2(SD2) Version 8, Harmonized Biometric Vocabulary, November 2008

Next Terms Alphabetically

Biometric Capture Process

Biometric Capture Subject

Biometric Capture Subsystem

Biometric Capture Process

[1] A process of collecting or attempting to collect signals from a biometric characteristic and converting them to a captured biometric sample.

[2] Series of actions undertaken to affect a biometric capture.

Source

[1] JTC001-SC37-n-2263 Text of Standing Document 2(SD2) Version 8, Harmonized Biometric Vocabulary, November 2007

[2] ISO/IEC 2382-38

Next Terms Alphabetically

Biometric Capture Subject

Biometric Capture Subsystem

Biometric Characteristic

Biometric Capture Subject

Individual who is the subject of a biometric capture process.

Source

International Organization for Standardization. (2017). Information technology - Vocabulary - Part 37: Biometrics. https://www.iso.org/standard/66693.html

Next Terms Alphabetically

Biometric Capture Subsystem

Biometric Characteristic

Biometric Characteristics Examiner

Index

Biometric Capture Subsystem

Biometric capture devices and any sub-processes required to execute a biometric capture process.

Source

International Organization for Standardization. (2017). Information technology - Vocabulary - Part 37: Biometrics. https://www.iso.org/standard/66693.html

Next Terms Alphabetically

Biometric Characteristic

Biometric Characteristics Examiner

Biometric Claim

Biometric Characteristic

[1] A biological and behavioral characteristic of a biometric subject that can be detected and from which distinguishing, repeatable biometric features can be extracted for the purpose of automated recognition of biometric subjects.

[2] DEPRECATED: biometric: (noun) Biological and behavioral characteristic of an individual from which distinguishing, repeatable biometric features can be extracted for the purpose of biometric recognition. EXAMPLE Examples of biometric characteristics are: Galton ridge structure, face topography, facial skin texture, hand topography, finger topography, iris structure, vein structure of the hand, ridge structure of the palm, retinal pattern, handwritten signature dynamics, etc.

Source

[1] Derived from JTC001-SC37-n-2263 Text of Standing Document 2(SD2) Version 8, Harmonized Biometric Vocabulary, November 2007

[2] ISO/IEC 2382-38

Next Terms Alphabetically

Biometric Characteristics Examiner

Biometric Claim

Biometric Concealer

Biometric Characteristics Examiner

Individual with authority to assess biometric characteristics and who does so for the purpose of resolving a biometric claim.

Source

International Organization for Standardization. (2017). Information technology - Vocabulary - Part 37: Biometrics. https://www.iso.org/standard/66693.html

Next Terms Alphabetically

Biometric Claim

Biometric Concealer

Biometric Data

Biometric Claim

Claim that a biometric capture subject is or is not the bodily source of a specified or unspecified biometric reference.

Source

ISO/IEC 2382-38

Next Terms Alphabetically

Biometric Concealer

Biometric Data

Biometric Data Block

Index

Biometric Concealer

Subversive biometric capture subject who performs a biometric concealment attack.

Source

International Organization for Standardization. (2017). Information technology - Vocabulary - Part 37: Biometrics. https://www.iso.org/standard/66693.html

Next Terms Alphabetically

Biometric Data

Biometric Data Block

Biometric Data Record

Biometric Data

Biometric sample or aggregation of biometric samples at any stage of processing, e.g., biometric reference, biometric probe, biometric feature or biometric property.

Source

International Organization for Standardization. (2017). Information technology - Vocabulary - Part 37: Biometrics. https://www.iso.org/standard/66693.html

Next Terms Alphabetically

Biometric Data Block

Biometric Data Record

Biometric Data Subject

Index

Biometric Data Block

A block of data with a defined format that contains one or more biometric samples or biometric templates.

Source

JTC001-SC37-n-2263 Text of Standing Document 2(SD2) Version 8, Harmonized Biometric Vocabulary, November 2008

Next Terms Alphabetically

Biometric Data Record

Biometric Data Subject

Biometric Database

Biometric Data Record

Data record containing biometric data.

Source

International Organization for Standardization. (2017). Information technology - Vocabulary - Part 37: Biometrics. https://www.iso.org/standard/66693.html

Next Terms Alphabetically

Biometric Data Subject

Biometric Database

Biometric Enrollee

Biometric Data Subject

Individual whose individualized biometric data is within the biometric system.

Source

International Organization for Standardization. (2017). Information technology - Vocabulary - Part 37: Biometrics. https://www.iso.org/standard/66693.html

Next Terms Alphabetically

Biometric Database

Biometric Enrollee

Biometric Database

Biometric Database

[1] A collection of one or more computer files. For biometric systems, these files could consist of biometric sensor readings, templates, match results, related biometric subject information, etc.

[2] Database of biometric data record(s).

Source

[1] Derived from National Science & Technology Council (NSTC), 14 September 2006

[2] ISO/IEC 2382-38

Next Terms Alphabetically

Biometric Enrollee

Biometric Enrollment Data Record

Biometric Enrollment Database

Biometric Enrollee

(Biometric Enrollee) Biometric data subject whose biometric data is held in a biometric enrollment database.

Source

International Organization for Standardization. (2017). Information technology - Vocabulary - Part 37: Biometrics. https://www.iso.org/standard/66693.html

Next Terms Alphabetically

Biometric Enrollment Data Record

Biometric Enrollment Database

Biometric Entry - Exit

Biometric Enrollment Data Record

(Biometric Enrolment Data Record) Data record attributed to a biometric data subject, containing non-biometric data and associated with biometric reference identifier(s)

Source

International Organization for Standardization. (2017). Information technology - Vocabulary - Part 37: Biometrics. https://www.iso.org/standard/66693.html

Next Terms Alphabetically

Biometric Enrollment Database

Biometric Entry - Exit

Biometric Feature

Biometric Enrollment Database

Database of biometric enrolment data record(s).
Note 1 to entry: A database of biometric data not attributable to biometric data subjects is a biometric database, but not a biometric enrollment database, e.g., a database utilized in the training of a Universal Background Model.

Source

International Organization for Standardization. (2017). Information technology - Vocabulary - Part 37: Biometrics. https://www.iso.org/standard/66693.html

Next Terms Alphabetically

Biometric Entry - Exit

Biometric Feature

Biometric Feature Extraction Process

Biometric Entry - Exit

The process of verifying the identities of people both entering and leaving the United States via biometrics. The implementation of biometric technology stems from the 9/11 Commission Report which authorized the U.S. Government to use an automated system to record the arrivals and departures of visitors at all air, sea and land ports of entry. As technologies have evolved, facial comparison has proven to be one of the most effective solutions. Following years of testing and pilots, CBP has successfully operationalized and deployed facial biometric comparison technology, known as the Traveler Verification Service (TVS), to support comprehensive biometric entry and exit procedures in the air, land, and sea environments.

Source

https://www.cbp.gov/travel/biometrics

Next Terms Alphabetically

Biometric Feature

Biometric Feature Extraction Process

Biometric File

Biometric Feature

Numbers or labels extracted from biometric samples and used for comparison.

Source

JTC001-SC37-n-2263 Text of Standing Document 2(SD2) Version 8, Harmonized Biometric Vocabulary, November 2007

Next Terms Alphabetically

Biometric Feature Extraction Process

Biometric File

Biometric Identification Application

Biometric Feature Extraction Process

A process applied to a biometric sample with the intent of isolating and outputting repeatable and distinctive numbers or labels which can be compared to those extracted from the other biometric samples.

Source

JTC001-SC37-n-2263 Text of Standing Document 2(SD2) Version 8, Harmonized Biometric Vocabulary, November 2007

Next Terms Alphabetically

Biometric File

Biometric Identification Application

Biometric Identification Decision

Biometric File

The standardized individual data set resulting from a collection action (biometric sample and contextual data).

Source

Capstone Concept of Operations for DoD Biometrics in Support of Identity Superiority, November 2007

Next Terms Alphabetically

Biometric Identification Application

Biometric Identification Decision

Biometric Identification System

Biometric Identification Application

A system which contains an open-set or closed-set identification application.

Source

JTC001-SC37-n-2263 Text of Standing Document 2(SD2) Version 8, Harmonized Biometric Vocabulary, November 2008

Next Terms Alphabetically

Biometric Identification Decision

Biometric Identification System

Biometric Impostor

Biometric Identification Decision

Comparison decision as to whether a biometric reference(s) of a particular biometric data subject is in a biometric reference database.

Source

International Organization for Standardization. (2017). Information technology - Vocabulary - Part 37: Biometrics. https://www.iso.org/standard/66693.html

Next Terms Alphabetically

Biometric Identification System

Biometric Impostor

Biometric Mated Comparison Trial

Biometric Identification System

System that aims to perform biometric identification.

Source

International Organization for Standardization. (2017). Information technology - Vocabulary - Part 37: Biometrics. https://www.iso.org/standard/66693.html

Next Terms Alphabetically

Biometric Impostor

Biometric Mated Comparison Trial

Biometric Non-Mated Comparison Trial

Biometric Impostor

Subversive biometric capture subject who performs a biometric impostor attack.
Note 1: An impostor is a person who assumes a false identity in order to deceive or defraud.
Note 2: An impersonator pretends to be another person for entertainment or fraud.

Source

International Organization for Standardization. (2017). Information technology - Vocabulary - Part 37: Biometrics. https://www.iso.org/standard/66693.html

Next Terms Alphabetically

Biometric Mated Comparison Trial

Biometric Non-Mated Comparison Trial

Biometric Operational Personnel

Index

Biometric Mated Comparison Trial

Comparison of a biometric probe and a biometric reference from the same biometric capture subject and the same biometric characteristic as part of a performance test
Note 1 to entry: Biometric mated comparison trials have historically been referred to as "genuine trials", however, the term "genuine" historically implied an intent on the part of the biometric data subject. Ultimately the trial has nothing to do with the intention of the biometric capture subject.

Source

International Organization for Standardization. (2017). Information technology - Vocabulary - Part 37: Biometrics. https://www.iso.org/standard/66693.html

Next Terms Alphabetically

Biometric Non-Mated Comparison Trial

Biometric Operational Personnel

Biometric Presentation

Index

Biometric Non-Mated Comparison Trial

Comparison of a biometric probe and a biometric reference from different biometric data subjects as part of a performance test.

Source

International Organization for Standardization. (2017). Information technology - Vocabulary - Part 37: Biometrics. https://www.iso.org/standard/66693.html

Next Terms Alphabetically

Biometric Operational Personnel

Biometric Presentation

Biometric Query

Biometric Operational Personnel

Individuals, other than the biometric capture subjects, who take an active role in the operation of the biometric system.

Source

International Organization for Standardization. (2017). Information technology - Vocabulary - Part 37: Biometrics. https://www.iso.org/standard/66693.html

Next Terms Alphabetically

Biometric Presentation

Biometric Query

Biometric Reference Adaptation

Biometric Presentation

Interaction of the biometric capture subject and the biometric capture subsystem to obtain a signal from a biometric characteristic.

Source

International Organization for Standardization. (2017). Information technology - Vocabulary - Part 37: Biometrics. https://www.iso.org/standard/66693.html

Next Terms Alphabetically

Biometric Query

Biometric Reference Adaptation

Biometric Reference Data Record

Biometric Query

Biometric sample or biometric feature set input to an algorithm for biometric comparison to a biometric reference(s).

Source

International Organization for Standardization. (2017). Information technology - Vocabulary - Part 37: Biometrics. https://www.iso.org/standard/66693.html

Next Terms Alphabetically

Biometric Reference Adaptation

Biometric Reference Data Record

Biometric Reference Database

Biometric Reference Adaptation

Automatic incremental updating of a biometric reference.

Source

International Organization for Standardization. (2017). Information technology - Vocabulary - Part 37: Biometrics. https://www.iso.org/standard/66693.html

Next Terms Alphabetically

Biometric Reference Data Record

Biometric Reference Database

Biometric Reference Identifier

Biometric Reference Data Record

Indexed data record containing biometric reference(s).

Source

International Organization for Standardization. (2017). Information technology - Vocabulary - Part 37: Biometrics. https://www.iso.org/standard/66693.html

Next Terms Alphabetically

Biometric Reference Database

Biometric Reference Identifier

Biometric Representation

Biometric Reference Database

Database of biometric reference data records.

Source

International Organization for Standardization. (2017). Information technology - Vocabulary - Part 37: Biometrics. https://www.iso.org/standard/66693.html

Next Terms Alphabetically

Biometric Reference Identifier

Biometric Representation

Biometric Search

Biometric Reference Identifier

Pointer to a biometric reference data record in the biometric reference database.

Source

International Organization for Standardization. (2017). Information technology - Vocabulary - Part 37: Biometrics. https://www.iso.org/standard/66693.html

Next Terms Alphabetically

Biometric Representation

Biometric Search

Biometric Subversive Concealer

Biometric Representation

Biometric sample or biometric feature set.

Source

International Organization for Standardization. (2017). Information technology - Vocabulary - Part 37: Biometrics. https://www.iso.org/standard/66693.html

Next Terms Alphabetically

Biometric Search

Biometric Subversive Concealer

Biometric System Operator

Biometric Search

Examine a biometric reference database against a biometric probe to return either a biometric candidate list or a comparison decision that the biometric probe does or does not match with one or more biometric references.

Source

International Organization for Standardization. (2017). Information technology - Vocabulary - Part 37: Biometrics. https://www.iso.org/standard/66693.html

Next Terms Alphabetically

Biometric Subversive Concealer

Biometric System Operator

Biometric System Owner

Biometric Subversive Concealer

Subversive biometric capture subject who attempts to avoid being matched to their own biometric reference.

Source

International Organization for Standardization. (2017). Information technology - Vocabulary - Part 37: Biometrics. https://www.iso.org/standard/66693.html

Next Terms Alphabetically

Biometric System Operator

Biometric System Owner

Biometric Verification Decision

Biometric System Operator

Person or organization who executes policies and procedures in the administration of a biometric system.

