

Indiana Intelligence Fusion Center

Face Recognition Policy

February 2026



The Indiana Intelligence Fusion Center Face Recognition Policy represents the privacy policy applicable to all IIFC operations and activities.

INDIANA INTELLIGENCE FUSION CENTER FACIAL RECOGNITION PRIVACY POLICY

TABLE OF CONTENTS

A.	PURPOSE STATEMENT	4
B.	POLICY APPLICABILITY and LEGAL COMPLIANCE	4
C.	GOVERNANCE and OVERSIGHT	5
D.	INFORMATION	5
E.	ACQUIRING and RECEIVING FACE RECOGNITION INFORMATION.....	7
F.	USE OF FACE RECOGNITION INFORMATION.....	7
G.	SHARING and DISSEMINATING FACE RECOGNITION INFORMATION.....	8
H.	DATA QUALITY ASSURANCE	8
I.	DISCLOSURE REQUESTS	9
J.	SECURITY and MAINTENANCE.....	9
K.	INFORMATION RETENTION and DESTRUCTION	9
K.1	ACCOUNTABILITY and ENFORCEMENT	10
K.2	ENFORCEMENT	10
	APPENDIX A	11
	APPENDIX B	28
	APPENDIX C	34
	Appendix D.....	48

{Page intentionally left blank}

A. PURPOSE STATEMENT

Facial recognition technology involves the ability to examine and compare distinguishing characteristics of a human face through the use of biometric algorithms contained within a software application. This technology can be a valuable investigative tool to detect and prevent criminal activity, reduce an imminent threat to health or safety, and help in the identification of deceased persons, or persons unable to identify themselves. The **Indiana Intelligence Fusion Center (IIFC)** has implemented a face recognition program to support the investigative efforts of law enforcement and public safety agencies both within and outside the State of Indiana.

It is the purpose of this policy to provide Indiana Intelligence Fusion Center personnel with guidelines and principles for the collection, access, use, dissemination, retention, and purging of images and related information applicable to the implementation of a face recognition (FR) program. This policy will ensure that all FR uses are consistent with authorized purposes.

This policy is intended to protect privacy, civil rights, and civil liberties:

- Increasing public safety and improving national security.
- Minimizing the threat and risk of injury to all individuals.
- Protecting the integrity of the criminal investigatory, criminal intelligence, and justice system processes and information.

All deployments of the face recognition program are for law enforcement purposes only. The provisions of this policy are provided to support authorized use of face recognition.

B. POLICY APPLICABILITY and LEGAL COMPLIANCE

The policy is applicable to all personnel working in direct support of the IIFC.

This policy was established to provide guidelines on how the IIFC uses lawfully obtained images. This policy applies to:

- Images contained in a known identity face image repository and its related identifying information.
- The face image searching process.
- Any results from face recognition searches that may be accessed, searched, used, evaluated, retained, disseminated, and purged by the IIFC.
- Probe images of unknown suspects will be treated as a tip.

An outside agency, or investigators from an outside agency, may request face recognition searches to assist with investigations only if:

- The outside agency is a law enforcement agency or provides a law enforcement function that is making the request based on a valid law enforcement purpose that falls within the authorized uses listed in the IIFC Privacy Policy and/or Indiana State law. The requestor shall provide their contact information (requestor's name, requestor's agency, address, and phone number), and lawful reason for the request. The result of a face recognition search is provided by the Indiana

Intelligence Fusion Center only as an investigative lead and IS NOT TO BE CONSIDERED A POSITIVE IDENTIFICATION OF ANY SUBJECT. Any possible connection or involvement of any subject to the investigation must be determined through further investigation and investigative resources.

C. GOVERNANCE and OVERSIGHT

Primary responsibility for the operation of the IIFC, its justice systems, operations, and coordination of personnel; the receiving, seeking, retention, evaluation, information quality, analysis, destruction, sharing, or disclosure of information; and the enforcement of this policy is assigned to the IIFC Administrator, who also must adhere to all enforcement procedures outlined in this policy.

IIFC privacy compliance is guided by a trained Privacy Officer who is appointed by the IIFC Administrator. Violations of the privacy policy can be reported to the IIFC Administrator or to the Privacy Officer. Reporting can be made in person, in writing, or via any electronic communication.

D. INFORMATION

The Indiana Intelligence Fusion Center may collect criminal intelligence information only if:

- Reasonable suspicion exists that the subject of the criminal intelligence information is involved with or has knowledge of possible criminal or terrorist activity; and
- The criminal intelligence information is relevant to the criminal or terrorist activity.

IIFC personnel are required to adhere to the ISE- SAR Functional Standard and state and federal laws for the receipt, collection, assessment, storage, access, dissemination, retention, and security of Suspicious Activity Reporting (SAR) information.

Subject to the policies and procedures specified in this policy, the IIFC may retain information, such as tips and leads or suspicious activity report (SAR) information, based on suspicion that behaviors are reasonably indicative of pre-operational planning associated with terrorism, as it pertains to terrorism.

- The ISE-SAR Functional Standard *does not alter law enforcement officers' constitutional obligations when interacting with the public*. This means, for example, that constitutional protections and agency policies and procedures that apply to a law enforcement officer's authority to stop, stop and frisk ("Terry Stop"), request identification, or detain and question an individual apply in the same measure to observed behavior *that is reasonably indicative of pre-operational planning associated with terrorism*. It is also important to recognize that many terrorism-related activities are now being funded via local or regional criminal organizations whose direct association with terrorism *may be tenuous*. This places law enforcement and homeland security professionals in the unique, yet demanding, position of identifying suspicious behaviors *as a by-product or secondary element in a criminal enforcement or investigative activity*.

The IIFC incorporates the gathering, processing, reporting, analyzing, and sharing of terrorism-related suspicious activities and incidents (SAR process) into existing processes and systems used to manage other crime-related information and criminal intelligence, thus leveraging existing policies and protocols

utilized to protect the information, as well as constitutional rights, including personal privacy and other civil liberties, and civil rights.

The IIFC will not seek or retain, and information-originating agencies will agree not to submit, information about individuals or organizations solely on the basis of their race, ethnicity, citizenship, place of origin, age, disability, gender, or sexual orientation; nor religious, political, social views, or activities; nor their participation in a particular noncriminal organization or lawful event.

The IIFC applies restriction labels to all disseminated information released to an authorized user, and ensures that any agency-originated information has also applied appropriate restriction labels. The labels pertain to the following:

- The information pertains to all individuals pursuant to IC 10-11-9-4; and
- The information is subject to Federal and Indiana state laws restricting access, use, or disclosure, including, but not limited to, 18 USC 2721, IC 35-38-9 et seq., IC 31-39-8 et seq., IC 4-1-10 et seq., IC 5-2 et seq., IC 5-14-3 et seq., and 28 CFR Part 23.

IIFC personnel will, upon receipt of information, assess the information to determine or review its nature, usability, and quality. Personnel will assign categories to the information (or ensure that the originating agency will assign categories to the information) to reflect the assessment, such as:

- The reliability of the source (for example, reliable, usually reliable, unreliable, unknown); and
- The validity of the content (for example, confirmed, probable, doubtful, cannot be judged).

At the time a decision is made to retain information, it will be labeled (by record, data set, or system of records), to the maximum extent feasible, pursuant to applicable limitations on access and sensitivity of disclosure to:

- Not interfere with or compromise pending criminal investigations.
- Protect an individual's right of privacy, civil rights, and civil liberties;

The IIFC will identify and review information that is originated by the IIFC prior to sharing that information in the ISE.

The IIFC will keep a record of the source of all information retained by the agency in accordance with federal guidelines and state law.

The IIFC will make every reasonable effort to ensure that information sought or retained is derived from dependable and trustworthy sources of information; accurate; current; complete, including the relevant context in which it was sought or received and other related information; and merged with other information about the same individual or organization only when the applicable standard has been met.

At the time of retention in the system, the information will be labeled regarding its level of quality.

The labeling of retained information will be reevaluated when new information is gathered that has an impact on the confidence (validity and reliability) of the previously retained information.

The IIFC investigates in a timely manner and will make every reasonable effort to ensure that information will be corrected, deleted from the system, or not used when the agency/center learns that the information is erroneous, misleading, obsolete, or otherwise unreliable; the source of the information did not have authority to gather the information or to provide the information to the agency; or the source used prohibited means to gather the information, except when the source did not act as an agent to a bona fide law enforcement officer.

Information acquired or received by the IIFC or accessed from other sources will be analyzed only by qualified individuals who have successfully completed a background check and appropriate security clearance, where applicable, and have been selected, approved, and trained accordingly.

E. ACQUIRING and RECEIVING FACE RECOGNITION INFORMATION

For the purpose of performing face recognition searches, the IIFC and authorized IIFC personnel will obtain probe images or accept probe images from law enforcement or participating agencies only per the IIFC Privacy Policy.

