Scientific Working Group on Digital Evidence

SWGDE Best Practices for Image Authentication

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 Best Practices for Image Authentication

Table of Contents

1. Purpose

The purpose of this document is to provide best practices for forensic practitioners when examining images for authentication. For the purposes of this document, "imagery" can refer to a series of images depicting the same subject or a video.

2. Scope

This document provides basic information and best practices on the evidentiary value, methodology, range of conclusions, and limitations when conducting image authentication as a part of image analysis. The intended audience is examiners in a lab setting.

Image authentication is used to determine whether the imagery is a true and accurate representation of subjects and events. Similarly, image authentication does not answer specific questions about the subject(s), object(s), or event(s) within an image, such as "Is a specific object present?" "What happened?" or "Where is the scene depicted?" These are all examples of questions answered through image content analysis.

Image authentication must not be confused with the requirement to demonstrate the integrity of the evidence as a precondition to admissibility in court. Integrity ensures that the information presented is complete and unaltered from the time of acquisition until its final disposition. For example, the use of a hash function can verify that a copy of a digital image file is identical to the file from which it was copied, but it cannot demonstrate the veracity of the scene depicted in the image.

Image authentication and image content analysis may be performed in conjunction, depending on the use of the imagery.

3. Definitions

Image Authentication **–** The application of image science and domain expertise to discern if a questioned image or video is an accurate representation of the original data by some defined criteria, and/or the determination of the original source of the image.

Image Content **–** Visual information within an image, such as, subjects/objects, artifacts (due to compression and/or capture), and physical aspects of the scene.

Image Structure **–** Non-visual information about the image itself, such as, file type, file compression, metadata, or the origin of the image.

Manipulate **–** To alter the visual appearance of an image or specific features within an image resulting in misrepresentation or erroneous interpretation.

Manipulation **–** The process of altering the visual appearance of an image or specific features within an image resulting in misrepresentation or erroneous interpretation.

Staging **–** The physical alteration of a scene prior to image acquisition.

Computer Generation **–** The creation of still or animated content with imaging software.

4. Limitations

This document will not describe discipline-specific analytical techniques outside of image analysis or the limitations associated with them, only the process for performing image authentication and the general manner used to formulate a conclusion.

This document is not intended to be a training manual or a specific operating procedure. Practitioners performing image authentication should have sufficient training and experience in image science to allow the formation of a conclusion. For further information, refer to *SWGDE Training Guidelines for Image Analysis, Video Analysis, and Photography*.

The state of the art in digital imagery is such that in a single image, manipulations can be performed which a trained forensic practitioner may not adequately detect. Therefore, image authentication should be performed on a series of images depicting the same or similar subjects, or on video.

The detection of staging, the physical alteration of the scene prior to acquisition, may require coordination with scene investigators, correlation of image features with the real features at the scene, or comparison with other images of the scene or subject.

This document is not all-inclusive and does not contain information related to specific products. This document should not be construed as legal advice.

5. Background Information on Digital Manipulations

As noted above, it is technically feasible to manipulate an image, particularly a single still image, in a manner that may not be detectable by subsequent analysis using currently available tools and techniques. This process is becoming easier, as software applications are introduced specifically for this purpose. However, multiple issues are presented and should be considered as a part of any examination of imagery for the purposes of authentication. Those issues are:

- Does another party have access to the imagery?
- Does another party have the skill level necessary to perform the manipulations?
- Does another party have the time necessary to perform the suspected manipulations?
- Does another party have the hardware and software necessary to perform the suspected manipulations?
- Does the imagery have fine detail, which ultimately requires a higher level of skill to manipulate undetectably?
- Is the image content complex, including physical interactions of people with one another, as well as the environment?

All these questions should be taken into consideration when practitioners examine evidence for the purposes of authentication. For instance, changing the color of a simple object in an image may be easy to achieve, but it would present a greater artistic and technical challenge to alter an image of an adult to appear to be a young child. Complex manipulations of this nature would be more likely to leave features indicating the imagery has been manipulated.