Source

International Organization for Standardization. (2017). Information technology - Vocabulary - Part 37: Biometrics. https://www.iso.org/standard/66693.html

Next Terms Alphabetically

Biometric System Owner

Biometric Verification Decision

Biometric Verification System

Biometric System Owner

Person or organization with overall accountability for the acquisition, implementation and operation of the biometric system.

Source

International Organization for Standardization. (2017). Information technology - Vocabulary - Part 37: Biometrics. https://www.iso.org/standard/66693.html

Next Terms Alphabetically

Biometric Verification Decision

Biometric Verification System

Biometrically Enabled Intelligence

Biometric Verification Decision

Comparison decision determining the validity of a biometric claim in a verification transaction.

Source

International Organization for Standardization. (2017). Information technology - Vocabulary - Part 37: Biometrics. https://www.iso.org/standard/66693.html

Next Terms Alphabetically

Biometric Verification System

Biometrically Enabled Intelligence

Biometrically Enabled Physical Access

Biometric Verification System

System that aims to perform biometric verification.

Source

International Organization for Standardization. (2017). Information technology - Vocabulary - Part 37: Biometrics. https://www.iso.org/standard/66693.html

Next Terms Alphabetically

Biometrically Enabled Intelligence

Biometrically Enabled Physical Access

Biometrically Enabled Watchlist (BEWL)

Biometrically Enabled Intelligence

Intelligence information associated with biometrics data e.g., pattern analysis of a biometric subject's encounters with biometrics systems, judgments about a biometric subject disposition or intent based on biometric matches with forensic data, etc.

Source

Derived from DoD D 8521.AAE DoD BIOMETRICS PROGRAM

Next Terms Alphabetically

Biometrically Enabled Physical Access

Biometrically Enabled Watchlist (BEWL)

Biometrically Enabled Physical Access

The process of granting access to installations and facilities using biometrics.

Source

Derived from Capstone Concept of Operations for DoD Biometrics in Support of Identity Superiority, November 2007

Next Terms Alphabetically

Biometrically Enabled Watchlist (BEWL)

Capillary Electrophoresis

Capture Attempt

Biometrically Enabled Watchlist (BEWL)

Any list of person of interests (POI), with individuals identified by biometric sample instead of by name, and the desired/recommended disposition instructions for each individual. However, there first must be an acceptable degree of certainty that there is some indication of past behavior attributable to the individual that belongs to the biometric sample in order to estimate the level of threat posed by that individual. Even upon encounter or capture, we may never know an individuals' true identity, but that is immaterial as long as the linkage between the biometric sample and past threat behavior is established. No practicable standard currently exists for BEWLs, but the minimum content of a BEWL record is (1) a biometric identity (biometric sample linked to a POI), (2) a category of interest or threat commonly referred to as a tier, (3) the recommended action(s) to taken upon next encounter, and (4) notification instructions. The classification of the information within the BEWL can be up to TS/SCI/ORCON. In most instances the information will be releasable or at the UNCLASSIFIED// FOUO level to facilitate sharing.

Source

The DoD Biometrically Enabled Watchlist (BEWL) A Federated Approach, May 3, 2008

Next Terms Alphabetically

Capillary Electrophoresis

Capture Attempt

Capture Task

Capillary Electrophoresis

(See Electrophoresis, STR, PCR). [Capillary electrophoresis is a form of electrophoresis that uses a long narrow capillary tube, usually filled with a polymer, through which DNA STRs, isolated and amplified in the PCR step, move under the influence of an electric field. Smaller (shorter) STRs move faster and bigger (longer) STRs move slower through the capillary to a laser detector at the end of the capillary. The laser illuminates different colored fluorophores (fluorescent markers) attached to each STR type in the PCR step, as each now spatially separated STR group passes the illuminator/detector. The timing of each group's detector passage and the color of the attached fluorophores allows the STRs to be "measured" for length (size) and disambiguated for their original DNA locus. Special software and a control sample called an allelic ladder ensure STR sizing precision is consistent from run-to-run.]

Source

Butler, John M., "Capillary Electrophoresis", Advanced Topics in Forensic DNA Typing: Methodology, 2012.

[IBIA]

Next Terms Alphabetically

Capture Attempt

Capture Task

Capture Transaction

Capture Attempt

Activity with the intent of producing a captured biometric sample.

Source

International Organization for Standardization. (2017). Information technology - Vocabulary - Part 37: Biometrics. https://www.iso.org/standard/66693.html

Next Terms Alphabetically

Capture Task

Capture Transaction

Captured Biometric Sample

Capture Task

Prescribed set of biometric capture subject behaviors in a capture attempt.

Source

International Organization for Standardization. (2017). Information technology - Vocabulary - Part 37: Biometrics. https://www.iso.org/standard/66693.html

Next Terms Alphabetically

Capture Transaction

Captured Biometric Sample

Claimant

Capture Transaction

One or more capture attempts with the intent of acquiring all of the biometric data from a biometric capture subject necessary to produce either a biometric reference or a biometric probe.

Source

International Organization for Standardization. (2017). Information technology - Vocabulary - Part 37: Biometrics. https://www.iso.org/standard/66693.html

Next Terms Alphabetically

Captured Biometric Sample

Claimant

Cognizant Presentation

Captured Biometric Sample

DEPRECATED: raw biometric sample Biometric sample resulting from a biometric capture process.

Source

International Organization for Standardization. (2017). Information technology - Vocabulary - Part 37: Biometrics. https://www.iso.org/standard/66693.html

Next Terms Alphabetically

Claimant

Cognizant Presentation

Comparison Score

Claimant

Individual making a claim that can be verified biometrically.
Note 1 to entry: The claimant need not be the biometric data subject.

Source

International Organization for Standardization. (2017). Information technology - Vocabulary - Part 37: Biometrics. https://www.iso.org/standard/66693.html

Next Terms Alphabetically

Cognizant Presentation

Comparison Score

Comparison Trial

Cognizant Presentation

Presentation made with the biometric capture subject's awareness.

Source

International Organization for Standardization. (2017). Information technology - Vocabulary - Part 37: Biometrics. https://www.iso.org/standard/66693.html

Next Terms Alphabetically

Comparison Score

Comparison Trial

Conformant Capture Attempt

Comparison Score

DEPRECATED: matching score Numerical value (or set of values) resulting from a comparison.

Source

International Organization for Standardization. (2017). Information technology - Vocabulary - Part 37: Biometrics. https://www.iso.org/standard/66693.html

Next Terms Alphabetically

Comparison Trial

Conformant Capture Attempt

Cooperative Biometric Capture Subject

Index

Comparison Trial

Single biometric probe to biometric reference comparison in a test of performance.

Source

International Organization for Standardization. (2017). Information technology - Vocabulary - Part 37: Biometrics. https://www.iso.org/standard/66693.html

Next Terms Alphabetically

Conformant Capture Attempt

Cooperative Biometric Capture Subject

Cooperative Presentation

Index

Conformant Capture Attempt

Actions that comply with the capture task.

Source

International Organization for Standardization. (2017). Information technology - Vocabulary - Part 37: Biometrics. https://www.iso.org/standard/66693.html

Next Terms Alphabetically

Cooperative Biometric Capture Subject

Cooperative Presentation

Core

Cooperative Biometric Capture Subject

Biometric capture subject motivated to achieve a successful completion of the biometric acquisition process.

Source

International Organization for Standardization. (2017). Information technology - Vocabulary - Part 37: Biometrics. https://www.iso.org/standard/66693.html

Next Terms Alphabetically

Cooperative Presentation

Core

Crosslinks

Cooperative Presentation

Presentation by a cooperative biometric capture subject

Source

International Organization for Standardization. (2017). Information technology - Vocabulary - Part 37: Biometrics. https://www.iso.org/standard/66693.html

Next Terms Alphabetically

Core

Crosslinks

Dactyloscopy

Core

The approximate center of a fingerprint.

Source

https://www.crime-scene-investigator.net/fbiscienceoffingerprints.html#:~:text=The%20delta%20is%20the%20point,center%20of%20the%20finger%20impression.

Next Terms Alphabetically

Crosslinks

Dactyloscopy

Deepfakes

Crosslinks

Crosslinks are biometric records that erroneously contain data from different individuals.

Source

IBIA

Next Terms Alphabetically

Dactyloscopy

Deepfakes

Delta

Dactyloscopy

The science of fingerprint identification.

Source

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/267523/FingerprintTerminology.pdf

Next Terms Alphabetically

Deepfakes

Delta

Demographic differentials

Deepfakes

Defined by Oxford Languages to be a video of a person in which their face or body has been digitally altered so that they appear to be someone else, typically used maliciously or to spread false information. The word is a 21st century concatenation of "deep" and "fakes". Deep refers to either "deep learning" or "deep neural networks" or "deep generative methods" — the technology used to create the fake videos.
Beyond the dictionary definition, deepfakes can also refer to audio content, such as deepfake audios to attempt to spoof speaker recognition systems. Deepfakes can be created but can also be alterations of existing samples.

Source

Oxford Languages, IBIA, and ISO SC37

Next Terms Alphabetically

Delta

Demographic differentials

Demographics

Index

Delta

[In fingerprint analysis] the delta is the point from which to start in ridge counting. [For instance] in the loop type pattern the ridges intervening between the delta and the core are counted.

Source

https://www.crime-scene-investigator.net/fbiscienceoffingerprints.html#:~:text=The%20delta%20is%20the%20point,center%20of%20the%20finger%20impression%20

Next Terms Alphabetically

Demographic differentials

Demographics

Detection and Identification Rate

Demographic differentials

Observed differences (e.g., error rates) between demographic classes of subjects in the ability of a face recognition algorithm to match two images of the same person.

Source

NISTIR 8280, Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects, December 2019.

Next Terms Alphabetically

Demographics

Detection and Identification Rate

Detection Error Tradeoff (DET) Curve

Demographics

The qualities (such as age, [race], sex and income) of a [person or] specific group of people.

Source

The Britannica Dictionary [additions by IBIA]

Next Terms Alphabetically

Detection and Identification Rate

Detection Error Tradeoff (DET) Curve

Difference Score

Detection and Identification Rate

The rate at which biometric subjects, who are in a database, are properly identified in an open-set identification (watchlist) application.

Source

Derived from National Science & Technology Council (NSTC), 14 September 2006

Next Terms Alphabetically

Detection Error Tradeoff (DET) Curve

Difference Score

Digital Driver's License (DDL)

Detection Error Tradeoff (DET) Curve

A graphical plot of measured error rates. DET curves typically plot matching error rates (false nonmatch rate vs. false match rate) or decision error rates (false reject rate vs. false accept rate).

Source

National Science & Technology Council (NSTC), 14 September 2006

Next Terms Alphabetically

Difference Score

Digital Driver's License (DDL)

Digital Identity

Difference Score

A value returned by a biometric algorithm that indicates the degree of difference between a biometric sample and a reference.

Source

National Science & Technology Council (NSTC), 14 September 2006

Next Terms Alphabetically

Digital Driver's License (DDL)

Digital Identity

Digital Wallet

Digital Driver's License (DDL)

Also known as a mobile driver's license (mDL), it is a driver's license that is provisioned to (digitized for storage on) a mobile device with the capability to be updated in real time. It is comprised of the same data elements that are used to produce a physical driver's license, however, the data is transmitted electronically to a relying party's reader device and authenticated. At present, a DDL is not a replacement for a physical driver's license but is intended as a supplement. The DDL is an improvement over physical credentials which can be lost or stolen, become broken or damaged, contain outdated information, offer too much information (including personally identifiable information), and can more easily be replicated by counterfeiters. The DDL offers safe, secure, and trustable technologies that allow for touchless transactions, selective information release, and data protection.

Source

https://www.aamva.org/topics/mobile-driver-license#?wst=4a3b89462cc2cff2cbe0c7accde57421 and IBIA

Next Terms Alphabetically

Digital Identity

Digital Wallet

Dissimilarity Score

Digital Identity

Digital identity is the unique representation of a subject engaged in an online transaction.

Source

Grassi, P. A., Garcia, M. E., & Fenton, J. L. (2020). NIST Special Publication 800-63-3 Digital Identity Guidelines. NIST. https://doi.org/https://doi.org/10.6028/NIST.SP.800-63-3

Next Terms Alphabetically

Digital Wallet

Dissimilarity Score

Distal

Digital Wallet

Sometimes called an e-wallet, or mobile wallet, a typical digital wallet is a secure (encrypted) storage application running on a computer or smart phone that restricts content access to an authorized user. People use them primarily for storage of passwords, identity information, memberships and credit card information, but uses are varied and growing, including event and transportation tickets, vaccination records, and driver's licenses.

Source

IBIA

Next Terms Alphabetically

Dissimilarity Score

Distal

DNA

Dissimilarity Score

Comparison score that decreases with similarity.

Source

International Organization for Standardization. (2017). Information technology - Vocabulary - Part 37: Biometrics. https://www.iso.org/standard/66693.html

Next Terms Alphabetically

Distal

DNA

Duplicate Enrollment Check

Distal

[In human anatomy] this refers to something that is the farthest away from the centre or point of attachment. For example, the distal flexures of the finger are the creases in the fingers furthest away from the palm, between the top and middle phalanges [bones] of the finger. [Relevant to palm print biometrics.]

Source

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/267523/FingerprintTerminology.pdf

Next Terms Alphabetically

DNA

Duplicate Enrollment Check

Electronic Biometric Transmission...

DNA

DNA (deoxyribonucleic acid) is the molecule that carries genetic information for the development and functioning of organisms including humans. DNA is an increasingly useful biometric and is encountered most often in forensics and healthcare. The sequence of the four bases along DNA's double helix backbone encodes biological information, such as the instructions for making a protein or RNA molecule. Segments of the sequence can also be useful for identification purposes. For forensics, current DNA identification technologies measure short tandem repeat sequences (STRs) in the nuclear or mitochondrial DNA. The chosen STR sequences (typically 20 for FBI CODIS) are not linked to any known genetic characteristics but vary from person to person in accordance with well-known population statistics. For this reason, measuring the lengths of these STRs (in a lab or rapid DNA identification instruments) provides a highly accurate and easily stored attribute that can be compared to others for potential identification, lead generation, exclusion, or family matching of an individual or individuals. [Isolation, amplification and measuring of the STRs is usually done through process steps that include extraction, polymerase chain reaction (PCR) and electrophoresis.]