Information gathering (acquisition and access) and investigative techniques used by the IIFC and information-originating agencies are in compliance with and will adhere to applicable federal guidelines and state law.

Information gathering techniques used by the IIFC will (and for originating agencies should) be the least intrusive means necessary in the particular circumstances to gather information it is authorized to seek or retain.

The IIFC will make every effort to contract only with commercial database entities that provide an assurance that their methods for gathering personally identifiable information comply with applicable federal, state, local, tribal, and territorial laws, statutes, and regulations and that these methods are not based on misleading information collection practices.

F. USE OF FACE RECOGNITION INFORMATION

The IIFC does not connect the face recognition system to any interface that performs live video surveillance, including surveillance cameras, drone footage, body-worn cameras, or other mass-surveillance tools.

The following describes the Indiana Intelligence Fusion Center's (IIFC) manual face recognition search procedure, which is conducted in accordance with the IIFC Privacy Policy and this policy.

- Trained IIFC analysts may initially run probe images without filters, using a filtered search as a secondary search, if needed. In some cases, enhancements may be considered after running an image as is against the image repository in accordance with best established practices (See Appendix B). All enhancements and queries will be documented for audit purposes in accordance with best established practices (See Appendix C).
- In the automated search, most likely candidates are returned to the analyst, manually compared with the probe images, and then examined by an analyst. Analysts shall conduct the comparison of images, biometric identifiers, and biometric information in accordance with their training set

by best established practices (see Appendix D).

- If no likely candidates are found, the requesting entity will be informed of the results. In the case of a negative result, the images examined by the analyst will not be provided to the requesting entity.
- If likely candidates are found, analysts should submit the original probe images and subsequent examination results for a peer review.
- If the peer reviewer agrees with the initial findings, then the analyst will conduct an initial background investigation on potential matches, comparing information to known criminal case details before disseminating potential leads to the originating agency.
- The results of a face recognition search are considered advisory in nature as an investigative lead only, and do not establish probable cause.

G. SHARING and DISSEMINATING FACE RECOGNITION INFORMATION

Face recognition search information derived from the IIFC will not be:

- Sold, published, exchanged, or disclosed to commercial or private entities or individuals except as required by applicable law and to the extent authorized by the IIFC's agreement with the commercial vendor.
- Disclosed or published without prior notice to the originating entity that such information is subject to disclosure or publication.
- Disclosed to unauthorized individuals or those not having a valid Right to Know and Need to Know.

H. DATA QUALITY ASSURANCE

Any enhancements made to a probe image will be made on a copy, saved as a separate image, and documented to indicate what enhancements were made, including the date and time of change.

- IIFC analysts will analyze, review, and evaluate the quality and suitability of probe images.
- The IIFC considers the results, if any, of a face recognition search to be advisory in nature as an investigative lead only. Face recognition search results are **not** considered positive identification of a subject and do not, on their own, establish probable cause, without further investigation. Any possible connection or involvement of the subject(s) to the investigation must be determined through further investigative methods.

The IIFC will make every reasonable effort to perform routine maintenance, upgrades and enhancements, testing, and refreshes of the face recognition system to ensure proper performance, including the following:

- Personnel shall assess the face recognition system on a regular basis to ensure performance and accuracy.
- Malfunctions or deficiencies of the system will be reported upon discovery of the malfunctions or deficiencies.

The integrity of information depends on quality control and correction of recognized errors which is key to mitigating the potential risk of misidentification or inclusion of individuals in a possible identification.

The IIFC will investigate, in a timely manner, alleged errors and malfunctions or deficiencies of face recognition information or, if applicable, will request that the originating agency or vendor investigate the alleged errors and malfunctions or deficiencies. The IIFC will correct the information or advise the process for obtaining correction of the information.

I. DISCLOSURE REQUESTS

Face recognition information will only be disclosed to the public in accordance with IIFC's privacy policy.

J. SECURITY and MAINTENANCE

- All results produced by the IIFC as a result of a face recognition search are disseminated by secured electronic means (such as an official government e-mail address). Non-electronic disseminations will be conducted personally or by phone with the requestor or designee.
- All face recognition equipment, face recognition software, algorithm, thresholds, and components will be properly maintained by the manufacturer.
- The IIFC and contributing entities will store face recognition information in a manner that ensures it cannot be modified, accessed, or purged except by personnel authorized to take such actions.
- Authorized access to the IIFC face recognition system will be granted only to personnel whose positions and job duties require such access.
- Usernames and passwords to the face recognition system are not transferable, must not be shared by IIFC personnel, and must be kept confidential.
- Queries made to the IIFC's face recognition system will be logged into the system identifying the user initiating the query. All user access, including participating agency access, and queries are subject to review and audit.
- The IIFC will maintain an audit trail of requested, accessed, searched, or disseminated IIFC held face recognition information by the manufacturer. An audit trail will be kept for requests, access, and searches of face recognition information for specific purposes and of what face recognition information is disseminated to each individual in response to the request.

K. INFORMATION RETENTION and DESTRUCTION

- All images utilized by the IIFC will be stored for a period determined by the IIFC Privacy Policy.
- Once a face recognition image is downloaded by IIFC personnel and incorporated into a criminal intelligence record or an investigative case file, the face recognition information is then considered criminal intelligence or investigative information, and the laws, regulations, and policies applicable to that type of information or criminal intelligence govern its use.
- Any images that do not originate with the IIFC will remain in the custody and control of the originating agency and will not otherwise be transferred to any other entity without authorization from the originating agency. Images provided by an agency will be considered lead information and retained per the IIFC privacy policy pertaining to lead information, until such time that the originating agency provides an update to IIFC.
- The IIFC retains the right to remove images from the repository earlier than the retention period, based on the limitations of information storage requirements and subject to any applicable record

retention laws and statutory disclosure mandates. Early removal, however, will not be used as a means for intentionally interfering with a lawful complaint or a public records request. The retention period may be modified at any time by the IIFC subject to applicable legal requirements.

- Any persons confirmed to be innocent will be purged from the system immediately upon notification.
- Face recognition search results may be saved within the entity's system audit log for audit purposes only.

K.1 ACCOUNTABILITY and ENFORCEMENT

- The IIFC will follow procedures and practices by which it can ensure and evaluate the compliance of users with the face recognition system requirements and with the provisions of this policy and applicable law. This will include logging access to face recognition information, may include any type of medium or technology (e.g., physical servers, virtual machines, and mobile devices) used in a work-related activity, and will entail periodic random auditing of these systems so as not to establish a discernable pattern that may influence users' actions. These audits will be mandated at least annually.

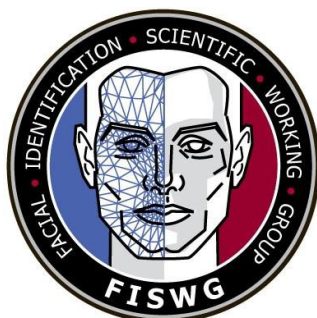
K.2 ENFORCEMENT

The IIFC will operate in a secure environment and apply physical, administrative, and technical safeguards to protect facial recognition data at rest, in motion, and in use. Safeguards may include strong authentication (including multifactor authentication), encrypted communications, firewalls, and role-based access controls.

Access to IIFC facial recognition systems from outside IIFC facilities will be allowed only over secure networks. User credentials are not transferable and must not be shared.

Breach notification: The IIFC will notify affected individuals when personal information is reasonably believed to have been breached by an unauthorized person and access threatens physical, reputational, or financial harm, consistent with law enforcement needs and applicable law. The IIFC will also notify the originating agency from which it received personal information of suspected or confirmed breaches.

APPENDIX A



Disclaimer:

As a condition to the use of this document and the information contained herein, the Facial Identification Scientific Working Group (FISWG) requests notification by e-mail before or contemporaneously to the introduction of this document, or any portion thereof, as a marked exhibit offered for or moved into evidence in any judicial, administrative, legislative, or adjudicatory hearing or other proceeding (including discovery proceedings) in the United States or any foreign country. Such notification shall include: 1) the formal name of the proceeding, including docket number or similar identifier; 2) the name and location of the body conducting the hearing or proceeding; and 3) the name, mailing address (if available) and contact information of the party offering or moving the document into evidence. Subsequent to the use of this document in a formal proceeding, it is requested that FISWG be notified as to its use and the outcome of the proceeding. Notifications should be sent to: chair@fiswg.org

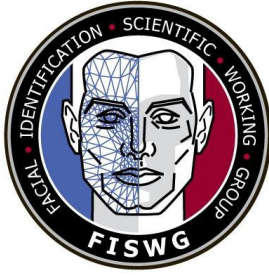
Redistribution Policy:

FISWG grants permission for redistribution and use of all publicly posted documents created by FISWG, provided that the following conditions are met:

Redistributions of documents, or parts of documents, must retain the FISWG cover page containing the disclaimer.

