SWGDE Guidelines for Forensic Image Analysis

Disclaimer:
As a condition to the use of this document and the information contained therein, the SWGDE requests notification by e-mail before or contemporaneous 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; 3) subsequent to the use of this document in a formal proceeding please notify SWGDE as to its use and outcome; 4) the name, mailing address (if available) and contact information of the party offering or moving the document into evidence. Notifications should be sent to secretary@swgde.org.

It is the reader's responsibility to ensure they have the most current version of this document. It is recommended that previous versions be archived.

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

1. Redistribution of documents or parts of documents must retain the SWGDE cover page containing the disclaimer.
2. Neither the name of SWGDE nor the names of contributors may be used to endorse or promote products derived from its documents.
3. Any reference or quote from a SWGDE document must include the version number (or create date) of the document and mention if the document is in a draft status.

Requests for Modification:
SWGDE encourages stakeholder participation in the preparation of documents. Suggestions for modifications are welcome and must be forwarded to the Secretary in writing at secretary@swgde.org. The following information is required as a part of the response:

a) Submitter's name
b) Affiliation (agency/organization)
c) Address
d) Telephone number and email address
e) Document title and version number
f) Change from (note document section number)
g) Change to (provide suggested text where appropriate; comments not including suggested text will not be considered)
h) Basis for change

Intellectual Property:
Unauthorized use of the SWGDE logo or documents without written permission from SWGDE is a violation of our intellectual property rights.

Individuals may not misstate and/or over represent duties and responsibilities of SWGDE work. This includes claiming oneself as a contributing member without actively participating in SWGDE meetings; claiming oneself as an officer of SWGDE without serving as such; claiming sole authorship of a document; use the SWGDE logo on any material and/or curriculum vitae.

Any mention of specific products within SWGDE documents is for informational purposes only; it does not imply a recommendation or endorsement by SWGDE.

SWGDE Guidelines for Forensic Image Analysis

Table of Contents

1. Objective 4
2. SWGDE Position on Forensic Image Analysis 4
3. Introduction 4
4. Forensic Image Analysis – General Tasks 4
4.1 Technical Preparation 4
4.2 Examination 4
4.3 Interpretation 5
5. Forensic Image Analysis – Specific Areas of Analysis 5
5.1 Photogrammetry 5
5.2 Photographic Comparisons 6
5.3 Content Analysis 7
5.4 Image Authentication 8
6. Best Practices 8
6.1 Evidence Management 8
6.2 Quality Control and Quality Assurance 8
6.3 Security 8
6.4 Documentation 9
6.5 Training, Competency, and Proficiency 9
6.6 Standard Operating Procedures (SOPs) 9
6.7 Work Flow 10

1. Objective

(Note: This document is an update to the version previously released as SWGIT Section 12 – Best Practices for Forensic Image Analysis.)

The objective of this document is to provide personnel with guidance regarding practices appropriate when performing a variety of analytic tasks involving images, regardless of the knowledge domain that is the subject of analysis.

2. SWGDE Position on Forensic Image Analysis

Forensic image analysis is a forensic science. It has been practiced since the early days of photography, dating at least to 1851 when Marcus A. Root conducted the first documented example of Forensic Image Authentication. Through microscopic examination, Root revealed that the color daguerreotype “process” promoted by Reverend Levi Hill was actually the product of hand coloring, not a breakthrough in photographic science (Davis, Photography, Brown & Benchmark, 1995). In addition to being an accepted scientific practice in the forensic community, image analysis is also recognized in other disciplines including medicine, intelligence, geology, astronomy, agriculture, and others.

3. Introduction

Forensic Image Analysis is the application of image science and domain expertise to interpret the content of an image and/or the image itself in legal matters. Major sub-disciplines of Forensic Image Analysis with law enforcement applications include: Photogrammetry, Photographic Comparison, Content Analysis, and Image Authentication.

The process of Forensic Image Analysis can involve several different tasks, regardless of the type of image analysis performed. These tasks fall into three categories: Technical Preparation, Examination, and Interpretation. These tasks are described below. The general principles and procedures used in these tasks are the same regardless of the format or media in which the images are recorded. For the purposes of this document, the word “image” refers to an imitation or representation of a subject or object derived from still photography or video.