Source

https://www.ibia.org/biometrics-and-identity/biometric-technologies/dna#:~:text=DNA%20Biometrics,the%20nuclear%20or%20mitochondrial%20DNA. https://www.genome.gov/genetics-glossary/Deoxyribonucleic-Acid, [IBIA]

Next Terms Alphabetically

Duplicate Enrollment Check

Electronic Biometric Transmission...

Electronic Fingerprint Transmission...

Duplicate Enrollment Check

[1] The comparison of a recognition biometric sample/biometric feature/biometric model to some or all of the biometric references in the enrollment database to determine if any similar biometric reference exists.

[2] (Duplicate Biometric Enrolment Check) Biometric identification check that may be performed as a part of the biometric enrollment process to ascertain the existing enrollment status of biometric data subject.

Source

[1] JTC001-SC37-n-2263 Text of Standing Document 2(SD2) Version 8, Harmonized Biometric Vocabulary, November 2007

[2] International Organization for Standardization. (2017). Information technology - Vocabulary - Part 37: Biometrics. https://www.iso.org/standard/66693.html

Next Terms Alphabetically

Electronic Biometric Transmission...

Electronic Fingerprint Transmission...

Electrophoresis

Electronic Biometric Transmission Specification (EBTS)

Describes customizations of the Federal Bureau of Investigation (FBI) Electronic Fingerprint Transmission Specification (EFTS) transactions that are necessary to utilize the Department of Defense (DoD) Automated Biometric Identification System (ABIS). Any DoD entity that wishes to interface with the DoD ABIS must conform to the DoD EBTS.

Source

Department of Defense Electronic Biometric Transmission Specification 23 August 2005 Version 1.1 DIN: DOD_BMO_TS_EBTS_Aug05_01.01

Next Terms Alphabetically

Electronic Fingerprint Transmissio...

Electrophoresis

Encryption

Electronic Fingerprint Transmission Specification (EFTS)

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

Source

National Science & Technology Council (NSTC), 14 September 2006

Next Terms Alphabetically

Electrophoresis

Encryption

Enhanced Driver's License (EDL)

Electrophoresis

Electrophoresis is a laboratory technique used to separate DNA, RNA or protein molecules based on their size and electrical charge. An electric current is used to move the molecules through a gel or other matrix. Pores in the gel or matrix work like a sieve, allowing smaller molecules to move faster than larger molecules. To determine the size of the molecules in a sample, standards of known sizes are separated on the same gel and then compared to the sample.

Source

https://www.genome.gov/genetics-glossary/Electrophoresis#:~:text=Electrophoresis%20is%20a%20laboratory%20technique,a%20gel%20or%20other%20matrix.

Next Terms Alphabetically

Encryption

Enhanced Driver's License (EDL)

Enroll

Encryption

The act of transforming data using cryptography 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. Often used to protect data (biometric and other types) at rest and in transit. Homomorphic encryption promises to allow data to be encrypted even when being processed.

Source

IBIA

Next Terms Alphabetically

Enhanced Driver's License (EDL)

Enroll

Enrollment

Enhanced Driver's License (EDL)

Enhanced Drivers Licenses (EDLs) are state-issued enhanced drivers licenses that provide proof of identity and U.S. citizenship when crossing the U.S. border in a vehicle. They are issued in a secure process and include technology that makes travel easier. EDLs are a low-cost, convenient option for entering the United States from Canada, Mexico or the Caribbean through a land or sea port of entry, in addition to serving as a permit to drive.

DHS has been working with individual states to enhance their drivers licenses and identification documents to comply with travel rules under the Western Hemisphere Travel Initiative (WHTI). Enhanced driver's licenses make it easier for U.S. citizens to cross the border into the United States because they include:

- *a vicinity Radio Frequency Identification (RFID) chip that will signal a secure system to pull up your biographic and biometric data for the CBP officer as you approach the border inspection booth; and,*
- *a Machine-Readable Zone (MRZ) or barcode that the CBP officer can read electronically if RFID isn't available.*

Source

https://www.dhs.gov/enhanced-drivers-licenses-what-are-they

and

https://help.cbp.gov/s/article/Article-1269?language=en_US

Next Terms Alphabetically

Enroll

Enrollment

Equal Error Rate (EER)

Enroll

Create and store, for a biometric subject, an enrollment data record that includes biometric reference(s) and typically, nonbiometric data.

Source

Derived from JTC001-SC37-n-2263 Text of Standing Document 2(SD2) Version 8, Harmonized Biometric Vocabulary, November 2007

Next Terms Alphabetically

Enrollment

Equal Error Rate (EER)

Error Rates

Enrollment

[1] The process of collecting a biometric sample from a biometric subject, converting it into a biometric reference, and storing it in the biometric system's database for later comparison.

[2] (Biometric Enrolment) DEPRECATED: registration
Act of creating and storing a biometric enrollment data record in accordance with an enrollment policy.

Source

[1] Derived from National Science & Technology Council (NSTC), 14 September 2006

[2] International Organization for Standardization. (2017). Information technology - Vocabulary - Part 37: Biometrics. https://www.iso.org/standard/66693.html

Next Terms Alphabetically

Equal Error Rate (EER)

Error Rates

Expanded Maritime Interdiction...

Equal Error Rate (EER)

For a biometric algorithm, the error rate (as a result of threshold setting) where the false match (or false identification) rate equals the false non-match (or false non-identification) rate. Generally, the lower the number, the better the performance.

Source

IBIA

Next Terms Alphabetically

Error Rates

Expanded Maritime Interdiction...

Face Analytics

Error Rates

Characterizing expected error performance in biometric algorithms is done by running tests using a large gallery of biometric samples to determine how often probe subjects are identified correctly, how often subjects are mis-identified and how often subjects are missed. Ratios of the respective numbers against the total number of probes comprise the rates for each. For verification applications: FMR = false match rate = fraction, wrong subjects accepted FNMR = false non-match rate = fraction, correct subjects rejected. For identification applications: FPIR = false positive identification rate = fraction, wrong subjects identified. FNIR = false non-identification rate = fraction, correct subject not identified, but in the gallery.

Source

IBIA

Next Terms Alphabetically

Expanded Maritime Interdiction...

Face Analytics

Face Detection

Expanded Maritime Interdiction Operation (EMIO)

A key maritime component needed to support the global war on terrorism by deterring, delaying, and disrupting the movement of terrorists and terrorist related materials and personnel at sea. U.S. Navy ships operating in the Central Command's (CENTCOM) Area of Responsibility (AOR) have the capability to collect and forward biometric data from potential terrorists for searching against databases.

Source

Derived from Biometrics Task Force and Navy Team for Success January 2007

Next Terms Alphabetically

Face Analytics

Face Detection

Face Pose

Face Analytics

Term for the set of classifiers (software analytics) that analyze a face image to estimate age, sex, expression, emotion, alertness, or gaze direction, among other characteristics. Salient applications are in marketing and vehicle safety.

Source

IBIA

Next Terms Alphabetically

Face Detection

Face Pose

Face Recognition

Face Detection

Term for an algorithm (analytic) that detects the presence and location of faces in an image. Applications include locating individual faces in a crowd, and/or serving as a pre-processor for face analytics or face recognition/verification.

Source

IBIA

Next Terms Alphabetically

Face Pose

Face Recognition

Face Verification

Face Pose

When capturing face images for face recognition, the orientation of the subject's face has traditionally been of concern. For instance, in traditional mug shots, a frontal and a profile image is taken. The orientation of the head is called "pose", and is characterized by measurements of yaw, roll, and pitch. Yaw is turning the head either left or right of straight-on frontal. Roll is tilting the head toward one shoulder or the other. Pitch is tilting the head up or down, directly away from or toward the chest.

Source

IBIA

Next Terms Alphabetically

Face Recognition

Face Verification

Failure to Acquire (FTA)

Face Recognition

A biometric modality that uses an image of the subject's face for recognition purposes. [This term is most often applied to 1:N searches to see if an unknown (probe) face exists in a previously established collection (gallery) of face images. Often used for lead generation in forensic applications.]

Source

Derived from National Science & Technology Council (NSTC), 14 September 2006.

[IBIA]

Next Terms Alphabetically

Face Verification

Failure to Acquire (FTA)

Failure to Acquire Rate

Face Verification

A biometric modality that uses an image of the subject's face for verification purposes. This term is most often applied to 1:1 matches to see if a face matches that of a known person. This technique is used to verify people against drivers' licenses (TSA CAT2) or passports (CBP). It is also used in facility or campus access control applications.

Source

IBIA, derived from NSTC

Next Terms Alphabetically

Failure to Acquire (FTA)

Failure to Acquire Rate

Failure to Capture (FTC)

Failure to Acquire (FTA)

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

[2] Failure to accept for subsequent comparison the output of a biometric capture process, a biometric sample of the biometric characteristic of interest.

Source

[1] National Science & Technology Council (NSTC), 14 September 2006

[2] International Organization for Standardization. (2017). Information technology - Vocabulary - Part 37: Biometrics. https://www.iso.org/standard/66693.html

Next Terms Alphabetically

Failure to Acquire Rate

Failure to Capture (FTC)

Failure to Enroll (FTE)

Failure to Acquire Rate

[1] The frequency of a failure to acquire.

[2] Proportion of a specified set of biometric acquisition processes that were failures to acquire.

Source

[1] National Information Assurance Partnership, US Government Biometric Verification Mode Protection Profile for Medium Robustness Environments v1.0, 15 November 2003, Sponsored by the DoD Biometrics Management Office (BMO) and the National Security Agency (NSA)

[2] International Organization for Standardization. (2017). Information technology - Vocabulary - Part 37: Biometrics. https://www.iso.org/standard/66693.html

Next Terms Alphabetically

Failure to Capture (FTC)

Failure to Enroll (FTE)

Failure to Enroll Rate

Failure to Capture (FTC)

Failure of the biometric capture process to produce a captured biometric sample of the biometric characteristic of interest.

Source

International Organization for Standardization. (2017). Information technology - Vocabulary - Part 37: Biometrics. https://www.iso.org/standard/66693.html

Next Terms Alphabetically

Failure to Enroll (FTE)

Failure to Enroll Rate

False Acceptance

Failure to Enroll (FTE)

[1] Failure of a biometric system to form a proper enrollment reference for a biometric subject. Common failures include biometric subjects 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.

[2] (Failure to Enrol) Failure to create and store a biometric enrollment data record for an eligible biometric capture subject, in accordance with a biometric enrollment policy. Note 1 to entry: Not enrolling someone ineligible to enroll is not a failure to enroll

Source

[1] Derived from National Science & Technology Council (NSTC), 14 September 2006

[2] International Organization for Standardization. (2017). Information technology - Vocabulary - Part 37: Biometrics. https://www.iso.org/standard/66693.html

Next Terms Alphabetically

Failure to Enroll Rate

False Acceptance

False Acceptance Rate (FAR)

Failure to Enroll Rate

[1] The probability that a biometric system will have a failure-to-enroll.

[2] (Failure-to-enroll Rate) Proportion of a specified set of biometric enrollment transactions that resulted in a failure to enroll.

Source

[1] National Information Assurance Partnership, US Government Biometric Verification Mode Protection Profile for Medium Robustness Environments v1.0, 15 November 2003, Sponsored by the DoD Biometrics Management Office (BMO) and the National Security Agency (NSA)

[2] International Organization for Standardization. (2017). Information technology - Vocabulary - Part 37: Biometrics. https://www.iso.org/standard/66693.html

Next Terms Alphabetically

False Acceptance

False Acceptance Rate (FAR)

False Alarm Rate

False Acceptance

[1] When a biometric system incorrectly identifies a biometric subject or incorrectly authenticates an imposter against a claimed identity.

[2] (Biometric False Acceptance) Error of accepting a biometric claim that should have been rejected in accordance with an authoritative statement on the origin of the biometric probe and the biometric reference.

Source

[1] Derived from National Information Assurance Partnership, US Government Biometric Verification Mode Protection Profile for Medium Robustness Environments v1.0, 15 November 2003, Sponsored by the DoD Biometrics Management Office (BMO) and the National Security Agency (NSA)

[2] International Organization for Standardization. (2017). Information technology - Vocabulary - Part 37: Biometrics. https://www.iso.org/standard/66693.html

Next Terms Alphabetically

False Acceptance Rate (FAR)

False Alarm Rate

False Match

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 acceptance, which occurs when a biometric subject is incorrectly matched to another biometric subject's existing biometric. Example: Frank claims to be John and the system verifies the claim.

Source

Derived from National Science & Technology Council (NSTC), 14 September 2006

Next Terms Alphabetically

False Alarm Rate

False Match

False Match Rate (FMR)

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 a biometric subject 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 biometric subject is identified (the system alarms on John when John is in the database, but the system thinks John is Steve).

Source

Derived from National Science & Technology Council (NSTC), 14 September 2006

Next Terms Alphabetically

False Match

False Match Rate (FMR)

False Non-Match

False Match

The comparison decision of 'match' for a biometric sample (probe) and a biometric reference that are not from the same source.

Source

JTC001-SC37-n-2263 Text of Standing Document 2(SD2) Version 8, Harmonized Biometric Vocabulary, November 2007

Next Terms Alphabetically

False Match Rate (FMR)

False Non-Match

False Non-Match Rate (FNMR)

False Match Rate (FMR)

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

[2] Proportion of the completed biometric non-mated comparison trials that result in a false match.

Source

[1] Derived from National Science & Technology Council (NSTC), 14 September 2006

[2] International Organization for Standardization. (2017). Information technology - Vocabulary - Part 37: Biometrics. https://www.iso.org/standard/66693.html

Next Terms Alphabetically

False Non-Match

False Non-Match Rate (FNMR)

False Rejection

False Non-Match

[1] A comparison decision of 'no-match' for a recognition biometric sample and a biometric reference that are from the same source.

[2] Comparison decision of "non-match" for a biometric probe and a biometric reference that are from the same biometric capture subject and of the same biometric characteristic.