Neither the name of FISWG, nor the names of its contributors, may be used to endorse or promote products derived from its documents.

Any reference or quote from a FISWG document must include the version number (or creation date) of the document and mention if the document is in a draft status.



Glossary

Accessories

Removable items (e.g., glasses, sunglasses, colored contact lenses, Bluetooth devices, headphones, piercings, bandages) that are worn on, in, or near the face that may obstruct any head, face, or neck features.

ACE-V

A scientific method of analysis, comparison, evaluation, and verification utilized in most comparative processes.

Ad Hoc Image

See *Uncontrolled Image*.

Alterations

Refers to any intentional modification to the face with the exception of scarring.

Analysis

(1) The assessment of an image to determine suitability for comparison, including the ability to discriminate significant features. (2) The first step of the ACE-V method.

Anthropometry

Scientific study of the measurements and proportions of the human body.

Aspect Ratio

Ratio of width to height. This can be specific to pixels or images.

Assessment

A quick image-to-person or image-to-image comparison typically conducted in a high throughput environment (e.g., screening and access control applications or field operations).

Atmospheric Distortion

Uneven magnification or illumination of elements within an image that may obscure details.

Backlight

A light source placed behind a subject in a controlled capture that reduces background shadows.

Barrel Distortion

A type of lens distortion which is observed as straight lines appearing to bend away from the center of the image, with the center of the image enlarged.

Batch Mode Search

A mode of searching in which a group of probes are simultaneously or sequentially launched. Such computer resource intensive searches are usually performed during non-peak usage hours (e.g., nights or weekends). Also known as batch search mode.

Bias

An inclination of temperament or outlook. (Webster). A systemic tendency to over- or under-estimate the true value of a measurement. Bias can result from human factors or from factors related to the method or calculation being used.

See also *Cognitive Bias*, *Confirmation Bias*, and *Contextual Bias*.

Binning

(1) Any technique used by a Facial Recognition System (FRS) to organize or optimize searching based upon some piece(s) of metadata. (2) Process of parsing (examining) or classifying data in order to accelerate and/or improve biometric matching.

Biometric Match

A determination that two biometric samples (see biometrics below) correspond to the same source based on some level of computer-evaluated similarity. This does not inherently imply that the probe and candidate are the same person.

Biometrics

The measurement and analysis of unique physical or behavioral characteristics, especially as means of verifying a personal identity (Webster).

Capture

The process of collecting a biometric sample from an individual.

Certification Authority

A body that issues a (biometric) document and certifies that the data stored on the document is genuine.

Characteristic Descriptors

Minutiae of the component characteristics.

Cheeks

Refers to the regions of the face surrounded by the eyes, ears, nose, mouth, chin, and jawline.

Chin

Refers to the area of the face defined by the lower jaw below the mouth.

Chromatic Aberration

Color fringing that creates color and tonal changes in the high contrast areas of an image.

Class Characteristics

Characteristics common to many individuals within a group (e.g., the overall shape of the nose, eyes, mouth).

Clustering

The automated grouping of people represented within a collection of facial images based on computer evaluated similarity.

CMYK

The color gamut spectrum widely used in printing. Cyan, Magenta, Yellow, and Black.

Cognitive Bias (1) A mental error caused by one's simplified information processing strategies. It does not result from any emotional or intellectual predisposition toward a certain judgment, but rather from subconscious mental procedures for processing information. (2) A mental error that is consistent and predictable. (3) Influences that may affect the reliability and validity of one's observations and conclusions.

Color Depth

The bit scale of the image, e.g., 8 bit grayscale and 24 or 48 bit RGB (Red, Green, Blue).

Color Misrepresentation

A change in the actual color of subjects or objects depicted in an image.

Comparison

The second step of the ACE-V method; the examination of two or more samples to establish similarities and dissimilarities.

Complex Distortion

A combination of both barrel and pin cushioning, and can result in uneven magnification of the image.

Compression

The process of reducing the size of a data file.

Conclusion

A reasoned deduction or inference.

Confirmation Bias

Tendency to focus on data or interpret information in a manner that supports one's preconceptions.

Contextual Bias

Influence of extraneous information that is not needed to draw the conclusion.

Control

A sample or standard against which other conditions can be compared in a scientific experiment.

Controlled Image

An image captured in accordance with facial identification (FI) or facial recognition (FR) standards or guidelines.(e.g., a driver's license photo).

CSI Effect

The perception of the near-infallibility of forensic science in response to popular media.

Descreen

The array of dots used in the halftone or desktop printing processes is called a screen where the color dots are placed at different angles, and a scanning software option can be used to minimize the screen pattern by use of a screen frequency filter algorithm.

Digital Zoom

Method of decreasing the apparent angle of view of a digital image accomplished by cropping an image down to a centered area with the same aspect ratio as the original. Digital zoom could be misleading because it enlarges the image without adding extra details.

Doppelganger

An apparition or double of a living person.

Dots per Inch

The resolution setting of the printer and resolution capture for printed media.

Ears

Refers to the external characteristics of the ears.

Enroll

The act of capturing a sample, creating a template, and entering the template into a database.

Evaluation

The third step of the ACE-V method, where an examiner assesses the value of the details observed during the analysis and comparison steps and reaches a conclusion. Ascertaining the value of dissimilarities and similarities between two facial images.

Examination

A comparison of image(s)-to-image(s) often used in a forensic application.

EXIF

(1) Acronym for exchangeable image file format. (2) EXIF is a specification for the image file format used by some digital cameras to add image capture metadata to file formats. EXIF headers can be found in file formats such as JPEG, TIFF, and RIFF WAV.

Expression

Change in facial characteristics resulting from muscle movement or position.

Eyebrows

Refers to the strips of hair above the eyes.

Eyes

Refers to the orbital region below the eyebrows and above the cheeks.

Face Detection

Automated determination of the locations and sizes of human faces in digital images.

Face Recognition

(1) By humans, the cognitive process by which an observer identifies a person as being one they have seen before. (2) By automated systems, the automated searching of a facial image (probe) against a known collection typically resulting in a list of candidates ranked by computer-evaluated similarity score.

Face/Head Composition

Overall configuration of the facial components, to include their alignment and relative sized, internal to a single face.

Face Matching

A type of face identification task requiring a perceptual decision whether two simultaneously presented faces (photo, video, live) depict the same person or different people.

Face/Head Outline

Overall shape of the head (cranial vault) and face.

Facial Assessor

A human conducting a comparison in a high throughput environment (see Assessment).

Facial Comparison

In facial identification, a manual process to identify similarities or dissimilarities between two (or more) facial images or facial image(s) and a live subject for the purpose of determining if they represent the same person or different person.

Facial Components

Gross features considered in virtually all comparison.

Facial Examination

A human undertaking a formal systematic examination (e.g., ACE-V) of facial images to determine if the same person is depicted.

Facial Hair

Refers to the hair on the face typically covering the cheeks, chin/jaw, upper and lower lip, and neck of the face.

Facial Identification (FI)

The discipline of image-based comparisons of human facial features.

Facial Line

Refers to wrinkles, folds, or creases.

Facial Mapping

(1) The process of locating defined anthropometric landmarks. (2) A colloquial term often mistakenly used to describe facial comparison.

Facial Marks

Refers to portions of the skin that contain a different level of pigment than the rest of the surrounding skin.

Facial Review

(1) The review of a candidate list to identify possible matches. (2) One-to-one verification conducted in a high-throughput environment (e.g., border crossing).

False Match Rate (FMR)

Proportion of the completed biometric non-mated comparison trials that result in a false match. This will be referred to as FAR (false acceptance rate) and does not include errors from images which do not create valid templates.

False Non-Match Rate (FNMR)

Proportion of the completed biometric mated comparison trials that result in a false non-match. This will be referred to as FRR (false reject rate) and does not include errors from images which do not create valid templates.

Familiar Faces

Faces of people known to an observer.

Features

(1) Observable class or individual characteristics of the face. (2) The components of biometric templates.

Feedback

Information provided to trainees to minimize the gap between their current and optimal performance.

Forehead

Refers to the part of the face above the eyes, including the brow ridges.

Forensic Report

A document whose intent it is to provide information to assist a trier of fact (e.g., judge or jury).

Frontal Pose

A facial image captured directly in front of the subject with the focal plane approximately parallel to the plane of the subject's face.

Gallery

The FR system's database, which typically contains all known-person templates.

Gnathism

Apparent convexity or concavity of the mouth complex, related to the relative projection of the upper or lower teeth, or both).

Gonial Angle

The point at which the lower border of the mandible abruptly changes direction from a primarily horizontal line to a primarily vertical line.

Guideline

Recommended practice that allows some discretion or leeway in its interpretation, implementation, or use.

Hair

Refers to the shape and distribution of head hair and does not include other facial hair (eyebrows, lashes, facial hair).