In addition, practitioners of authentication techniques must be knowledgeable not only in photographic and analytical techniques but should be equally knowledgeable about techniques used to manipulate or create imagery. Common manipulation techniques include:

- Alteration – The changing of image features through artistic means.
- Compositing – The duplication and combination of elements from one or more images, including, but not limited to, techniques of cloning and cut-and-paste.
- Morphing – The automated transformation of components of one image onto those of another, involving a sequence of intermediate images demonstrating incremental change. Morphing is a combination of alteration and compositing.
- Image creation – The creation of image content entirely through artistic means. One example is the creation of virtual humans using 3-D modeling software (e.g., computer-generated).

The detection of computer generated imagery is established through an examination of the characteristics of humans depicted. Human characteristics can be challenging to reproduce via computer generation or other artistic means, including, but not limited to, skin-to-skin contact (including at the knee and arm joints), skin-to-object contact, fine detail (such as hair, ear shape & creases), translucent qualities in skin, and skin textures (pores, blemishes). The forensic practitioner should also be aware of the potential for computer generation to be masked through changes in luminance (e.g., artificially lowering light levels in a scene).

6. Evidence Preparation

General guidelines concerning the preparation of evidence for image authentication are provided as follows:

6.1 Review the request for examination to determine the subject matter of the image authentication. Information regarding the suspected tampering may be considered.

6.2 Based on the request, determine if the image quantity and/or quality will have an effect on the degree to which an examination can be completed.

6.2.1 If the specified quantity and/or quality criteria are not met, determine if it is possible to obtain additional images. If additional images cannot be obtained, this may preclude the practitioner from conducting an examination, or the results of the examination may be limited.

6.3 Identify the submitted imagery relevant to the analysis.

7. Method

There is no one specific methodology for image authentication, as the methods used will depend on the requested examination. However, any methodology applied to image authentication should incorporate both image content and image structure.

The repeatability of the procedure and documentation of the workflow is of paramount importance. Documentation should be performed contemporaneously.

7.1 The original imagery shall be preserved. Any processing should be applied only to a working copy of the imagery.

7.2 Assess the image structure to determine whether factors are present that can answer the examination request. Image structure examinations may include, but are not limited to:

- 7.2.1 An examination of the file format of the imagery.
- 7.2.2 An examination of the metadata of the imagery. Metadata may be useful in identifying the source and processing history of the file, but can be limited, absent, or altered. Metadata may include:
  - 7.2.2.1 Camera make/model/serial number
  - 7.2.2.2 Date/time of creation or alteration
  - 7.2.2.3 Camera settings
  - 7.2.2.4 Resolution and image size
  - 7.2.2.5 Global Positioning System (GPS) coordinates/elevation
  - 7.2.2.6 Processing/image history
  - 7.2.2.7 Original file name
  - 7.2.2.8 Lens or flash information
  - 7.2.2.9 Frame rate
  - 7.2.2.10 Thumbnail information
- 7.2.3 An examination of the imagery file packaging (container analysis). This analysis may include but is not limited to:
  - 7.2.3.1 Hex level header, footer, or other information about the file
  - 7.2.3.2 Exchangeable image file format (EXIF) information
  - 7.2.3.3 Bit level analysis of the file structure
- 7.2.4 An examination of noise within the image. This analysis may include but is not limited to:
  - 7.2.4.1 Photo-Response Non-Uniformity (PRNU), this noise signature can be used to correlate images from the same source.
  - 7.2.4.2 Stochastic noise evaluation can be used to show consistency between images from the same sensor manufacturer.