Source

[1] JTC001-SC37-n-2263 Text of Standing Document 2(SD2) Version 8, Harmonized Biometric Vocabulary, November 2007

[2] International Organization for Standardization. (2017). Information technology - Vocabulary - Part 37: Biometrics. https://www.iso.org/standard/66693.html

Next Terms Alphabetically

False Non-Match Rate (FNMR)

False Rejection

False Rejection Rate (FRR)

False Non-Match Rate (FNMR)

[1] 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.

[2] Proportion of the completed biometric mated comparison trials that result in a false non-match.

Source

[1] National Science & Technology Council (NSTC), 14 September 2006

[2] International Organization for Standardization. (2017). Information technology - Vocabulary - Part 37: Biometrics. https://www.iso.org/standard/66693.html

Next Terms Alphabetically

False Rejection

False Rejection Rate (FRR)

Feature Extraction

False Rejection

[1] The failure of a biometric system to identify a biometric subject or to verify the legitimate claimed identity of a biometric subject.

[2] (Biometric False Rejection) Error of rejecting a biometric claim that should have been accepted in accordance with an authoritative statement on the origin of the biometric probe and the biometric reference.

Source

[1] Derived from National Information Assurance Partnership, US Government Biometric Verification Mode Protection Profile for Medium Robustness Environments v1.0, 15 November 2003, Sponsored by the DoD Biometrics Management Office (BMO) and the National Security Agency (NSA)

[2] International Organization for Standardization. (2017). Information technology - Vocabulary - Part 37: Biometrics. https://www.iso.org/standard/66693.html

Next Terms Alphabetically

False Rejection Rate (FRR)

Feature Extraction

Features

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 rejection. A false rejection occurs when a biometric subject is not matched to his/her own existing biometric template. Example: John claims to be John, but the system incorrectly denies the claim.

Source

Derived from National Science & Technology Council (NSTC), 14 September 2006

Next Terms Alphabetically

Feature Extraction

Features

Fingerprint

Feature Extraction

[1] The process of converting observed features of a biometric sample into a data representation so that it can be efficiently stored and later quickly and accurately compared to another sample.

[2] (Biometric Feature Extraction) Process applied to a biometric sample with the intent of isolating and outputting repeatable and distinctive numbers or labels which can be compared to those extracted from other biometric samples.

Source

[1] IBIA

[2] International Organization for Standardization. (2017). Information technology - Vocabulary - Part 37: Biometrics. https://www.iso.org/standard/66693.html

Next Terms Alphabetically

Features

Fingerprint

Fingerprint Recognition

Features

[1] Distinctive characteristic(s) observable or derived from a biometric sample.

[2] (Biometric Feature) Numbers or labels extracted from biometric samples and used for comparison.

Source

[1] National Science & Technology Council (NSTC), 14 September 2006

[2] International Organization for Standardization. (2017). Information technology - Vocabulary - Part 37: Biometrics. https://www.iso.org/standard/66693.html

Next Terms Alphabetically

Fingerprint

Fingerprint Recognition

Fingerprint Scanning

Fingerprint

The image left by the minute ridges and valleys found on the hand of every person. In the fingers and thumbs, these ridges form patterns of loops, whorls and arches.

Source

Federal Bureau of Investigation (FBI) website, Taking Legible Fingerprints

Next Terms Alphabetically

Fingerprint Recognition

Fingerprint Scanning

Fingerprint Segmentation

Fingerprint Recognition

A biometric modality that uses the physical structure of a biometric subject's fingerprint for recognition purposes. Important features used in most fingerprint recognition systems are minutia(e) points that include bifurcations and ridge endings.

Source

Derived from National Science & Technology Council (NSTC), 14 September 2006

Next Terms Alphabetically

Fingerprint Scanning

Fingerprint Segmentation

Flats

Fingerprint Scanning

Acquisition and recognition of a biometric subject's fingerprint characteristics for identification purposes. This process allows the recognition of a biometric subject through quantifiable physiological characteristics that detail the unique identity of an individual.

Source

Derived from The Intel Corporation website, Biometric User Authentication: Fingerprint Sensor Product Guidelines, Version 1.03, September 2003

Next Terms Alphabetically

Fingerprint Segmentation

Flats

Footprint Identification

Fingerprint Segmentation

Segmentation is the automated (and often manually reviewed) separation of an image of N fingers into N images of individual fingers. N is usually four, for the index through little finger, and two for a capture of two thumbs.

Source

https://csrc.nist.gov/glossary/term/fingerprint_segmentation

Next Terms Alphabetically

Flats

Footprint Identification

Force Protection (FP)

Flats

A method of fingerprint capture. Identification flat impressions are taken simultaneously without rolling. These are referred to as plain, slap, or flat impressions. The individual's right and left four fingers should be captured first, followed by the two thumbs (4-4-2 method). Instituting this finger capture method ensures the highest level of fingerprint sequence accuracy.

Source

https://le.fbi.gov/science-and-lab/biometrics-and-fingerprints/biometrics/recording-legible-fingerprints

Next Terms Alphabetically

Footprint Identification

Force Protection (FP)

Foreign Humanitarian Assistance (FHA)

Footprint Identification

Feet and toes have friction ridges, like fingers and palms, that can be used for identification purposes. Footprint identification analyzes images or impressions of friction ridges from bare feet, for the purpose of attributing them to an individual.

Source

IBIA

Next Terms Alphabetically

Force Protection (FP)

Foreign Humanitarian Assistance (FHA)

Forensic

Index

Force Protection (FP)

Preventive measures taken to mitigate hostile actions against Department of Defense personnel (to include family members), resources, facilities, and critical information by using biometrics to positively link identity information to a given physical individual. Force protection does not include actions to defeat the enemy or protect against accidents, weather, or disease. Also called FP.

Source

Derived from Joint Publication 30, Joint Operations,17 September 2006

Next Terms Alphabetically

Foreign Humanitarian Assistance (FHA)

Forensic

Fraudulent Biometric Enrollment...

Foreign Humanitarian Assistance (FHA)

Programs conducted to relieve or reduce the results of natural or manmade disasters or other endemic conditions such as human pain, disease, hunger, or privation that might present a serious threat to life or that can result in great damage to or loss of property. Foreign humanitarian assistance (FHA) provided by US forces is limited in scope and duration. The foreign assistance provided is designed to supplement or complement the efforts of the host nation civil authorities or agencies that may have the primary responsibility for providing FHA. FHA operations are those conducted outside the United States, its territories, and possessions. Also called FHA. Biometrics can be used as an enabler for personal identification for humanitarian assistance distribution.

Source

Derived from Joint Publication 30, Joint Operations,17 September 2006

Next Terms Alphabetically

Forensic

Fraudulent Biometric Enrollment...

Friction Ridge

Forensic

Relates to the use of science or technology in the investigation and establishment of facts or evidence. Collected biometric samples could then be linked to nonbiometric forensic evidence.

Source

Derived from Capstone Concept of Operations for DoD Biometrics in Support of Identity Superiority, November 2006

Next Terms Alphabetically

Fraudulent Biometric Enrollment...

Friction Ridge

Full Enrollment

Fraudulent Biometric Enrollment Data Record

Biometric enrollment data record created or modified for the purpose of supporting wrongful or criminal activity.
Note 1 to entry: Records that are inadvertently erroneous or created for test purposes are not considered fraudulent.

Source

International Organization for Standardization. (2017). Information technology - Vocabulary - Part 37: Biometrics. https://www.iso.org/standard/66693.html

Next Terms Alphabetically

Friction Ridge

Full Enrollment

Gait

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.

Source

National Science & Technology Council (NSTC), 14 September 2006

Next Terms Alphabetically

Full Enrollment

Gait

Gallery

Full Enrollment

Enrollment of biometric data on a subject that includes 14 fingerprint images (4 slaps, 10 rolls), 5 face photos, 2 irises, and required text fields. The sample must be EBTS compliant. Typically used for detainees, locally hire screenings, and other applications.

Source

Initial Capabilities Document (ICD) for Biometrics in Support of Personnel Identity (BSPI) (Draft), 30 Jun 2007

Next Terms Alphabetically

Gait

Gallery

Hamming Distance (HD)

Gait

A biometric subject's manner of walking. Gait as a biometric can be useful because it can be observed at a distance and is thought to be unique to each individual who walks. This is because anatomical, sociocultural, and genetic factors, as well as simply one's habits and personality, shape the silhouette of movement by which any individual travels. Gait metrics have also emerged as an indicator of health, as in the Apple Health app for iPhones.

Source

Derived from National Science & Technology Council (NSTC), 14 September 2006. https://blog.ansi.org/2018/05/gait-analysis-walk-biometric-identification/#gref. https://www.nature.com/articles/s41598-023-32550-3

Next Terms Alphabetically

Gallery

Hamming Distance (HD)

Hand Geometry Recognition

Gallery

The biometric system's database, or set of known biometric subjects, for a specific implementation or evaluation experiment.

Source

Derived from National Science & Technology Council (NSTC), 14 September 2006

Next Terms Alphabetically

Hamming Distance (HD)

Hand Geometry Recognition

Hand Scan

Hamming Distance (HD)

The number of noncorresponding digits in a string of binary digits; used to measure dissimilarity. Hamming distances are used in many Daugman iris recognition algorithms.

Source

National Science & Technology Council (NSTC), 14 September 2006

Next Terms Alphabetically

Hand Geometry Recognition

Hand Scan

Homeland Advanced Recognition...

Hand Geometry Recognition

A biometric modality that measures the physical structure (geometry) of a biometric subject's hand for recognition purposes.

Source

Derived from National Science & Technology Council (NSTC), 14 September 2006

Next Terms Alphabetically

Hand Scan

Homeland Advanced Recognition...

Hypothenar

Hand Scan

Print from the outer side of the palm.

Source

Initial Capabilities Document (ICD) for Biometrics in Support of Personnel Identity (BSPI) (Draft), 30 Jun 2007

Next Terms Alphabetically

Homeland Advanced Recognition...

Hypothenar

IDENT

Homeland Advanced Recognition Technology (HART)

The Homeland Advanced Recognition Technology System (HART) replaces the legacy Automated Biometric Identification System (IDENT) as the primary Department of Homeland Security (DHS) system for storage and processing of biometric and associated biographic information for national security; law enforcement; immigration and border management; intelligence; background investigations for national security positions and certain positions of public trust; and associated testing, training, management reporting, planning and analysis, development of new technologies, and other administrative uses. The Office of Biometric Identity Management (OBIM) will implement HART in phases. As of this writing, HART has not achieved Interim Operational Capability (IOC), a milestone necessary before consideration of IDENT retirement.

Source

https://www.dhs.gov/publication/dhsobimpia-004-homeland-advanced-recognition-technology-system-hart-increment-1

Next Terms Alphabetically

Hypothenar

IDENT

IDENT Exchange Messaging (IXM)

Hypothenar

The friction ridge detail on the palm, below the triradiate inter-digital area on the ulnar side [little finger side] of the palm between the little finger and wrist.

Source

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/267523/FingerprintTerminology.pdf

Next Terms Alphabetically

IDENT

IDENT Exchange Messaging (IXM)

Identification

IDENT

IDENT is the name for the multi-modal Automated Biometric Identification System that is the central DHS-wide system for storage and processing of biometric and associated biographic information for national security; law enforcement; immigration and border management; intelligence; background investigations for national security positions and certain positions of public trust; and associated testing, training, management reporting, planning and analysis, or other administrative uses. To be succeeded by HART.

Source

https://www.dhs.gov/publication/dhsnppdpia-002-automated-biometric-identification-system

Next Terms Alphabetically

IDENT Exchange Messaging (IXM)

Identification

Identification Rate

IDENT Exchange Messaging (IXM)

IXM (IDENT Exchange Messaging) is the exchange that provides common interfaces to OBIM stakeholders. OBIM is the Office of Biometric Identity Management under the U.S. Department of Homeland Security. IXM leverages existing industry data models, including NIEM 2.1, and ANSI/NIST-ITL 1-2011. IXM also promotes interoperability between OBIM IDENT and the FBI
Next Generation Identification (NGI) system (Integrated Automated Fingerprint Identification System (IAFIS) previously known legacy system). The earliest versions of IXM (version 1.0 through version 5.5) used a data model, vocabulary, and an XML schema based on the Global Justice XML Data Model (GJXDM). The GJXDM reference model was deprecated as a DHS standard in 2007 and was replaced by the NIEM.

Source

NIEM Biometrics Domain Enterprise Level Data Standards Execution Plan, February 2021.

Next Terms Alphabetically

Identification

Identification Rate

Identifier

Identification

[1] The one-to-many (1:N) 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 known identity of the biometric subject whose template was matched.

[2] Process of searching against a biometric enrollment database to find and return the biometric reference identifier(s) attributable to a single individual.
Note 1 to entry: Use of the term "authentication" as a substitute for biometric identification is deprecated.

Source

[1] Capstone Concept of Operations for DoD Biometrics in Support of Identity Superiority, November 2006

[2] International Organization for Standardization. (2017). Information technology - Vocabulary - Part 37: Biometrics. https://www.iso.org/standard/66693.html

Next Terms Alphabetically

Identification Rate

Identifier

Identify

Identification Rate

The rate at which a biometric subject in a database is correctly identified.

Source

Derived from National Science & Technology Council (NSTC), 14 September 2006

Next Terms Alphabetically

Identifier

Identify

Identity

Identifier

A unique data string used as a key in the biometric system to name a biometric subject's identity and its associated attributes. An example of an identifier would be a passport number.

Source

Derived from National Information Assurance Partnership, US Government Biometric Verification Mode Protection Profile for Medium Robustness Environments v1.0, 15 November 2003, Sponsored by the DoD Biometrics Management Office (BMO) and the National Security Agency (NSA)

Next Terms Alphabetically

Identify

Identity

Identity Assurance

Identify

Biometric search against a biometric enrollment database to find and return the biometric reference identifier(s) attributable to a single individual.

Source

International Organization for Standardization. (2017). Information technology - Vocabulary - Part 37: Biometrics. https://www.iso.org/standard/66693.html

Next Terms Alphabetically

Identity

Identity Assurance

Identity Claim

Identify

The set of attribute values (i.e., characteristics) by which a biometric subject is recognizable and that, within the scope of an identity manager's responsibility, is sufficient to distinguish that biometric subject from any other biometric subject and to distinguish the identity from any other identity.