Head Coverings

Removable objects (e.g., hats, caps, scarves, wigs, spit masks) that obstruct any head, face or neck features.

Histogram

A graph of a frequency distribution in which rectangles with bases on the horizontal axis are given widths equal to the class intervals and heights equal to the corresponding frequencies. In digital images, a histogram is frequently used to document the number of pixels of a given brightness value (e.g., 0-255).

Holistic Process

The innate human ability of comparing faces by looking at the face as a whole without specifically considering the component parts in isolation.

Horizontal video misalignment

Horizontal misalignment is observed where subjects and objects in the image are positioned differently between alternating horizontal lines of a video image.

Hot Spots

Bright areas of light reflection that reduce the visibility of features.

Identification

A task where the biometric system searches a database for a reference matching a submitted biometric sample and, if found, returns a corresponding identity.

Identity

The collective set of biographic data, images, or templates assigned to one person.

Individual Characteristics

Characteristics allowing one to differentiate between individuals having the same class characteristics (e.g., scars and marks).

Intentional Alteration

A temporary or permanent deliberation modification to the face (e.g., tattoos, piercings, make-up).

Interpolation

The process whereby the number of pixels comprising an image is increased based on the available pixels.

Investigative Lead Report

A document whose intent it is to provide information to operational personnel to assist them with meeting their objective.

Jawline

Refers to the area of the face defined by the lower border of the mandible between the chin and the gonial angle.

Known image

The image of an individual associated with a known or claimed identity and recorded electronically or by other medium (also known as exemplars).

Lamina

A clear/low opacity sheet of film or security designed film that is sealed onto a substrate by cold or hot adhesion.

Lens Flare

Haze, bright streaks, orbs, or polygonal bright regions within an images as a result of a bright light source.

Levels of Conclusion

A verbal or numeric scale that indicates the level of confidence regarding identification or exclusion of a source.

Lighting

The illumination of the subject.

Lighting Direction

The direction of the illumination source.

Lights Out

An automated conclusion based upon threshold scores with no human involvement.

Lines per Inch

A term in resolution setting in scanner software used for scanning original artwork for printing.

Lossless Compression

File size reduction process in which no data is lost and all data can be retrieved in its original form (e.g., TIF with LZW compression).

Lossy Compression

File size reduction process in which data is lost and cannot be retrieved in its original form (e.g., JPEG).

Make-up

Removable cosmetics (e.g., costume make-up, excessive make-up, facial make-up appendages) that are applied to the face that may obstruct any head, face, or neck features.

Match/Matching

See *Identification*.

Mentor

An individual who has competency, proficiency, and experience in the relevant role.

Mentorship

A program administered under the direction of a competent facial reviewer or examiner during the course of a trainee's professional development. Mentorship should include, but is not limited to, the evaluation of skills and competencies, the review and supervision of facial comparison casework, and where applicable, the observation of expert testimony.

Metadata

Non image-based information associated with an image file.

Mirroring

An image flipped in the horizontal plane.

Moiré

A moiré pattern occurs when a scene or an object that is being scanned contains repetitive details (such as lines, circles, dots, etc.) that exceed the sensor resolution.

Morphological Analysis

The direct comparison of class and individual facial characteristics without explicit measurement. The method of facial comparison in which the features and components of the face are compared.

Mouth

Refers to the entire oral region including the teeth and encompasses the philtrum.

Natural Expression

An expression where the facial characteristics and muscles are relaxed.

Neck

Refers to the transitional zone between the head and the trunk/limbs of the body.

Neutral Expression

An expression where the eyes are open and the mouth is closed.

Noise

Fixed, random, and semi-random spots, shapes, or patterns.

Nose

Refers to the entire nasal region.

Obstruction

Any object that blocks features (e.g., sunglasses or objects in the environment, such as a tree) partially or in totality.

Perspective

Camera to subject geometry, including both camera to subject distance and orientation of the camera relative to the subject.

Perspective Distortion

Warping or transformation introduced to an object's appearance in an image caused by insufficient subject to camera distance (e.g., larger nose or smaller ears). Photographs made from a distance of less than two meters tend to introduce noticeable perspective distortion. Magnification of the subjects' features that are closer to the camera making them appear larger than those further away.

Photo-Anthropometric Facial Comparison

Explicit measurement of landmarks on the face and comparison of these measurements between images.

Photographic Comparison

An assessment of the correspondence between features in images and known objects/images for the purpose of rendering an identification, elimination, or a qualified conclusion (as opposed to a demonstrative exhibit). The measurement of dimensions and angles of anthropological landmarks and other facial features visible in an image in order to quantify characteristics and proportions.

Pin-Cushioning Distortion

A type of lens distortion which is observed as straight lines appearing to bend towards the center of the image, with the center of the image more compressed.

Pitch

The rotation in degrees about the (horizontal) x-axis. Frontal poses have a pitch angle of 0 degrees. Positive angles represent faces looking down (a counter-clockwise rotation around the x-axis). (ISO/IEC 19794-5).

Pixels per Inch

Measurements of the pixel density of an electronic image device, such as a computer monitor or camera.

Poor Contrast

The limited distribution or separation of light and dark.

Pose

The orientation of the face with respect to the camera, consisting of pitch, roll, and yaw. Common poses are frontal and profile.

Printed Image

A printed image is the production of a digital image on a substrate by a direct or indirect printing process.

Probabilistic Model

Statistical analysis tool that estimates, on the basis of past (historical) data, the probability of an event occurring.

Probe

The facial image or template searched against the gallery in an FR system.

Questioned image

The image of an individual whose identity is unknown or in question and has been recorded.

Raw

A digital camera or scanner file format, usually proprietary, for minimally processed digital image data.

Registration

(1) Enrollment of an identity in an application using a biometric system. (2) The process by which two facial images are sized and aligned with each other for direct comparison.

Relative Frequency

How often facial features or combinations thereof occur in a given population.

Resolution

The act, process, or capability of distinguishing between two separate but adjacent elements of detail in an image. Resolution normally has three components: spatial (e.g., pixels per inch), spectral (e.g., number of colors), and radiometric (e.g., number of shades).

Review

A comparison of image-to-image often used in either investigative and operational leads or intelligence gathering applications.

RGB

A color gamut spectrum that stands for color channels Red, Green, and Blue.

Roll

The rotation in degrees about the z-axis (the horizontal axis from front to back). Frontal poses have a roll angle of zero degrees. Positive angles represent faces tilted toward their right shoulder (counter-clockwise rotation around the z-axis). A roll angle of zero degrees denotes that the left and right eye centers have identical Y coordinates (ISO/IEC 19794-5).

Rolling Shutter Effect

Skewing or stretching of fast moving objects in a an image where the sensor captures images line by line.

Samples per Inch

A generic term that can include of DPI, LPI, and PPI. SPI is the measurement of the resolution, in particular the number of individual samples that are taken in the space of one linear inch.

Scar

Refers to dysmorphic or discolored areas or both of skin where permanent damage has healed (that is, not recent damage).

Search

The act of comparing a probe against a gallery.

Search Result Set

The candidate list returned from a search.

Sharpness

The overall clarity and detail of the facial features.

Skin

Refers to the overall appearance of the skin.

Spoofing

In a biometric system, the process by which an imposter intentionally attempts to be recognized as another person or intentionally attempts to be missed as an existing identity in the gallery.

sRGB

Standard default color space of red, green, blue used for the Internet and for displaying or printing images.

Subject Acquisition Profile (SAP)

Facial image capture criteria described in ANSI/NIST-ITL 1-2007 (e.g., SAP Level 40 includes the requirement for 768 x 1024 pixels).

Substrate

A substrate in printing terms is a form of media on which a printed image is produced.

Superimposition

The process of creating an overlay of two aligned images and comparing them visually.

System Bias

(1) Errors repeatedly introduced through automation (e.g., errors in template generation or comparison). (2) Errors repeatedly introduced through operational practices in an organization or unit (e.g., improper lighting or camera position guidance).

Template

A set of biometric measurement data prepared by an FR system from a facial image.

Time-related changes

The natural variations to the face that occur as a function of time.

Uncontrolled Image

An image not captured in accordance with FI/FR standards or guidelines (e.g., a surveillance image).

Unfamiliar Faces

Faces of unknown or recently learned people.

Verification

(1) The final step of the ACE-V method; the review and independent analysis of the conclusion of another examiner. (2) In a biometric system, the process of conducting a one-to-one comparison.

Vignetting

A reduction in brightness and contrast towards the edges of an image.

Yaw

The rotation in degrees about the y-axis (vertical axis). Frontal poses have a yaw angle of zero degrees. Positive angles represent faces looking to their left (a counter-clockwise rotation around the y-axis). (ISO/IEC 19794-5).

