2021-S-0036 Standard Guide for Image Authenication

VITAL
Digital Evidence/Multimedia Scientific Area Committee
Organization of Scientific Area Committees (OSAC) for Forensic Science

DRAFT 1

Draft OSAC Proposed Standard

2021-S-0036Standard Guide for Image Authentication

Prepared by
VITAL Subcommittee
Version 1.0 - Open Comment
August 2021

Disclaimer:

This OSAC Proposed Standard was written by the Video/Imaging and Technology Analysis Subcommittee of the Organization of Scientific Area Committees (OSAC) for Forensic Science following a process that includes an open comment period. This Proposed Standard will be submitted to a standards developing organization and is subject to change.

There may be references in an OSAC Proposed Standard to other publications under development by OSAC. The information in the Proposed Standard, and underlying concepts and methodologies, may be used by the forensic-science community before the completion of such companion publications.

Any identification of commercial equipment, instruments, or materials in the Proposed Standard is not a recommendation or endorsement by the U.S. Government and does not imply that the equipment, instruments, or materials are necessarily the best available for the purpose.

1. Scope

1.1 This standard provides information on the evidentiary value, methodology, and limitations when conducting an image authentication examination as a part of forensic analysis. The intended audience is examiners in a laboratory setting.

1.2 For the purposes of this document, "imagery" refers to the subject matter being examined which may include a single image or a series of images from any source.

1.3 The scope of the document includes image content authentication and image source authentication but does not include the interpretation of image content. Neither image source nor content authentication answers 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 interpretation. For further information, see SWGDE Best Practices for Image Content Analysis.

1.4 Image authentication must not be confused with the requirement to demonstrate the integrity of the evidence as a precondition to admissibility in court. Maintaining evidentiary 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.

1.5 Image authentication and image content analysis may be performed in conjunction.

1.6 This document is not intended to be used as a step-by-step practice.

1.7 This document is a guide for performing image authentication and the general manner used to formulate an interpretation. It does not describe analytical techniques or the associated limitations.

1.8 This document is not intended to be a training manual or a specific operating procedure and does not provide the criteria for the assessment of examiner competency

1.9 The detection of staging is considered image content interpretation and is not within the scope of this document.

1.10 This document is not all-inclusive and does not contain information related to specific products.

1.11 *This standard cannot replace knowledge, skills, or abilities acquired through education, training, and experience, and is to be used in conjunction with professional judgment by individuals with such discipline-specific knowledge, skills, and abilities.*

1.12 *This standard does not purport to address all of the safety concerns, if any, associated with its use. It is the responsibility of the user of this standard to establish appropriate safety,*

health, and environmental practices and determine the applicability of regulatory limitations prior to use.

2. Referenced Documents

2.1 *ASTM Standards*:

2.1.1 E2825 Standard Guide for Forensic Digital Image Processing

2.1.2 E2916 Standard Terminology for Digital and Multimedia Evidence Examination

2.2 *SWGIT Material*:

2.2.1 SWGIT, Section 14: Best Practices for Image Authentication, updated January 11, 2013

2.3 *SWGDE Material*:

2.3.1 SWGDE Best Practices for Image Content Analysis, updated February 21, 2017

2.3.2 SWGDE Training Guidelines for Video Analysis, Image Analysis, and Photography, updated February 8, 2016

2.3.3 SWGDE Best Practices for Image Authentication, July 11, 2018

2.3.4 SWGDE Recommended Guidelines for Validation Testing, September 5, 2014

3. Terminology

3.1 *Definitions:*

3.1.1 **alter**, *v* –to change image features through image editing techniques

3.1.2 **composite**, *v* –to duplicate or combine elements from one or more images

3.1.3 **Computer-generated imagery**, *n* –the creation of digital content through non-photographic means

3.1.4 **image**, *n* –in image and video analysis, an imitation or representation of a person or thing drawn, painted, or photographed

3.1.5 **image authentication,** *n*–the process of determining whether the image source, or image content of the imagery is true or false

3.1.6 **image content**, *n*–visual information within an image, such as, subjects/objects, artifacts (due to compression and/or capture), and physical aspects of the scene

3.1.7 **image content authentication**, *n*–The process of determining whether the image content of the imagery is true or false

3.1.8 **image source**, *n*-the origin of an image, which may include the capture device or the provenance of the image

3.1.9 **image source authentication**, *n*–the process of determining whether the asserted provenance of the imagery is true or false

3.1.10 **image structure**, *n*–non-visual information about the image, such as file type, file compression, metadata, or the file properties of the image

3.1.11 **manipulate**, *v* –to alter the image structure, visual appearance or specific features within an image with the intention to cause misrepresentation or erroneous interpretation

3.1.12 **morph**, *v* –to transform components of one image onto those of another, often involving a sequence of intermediate images demonstrating incremental changes

3.1.13 **stage**, *v* –to alter a scene prior to image acquisition

4. Summary of Practice

4.1 Submitted files shall be preserved. Any processing shall be applied to a working copy of the imagery.

4.2 Steps taken and methods used shall be sufficiently documented to support the examiner's observations and to permit a comparably trained person to understand the examination performed.

4.3 Practitioners of image authentication should have sufficient training and expertise in image science to support observations and address potential sources of uncertainty in the analysis. For further information, see *SWGDE Training Guidelines for Video Analysis, Image Analysis, and Photography*.