Source

Derived from Capstone Concept of Operations for DoD Biometrics in Support of Identity Superiority, November 2006

Next Terms Alphabetically

Identity Assurance

Identity Claim

Identity Dominance

Identity Assurance

Operations that protect and defend identity information and management by ensuring their availability, integrity, authentication, confidentiality, intended use (privacy), and nonrepudiation.

Source

DoD Biometrics Strategy Working Group

Next Terms Alphabetically

Identity Claim

Identity Dominance

Identity Governance

Identity Claim

A statement that a biometric subject 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).

Source

Derived from NSTC Subcommittee on Biometrics IAW INCITS/M1 and ISO/IEC JIYC 2 SC37standards bodies, Aug 2006.

Next Terms Alphabetically

Identity Dominance

Identity Governance

Identity Management

Identity Dominance

The operational capability to achieve an advantage over an adversary by denying him the ability to mask his identity or counter our biometric technologies and processes. This is accomplished through the use of enabling technologies and processes to establish the identity of a biometric subject and to establish a knowledge base for that identity.

Source

Derived from Capstone Concept of Operations for DoD Biometrics in Support of Identity Superiority, November 2006

Next Terms Alphabetically

Identity Governance

Identity Management

Identity Protection

Identity Governance

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

Source

National Science & Technology Council (NSTC), 14 September 2006

Next Terms Alphabetically

Identity Management

Identity Protection

Identity Superiority

Identity Management

A business function that authenticates an individual to validate identity, DoD affiliation, and authorization of the credential holder. The centralized data repository delivers credentialing information and status for business functions within DoD for use as proof of identity and DoD affiliation is delivered by Identity Management.

Source

Capstone Concept of Operations for DoD Biometrics in Support of Identity Superiority, November 2006

Next Terms Alphabetically

Identity Protection

Identity Superiority

Imposter

Identity Protection

The process of safeguarding and ensuring the identities of individuals, devices, applications, and services are not compromised.

Source

Capstone Concept of Operations for DoD Biometrics in Support of Identity Superiority, November 2006

Next Terms Alphabetically

Identity Superiority

Imposter

Indifferent Biometric Capture Subject

Identity Superiority

The management, protection and dominance of identity information for friendly, neutral or unknown, and adversary subject through the application of military operations and business functions.

Source

Capstone Concept of Operations for DoD Biometrics in Support of Identity Superiority, November 2006

Next Terms Alphabetically

Imposter

Indifferent Biometric Capture Subject

Indifferent Presentation

Imposter

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.

Source

IBIA

Next Terms Alphabetically

Indifferent Biometric Capture Subject

Indifferent Presentation

Infrared

Indifferent Biometric Capture Subject

Biometric capture subject who is unconcerned with the achievement of a successful biometric acquisition process.

Source

International Organization for Standardization. (2017). Information technology - Vocabulary - Part 37: Biometrics. https://www.iso.org/standard/66693.html

Next Terms Alphabetically

Indifferent Presentation

Infrared

Integrated Automated Fingerprint...

Index

Indifferent Presentation

Presentation in which the biometric capture subject is unconcerned that the biometric capture process is occurring.

Source

International Organization for Standardization. (2017). Information technology - Vocabulary - Part 37: Biometrics. https://www.iso.org/standard/66693.html

Next Terms Alphabetically

Infrared

Integrated Automated Fingerprint...

Integrated Biometric System (IBS)

Index

Infrared

Light that lies outside the human visible spectrum at its red (low frequency) end. In the context of biometrics, infrared illumination is used to image irises for iris recognition, though it can also be used to image faces.

Source

IBIA

Next Terms Alphabetically

Integrated Automated Fingerprint...

Integrated Biometric System (IBS)

Intermediate Biometric Sample

Integrated Automated Fingerprint Identification System (IAFIS)

The FBI's prior largescale ten fingerprint (open set) identification system that was used for criminal history background checks and identification of latent prints discovered at crime scenes. This system provided automated and latent search capabilities, electronic image storage, and electronic exchange of fingerprints and responses. IAFIS was replaced by the FBI's Next Generation Identification system (NGI) after it achieved Full Operational Capability (FOC) on September 15, 2014.

Source

National Science & Technology Council (NSTC), 14 September 2006

Next Terms Alphabetically

Integrated Biometric System (IBS)

Intermediate Biometric Sample

Intermediate Biometric Sample...

Integrated Biometric System (IBS)

The Integrated Biometric System (IBS) supports the U.S. Department of State (DoS) Bureau of Consular Affairs mission requirements for issuing visas to foreign nationals and passports to U.S. citizens. The IBS is an enterprise-level, facial-recognition matching service. Face recognition technology is used to facilitate anti-fraud goals of the U.S. DoS's existing travel document issuance processes. IBS provides DoS the ability to add, delete, and search millions of photographic images for the same person prior to the issuance of travel documents.

Source

https://www.state.gov/wp-content/uploads/2022/02/Integrated-Biometric-System-IBS-PIA.pdf

Next Terms Alphabetically

Intermediate Biometric Sample

Intermediate Biometric Sample...

Intermediate Biometric Sample...

Intermediate Biometric Sample

Biometric sample resulting from intermediate biometric sample processing. EXAMPLE Biometric samples that have been cropped, down-sampled, compressed, or enhanced are examples of intermediate biometric samples.

Source

International Organization for Standardization. (2017). Information technology - Vocabulary - Part 37: Biometrics. https://www.iso.org/standard/66693.html

Next Terms Alphabetically

Intermediate Biometric Sample...

Intermediate Biometric Sample...

International Organization for...

Intermediate Biometric Sample Processing

Any manipulation of a biometric sample that does not produce biometric features. EXAMPLE Examples of intermediate biometric sample processing include cropping, down-sampling, compression, conversion to data interchange formats standard and image enhancement.

Source

International Organization for Standardization. (2017). Information technology - Vocabulary - Part 37: Biometrics. https://www.iso.org/standard/66693.html

Next Terms Alphabetically

Intermediate Biometric Sample...

International Organization for...

Interoperability

Intermediate Biometric Sample Processing

Biometric sample resulting from intermediate biometric sample processing.

Source

International Organization for Standardization. (2017). Information technology - Vocabulary - Part 37: Biometrics. https://www.iso.org/standard/66693.html

Next Terms Alphabetically

International Organization for...

Interoperability

Iris Code©

International Organization for Standardization (ISO)

ISO (International Organization for Standardization) is an independent, non-governmental international organization with a membership of 168 national standards bodies. Through its members, it brings together experts to share knowledge and develop voluntary, consensus-based, market relevant International Standards that support innovation and provide solutions to global challenges.

Source

https://www.iso.org/about-us.html

Next Terms Alphabetically

Interoperability

Iris Code©

Iris Recognition

Interoperability

The conditions achieved among communications electronic (CE) equipment systems or items of CE equipment when information or services can be exchanged directly and satisfactorily between them and their users.

Source

Joint Publication 60, Joint Communication Systems, 20 March 2006

Next Terms Alphabetically

Iris Code©

Iris Recognition

Keystroke Dynamics

Iris Code©

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

Source

National Science & Technology Council (NSTC), 14 September 2006

Next Terms Alphabetically

Iris Recognition

Keystroke Dynamics

Know Your Customer (KYC)

Iris Recognition

A biometric modality that uses an image of the physical structure of a biometric subject's iris for recognition purposes. The iris muscle is the colored portion of the eye surrounding the pupil.

Source

Derived from National Science & Technology Council (NSTC), 14 September 2006

Next Terms Alphabetically

Keystroke Dynamics

Know Your Customer (KYC)

Latent Fingerprint

Index

Keystroke Dynamics

A biometric modality that uses the cadence of a biometric subject's typing pattern for recognition.

Source

Derived from National Science & Technology Council (NSTC), 14 September 2006

Next Terms Alphabetically

Know Your Customer (KYC)

Latent Fingerprint

Latent Sample

Know Your Customer (KYC)

KYC references a set of guidelines that financial institutions and businesses follow to verify the identity, suitability, and risks of a current or potential customer. The goal is to identify suspicious behavior such as money laundering and financial terrorism before it ever materializes.

Source

https://www.dowjones.com/professional/risk/glossary/know-your-customer/

Next Terms Alphabetically

Latent Fingerprint

Latent Sample

Live Capture

Latent Fingerprint

A fingerprint "image" left on a surface that was touched by a biometric subject. 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.

Source

Derived from National Science & Technology Council (NSTC), 14 September 2006

Next Terms Alphabetically

Latent Sample

Live Capture

Live Scan

Latent Sample

A biometric residue that is dormant, inactive, or non-evident but can be captured, measured and stored. It may be difficult to see but can be made visible to scrutiny. A residue left on a medium that came in contact with a biometric subject.

Source

Derived from Capstone Concept of Operations for DoD Biometrics in Support of Identity Superiority, November 2006

Next Terms Alphabetically

Live Capture

Live Scan

Liveness

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).

Source

National Science & Technology Council (NSTC), 14 September 2006

Next Terms Alphabetically

Live Scan

Liveness

Liveness Detection

Live Scan

Occurs when taking a fingerprint or palm print directly from a biometric subject's hand.

Source

Derived from ANSI/NISTITL 12000, Data Format for the Interchange of Fingerprint, Facial, & Scar mark & Tattoo Information

Next Terms Alphabetically

Liveness

Liveness Detection

Logical Access

Liveness

The quality or state of being live or alive. Can refer to the real-time nature of a broadcast, the reverberant quality of a room, or (more germane in this context) the observable characteristics and behaviors of a living (not dead or artificial) being (like a human).

Source

https://www.merriam-webster.com/dictionary/liveness and IBIA

Next Terms Alphabetically

Liveness Detection

Logical Access

Loop

Liveness Detection

A technique used to ensure that the biometric sample submitted is from a real (living) biometric subject (person). A liveness detection method can help protect the system against some types of spoofing attacks.

Source

Derived from National Science & Technology Council (NSTC), 14 September 2006

Next Terms Alphabetically

Logical Access

Loop

Machine Learning (ML)

Logical Access

Process of granting access to information system resources to authorized users, programs, processes, or other systems. The controls and protection mechanisms that limit users' access to information and restrict their forms of access to only what is appropriate.

Source

Capstone Concept of Operations for DoD Biometrics in Support of Identity Superiority, November 2006

Next Terms Alphabetically

Loop

Machine Learning (ML)

Match

Loop

A fingerprint pattern in which the friction ridges enter from either side, curve sharply and pass out near the same side they entered. This pattern will contain one core and one delta.

Source

National Science & Technology Council (NSTC), 14 September 2006

Next Terms Alphabetically

Machine Learning (ML)

Match

Match

Machine Learning (ML)

The use and development of computer systems that are able to learn and adapt without following explicit instructions, by using algorithms, [classifiers] and statistical models to analyze and draw inferences from patterns in [training] data. [The recent dramatic reductions in biometric algorithm error rates are in large part due to the adoption of ML techniques for biometrics.]

Source

Oxford Dictionary

[IBIA]

Next Terms Alphabetically

Match

Match

Match-on-Card

Match

[DEPRECATED]
The process of accurately identifying or verifying the identity of a biometric subject by comparing a standardized biometric file to an existing source of standardized biometric data and scoring the level of confidence of the match. Matching consists of either a one-to-one (verification) or one-to-many (identification) search.

Source

[International Organization for Standardization. (2017). Information technology - Vocabulary - Part 37: Biometrics. https://www.iso.org/standard/66693.html]

Derived from Capstone Concept of Operations for DoD Biometrics in Support of Identity Superiority, November 2006

Next Terms Alphabetically

Match

Match-on-Card

Mated (adjective)

Match

(Noun) Comparison decision stating that the biometric probe(s) and the biometric reference are from the same source.
Note 1 to entry: Historically, the word match has been used as a verb to indicate the act of comparison and decision making. As 'match' is the decision coming out of the comparison process, its use as a verb is deprecated in favor of compare.

Source

International Organization for Standardization. (2017). Information technology - Vocabulary - Part 37: Biometrics. https://www.iso.org/standard/66693.html

Next Terms Alphabetically

Match-on-Card

Mated (adjective)

Medial

Match-on-Card

The ability of a Smart Card to perform a biometric match, usually a 1:1 match, to a reference biometric stored within the Smart Card. Match-on-card can be performed either by presenting the Smart Card with a probe biometric or having a biometric sensor contained within the Smart Card form factor.

Source

IBIA

Next Terms Alphabetically

Mated (adjective)

Medial

Mimic

Mated (adjective)

Of or having to do with a paired biometric probe and biometric reference that are from the same biometric characteristic of the same biometric data subject.

Source

International Organization for Standardization. (2017). Information technology - Vocabulary - Part 37: Biometrics. https://www.iso.org/standard/66693.html

Next Terms Alphabetically

Medial

Mimic

Minutia(e) Point

Index

Medial

[In human anatomy} the centre or middle, for example the medial section of [a] phalange [finger or toe bone]. [Relevant to palm print biometrics.]

Source

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/267523/FingerprintTerminology.pdf , [IBIA]

Next Terms Alphabetically

Mimic

Minutia(e) Point

Mobile Digital Identity

Mimic

The presentation of a live biometric measure in an attempt to fraudulently impersonate someone other than the submitter.

Source

National Science & Technology Council (NSTC), 14 September 2006

Next Terms Alphabetically

Minutia(e) Point

Mobile Digital Identity

Mobile Driver's License (mDL)

Minutia(e) Point

The point where a friction ridge begins, terminates, or splits into two or more ridges. Minutia(e) are friction ridge characteristics that are used to individualize a fingerprint image.

Source

ANSI/NISTITL 12000, Data Format for the Interchange of Fingerprint, Facial, & Scar mark & Tattoo Information

Next Terms Alphabetically

Mobile Digital Identity

Mobile Driver's License (mDL)

Modality

Mobile Digital Identity

A Digital identity held within a mobile device and presented to Relying Parties from a mobile device under the control of the mobile device user.