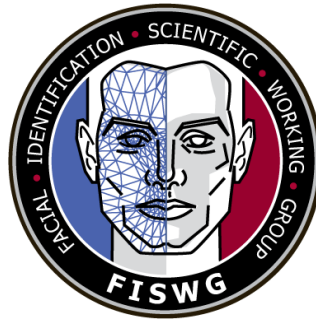
YUV422

A color space standard used by many digital video cameras.

FISWG documents can be found at: www.FISWG.org

{Remainder of page Intentionally left blank}

APPENDIX B



Disclaimer:

As a condition to the use of this document and the information contained herein, the Facial Identification Scientific Working Group (FISWG) requests notification by e-mail before or contemporaneously to the introduction of this document, or any portion thereof, as a marked exhibit offered for or moved into evidence in any judicial, administrative, legislative, or adjudicatory hearing or other proceeding (including discovery proceedings) in the United States or any foreign country. Such notification shall include: 1) the formal name of the proceeding, including docket number or similar identifier; 2) the name and location of the body conducting the hearing or proceeding; and 3) the name, mailing address (if available) and contact information of the party offering or moving the document into evidence. Subsequent to the use of this document in a formal proceeding, it is requested that FISWG be notified as to its use and the outcome of the proceeding. Notifications should be sent to: chair@fiswg.org

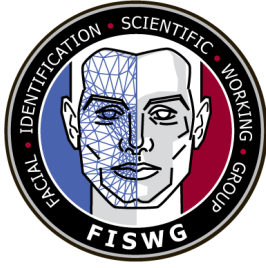
Redistribution Policy:

FISWG grants permission for redistribution and use of all publicly posted documents created by FISWG, provided that the following conditions are met:

Redistributions of documents, or parts of documents, must retain the FISWG cover page containing the disclaimer.

Neither the name of FISWG, nor the names of its contributors, may be used to endorse or promote products derived from its documents.

Any reference or quote from a FISWG document must include the version number (or creation date) of the document and mention if the document is in a draft status.



Minimum Guidelines for Facial Image Comparison Documentation

1. Scope

1.1. The purpose of this document is to provide minimum guidelines and a common baseline of information for facial image comparison documentation.

1.1.1. Documentation refers to any hard copy or electronic material that provides official information or serves as a record. Examples include, but are not limited to, notes, images with markups and annotations, narratives, worksheets, investigative lead or forensic reports, or any combination thereof.

1.2. This document does not discuss methods for how to conduct a facial image comparison, opinion scale(s), or details that may be agency specific.

2. Referenced Documents

2.1 ASTM Standards:¹

E3149 Standard Guide for Facial Image Comparison Feature List for Morphological Analysis

2.2 FISWG Standards:²

FISWG Physical Stability of Facial Features of Adults

FISWG Guide for Role-Based Training in Facial Comparison

FISWG Standard Practice/Guide for Image Processing to Improve Automated Facial Recognition Search Performance

FISWG Facial Comparison Overview and Methodology Guidelines

2.3 OSAC Standards:³

¹ For referenced ASTM standards, visit www.nist.gov/osac/astm-launch-code, or the ASTM website, www.astm.org, or contact ASTM Customer Service at service@astm.org. For Annual Book of ASTM.

² Available from Facial Identification Scientific Working Group (FISWG), <http://www.fiswg.org/documents>.

³ Available from Organization of Scientific Area Committees for Forensic Science (OSAC), <https://www.nist.gov/organization-scientific-area-committees-forensic-science/digitalmultimedia-scientific-area-committee>.

OSAC Standard Framework for Developing Discipline Specific Methodology for ACE-V

3. Terminology

3.1 Definitions:

3.1.1 *forensic report*—a document whose intent it is to provide information to assist a trier of fact (e.g., judge or jury).

3.1.2 *investigative lead report*—a document whose intent it is to provide information to operational personnel to assist them with meeting their objective (e.g., investigator, detective, or analyst).

4. Significance and Use

4.1 Documentation of a facial image comparison is generally performed by practitioners during a review or examination. Assessments are often undocumented due to the nature of the comparison.

4.2 These guidelines should be used as a reference by the practitioner to adequately record the facial image comparison process.

4.3 This document outlines the information needed to provide a clear understanding of the process conducted during a facial image comparison to the recipient.

4.4 The sections below provide recommended minimum guidelines for documentation intended to complement agency specific needs/procedures. These are not mandatory documentation or reporting requirements.

5. Items to Document for a Facial Image Comparison

These items are not presented in order of relative importance or priority.

5.1 Case identifier

5.2 Date received

5.3 Date searched/compared

5.4 Date of image capture (if available)

5.5 Requestor name and contact information

5.6 Relevant case information (if provided)

5.7 Organization conducting examination

5.8 Practitioner(s) name and contact information

5.9 Details and scope of the request (if provided)

5.10 Source of image(s)

5.11 File name/identifier of image(s) received

5.12 Indication of whether a facial recognition (FR) search was conducted and the results

5.13 Database searched, and any image galleries within the database (if relevant)

5.14 Disclaimer – agencies should include their own disclaimer identifying the limitations of the comparison method used and the intended usage of the report

5.15 Reference to comparison method used

5.16 Description of the disposition of both received and processed image(s), and record of storage and retention

6. Analysis

6.1 Determination of image suitability for facial recognition search or facial comparison

6.2 Image analysis documentation, to include, but not limited to, factors such as lighting conditions, image resolutions, obstructions, and pose

6.3 Indicate whether or not images meet agency specific requirements for comparison

6.4 Explanation for determination when images do not meet agency specific requirements

6.5 Processed image(s) (if applicable)

6.6 File name/identifier of processed image(s) (if applicable)

6.7 Steps taken to process image(s) (e.g., cropping, rotating, adjusting exposure)

7. Comparison

7.1 Compare and document features of the face in each image, as defined in the ASTM E3149 Facial Image Comparison Feature List for Morphological Analysis

7.2 Observe and document effects of imaging conditions and physical stability of facial components or component characteristics

7.3 A visual example of the compared facial images as per agency guidelines

8. Evaluation

8.1 Opinion scale used

8.2 Definitions or information and interpretation of what supports an opinion (if applicable)

8.3 Opinion reached with reasoning

9. Verification

9.1 Verification in accordance with agency procedures

10. Additional Information

10.1 In accordance with an agency's data retention policies and quality management systems, additional information should be documented or saved (hardcopy/digital). Examples include:

10.1.1 Written and verbal correspondence (e.g., email, case notes, reports)

10.1.2 Received image(s)

10.1.3 Processed image(s)

10.1.4 Chain of custody

10.1.5 Software, algorithm, tools, or other technology utilized

10.1.5.1 Vendor name(s)

10.1.5.2 Version(s)

10.1.5.3 Specific configuration(s)

10.1.5.4 Date(s) implemented

10.1.5.5 Validation testing (if applicable)

10.1.6 Agency accreditation

10.1.7 Agency comparison method

10.1.8 Agency Standard Operating Procedures (SOP)

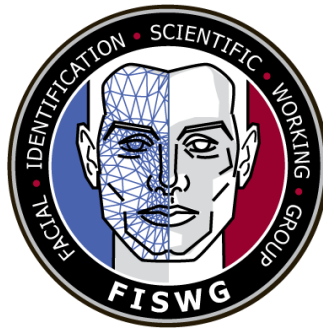
10.1.9 Practitioner qualifications

10.1.10 Training: proficiency and competency testing and results

FISWG documents can be found at: www.fiswg.org

{Remainder of page Intentionally left blank}

APPENDIX C



Disclaimer:

As a condition to the use of this document and the information contained herein, the Facial Identification Scientific Working Group (FISWG) requests notification by email before or contemporaneously to the introduction of this document, or any portion thereof, as a marked exhibit offered for or moved into evidence in any judicial, administrative, legislative, or adjudicatory hearing or other proceeding (including discovery proceedings) in the United States or any foreign country. Such notification shall include: 1) the formal name of the proceeding, including docket number or similar identifier; 2) the name and location of the body conducting the hearing or proceeding; and 3) the name, mailing address (if available) and contact information of the party offering or moving the document into evidence. Subsequent to the use of this document in a formal proceeding, it is requested that FISWG be notified as to its use and the outcome of the proceeding. Notifications should be sent to: chair@fiswg.org

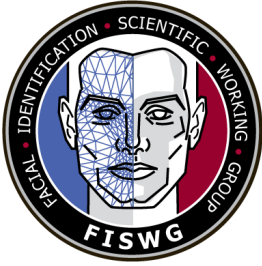
Redistribution Policy:

FISWG grants permission for redistribution and use of all publicly posted documents created by FISWG, provided that the following conditions are met:

Redistributions of documents, or parts of documents, must retain the FISWG cover page containing the disclaimer.

Neither the name of FISWG, nor the names of its contributors, may be used to endorse or promote products derived from its documents.

Any reference or quote from a FISWG document must include the version number (or creation date) of the document and mention if the document is in a draft status.