4. Forensic Image Analysis – General Tasks

4.1 Technical Preparation

Technical preparation is the performance of preliminary evidence related tasks such as, calibration, function checking, creating working copies, or output. Note that there is a wide gamut of technical decision making within the various responsibilities covered by technical preparation actions.

4.2 Examination

Examination is the application of image science expertise to the extraction of information from images, the characterization of image features, and the interpretation of image structure. Examples include, but are not limited to: compression effects, metadata collection, feature detection, extraction of Photo Response Non-Uniformity signature, image alteration evaluation, and the development of case-specific image exploration strategies. Image enhancement, image restoration, and other image processing activities intended to improve the visual appearance of features in an image are examination tasks.

4.3 Interpretation

Interpretation, as used here, is the application of specific subject matter expertise to draw conclusions about subjects or objects depicted in images. Examples include, but are not limited to: patterned injury analysis, source determination, object classification, mensuration, determination of the presence of computer-generated imagery, or a military expert drawing conclusions about content of aerial surveillance images.

Note: *Technical Preparation, Examination, and Interpretation are tasks, not job descriptions, or roles. An individual may perform part of one task or a combination of multiple tasks within the organizational structure of any given activity. Each of these tasks requires its own training and qualification.*

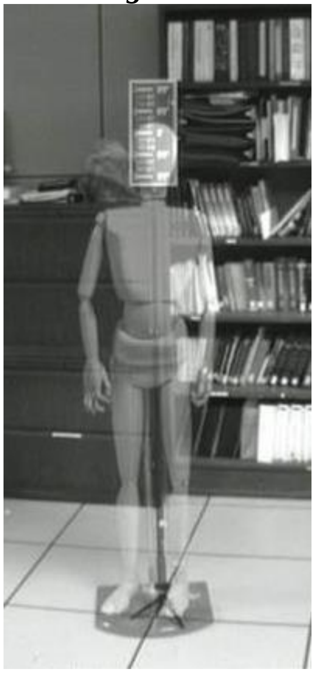
5. Forensic Image Analysis – Specific Areas of Analysis

5.1 Photogrammetry

"Photogrammetry is the art, science, and technology of obtaining reliable information about physical objects and the environment through the processes of recording, measuring, and interpreting photographic images and patterns of electromagnetic radiant energy and other phenomena." [As ng]. In forensic applications, photogrammetry (sometimes called "mensuration") most commonly is used to extract dimensional information from images, such as the height of subjects depicted in surveillance images and accident scene reconstruction. Other forensic photogrammetric applications include velocity determination, visibility, and spectral analyses.

Figure 1 illustrates an example of a photogrammetric analysis (Reverse Projection) conducted to determine the height of a subject depicted in a surveillance photograph.

Figure 1.



5.2 Photographic Comparisons

Photographic comparison is the process of comparing object(s) or person(s) when at least one of the items in question is captured in imagery, and making an assessment of the correspondence between features of the captured imagery for rendering an opinion regarding identification or elimination (as opposed to a demonstrative exhibit). Examples of photographic comparisons include, but are not limited to:

- A facial comparison between an unknown subject depicted in a surveillance image with an identified suspect; (see www.FISWG.org for more information)
- The comparison of objects such as vehicles depicted in surveillance images with those recovered in an investigation;

Photographic comparisons are frequently referred to as "side-by-side" comparisons since they usually involve a comparison of class and individualizing characteristics in imagery. The scientific basis and technical processes involved in photographic comparisons are comparable to those used in other forensic disciplines such as fingerprint analysis. Any methodology applied to photographic comparison should incorporate an analysis of the imagery, a comparison of individual features, an evaluation of the significance of the comparison, and a verification of the comparison. The repeatability of the procedure and documentation of the workflow is of paramount importance. Statistical analysis, if attainable, may be used as a component of evaluation, but is not required.