Source

IBIA

Next Terms Alphabetically

Mobile Driver's License (mDL)

Modality

Mode

Mobile Driver's License (mDL)

Also known as a digital driver's license (DDL), it is a driver's license that is provisioned to (digitized for storage on) a mobile device with the capability to be updated in real time. It is comprised of the same data elements that are used to produce a physical driver's license, however, the data is transmitted electronically to a relying party's reader device and authenticated. At present, an mDL is not a replacement for a physical driver's license but is intended as a supplement. The mDL is an improvement over physical credentials which can be lost or stolen, become broken or damaged, contain outdated information, offer too much information (including personally identifiable information), and can more easily be replicated by counterfeiters. The mDL offers safe, secure, and trustable technologies that allow for touchless transactions, selective information release, and data protection.

Source

https://www.aamva.org/topics/mobile-driver-license#?wst=4a3b89462cc2cff2cbe0c7accde57421 and IBIA

Next Terms Alphabetically

Modality

Mode

Model

Modality

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

Source

National Science & Technology Council (NSTC), 14 September 2006

Next Terms Alphabetically

Mode

Model

Multi-Modal

Mode

DEPRECATED: biometric: (noun)
Combination of a biometric characteristic type, a sensor type and a processing method.

Source

International Organization for Standardization. (2017). Information technology - Vocabulary - Part 37: Biometrics. https://www.iso.org/standard/66693.html

Next Terms Alphabetically

Model

Multi-Modal

Multimodal Biometric System

Model

[1] A representation used to characterize a biometric subject. Behavioral-based biometric systems, because of the inherently dynamic characteristics, use models rather than static templates.

[2] (Biometric Model) Stored function generated from biometric data.

Source

[1] Derived from National Science & Technology Council (NSTC), 14 September 2006

[2] International Organization for Standardization. (2017). Information technology - Vocabulary - Part 37: Biometrics. https://www.iso.org/standard/66693.html

Next Terms Alphabetically

Multi-Modal

Multimodal Biometric System

National Information Exchange...

Multi-Modal

Multiple in at least 2 out of 3 constituents of a mode in a single biometric system.
Note 1 to entry: Multiple implies difference in type.

Source

International Organization for Standardization. (2017). Information technology - Vocabulary - Part 37: Biometrics. https://www.iso.org/standard/66693.html

Next Terms Alphabetically

Multimodal Biometric System

National Information Exchange...

National Institute of Standards...

Multimodal Biometric System

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

[2] (Multi-Modal) Multiple in at least 2 out of 3 constituents of a mode in a single biometric system.
Note 1 to entry: Multiple implies difference in type.

Source

[1] Capstone Concept of Operations for DoD Biometrics in Support of Identity Superiority, November 2006

[2] International Organization for Standardization. (2017). Information technology - Vocabulary - Part 37: Biometrics. https://www.iso.org/standard/66693.html

Next Terms Alphabetically

National Information Exchange...

National Institute of Standards...

NATO STANAG 4715

National Information Exchange Model (NIEM)

NIEM is a dictionary of agreed-upon terms, definitions, relationships, and formats that are independent of how information is stored in individual systems. The NIEM model includes community-specific elements, as well as core elements that are commonly agreed to by the communities who use NIEM. For example, common elements in the NIEM core include "person," "location," "item," "organization," and "activity."

The NIEM Biometrics domain is part of a coordinated global effort to maintain and refine operations focused on security, intelligence, law enforcement, international trade, travel and immigration by means of identity management and assurance.

Source

https://www.niem.gov/about-niem

and

https://www.niem.gov/communities/biometrics

Next Terms Alphabetically

National Institute of Standards...

NATO STANAG 4715

Negative Biometric Claim

National Institute of Standards and Technology (NIST)

A nonregulatory 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 wellbeing of the nation and helps improve, among many other things, the nation's homeland security. NIST conducts highly respected independent testing of biometric algorithms and publishes the results. Organizations, particularly government organizations, consider NIST test results when selecting a biometric algorithm.

Source

National Institute of Standards and Technology, IBIA

Next Terms Alphabetically

NATO STANAG 4715

Negative Biometric Claim

Neural Network

NATO STANAG 4715

The NATO Nations have endorsed the concept of biometrics data in support to operations. To accelerate the development of interoperability in this domain, under the Defence Against Terrorism Programme of Work, NABIS (NATO Automated Biometric Identification System) implemented STANAG 4715 which is a mechanism for achieving a high degree of interoperability [between NATO nations] in the biometrics domain.

Source

https://journal.mta.ro/articole/40/NATO%20Automated%20Biometric%20Identification%20System%20(NABIS).pdf

Next Terms Alphabetically

Negative Biometric Claim

Neural Network

Next Generation Identification...

Negative Biometric Claim

Assertion that a biometric capture subject is not the source of specified or unspecified biometric reference(s) in a biometric reference database.
Note 1 to entry: Specified means there is a non-biometric input, such as a PIN, name or ID number, pointing to particular biometric reference(s). Unspecified means there is no such non-biometric input provided.

Source

International Organization for Standardization. (2017). Information technology - Vocabulary - Part 37: Biometrics. https://www.iso.org/standard/66693.html

Next Terms Alphabetically

Neural Network

Next Generation Identification...

NIST Fingerprint Image Quality (NFIQ)

Neural Network

A computer system modeled on the human brain and nervous system.
[Often used for machine learning (ML).]

Source

Oxford Dictionary

[IBIA]

Next Terms Alphabetically

Next Generation Identification...

NIST Fingerprint Image Quality (NFIQ)

Non-Conformant Capture Attempt

Next Generation Identification system (NGI)

The FBI NGI system is a multi-modal biometric identification system used to facilitate criminal investigations and civil investigations like background checks. Succeeding the IAFIS system, the NGI system improved the efficiency and accuracy of biometric services to address evolving local, state, tribal, federal, territorial, and international criminal justice requirements. Capabilities include a national Rap Back service; the Interstate Photo System and face recognition search; fingerprint verification services; latent, palm and 10-print identification service; deceased person services; iris services; and scars, marks and tattoo services.

Source

https://le.fbi.gov/science-and-lab/biometrics-and-fingerprints/biometrics/next-generation-identification-ngi

Next Terms Alphabetically

NIST Fingerprint Image Quality (NFIQ)

Non-Conformant Capture Attempt

Non-match

NIST Fingerprint Image Quality (NFIQ)

NIST Fingerprint Image Quality (NFIQ) 2 is open source software that links image quality of optical and ink 500 PPI fingerprints to operational recognition performance. This allows quality values to be tightly defined and then numerically calibrated, which in turn allows for the standardization needed to support a worldwide deployment of fingerprint sensors with universally interpretable image qualities. NFIQ 2 quality features are formally standardized as part of ISO/IEC 29794-4 and serve as the reference implementation of the standard.

Source

https://www.nist.gov/services-resources/software/nfiq-2

Next Terms Alphabetically

Non-Conformant Capture Attempt

Non-match

Non-Mated (Adjective)

Non-Conformant Capture Attempt

Interactions of the biometric capture subject and the biometric capture subsystem that does not comply with the capture task.

Source

International Organization for Standardization. (2017). Information technology - Vocabulary - Part 37: Biometrics. https://www.iso.org/standard/66693.html

Next Terms Alphabetically

Non-match

Non-Mated (Adjective)

Non-Subversive Biometric Capture...

Index

Non-match

[1] A decision that the recognition biometric sample(s) and the biometric reference are not from the same source.

[2] Non-match: (Noun) Comparison decision stating that the biometric probe(s) and the biometric reference are not from the same source.

Source

[1] JTC001-SC37-n-2263 Text of Standing Document 2(SD2) Version 8, Harmonized Biometric Vocabulary, November 2007

[2] International Organization for Standardization. (2017). Information technology - Vocabulary - Part 37: Biometrics. https://www.iso.org/standard/66693.html

Next Terms Alphabetically

Non-Mated (Adjective)

Non-Subversive Biometric Capture...

Non-Subversive User

Index

Non-Mated (Adjective)

Of or having to do with a paired biometric probe and biometric reference that are not from the same biometric characteristic of the same biometric data subject.
Note 1 to entry: While 'non-match' is the result of a biometric comparison decision, 'non-mated' is a statement, based on non-biometric information, concerning the origin of the source of the biometric probe and the biometric reference.

Source

International Organization for Standardization. (2017). Information technology - Vocabulary - Part 37: Biometrics. https://www.iso.org/standard/66693.html

Next Terms Alphabetically

Non-Subversive Biometric Capture...

Non-Subversive User

One-to-Many

Non-Subversive Biometric Capture Subject

Biometric capture subject who does not attempt to subvert the correct and intended system policy of the biometric capture subsystem.

Source

International Organization for Standardization. (2017). Information technology - Vocabulary - Part 37: Biometrics. https://www.iso.org/standard/66693.html

Next Terms Alphabetically

Non-Subversive User

One-to-Many

One-to-Many Comparison

Non-Subversive User

User of a biometric system who does not attempt to subvert the correct and intended system policy.

Source

International Organization for Standardization. (2017). Information technology - Vocabulary - Part 37: Biometrics. https://www.iso.org/standard/66693.html

Next Terms Alphabetically

One-to-Many

One-to-Many Comparison

One-to-Many Search

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.

Source

Capstone Concept of Operations for DoD Biometrics in Support of Identity Superiority, November 2006

Next Terms Alphabetically

One-to-Many Comparison

One-to-Many Search

One-to-One

One-to-Many Comparison

DEPRECATED: one-to-few
Process in which biometric probe(s) of one biometric data subject is compared against the biometric references of more than one biometric data subject to return a set of comparison scores.
Note 1 to entry: The term "compared" refers to comparison in the biometric sense.

Source

International Organization for Standardization. (2017). Information technology - Vocabulary - Part 37: Biometrics. https://www.iso.org/standard/66693.html

Next Terms Alphabetically

One-to-Many Search

One-to-One

One-to-One Comparison

One-to-Many Search

Process in which biometric probe(s) of one biometric data subject is searched against the biometric references of more than one biometric data subject to return a biometric candidate list or a comparison decision.
Note 1 to entry: The term "searched", in the above definition, refers to biometric search.

Source

International Organization for Standardization. (2017). Information technology - Vocabulary - Part 37: Biometrics. https://www.iso.org/standard/66693.html

Next Terms Alphabetically

One-to-One

One-to-One Comparison

Open-set Identification

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). The identification task can be accomplished by a series of one-to-one comparisons.

Source

Capstone Concept of Operations for DoD Biometrics in Support of Identity Superiority, November 2006

Next Terms Alphabetically

One-to-One Comparison

Open-set Identification

Operational Evaluation

One-to-One Comparison

Process in which biometric probe(s) from one biometric data subject is compared to biometric reference(s) from one biometric data subject to produce a comparison score.

Source

International Organization for Standardization. (2017). Information technology - Vocabulary - Part 37: Biometrics. https://www.iso.org/standard/66693.html

Next Terms Alphabetically

Open-set Identification

Operational Evaluation

Own Race Bias (ORB)

Open-set Identification

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

Source

Derived from National Science & Technology Council (NSTC), 14 September 2006

Next Terms Alphabetically

Operational Evaluation

Own Race Bias (ORB)

Palm Print Recognition

Index

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.

Source

National Science & Technology Council (NSTC), 14 September 2006

Next Terms Alphabetically

Own Race Bias (ORB)

Palm Print Recognition

Performance

Own Race Bias (ORB)

The own-race bias (ORB) phenomenon in peoples' memory for human faces is the finding that faces from people of their own race are better remembered when compared with their memories for faces of other less familiar races. The phenomenon has been known and researched for over 30 years.

Source

Meissner, C. A., & Brigham, J. C. (2001). Thirty years of investigating the own-race bias in memory for faces: A meta-analytic review. Psychology, Public Policy, and Law, 7(1), 3–35. https://doi.org/10.1037/1076-8971.7.1.3

Next Terms Alphabetically

Palm Print Recognition

Performance

Periocular Recognition

Palm Print Recognition

A biometric modality that uses the physical structure of a biometric subject's palm print for recognition purposes. [Includes friction ridges and crease lines that exist on palms.]

Source

Derived from National Science & Technology Council (NSTC), 14 September 2006.

[IBIA]

Next Terms Alphabetically

Performance

Periocular Recognition

Person of Interest

Performance

A catch-all phrase for describing a measurement of the characteristics, such as accuracy or speed, of a biometric algorithm or system.

Source

National Science & Technology Council (NSTC), 14 September 2006

Next Terms Alphabetically

Periocular Recognition

Person of Interest

Personal Identification Number (PIN)

Periocular Recognition

A biometric modality that uses the eyes and the region surrounding the eyes (periocular region) for recognition purposes. The approach gained momentum during the SARS-CoV-2 pandemic due to the widespread use of face masks and the initially poor performance of face recognition algorithms against masked faces.

Source

IBIA

Next Terms Alphabetically

Person of Interest

Personal Identification Number (PIN)

Personal Identity Verification (PIV)...

Person of Interest

An individual for whom information needs or discovery objectives exist.

Source

The DoD Biometrically Enabled Watchlist (BEWL) A Federated Approach, May 3, 2007

Next Terms Alphabetically

Personal Identification Number (PIN)

Personal Identity Verification (PIV)...

Pixel

Personal Identification Number (PIN)

A number used in conjunction with an access control system as a secondary credential by the user to ensure the holder of the access control card is the authorized user. [May be one of the factors used in multi-factor authentication (in addition to smart cards and biometrics, for example).]

Source

Naval Facilities Engineering Service Center, Antiterrorism Team website, Glossary of Terms [IBIA]

Next Terms Alphabetically

Personal Identity Verification (PIV)...

Pixel

Pixels Per Inch (PPI)

Personal Identity Verification (PIV) Credential

A PIV credential is a U.S. federal government-wide credential (smart card) used to access federally controlled facilities and information systems at the appropriate security level. PIV credentials have certificates and key pairs, pin numbers, biometrics like fingerprints and pictures, and other unique identifiers. When these items are put together in a PIV credential, the credential provides the capability to implement multifactor authentication for networks, applications, and buildings.