7.3 Assess the image content to determine whether factors are present that can answer the examination request. Image content examinations may include, but are not limited to a review of the following:

- 7.3.1 Artifact features
  - 7.3.1.1 Chromatic aberrations
  - 7.3.1.2 Breaks in compression blocking or patterns
  - 7.3.1.3 Mapping of motion vectors
- 7.3.2 Physical aspects of the scene
  - 7.3.2.1 Lighting, contrast
  - 7.3.2.2 Scale
  - 7.3.2.3 Composition
  - 7.3.2.4 Physics
  - 7.3.2.5 Temporal or geographic inconsistencies
- 7.3.3 Human characteristics
  - 7.3.3.1 Hair detail
  - 7.3.3.2 Scars, bruises, or blemishes
  - 7.3.3.3 Creases
  - 7.3.3.4 Vein patterns
  - 7.3.3.5 Skin contact
  - 7.3.3.6 Movement
- 7.3.4 Evidence of staging
- 7.3.5 Photographic conditions
  - 7.3.5.1 Focus
  - 7.3.5.2 Depth of field
  - 7.3.5.3 Sharpness/blur
  - 7.3.5.4 Perspective
  - 7.3.5.5 Grain structure
  - 7.3.5.6 Noise
  - 7.3.5.7 Lens distortion

8. Conclusions

While, by definition, it is impossible to prove a negative result, it is possible, through a thorough examination, to determine that it is unlikely the imagery has been manipulated or digitally created. Conversely, if alterations are detected, the forensic practitioner may reach the conclusion that the imagery is not authentic.

The provenance or source of an image may be determined as a result of the examination as detailed above. However, lack of information in support of camera source identification does not preclude the possibility the imagery was captured by the camera in question.

The formation of a conclusion should include the following steps:

8.1 Assess the significance of each observed characteristics.

8.2 Based on the observed features and any research performed, form a conclusion to address the requested analysis. Conclusions must be properly qualified and address the limitations of the methodology and research.

8.3 Report the conclusion, as well as a clear indication of the strength of the conclusion (when appropriate).

8.3.1 Practitioners should report the observed features, including those that support the specified conclusion.

8.3.2 Conclusions should not be reported in terms of numerical probability without a proper scientific foundation and/or related research.

8.4 The results of the examination must undergo independent review by a comparably trained individual. If disputes arise during review, a means for resolution of issues should be in place.

9. Limitations of Methodology

The strength of conclusions will be limited by the quality of the imagery, the quantity of the imagery, the detection of inconsistent features, and the availability of reference material, as needed. Based on these factors, it is possible the requested examination cannot be fulfilled. Forensic practitioners should take care not to overstate conclusions.

One potential source of uncertainty in any forensic analysis results from bias. It is the responsibility of the organization and the practitioner to minimize the effects of bias when conducting examinations and performing reviews. Minimizing the effects of bias can be accomplished through awareness, training, documentation (of any potential sources for bias and the steps taken to minimize), and quality assurance measures, including the limitation of task irrelevant information and blind verification.

Appendix A: Work Flow Example 1

A local police department receives a report of possible child exploitation and downloads imagery from the internet. After retrieval, a compact disc containing images is turned over to a forensic laboratory to determine if the child depicted in the imagery is real, and/or to determine if any manipulations have occurred to the images.

Following the methodology described above, the laboratory proceeds:

1. The request is reviewed and it is:
   a. determined that this type of analysis is conducted;
   b. determined that all necessary items to support the requested exam have been submitted;
   c. determined that the laboratory has the necessary equipment, materials, and resources needed to conduct the requested analysis; and
   d. assigned to an analyst.

2. The analyst acquires the necessary imagery.
   a. The analyst calls the investigating agency/organization and determines that the best quality images have been submitted, and all images have been received.
   b. The analyst reviews the images and selects relevant images for further analysis.

3. The analyst makes copies of the selected imagery for use as working copies and safely stores the received disc.

4. The analyst examines the imagery file structures, to include an examination of the file formats and associated metadata. The analyst determines there is no GPS information and the file creation dates and file modification dates are the same. The analyst similarly determines the files contain basic camera setting information and thumbnail images are present. This information is documented in the case notes.