Figure 2 illustrates demonstrative exhibits from a facial comparison exam, with extremely strong support for the proposition that the subject is the same person in both images.

Figure 2.

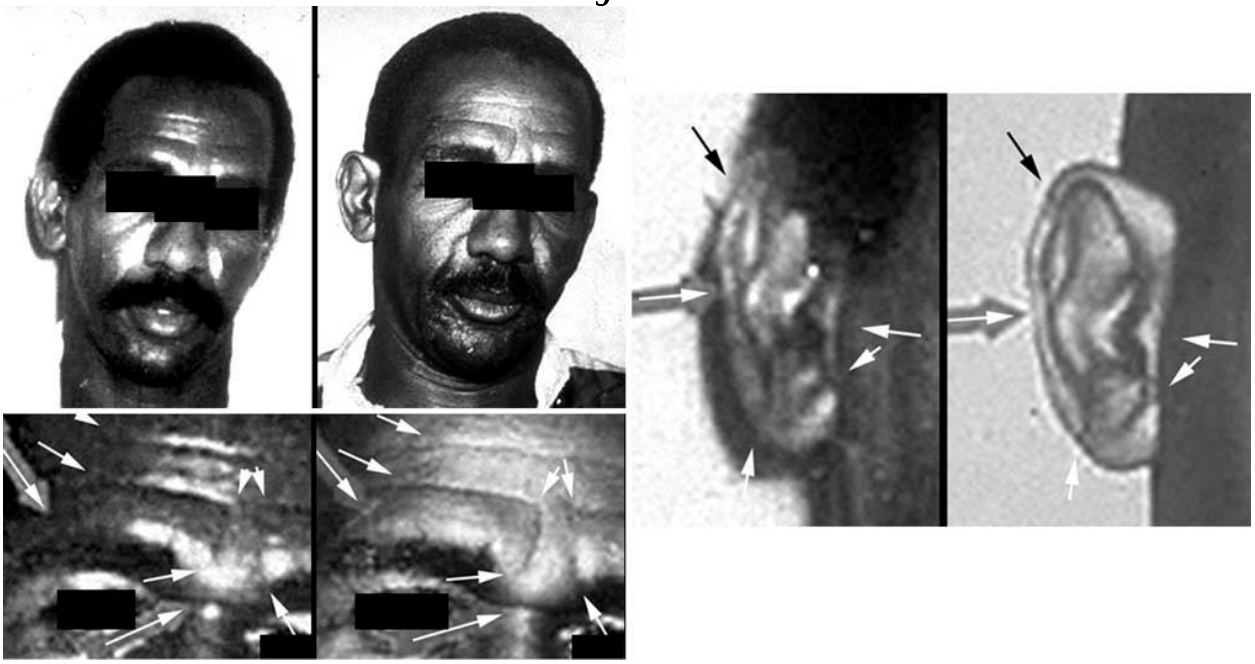
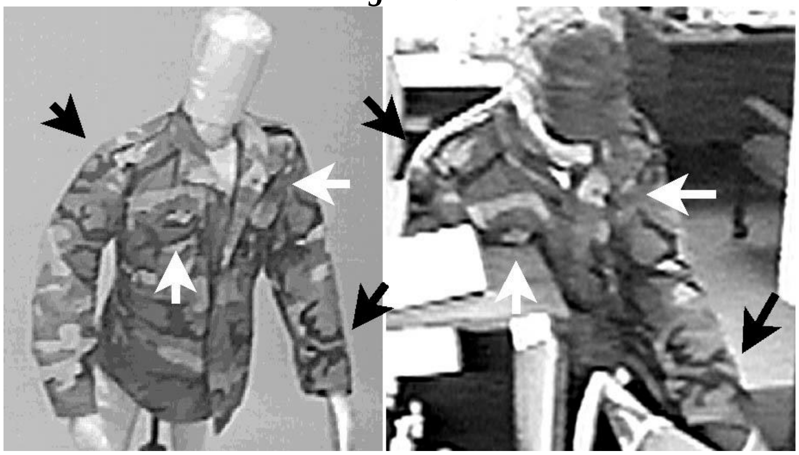


Figure 3 illustrates a demonstrative exhibit from a clothing comparison examination, with extremely strong support for the proposition that the camouflage jacket is the same one in both images.