Source

https://playbooks.idmanagement.gov/piv/

Next Terms Alphabetically

Pixel

Pixels Per Inch (PPI)

Pixels Per Inch (PPI)

Pixel

Short for picture element. This is the smallest addressable element of a digital imaging device or display array that can be assigned a display value (e.g. color and brightness). Denser, higher numbers of pixels in the array generally yield higher resolutions of images.

Source

IBIA

Next Terms Alphabetically

Pixels Per Inch (PPI)

Pixels Per Inch (PPI)

Plantar

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. This is often of interest for face recognition, wherein some algorithms work best with a certain minimum number of pixels between the eyes of a captured face image (e.g. 150).

Source

IBIA

Next Terms Alphabetically

Pixels Per Inch (PPI)

Plantar

Plantar Mark

Pixels Per Inch (PPI)

The number of picture elements per inch that a fingerprint scanner can resolve and capture. For example, 500 PPI or 1000 PPI. Higher numbers of PPI indicates an ability to resolve finer details.

Source

IBIA

Next Terms Alphabetically

Plantar

Plantar Mark

Plantar Prints

Plantar

Related to the sole of the foot.

Source

Oxford Languages

Next Terms Alphabetically

Plantar Mark

Plantar Prints

Platen

Plantar Mark

An impression from a foot left under uncontrolled circumstances.

Source

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/267523/FingerprintTerminology.pdf

Next Terms Alphabetically

Plantar Prints

Platen

Polydactylism

Plantar Prints

An impression of the friction ridges of any or all of the foot taken under controlled conditions.

Source

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/267523/FingerprintTerminology.pdf

Next Terms Alphabetically

Platen

Polydactylism

Polymerase Chain Reaction (PCR)

Platen

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

Source

International Association for Biometrics (iAfB) and International Computer Security Association (ICSA), 1999 Glossary of Biometric Terms

Next Terms Alphabetically

Polydactylism

Polymerase Chain Reaction (PCR)

Pores

Polydactylism

The condition in which a person's hand or foot has more than five digits.

Source

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/267523/FingerprintTerminology.pdf

Next Terms Alphabetically

Polymerase Chain Reaction (PCR)

Pores

Poroscopy

Polymerase Chain Reaction (PCR)

Polymerase chain reaction (abbreviated PCR) is a laboratory technique for rapidly producing (amplifying) millions to billions of copies of a specific segment of DNA, which can then be studied in greater detail. PCR involves using short synthetic DNA fragments called primers to select a segment of the genome to be amplified, and then multiple rounds of DNA synthesis to amplify that segment.

Source

https://www.genome.gov/genetics-glossary/Polymerase-Chain-Reaction#:~:text=Polymerase%20chain%20reaction%20(abbreviated%20PCR,be%20studied%20in%20greater%20detail.

Next Terms Alphabetically

Pores

Poroscopy

Positive Biometric Claim

Pores

Small openings on friction ridges through which sweat is released.

Source

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/267523/FingerprintTerminology.pdf

Next Terms Alphabetically

Poroscopy

Positive Biometric Claim

Presentation Attack

Poroscopy

A study of the size, shape, and arrangement of pores on the friction ridges.

Source

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/267523/FingerprintTerminology.pdf

Next Terms Alphabetically

Positive Biometric Claim

Presentation Attack

Presentation Attack Detection

Positive Biometric Claim

Assertion that a biometric capture subject is the source of specified or unspecified biometric reference(s) in a biometric reference database.
Note 1 to entry: Specified means there is a non-biometric input, such as a PIN, name or ID number, pointing to particular biometric reference(s). Unspecified means there is no such non-biometric input provided.

Source

International Organization for Standardization. (2017). Information technology - Vocabulary - Part 37: Biometrics. https://www.iso.org/standard/66693.html

Next Terms Alphabetically

Presentation Attack

Presentation Attack Detection

Probe

Presentation Attack

Presentation to the biometric data capture subsystem with the goal of interfering with the operation of the biometric system. Examples: holding up a picture of a face to a face camera; applying fake fingerprints to a fingerprint reader.

Source

https://csrc.nist.gov/glossary/term/presentation_attack

Next Terms Alphabetically

Presentation Attack Detection

Probe

Proximal

Presentation Attack Detection

Automated determination of a presentation attack. A subset of presentation attack determination methods, referred to as liveness detection, involves measurement and analysis of anatomical characteristics or involuntary or voluntary reactions, in order to determine if a biometric sample is being captured from a living subject present at the point of capture.

Source

https://csrc.nist.gov/glossary/term/presentation_attack_detection

Next Terms Alphabetically

Probe

Proximal

Radio Frequency Identification (RFID)

Probe

[1] The biometric sample that is submitted to the biometric system to compare against one or more references in the gallery.

[2] (Biometric Probe) Biometric sample or biometric feature set input to an algorithm for biometric comparison to a biometric reference(s).

Source

[1] National Science & Technology Council (NSTC), 14 September 2006

[2] International Organization for Standardization. (2017). Information technology - Vocabulary - Part 37: Biometrics. https://www.iso.org/standard/66693.html

Next Terms Alphabetically

Proximal

Radio Frequency Identification (RFID)

Re-enrollment

Proximal

[In human anatomy, refers to a location] situated at the closest point of attachment; direction toward the body.

Source

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/267523/FingerprintTerminology.pdf [IBIA]

Next Terms Alphabetically

Radio Frequency Identification (RFID)

Re-enrollment

Receiver Operating Characteristics...

Radio Frequency Identification (RFID)

Technology that uses low-powered radio transmitters to read data stored in a transponder (tag). RFID tags can be passive (not self-powered) or active (powered). They can be used to track assets, manage inventory, authorize payments, and serve as electronic keys. RFID is not a biometric, but the technology can sometimes be used in conjunction with biometrics as an additional factor (or token) in multi-factor authentication (e.g. through a smart card or smart phone).

Source

IBIA

Next Terms Alphabetically

Re-enrollment

Receiver Operating Characteristics...

Recognition

Re-enrollment

Process of establishing a new biometric reference for a biometric data subject already enrolled in the biometric enrollment database.

Source

International Organization for Standardization. (2017). Information technology - Vocabulary - Part 37: Biometrics. https://www.iso.org/standard/66693.html

Next Terms Alphabetically

Receiver Operating Characteristics...

Recognition

Relying Party

Receiver Operating Characteristics (ROC)

A method of showing measured accuracy performance of a biometric system. A verification ROC curve graphically compares false acceptance rate (x-axis) vs. verification rate (y-axis). An open-set identification (watchlist) ROC compares false alarm rates vs. detection and identification rate.

Source

National Science & Technology Council (NSTC), 14 September 2006

Next Terms Alphabetically

Recognition

Relying Party

Resolution

Recognition

[1] 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 the verification, closed-set identification or open-set identification (watchlist).

[2] (Biometric Recognition) Automated recognition of individuals based on their biological and behavioral characteristics.

Source

[1] National Science & Technology Council (NSTC), 14 September 2006

[2] International Organization for Standardization. (2017). Information technology - Vocabulary - Part 37: Biometrics. https://www.iso.org/standard/66693.html

Next Terms Alphabetically

Relying Party

Resolution

Response Time

Index

Relying Party

A Relying Party is an entity or web-based service which may accept digital identities and biometric information for verification of access or authentication of a user to the Relying Party's service or application.

Source

IBIA

Next Terms Alphabetically

Resolution

Response Time

Retina Scans

Resolution

The number of pixels per unit distance in an image. Describes the sharpness and clarity of an image.

Source

IBIA

Next Terms Alphabetically

Response Time

Retina Scans

Ridge Ending

Response Time

The time used by a biometric system to return a decision on identification or verification of a biometric sample.

Source

International Association for Biometrics (iAfB) and International Computer Security Association (ICSA), 1999 Glossary of Biometric Terms

Next Terms Alphabetically

Retina Scans

Ridge Ending

Rolled Fingerprints

Retina Scans

A retinal scan looks at the complex network of vessels that supply the retina with blood. Using a retina scan as a biometric for identification purposes is a special subset of vein pattern recognition. A special scanning device is used to shoot a beam of light into the eye to capture the vein patter on the retina. To enroll, a person must be positioned very close to the scanner — much closer than for iris recognition. The retina is generally stable throughout a person's life, but its patterns can be altered by glaucoma, diabetes and retinal degenerative diseases. Retina scans are rarely used for biometric purposes and are used primarily by ophthalmologists and optometrists for eye exams and diagnostic purposes. Retina recognition is often confused with the more widely used iris recognition.

Source

https://www.irisid.com/iris-recognition-and-retinal-scans-are-not-the-same/

Next Terms Alphabetically

Ridge Ending

Rolled Fingerprints

Scars, Marks and Tattoos (SMT)

Ridge Ending

A minutiae point at the ending of a friction ridge.

Source

National Science & Technology Council (NSTC), 14 September 2006

Next Terms Alphabetically

Rolled Fingerprints

Scars, Marks and Tattoos (SMT)

Scenario Evaluation

Rolled Fingerprints

An image that includes fingerprint data from nail to nail, obtained by "rolling" each finger individually across a sensor.

Source

National Science & Technology Council (NSTC), 14 September 2006, IBIA

Next Terms Alphabetically

Scars, Marks and Tattoos (SMT)

Scenario Evaluation

Scent

Scars, Marks and Tattoos (SMT)

Refers to often unique or identifiable visible variations in the appearance of a person's skin, either by accidental injury (scars) or intentional design (marks and tattoos). SMTs can be a factor in the identification of people. Like biometrics, SMTs can be registered in an identity database, often with images and a searchable text description, and more recently searchable by means of enrollment of the SMT in an image database.

Source

IBIA

Next Terms Alphabetically

Scenario Evaluation

Scent

Segmentation

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.

Source

National Science & Technology Council (NSTC), 14 September 2006

Next Terms Alphabetically

Scent

Segmentation

Sensor

Scent

Scent in the form of human body odor is a biometric feature unique to each individual, and it can be used for authentication or identification. In addition to identification, body odor can be indicative of health, diet, stress, medications, recent activities, and emotions.

Source

https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9779205/

Next Terms Alphabetically

Segmentation

Sensor

Sequence Checking

Segmentation

The process of parsing the biometric signal of interest from the entire acquired data system. For example, finding individual finger images from a [4-finger] slap impression.

Source

National Science & Technology Council (NSTC), 14 September 2006

Next Terms Alphabetically

Sensor

Sequence Checking

Short Tandem Repeat (STR)

Sensor

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

Source

National Science & Technology Council (NSTC), 14 September 2006

Next Terms Alphabetically

Sequence Checking

Short Tandem Repeat (STR)

Signature Dynamics

Sequence Checking

Refers to checking fingerprint enrollment records for capture errors, especially out of sequence recordation, left-hand right-hand confusion, or capture inversion. For instance, capturing an index fingerprint as a pinkie and vice versa.

Source

IBIA

Next Terms Alphabetically

Short Tandem Repeat (STR)

Signature Dynamics

Similarity Score

Short Tandem Repeat (STR)

In human DNA, short tandem repeats (STRs) are short repeated sequences of DNA (2–6 base pairs) that account for approximately 3% of the human genome. The number of repeat units is highly variable among individuals, which offers a high power of discrimination when analyzed for identification purposes. It is a widely accepted notion that STRs are non-coding in nature and are therefore not implicated in gene expression.
[See "DNA"]

Source

https://www.frontiersin.org/articles/10.3389/fgene.2020.00884/full

Next Terms Alphabetically

Signature Dynamics

Similarity Score

Simplified Arrival

Signature Dynamics

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

Source

Derived from National Science & Technology Council (NSTC), 14 September 2006

Next Terms Alphabetically

Similarity Score

Simplified Arrival

Slap Fingerprint

Index

Similarity Score

[1] A value returned by a biometric algorithm that indicates the degree of similarity or correlation between a biometric sample and a reference.

[2] Comparison score that increases with similarity.

Source

[1] National Science & Technology Council (NSTC), 14 September 2006

[2] International Organization for Standardization. (2017). Information technology - Vocabulary - Part 37: Biometrics. https://www.iso.org/standard/66693.html

Next Terms Alphabetically

Simplified Arrival

Slap Fingerprint

Smart Card

Simplified Arrival

Simplified Arrival, CBP's enhanced international arrival process, uses facial biometrics at airports as one of many tools to verify travelers' identities. To begin this process, CBP uses flight manifest data and a facial comparison system, the Traveler Verification Service (TVS), to build a gallery of traveler photos collected from passports, visas, and other Department of Homeland Security encounters. The facial recognition matching process is initiated when the CBP officer takes a traveler's photo at the airport. TVS first compares the "live" photo of the traveler to the photos in the gallery, a step CBP refers to as the one-to-many (or 1:N) matching process. If the photos match, the CBP officer proceeds to determine whether the traveler may enter the United States. If no match to the gallery is found, the officer scans the traveler's document to access the traveler's digital photo, if available. TVS then compares the traveler's live photo to the photo in the document, a step known as the 1:1 matching process. If the result is a match, the CBP officer proceeds with the traveler's admissibility interview.

Source

https://www.oig.dhs.gov/sites/default/files/assets/2022-07/OIG-22-48-July22.pdf

Next Terms Alphabetically

Slap Fingerprint

Smart Card

Source

Slap Fingerprint

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

Source

National Science & Technology Council (NSTC), 14 September 2006

Next Terms Alphabetically

Smart Card

Source

Speaker Recognition

Smart Card

A plastic card with a built-in microprocessor, used typically for electronic processes such as financial transactions and personal identification.

Source

Oxford Languages

Next Terms Alphabetically

Source

Speaker Recognition

Speaker Verification

Source

An approved database and infrastructure that stores biometrics files.

Source

Capstone Concept of Operations for DoD Biometrics in Support of Identity Superiority, November 2006

Next Terms Alphabetically

Speaker Recognition

Speaker Verification

Speech Recognition

Speaker Recognition

A biometric modality that uses a biometric subject's speech, a feature influenced by both the physical structure of a biometric subject's vocal tract and the behavioral characteristics of the biometric subject, for recognition purposes. Sometimes referred to as 'voice recognition.' Most often associated with 1:N identification operations. 'Speaker Recognition' is not the same as 'Speech recognition' which recognizes the words being said and is not a biometric technology.