Standard Guide for Image Processing to Improve Facial Recognition Search Performance

1. Scope

1.1 The purpose of this document is to provide guidelines for processing a probe image in order to increase the likelihood that a potential candidate will be included among the search result set returned following a facial recognition system (FRS) search.

1.1.1 This process is not suitable for developing source opinions regarding an image.

1.1.2 The guideline does not address the necessary steps and processes for that type of examination.

2. Referenced Documents

2.1 ASTM Standards:

E2916 Terminology for Digital and Multimedia Evidence Examination¹

E2825 Standard Guide for Forensic Digital Image Processing

2.2 Other Standards:

ANSI/NIST-ITL-1-2011 Data Format for the Interchange of Fingerprint, Facial & Other Biometric Information²

FISWG Facial Recognition Systems Metadata Usage³

¹ For referenced ASTM standards, visit the ASTM website, www.astm.org, or contact ASTM Customer Service at service@astm.org. For Annual Book of ASTM Standards volume information, refer to the standard's Document Summary page on the ASTM website.

² For referenced ANSI/NIST documents, visit <https://www.nist.gov/programs-projects/ansinist-itl-standard>

³ For referenced FISWG documents, visit <https://fiswg.org/documents.html>

3. Terminology

3.1 Definitions:

3.1.1 *Lossy compression, n*—data reduction process that is not completely reversible, and some original data is irretrievably lost.

3.1.2 *Lossless compression, n*—a data reduction process that is completely reversible, such that all of the original data can be retrieved in the original form.

3.1.3 *Pixel aspect ratio, n*—the ratio of the width to the height of a rectangle, such as an image, a pixel, or an active video frame.

3.2 Acronyms:

3.2.1 *FRS, n*—Facial Recognition Systems

4. Summary of Guide

4.1 The image processing steps presented in this document are limited to the manual processing of images intended to be submitted as probe images for FRS searches. Internal image processing applied by the FRS and issues associated with still image extraction from video, scanning of printed imagery, and the use of forensic sketches, reconstructions, and composites are beyond the scope of this document.

5. Significance and Use

5.1 Introduction

5.1.1 Images that meet agreed upon international standards (such as ISO/IEC 19794-5: Face Image Data⁴) can normally be submitted to an FRS for searching with little or no operator intervention. Many FRS also include intrinsic mechanisms for correcting minor deviations in subject pose, image size, or vendor specific adjustments to the image. Manual processing may be beneficial for sub-optimal images (e.g. low resolution, heavily compressed or where the subject's pose, illumination, or expression is non-neutral). The image processing techniques presented in this document may be applied over an entire image or in localized areas of an image.

5.1.2 The image processing topics presented in this document are not intended to override recommendations for maintaining the quality of images intended for one-to-one comparison. These processes specifically apply to the preparation of a facial image for the purpose of submitting it as a probe into an automated FRS search to maximize the

⁴ Available from <https://www.iso.org/standard/38749.html>

likelihood that a potential candidate will be returned in the search result set. These processes are not to be used for identification purposes.

5.2 Important Notes

5.2.1 The goal of any image processing should be to optimize the image for searching by the FRS, not to create an aesthetically pleasing image. An image that looks 'good' is not necessarily the same as one that is optimized for use by an FRS due to image processing done within the vendor specific algorithms.

5.2.2 The effect of any manual image processing will vary with different FRS and in some cases may degrade performance rather than improve it.

5.2.3 Image processing to the probe image before an FRS search is different from the operational processes performed for the purpose of a one-to-one manual comparison.

5.2.4 Any decision regarding whether or not a candidate returned from an FRS search is from a possible common source as the subject in the probe image must be made based on a comparison with the original (unedited) image and NOT the processed image.

5.2.5 Agency specific or mandated notes and audit trails shall be done at all times. Document and preserve processed images regardless of search results.

5.2.6 The following sections of this document describe a series of steps with varying complexity for the manual processing of probe images of less-than-optimal quality for an FRS. They are intended to maximize the likelihood of returning a potential candidate from a search result set while minimizing the amount of processing of the probe image. The guidelines presented in this document may be adapted for agency specific policies and standard operating procedures.

6. Image File Management

6.1 **Initial Steps** – The initial steps for the management of probe imagery include, but are not limited to, the following:

6.1.1 Save original

6.1.1.1 The original untouched probe image should be kept in all cases. A read-only copy shall be made of the original probe image(s). No enhancements or modifications shall be made to these original probe image(s). When making any final comparisons, always use a working copy of the original probe image(s).

6.1.2 Make lossless working copies

6.1.2.1 All image processing steps should be done using a lossless file format.

6.1.2.2 Understanding the compatibility of image file formats for an FRS is critical because the original image(s) may be received in a variety of file formats. If a probe image is not in an FRS compatible format, follow the vendor's recommendations for conversion to a supported compatible format. This conversion (if needed) should be done as a last step from the lossless images being processed, prior to searching.

6.2 Generalize Search Steps – For the purpose of this document, “pass” refers to an assumption that following each progression of image processing, an FRS search will take place, and the resulting candidates will be assessed. It may not be prudent to run the probe image through an FRS search until it has been processed to a certain degree. In all examples of “passes” presented in this document it is assumed that for every sequential “pass”, the following steps shall be undertaken in every FRS search of a probe image. See Figure 1 below: **Simplified Image Processing Flow Chart**.

6.2.1 Verify eyes can be found.

6.2.1.1 This step can also be described as “localizing the face in the image”. This is critical to determine if the facial imagery utilized has limitations or systemic image conditions, which may cause a problem when submitting to the proprietary technology within an FRS.

6.2.2 Save interim image sets

6.2.2.1 All processed images used for searching shall be saved according to agency policy. Searching images with different enhancements (e.g., cropped, black and white, or grayscale) may result in different candidate sets.

6.2.3 Search and review results

6.2.3.1 FRS results shall be compared against the original probe image(s). If no potential candidates are returned in the search result set, the recommendation is to re-evaluate the image that was used in searching and apply further processing.

6.2.4 If available within the FRS, consider using metadata binning.

6.2.4.1 The FISWG document ***Facial Recognition Systems Metadata Usage***⁵ should be referenced where metadata is accessible which refines searches through reducing the logical size of the search database.