Figure 3.



5.3 Content Analysis

Content analysis, within the context of forensic image analysis, is the drawing of conclusions about an image. Targets for content analysis include, but are not limited to:

- the conditions under which, or the process by which, the image was captured or created;
- the physical aspects of the scene, including events captured;
- the classification of an object within an image; and/or

- the location or setting of the image content.

Examples include but are not limited to: vehicle make model determinations, license plate interpretation, image orientation, determining the presence or absence of specific objects, and logo determination.

5.4 Image Authentication

Image Authentication is the process of substantiation that the data is an accurate representation of what it purports to be. Authentication can be performed by the person harvesting the data through first-hand knowledge, or by an examiner in the lab.

The criteria for image authentication usually involve the interpretability of the data, and not simple format changes that do not alter the meaning or content of the data.

Examples include:

- Determining the degradation of a transmitted image;
- Determining whether a video is an original recording or an edited version;
- Evaluating the degree of information loss in an image saved using lossy compression.
- Determining whether an image contains feature-based modifications such as the addition or removal of elements in the image (e.g., adding bruises to a face).

This varies from integrity verification which is the process of confirming that the data presented is complete and unaltered since the time of acquisition. Integrity can be as simple as using a chain of custody, utilizing evidence preservation techniques, and/or generating hash values.

6. Best Practices

The following are guidelines that describe the SWGDE recommended best practices for the performance of forensic image analysis.

6.1 Evidence Management

Agencies should have documented procedures for the handling, transportation, and storage and documentation of evidence (chain of custody) to assure the integrity of the data.

6.2 Quality Control and Quality Assurance

Quality control and quality assurance policies and procedures should be implemented and documented. Technical and Administrative reviews are integral components of quality control.

6.3 Security

There should be procedures in place to maintain the security of the working data, all notes, and other such analysis-related materials to provide the level of security and privacy needed by the organization. For example, archived case-related materials should be stored in a manner that limits access. The degree of access will be agency- specific.

6.4 Documentation

The application of analytic techniques in a given case should be recorded to the degree that a similarly trained professional would reach a comparable analytical conclusion.

Agencies should establish standards for information included in, and the format for, reporting results.

The practitioner should also have available documentation that describes and justifies the use of any method involved in the analysis. Such documentation can include peer-reviewed journal articles, scientific conference proceedings, reference books, internal white papers, or the results of empirical studies.

6.5 Training, Competency, and Proficiency

Agencies employing image analysts should follow *SWGDE/SWGIT Guidelines & Recommendations for Training in Digital & Multimedia Evidence* and *SWGDE Proficiency Test Guidelines*.

Certification is one method to evaluate personnel. Certifications can be comprehensive, tool-based, or topic specific, and can be an additional tool in verifying technical skills and abilities. Comprehensive certifications generally require training be completed, as well as a specified amount of experience in the discipline, and the successful completion of an examination. Certifications can be beneficial and should be considered when appropriate and available.

Analysts should demonstrate competency in their discipline prior to being assigned unsupervised case work responsibilities. In addition, analysts should demonstrate proficiency and maintain continuing education activities. Agencies should document competency, proficiency, and continuing education of each analyst.

The practitioner should demonstrate:

- understanding of the scope of work and how it will be applied in the forensic environment;
- subject matter knowledge and competence;
- working knowledge of the potential image processing and evaluation techniques;
- working knowledge of applications and tools utilized in the specific agency;
- working knowledge of SWGDE guidelines for capturing, storing, and processing of imagery, including issues relating to topics such as data integrity and compression artifacts;
- understanding of legal precedent for the use of specific image processing techniques;
- knowledge of the techniques necessary to document the conclusions.

6.6 Standard Operating Procedures (SOPs)

There should be Standard Operating Procedures (SOPs) for the tasks being performed. These SOPs should reflect the work flow and be general enough to permit flexibility for the required tasks.