Source

Derived from National Science & Technology Council (NSTC), 14 September 2006

Next Terms Alphabetically

Speaker Verification

Speech Recognition

Spoofing

Speaker Verification

A type of biometric verification for confirming a biometric claim using input speech data.

Source

Wayman, J., Sawchak E., & Clarke, S. (2023). ISO/IEC JTC 1/SC 37 SD 2 Harmonized Biometric Vocabulary (v40)

Next Terms Alphabetically

Speech Recognition

Spoofing

Store

Speech Recognition

A technology that enables a machine to recognize spoken words. Speech recognition is not a biometric technology.

Source

National Science & Technology Council (NSTC), 14 September 2006

Next Terms Alphabetically

Spoofing

Store

Submission

Spoofing

The ability to fool a biometric sensor into recognizing an illegitimate biometric subject as a legitimate biometric subject (Verification) or into missing an identification of someone that is in the database.

Source

Derived from National Science & Technology Council (NSTC), 14 September 2006

Next Terms Alphabetically

Store

Submission

Subversive Biometric Capture Subject

Store

The process of enrolling, maintaining, and updating biometric files to make available standardized, current biometric information on biometric subjects when and where required. Biometric files are either enrolled or updated before they are stored.

Source

Capstone Concept of Operations for DoD Biometrics in Support of Identity Superiority, November 2006

Next Terms Alphabetically

Submission

Subversive Biometric Capture Subject

Subversive User

Submission

The process whereby a subject provides a biometric sample to a biometric system.

Source

National Science & Technology Council (NSTC), 14 September 2006

Next Terms Alphabetically

Subversive Biometric Capture Subject

Subversive User

Surveillance

Subversive Biometric Capture Subject

Biometric capture subject who attempts to subvert the correct and intended policy of the biometric capture subsystem.

Source

International Organization for Standardization. (2017). Information technology - Vocabulary - Part 37: Biometrics. https://www.iso.org/standard/66693.html

Next Terms Alphabetically

Subversive User

Surveillance

Tactical Enrollment

Index

Subversive User

User of a biometric system who attempts to subvert the correct and intended system policy.

Source

International Organization for Standardization. (2017). Information technology - Vocabulary - Part 37: Biometrics. https://www.iso.org/standard/66693.html

Next Terms Alphabetically

Surveillance

Tactical Enrollment

Template

Surveillance

Surveillance is using humans or machine automation to persistently observe an environment to derive intelligence, detect adverse behavior, or — when recorded — to forensically analyze circumstances leading up to an event of interest (perhaps for purposes of attribution). There are many forms of surveillance, including aerial imagery, data mining, social network analysis, computer, communications, RF (including RFID and geolocation), geophysical, audio (e.g., gunshot detection and location) and video surveillance. Credential matching (e.g., by TSA of drivers' licenses at airport checkpoints or by CBP of passport pictures at international ports) is legally required and is NOT surveillance.

Source

IBIA

Next Terms Alphabetically

Tactical Enrollment

Template

10 Print Match or Identification

Index

Tactical Enrollment

Enrollment of biometric data on a subject that includes at least 2 fingerprints (indexes), 2 iris prints, and required text fields. The sample must be EBTS compliant. Typically used when subject is not being detained, but a record of the encounter is required at an ICED site, raid, humanitarian assistance, etc. It is an identification leading to an enrollment of a subject utilizing biometric data that includes at least 1 fingerprint or 1 iris and capture identification number. Used when subject is being detained and full enrollment will be conducted at the detention facility or at a base access point, when a subject is applying for a job on a base and is escorted to the LEP screening site for full enrollment.

Source

Initial Capabilities Document (ICD) for Biometrics in Support of Personnel Identity (BSPI) (Draft), 30 Jun 07

Next Terms Alphabetically

Template

10 Print Match or Identification

Tethered Biometric System

Template

A digital representation of a biometric subject's distinct characteristics, representing information extracted from a biometric sample. Templates are used during biometric authentication as the basis for comparison.

Source

Derived from National Science & Technology Council (NSTC), 14 September 2006

Next Terms Alphabetically

10 Print Match or Identification

Tethered Biometric System

Thenar

10 Print Match or Identification

An absolute positive identification of a biometric subject by corresponding each of his or her 10 fingerprints to those in a system of record. Usually performed by an automated fingerprint identification system (AFIS) and verified by a human fingerprint examiner.

Source

Derived from Biometrics Task Force

Next Terms Alphabetically

Tethered Biometric System

Thenar

Threshold

Tethered Biometric System

Use of biometric sensors between deployed personnel within a robust command and control architecture.

Source

Biometrics Fusion Center

Next Terms Alphabetically

Thenar

Threshold

Throughput Rate

Thenar

[On a person's hand], the large cushion of the palm located at the base of the thumb. [Relevant to palm print biometrics.]

Source

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/267523/FingerprintTerminology.pdf , [IBIA]

Next Terms Alphabetically

Threshold

Throughput Rate

Token

Threshold

[1] (noun) 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.

[2] (noun) Numerical value (or set of values) at which a decision boundary exists.

[3] (verb) Eliminate biometric reference identifier(s) associated with biometric reference(s) and/or identifiers for biometric probe(s) that have failed to attain a level of any type of score.

Source

[1] National Science & Technology Council (NSTC), 14 September 2006

[2] International Organization for Standardization. (2017). Information technology - Vocabulary - Part 37: Biometrics. https://www.iso.org/standard/66693.html

[3] International Organization for Standardization. (2017). Information technology - Vocabulary - Part 37: Biometrics. https://www.iso.org/standard/66693.html

Next Terms Alphabetically

Throughput Rate

Token

Traveler Verification Service (TVS)

Throughput Rate

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

Source

National Science & Technology Council (NSTC), 14 September 2006

Next Terms Alphabetically

Token

Traveler Verification Service (TVS)

True Acceptance Rate

Token

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

Source

IBIA

Next Terms Alphabetically

Traveler Verification Service (TVS)

True Acceptance Rate

True Rejection Rate

Traveler Verification Service (TVS)

CBP deployed this facial recognition technology, known as the Traveler Verification Service (TVS), to support comprehensive biometric entry and exit procedures in the air, land, and sea environments. TVS provides face recognition services to, for example, Simplified Arrival and Global Entry operations at international ports.

Source

https://www.dhs.gov/publication/dhscbppia-056-traveler-verification-service

Next Terms Alphabetically

True Acceptance Rate

True Rejection Rate

Unacceptable Capture Attempt

True Acceptance 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.

Source

National Science & Technology Council (NSTC), 14 September 2006

Next Terms Alphabetically

True Rejection Rate

Unacceptable Capture Attempt

Uncooperative Biometric Capture...

Unacceptable Capture Attempt

Capture attempt that does not fulfil the requirements of a biometric capture process.

Source

International Organization for Standardization. (2017). Information technology - Vocabulary - Part 37: Biometrics. https://www.iso.org/standard/66693.html

Next Terms Alphabetically

Uncooperative Biometric Capture...

Uncooperative Presentation

Uncooperative User or Subject

Uncooperative Biometric Capture Subject

Biometric capture subject motivated to not achieve a successful biometric acquisition process.

Source

International Organization for Standardization. (2017). Information technology - Vocabulary - Part 37: Biometrics. https://www.iso.org/standard/66693.html

Next Terms Alphabetically

Uncooperative Presentation

Uncooperative User or Subject

Unidentified Biometric Data

Uncooperative Presentation

Presentation by an uncooperative biometric capture subject.
Note 1 to entry: Uncooperative presentation may or may not be a conformant capture attempt.
Note 2 to entry: To be uncooperative, the biometric capture subject must be aware that biometric data is being collected.

Source

International Organization for Standardization. (2017). Information technology - Vocabulary - Part 37: Biometrics. https://www.iso.org/standard/66693.html

Next Terms Alphabetically

Uncooperative User or Subject

Unidentified Biometric Data

Untethered Biometric System

Uncooperative User or Subject

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.

Source

IBIA

Next Terms Alphabetically

Unidentified Biometric Data

Untethered Biometric System

User (of a biometric system)

Unidentified Biometric Data

Biometric data whose biometric data subject is currently unknown.

Source

International Organization for Standardization. (2017). Information technology - Vocabulary - Part 37: Biometrics. https://www.iso.org/standard/66693.html

Next Terms Alphabetically

Untethered Biometric System

User (of a biometric system)

Valley

Untethered Biometric System

Collection, analysis and use of biometric sensors between deployed personnel outside of a robust command and control architecture.

Source

Biometrics Fusion Center

Next Terms Alphabetically

User (of a biometric system)

Valley

Vein Pattern Recognition

User (of a biometric system)

DEPRECATED: end user
Any person or organization interacting in any way with a biometric system.
Note 1 to entry: When discussing a particular class of users involved with biometric systems, the specific term for that class should be used. For example, those users whose biometric data is being collected should be referred to as biometric capture subjects.

Source

International Organization for Standardization. (2017). Information technology - Vocabulary - Part 37: Biometrics. https://www.iso.org/standard/66693.html

Next Terms Alphabetically

Valley

Vein Pattern Recognition

Verification

Valley

The area of a fingerprint surrounding a friction ridge that does not make contact with an incident surface under normal touch; the area of the finger between two friction ridges.

Source

ANSI INCITS 378-2004 Information technology - Finger Minutiae Format for Data Interchange

Next Terms Alphabetically

Vein Pattern Recognition

Verification

Verification Attempt

Vein Pattern Recognition

Sometimes also called vascular recognition or vein pattern authentication since it is most often used for personal authentication for access control, payment systems, or test candidate verification (e.g., the GMAT test). Useable vein patterns for biometrics include those of the fingers, palms, whole hand, retina, and sclera. Vascular patterns are unique to individuals and don't change with age. The modality is difficult to spoof or forge and is generally contact-less.

Source

IBIA

Next Terms Alphabetically

Verification

Verification Attempt

Verification Rate

Verification

[1] The one-to-one process of matching a biometric subject's biometric sample against his stored biometric file. Also known as Authentication.

[2] (Biometric Verification) Process of confirming a biometric claim through biometric comparison.
Note 1 to entry: Use of the term "authentication" as a substitute for biometric verification is deprecated.

Source

[1] Derived from Capstone Concept of Operations for DoD Biometrics in Support of Identity Superiority, November 2006

[2] International Organization for Standardization. (2017). Information technology - Vocabulary - Part 37: Biometrics. https://www.iso.org/standard/66693.html

Next Terms Alphabetically

Verification Attempt

Verification Rate

Verification Transaction

Verification Attempt

Biometric claim and capture attempt(s) that together provide the inputs for comparison(s).

Source

International Organization for Standardization. (2017). Information technology - Vocabulary - Part 37: Biometrics. https://www.iso.org/standard/66693.html

Next Terms Alphabetically

Verification Rate

Verification Transaction

Verify

Verification Rate

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

Source

Derived from National Science & Technology Council (NSTC), 14 September 2006

Next Terms Alphabetically

Verification Transaction

Verify

Voice Diarization

Verification Transaction

One or more verification attempts resulting in resolution of a biometric claim.

Source

International Organization for Standardization. (2017). Information technology - Vocabulary - Part 37: Biometrics. https://www.iso.org/standard/66693.html

Next Terms Alphabetically

Verify

Voice Diarization

Voice Recognition

Verify

Confirm a biometric claim through biometric comparisons.
Note 1 to entry: It is understood that, in general, biometric claims can neither be proven nor be refuted with certainty.

Source

International Organization for Standardization. (2017). Information technology - Vocabulary - Part 37: Biometrics. https://www.iso.org/standard/66693.html

Next Terms Alphabetically

Voice Diarization

Voice Recognition

Vulnerability

Voice Diarization

Voice diarization is a subset of audio diarization. Audio diarization is the process of annotating an input audio channel with information that attributes (possibly overlapping) temporal regions of signal energy to their specific sources. These sources can include particular speakers [voice diarization], music, background noise sources, and other signal source/channel characteristics. Diarization can be used for helping speech recognition, facilitating the searching and indexing of audio archives, and increasing the richness of automatic transcriptions, making them more readable.

Source

https://ieeexplore.ieee.org/abstract/document/1677976

Next Terms Alphabetically

Voice Recognition

Vulnerability

Watchlist

Voice Recognition

Recognizing an individual from voice data; recognition might be performed with different kinds of vocal sounds (e.g. speaking, singing, shouting, crying and whispering).

Source

Wayman, J., Sawchak E., & Clarke, S. (2023). ISO/IEC JTC 1/SC 37 SD 2 Harmonized Biometric Vocabulary (v40)

Next Terms Alphabetically

Vulnerability

Watchlist

Wavelet Scalar Quantization (WSQ)...

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.

Source

National Science & Technology Council (NSTC), 14 September 2006

Next Terms Alphabetically

Watchlist

Wavelet Scalar Quantization (WSQ)...

Whorl

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. The individual does not make an identity claim, and in some cases does not personally interact with the system whatsoever.

Source

National Science & Technology Council (NSTC), 14 September 2006

Next Terms Alphabetically

Wavelet Scalar Quantization (WSQ)...

Whorl

Wavelet Scalar Quantization (WSQ)

Provides the definitions, requirements, and guidelines for specifying the FBI's WSQ compression algorithm. The document specifies the class of encoders required, decoder process, and coded representations for compressed image data.

Source

Criminal Justice Information Services (CJIS) Electronic Fingerprint Transmission Specification IAFIS-doc-01078-7.1

Next Terms Alphabetically

Whorl

Whorl

A fingerprint pattern in which the ridges are circular or nearly circular. The pattern will contain 2 or more deltas.

Source

National Science & Technology Council (NSTC), 14 September 2006

Join IBIA Today

To find out more about IBIA, its mission, and the benefits of membership in our Association, please visit:
www.ibia.org/why-join/why-join

International Biometrics + Identity Association
1325 G Street, NW
Suite 500
Washington, DC 20005
www.ibia.org

IBIA International Biometrics+Identity Association

Identity Matters.