5. The analyst determines no image processing software tags exist within the metadata. This information is documented.

6. The analyst examines the content of the imagery. The following inconsistencies were observed and documented:
   a. The majority of the images showed no signs of lossy compression, but one significant portion of an image contained 8x8 jpeg blocking.
   b. The portion of the suspect image appears to have a light source inconsistent with the remainder of the image.
   c. The scale of the subject depicted in the suspect portion is inconsistent with objects in the remainder of the image.
   d. The depth-of-field in the suspect portion is inconsistent with objects in the remainder of the image.

7. The analyst concludes that one image of the submitted series appears to have been manipulated.

8. A comparably trained individual in the laboratory independently reviews the results of the examination.

9. The analyst issues a report. Per the laboratory's standard operating procedures, the report includes a review of the materials received, the request, the methods used, the results obtained, the basis for the conclusion, and the conclusion.

Appendix B: Work Flow Example 2

A local police department receives a report of possible child exploitation and downloads imagery from the internet. After retrieval, the police department develops a suspect and completes a search of the suspect's house pursuant to a search warrant. During the search, two cellular telephones are recovered. The investigating agency/organization contacts their laboratory to determine if the imagery was captured by the recovered cell phones.

Following the methodology described above, the laboratory proceeds:

1. The request is reviewed and it is:
   a. determined that this type of analysis is conducted;
   b. determined that all necessary items to support the requested exam have been submitted;
   c. determined that the laboratory has the necessary equipment, materials, and resources needed to conduct the requested analysis; and
   d. assigned to an analyst.

2. The analyst acquires the necessary materials.
   a. The analyst calls the investigating agency and determines that all imagery and questioned phones have been received.
   b. The analyst reviews the images and selects relevant images for further analysis.

3. The analyst makes copies of the selected imagery for use as working copies and safely stores the received evidence. The analyst also receives permission from the investigating agency to capture images with the questioned phones, thereby changing the data on the phones. The analyst is informed the phones in question have already been thoroughly documented and receives appropriate permissions.

4. The analyst examines the imagery file structure, to include an examination of the file formats and associated metadata. The analyst determines there is no GPS information, and no make, model or serial number captured in the imagery metadata. This information is documented in the case notes.

5. The analyst determines no image processing software tags exist within the metadata. This information is documented.

6. The analyst examines the content of the imagery. The average luminosity is determined to be above the threshold needed for examination.

7. The Photo-Response Non-Uniformity(PRNU) pattern is calculated for each of the relevant images.

8. Exemplar images are captured with the questioned phone cameras.

9. PRNU patterns are calculated for each set of exemplar images.

10. The PRNU patterns are compared between the questioned imagery and the exemplar images. A correlation value is calculated for each comparison.

11. Based on the correlation values calculated, the analyst reaches the conclusion that the examined images were captured by one of the questioned phones.

12. A comparably trained individual in the laboratory independently reviews the results of the examination.

13. The analyst issues a report. Per the laboratory's standard operating procedures, the report includes a review of the materials received, the request, the methods used, the results obtained, the basis for the conclusion, and the conclusion.

SWGDE Best Practices for Image Authentication

History

Revision	Issue Date	Section	History
1.0 DRAFT	2018-01-11	All	Initial draft created and SWGDE voted to release as a Draft for Public Comment.
1.0 DRAFT	2018-04-17	All	Formatting and technical edit performed for release as a Draft for Public Comment.
1.0 DRAFT	2018-06-14	2; 4; 6.2.1; 7.2.2; 9; Appendix A &B	Minor editorial changes and changed use of “practitioner” or “examiner” to “analyst” throughout. SWGDE voted to publish as an Approved document.
1.0	2019-07-11	--	Formatted and published as Approved version 1.0.