⁵ Available from: <https://www.fiswg.org/documents.html>

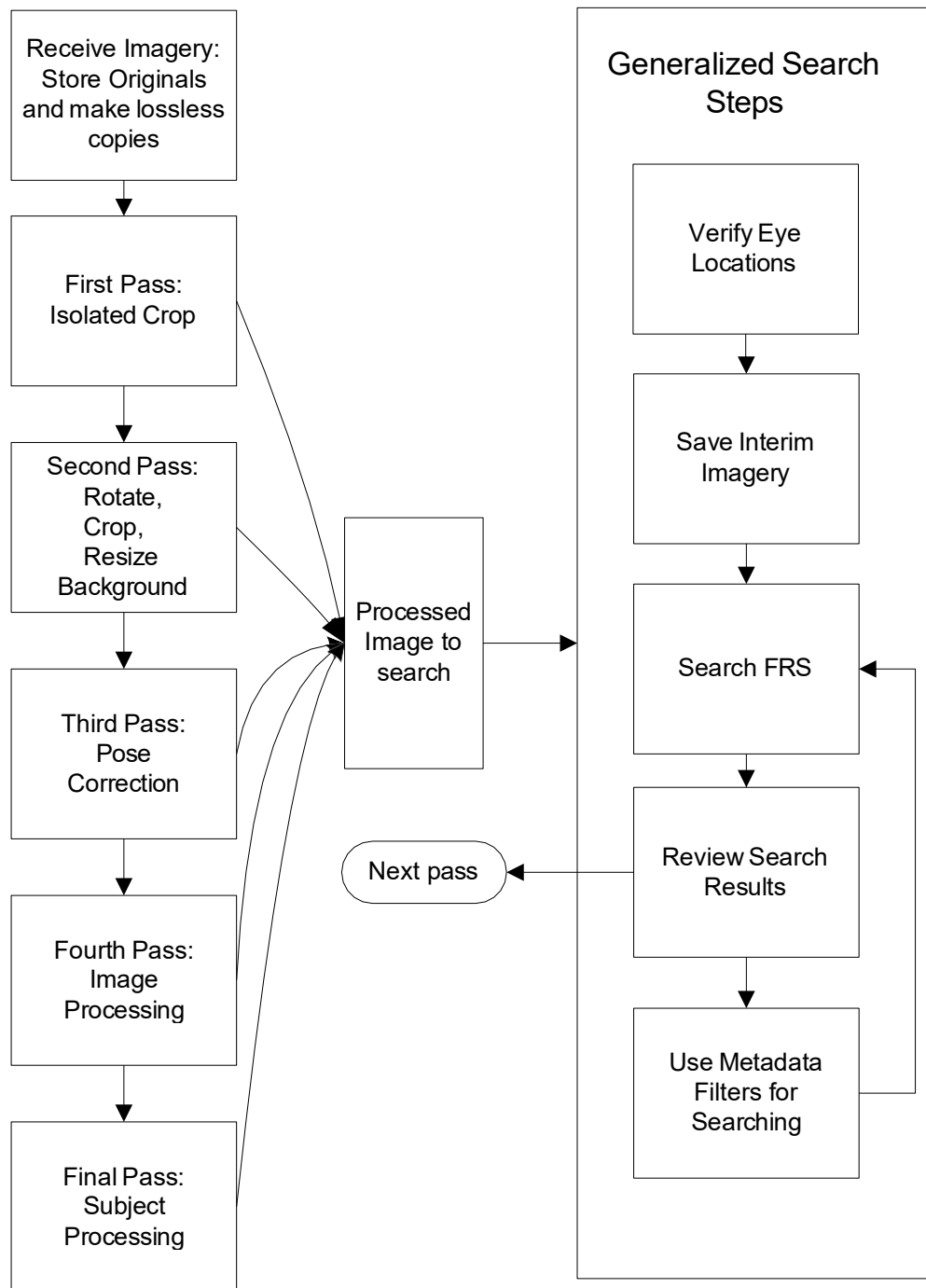


Figure 1: Simplified Image Processing Flow Chart

7. First Pass: Isolated Crop

7.1 The first pass should be initiated with the original image. The relevant face(s) should be cropped, if not undertaken automatically by the FRS. When cropping, ensure that the aspect ratio is maintained and aim to produce an image that is in accordance with ANSI/NIST- ITL-1-2011 or ISO specifications.

8. Second Pass: Rotate, Crop, Resize, Background

8.1 The second pass would be initiated when no potential candidates are found during the First Pass or when the nature of the image warrants minimal processing to yield additional candidates.

8.2 The second pass may include the tasks below, all of which are not necessarily required; however, if more than one is applied, they should be performed one at a time. When processing images, care should be taken to not remove or alter portions of the subject's head (e.g. portions of the ear, crown of the head, or portions of the neck).

8.3 Rotate – The image may be rotated around the roll axis to make the eye positions appear horizontally aligned.

8.4 Secondary Crop – The image processing steps done in this pass may require a secondary crop of the image. The goal of this crop is to produce an image that is more in accordance with the ANSI/NIST- ITL-1-2011 or ISO specifications.

8.5 Resize – Modify the size of the image to achieve a recommended interpupillary distance. This distance should be agency defined and based on FRS vendor recommendations (e.g. 90 pixels). Resizing of the images should be done in even multiples of the original image size while preserving the original image aspect ratio. For example: 90x120 pixels to 180x240 pixels to 270x360 pixels, etc.

8.6 Blur background – This is performed where the probe image has a non-neutral or busy background. The blurring process creates a consistent background preventing an FR engine from detecting items in the background. Examples include:

8.6.1 Surveillance photo with people or items in background.

8.6.2 An image captured with a background that varies in color and content.

8.7 Horizontal flip – This should be utilized if the probe image submitted may have been taken as a reflection, captured incorrectly, or been flipped left/right or right/left in transmission.

8.8 Aspect ratio correction – Mitigates the impact of an image that looks unnaturally stretched in the horizontal or vertical direction.

9. Third Pass: Pose Correction

9.1 Some legacy FRS algorithms have varying sensitivities to non-frontal facial imagery. Claims of performance degradations will vary, but it is broadly accepted that any non-frontal pose movements could negatively affect FRS performance. If the FRS algorithm has been tested and is proven to be pose invariant, then this step may not be needed. Check with the facial algorithm provider to verify this.

9.2 The standard definitions of pose angles are defined in: **NIST Special Publication 500-290 Edition 3 (2015)** and **ANSI/NIST-ITL 1-2011 Update: 2015 Data Format for the Interchange of Fingerprint, Facial, & Other Biometric Information**⁶ as referenced in Figure 2:

The Yaw and Roll angles shall be measured from the full-face pose position and have a range of values from -180 degrees to +180 degrees. The Pitch angle shall have a range of values from -90 degrees to +90 degrees. The pose angle set is given by Tait-Bryan angles as shown in Figure 26.

ANSI/NIST-ITL 1-2011: UPDATE 2015

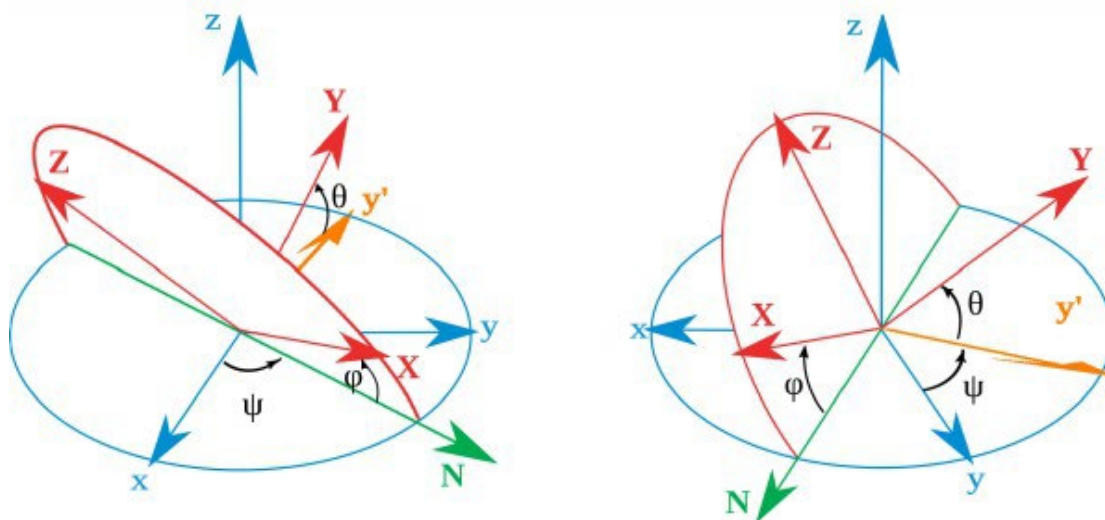


Figure 26: Tait-Bryan angles statically defined with the Z-X'-Y'' convention

⁶ Available from: <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.500-290e3.pdf>

The angles are defined relative to the frontal view of the subject, which has angles (0, 0, 0). Examples are shown in Figure 27.

Yaw angle: rotation about the vertical (y) axis. A positive Yaw angle is used to express the angular offset as the subject rotates from a full-face pose to his or her left (approaching a right profile). A negative Yaw angle is used to express the angular offset as the subject rotates from a full-face pose to his or her right (approaching a left profile).

Roll angle: rotation about the horizontal side-to-side (z) axis.

Pitch angle: rotation about the horizontal back to front (x) axis.

ANSI/NIST-ITL 1-2011: UPDATE 2015

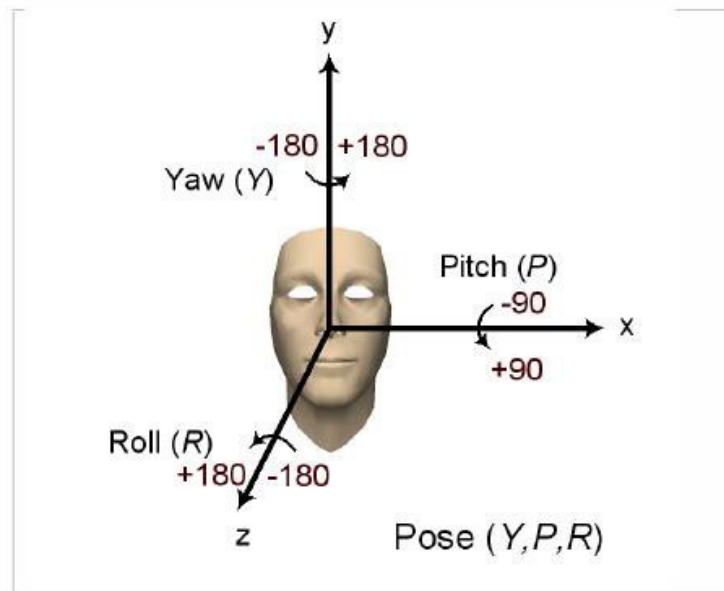


Figure 27: Pose angle set is with respect to the frontal view of the subject

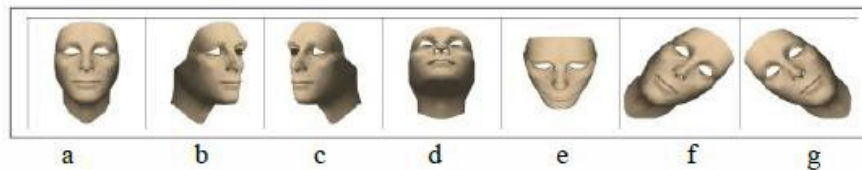


Figure 28: Examples of pose angles and their encodings.