6.7 Work Flow

The following describes a generalized sequence of actions involved in the analysis of an image and recommendations for their performance. The exact sequence will be agency specific.

1. Review of request for analysis.
   a. The agency must confirm that it performs the requested analysis.
   b. The agency must ensure the requestor has submitted all items needed to support the requested analysis or examination. Note: In some cases, it may be necessary for the agency to obtain additional items or information before analysis can be completed.
   c. The agency must confirm that it has the necessary equipment, materials, and resources needed to conduct the requested analysis.
   d. The agency must assign the analysis request to the appropriate personnel.
2. Acquisition of imagery.

   This is the implementation of the acquisition strategy determined in the initial assessment. It produces the image for the steps that follow. Often, analysis or examination may be performed on objects directly or on analog images. The primary or original image should be archived in a manner that permits verification. The image acquisition step is where the integrity of the primary or original data is initially established. Most often, subsequent steps are performed utilizing working copies, but in all cases, the integrity of the primary or original image(s) must be maintained.

   a. If possible, the original or primary image, or a bit-for-bit duplicate, should be available for analysis.
   b. Triage imagery
      i. The practitioner must determine if the submitted material is suitable for analysis.
      ii. The practitioner must determine if all of the submitted material, or only a subset of the material, is to be subjected to analysis.
3. Production of Working Copies.

   Produce working copies of images to be subjected to analysis. This may require conversion from other media.
4. Processing of Images to be Analyzed.

   *(**Note:** Guidance relating to forensic image processing and case-specific documentation requirements for forensic image processing can be found in the following documents: SWGDE Image Processing Guidelines and SWGIT Section 11 – Best Practices for Documenting Image Enhancement).*

   a. Design an image processing strategy. This is the application of domain knowledge to choose which processes to apply to the image to extract the information necessary for drawing a conclusion. The strategy should be justifiable. No single processing strategy is appropriate for all cases. This should be reflected in the organizational SOPs.

b. Identify the appropriate tools to implement the strategy. There should be some references/documentation that the selected tools are capable of implementing the strategy.

c. Implement the designed image processing strategy.

d. Assess results. Determine that the image processing strategy yielded results suitable for analysis.

    i. If the results are suitable for analysis, then proceed to the analysis (5). Otherwise, repeat process of designing an image processing strategy until suitable results are achieved (4a).

    Note: *Exploratory strategies that are not incorporated into the final work flow pathway need not be documented in case notes. Agencies may wish to document this fact in their SOPs.*

5. Analyze processed data.

    a. Determine if criteria necessary for reaching a conclusion are present in the processed image.

        i. Specific criteria for reaching a conclusion should be identified and documented.

        ii. In some cases, the criteria will reflect the subjective experience of the practitioner. Such conclusions should undergo an appropriate technical review.

    b. Reach conclusion.

6. Report Conclusions.

    a. The basis for, and uncertainty of, any conclusion should be reflected in the reporting.

    b. When a statistical basis for a conclusion can be made based on validated probability models, the conclusion should be quantitatively reported. It may be possible to provide bounds on probabilities based on incomplete knowledge.

    c. When statistical criteria do not exist, the conclusion should be reported in terms of the kind of features discerned. If no appropriate statistical model is available, a clear indication of the strength of a conclusion should be reported. This will necessarily be a descriptive statement and not a numerical probability. Care should be taken to avoid implying probability where none exists.

    d. The report format and contents should follow agency standards.

SWGDE Guidelines for Forensic Image Analysis

History

Revision	Issue Date	Section	History
1.0 DRAFT	2016-09-15	All	Initial draft created by updating *SWGIT Section 12 – Best Practices for Forensic Image Analysis*. SWGDE voted to release as a Draft for Public Comment.
1.0 DRAFT	2016-11-07	All	Formatted and technical edit performed for release as a Draft for Public Comment.
1.0	2017-01-12	None	Following period of Public Comment, no feedback was received and no edits were made. SWGDE voted to publish as an Approved document (Version 1.0).
1.0	2017-02-21	Formatting	Formatted and published as Approved Version 1.0.