The pose angles (Y, P, R) of (a) – (g) in Figure 28 are given by (0, 0, 0), (+45, 0, 0), (-45, 0, 0), (0, -45, 0), (0, +45, 0), (0, 0, -45), and (0, 0, +45), respectively.

The uncertainty in the pose angles is given by the range 0 to 90, inclusive. It shall denote approximately a maximum value of possible deviation in the measurement of the pose. This shall correspond to a two standard deviation confidence interval.

The encoding of angles is in ASCII format, with the minus sign “-” used to denote a negative value and the plus “+” sign optionally used to denote a positive value. Pose angle uncertainty angles are always positive.

Figure 2: NIST Special Publication 500-290 Edition 3 (2015)

9.3 Software for pose correction is dependent on policy or vendor recommendations. Any pose which varies more than 10 degrees in any direction from (0, 0, 0) could be considered a candidate for pose correction.

9.4 When pose correction is done, consideration shall be given to the following areas:

9.4.1 If available, select the proper gender and race.

9.4.2 Select any symmetric fill option.

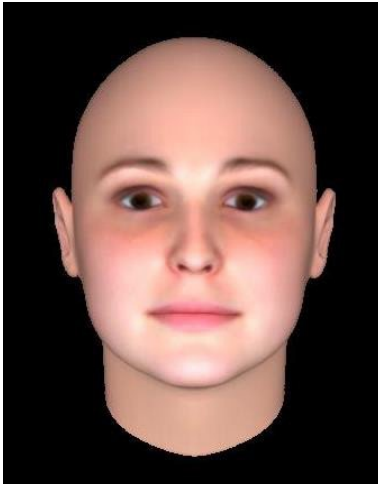
9.4.3 Place appropriate facial landmarks as needed.

9.4.4 Select the number of poses to generate.

9.4.4.1 Frontal

9.4.4.2 Slight left and right pose (e.g., +/- 15 degrees yaw)

9.4.4.3 Slight up and down pose (e.g., +/- 15 degrees pitch)

Pose	Example Image	Pose	Example Image
Original Image		Pose corrected frontal	

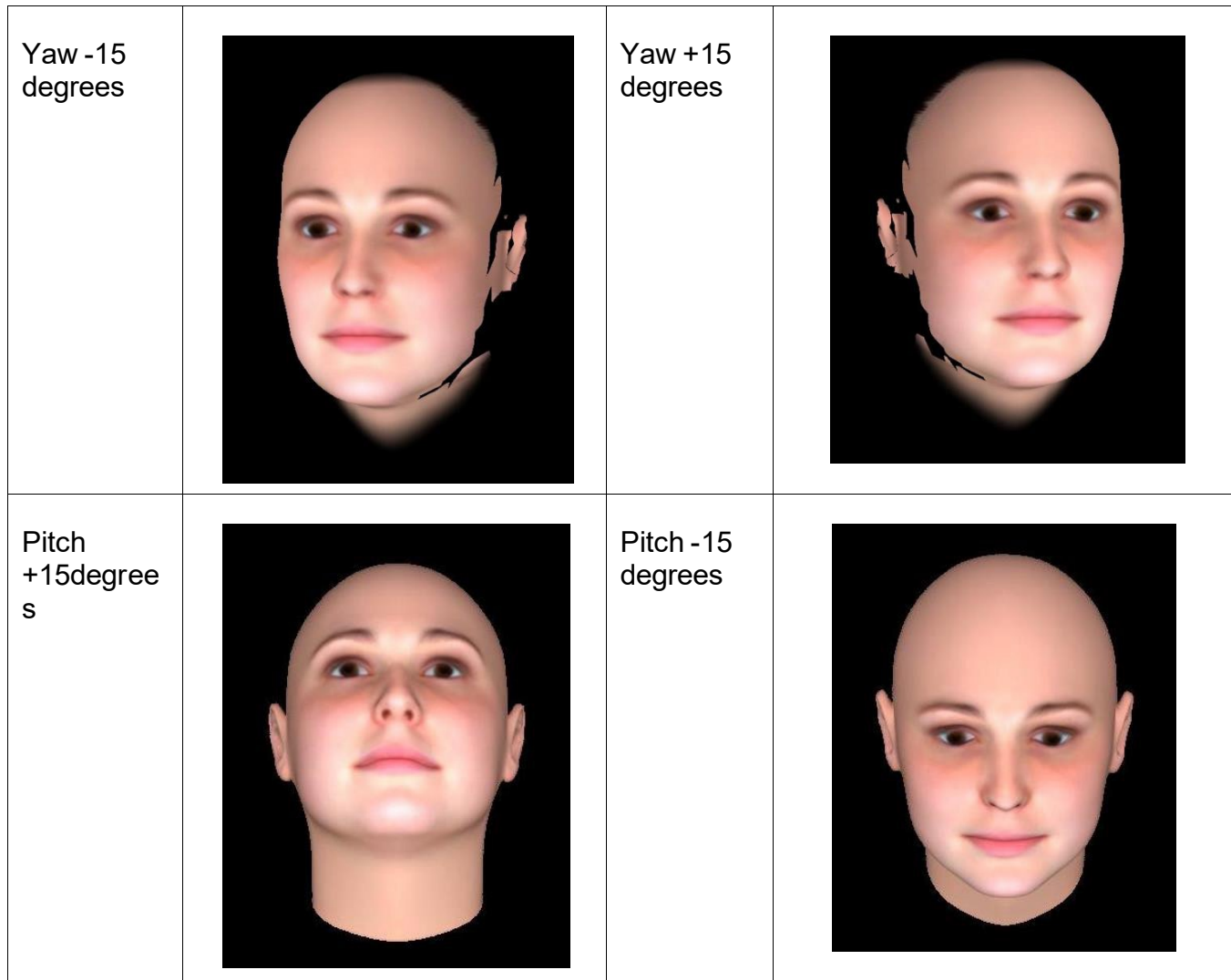


Figure 3: Pose Examples

9.4.5 When multiple poses are generated, searching each pose as individual probe images within unique searches may allow for pose variations within the gallery. Some FRS supplied search clients allow group searching where groups of related imagery can be searched and reviewed in bulk.

10. Fourth Pass: Image Processing

10.1 During the Fourth Pass, image processing may be applied to a working copy of the original image or an image resulting from any of the previous passes to attempt to produce a different candidate search result set.

10.2 Image processing may be performed externally of the FRS using widely available image editors (e.g. Adobe Photoshop and GNU Image Manipulation Program [GIMP]) with the resulting probe image being submitted for an FRS search. The image processing listed below may be applied to the entire image or to selected regions within the image and may include, but are not limited to:

10.2.1 Histogram equalization

10.2.2 Color/tint corrections

10.2.3 De-blurring or sharpening

10.2.4 Lens distortion correction

10.2.4.1 Some images, such as those from smart phones, automated teller machines (ATM's) and Body Worn Video cameras that use wide-angle lenses typically exhibit perspective ('barrel') distortion. Image processing software or manufacturers' provided lens correction data should be used to correct this prior to searching.

10.2.5 Grayscale conversion

10.2.6 Noise reduction

10.2.7 Brightness or contrast adjustment

10.2.8 Red eye reduction

11. Advanced Topic: Subject Processing

11.1 After previous passes have been completed (or rejected due to the nature of the image) additional processing steps targeted at the subject in the image may be used.

11.2 This type of processing may introduce external elements to the subject in the image. Agency procedures shall be followed to determine whether these measures can be applied to improve the likelihood of locating a potential candidate from an image returned in the candidate search result set from an FRS search.

11.3 Circumstances warranting this type of image processing include, but are not limited to, the following:

11.3.1 Facial landmarks obstructed by head coverings, accessories (e.g., jewelry or eyewear), hair, image artifacts, etc.,

11.3.2 Missing or obstructed facial landmarks due to extreme pose or expression (including closed eyes),

11.3.3 Intentional alterations of the subject's face (e.g., excessive make-up), or

11.3.4 Trauma (e.g., lacerations, blood, bruising), evidence of medical intervention (e.g., bandages, endotracheal tube, neck brace), or postmortem.

11.4 Examples of subject image processing include, but are not limited to, the following:

11.4.1 Replace or create missing facial landmarks on the subject.

11.4.2 Mirroring the probe image on the center line of the half face.

FISWG documents can be found at: www.fiswg.org

Appendix D

Receipt of IIFC Privacy Policy **By IIFC and Non-IIFC Personnel**

My signature below indicates that I have been provided a copy, have read it, and that I understand the Indiana Intelligence Fusion Center Privacy Policy. I understand that the Privacy Policy applies to me and that its violation may serve as a basis for disciplinary action, up to and including dismissal.

Signature: _____

Printed Name: _____

Date Signed: _____