5. Significance and Use

5.1 Image authentication may establish the probative value of imagery by determining whether it has been computer-generated or manipulated and/or by determining the source of the imagery. Authentication of imagery is important because image manipulation may be involved in criminal activity.

5.2 This guide describes methods that may determine if questioned imagery is a true representation of the submitted image by some defined criteria, and/or to determine the original source or content of the imagery.

5.3 Image manipulations can be accomplished through multiple means. Some types of image manipulation require little skill, because software applications exist specifically for this purpose. However, detection requires that practitioners of authentication techniques be knowledgeable in manipulation techniques. Common techniques that may result in image manipulation include one or a combination of alteration, compositing, and computer-generated imagery.

5.4 The detection of manipulations can be accomplished through multiple means. Forensic practitioners should examine the image content, image source and the image structure (including associated metadata).

5.5 Image content analysis refers to an examination of the visual characteristics which may include the consistency of the lighting (direction, quality, color, contrast, reflections), sharpness, depth-of-field, compression artifacts, image noise, relative size of objects or the presence of compositing artifacts.

5.6 Image structure analysis refers to examination of file metadata and format properties. For example, file metadata may identify image editing software and processing history, camera make, model, serial number and other identifying information. Format properties may be checked for consistency with files from the purported source.

5.7 Regarding issues of authenticity, possible factors include:

5.7.1 Manipulation could be masked through changes in contrast, contrast or multiple levels of image recompression, photocopy or screen grab of image and rescaling.

5.7.2 The skill level and the time necessary to perform manual computer-generated manipulations.

5.7.3 Based on advanced software algorithms, Generative Adversarial Networks(GAN) and Deepfake technology, it may be possible to manipulate an imagery in a manner that may not be detectable by subsequent analysis using currently available tools and techniques. Examination of a series of related images may assist in the authentication.

6. Evidence Assessment

6.1 Proper evidence handling procedures shall be employed. For additional information on proper evidence handling guidelines, refer to SWGDE Best Practices for Maintaining the Integrity of Imagery.

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

6.2.1 Review the request for examination to determine the subject matter of the image authentication. The scope of authentication can be extremely broad so examination requests should contain sufficient information to clarify the scope of the request and the question to be answered while limiting extraneous information.

6.2.2 Information regarding any suspected manipulation may be considered and may even be necessary to adequately clarify the question; however, examiners should be cognizant of the potential for inadvertent bias.

6.2.3 Determine if all, or some subset, of the submitted imagery is requested to be authenticated.

6.2.4 Based on the request, determine if the imagery is fit for purpose. Quantity and/or quality of imagery may influence the degree to which an examination can be completed.

6.2.5 If the imagery is not fit for purpose, determine if it is possible to obtain additional imagery. If additional imagery cannot be obtained, this may preclude the examiner from proceeding with an examination or may limit the strength of the results.

7. Methodology

7.1 The applied methods will depend on the requested examination. There is no single methodology for image authentication, however any methodology should incorporate both image content and image structure analysis.

7.2 The submitted imagery shall be preserved. Any processing shall be applied only to a working copy of the imagery. [Preservation may be limited if this is analog evidence.]

7.3 Tools, techniques, and procedures should be validated to ensure repeatability, refer to *SWGDE Recommended Guidelines for Validation Testing. Methodology*, workflow, and observations should be documented contemporaneously.

7.4 Subjective assessments should be recorded with sufficient information to support the examiner's observations, and the significance of the observation in the context of the overall analysis.

7.5 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:

7.5.1 An examination of the file format of the imagery.

7.5.2 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, inaccurate, or altered without necessarily changing image content. Metadata may include, but is not limited to:

7.5.2.1 Camera make/model/serial number,

7.5.2.2 Date/time of creation or alteration,

7.5.2.3 Camera settings,

7.5.2.4 Resolution and image size,

7.5.2.5 Camera rotation/orientation,

7.5.2.6 GPS coordinates/elevation, 7.5.2.7

Processing/image history,

7.5.2.8 Filename,

7.5.2.9 Lens or flash information,

7.5.2.10 Framerate, and

7.5.2.11 Thumbnail information.

7.5.3 An examination of the data file packaging (container analysis). This analysis may include, but is not limited to:

7.5.3.1 Hex level header, footer or other information about the file, and

7.5.3.2 EXIF information.

7.5.4 An examination of image noise. This analysis may include, but is not limited to:

7.5.4.1 Photo-Response Non-Uniformity (PRNU), this noise signature can be used to correlate images from the same source.

7.5.4.2 Stochastic noise evaluation can be used to show consistency between images from the same sensor manufacturer.

7.6 Assess the image content to determine whether factors are present that can answer the examination request.

7.6.1 Assessment of the image content may be performed visually and may be assisted by image processing or filtering techniques. For example, examination of discreet color channels, or adjusting tonal contrast may help to detect editing or compositing marks.

7.7 Image content examinations may include, but are not limited to a review of the following:

7.7.1 Photographic aspects:

7.7.1.1 Focus

7.7.1.2 Depth of field

7.7.1.3 Sharpness / blur

7.7.1.4 Perspective

7.7.1.5 Grain / noise structure

7.7.1.6 Lens distortion

7.7.2 Artifacts:

7.7.2.1 Chromatic aberrations

7.7.2.2 Compression blocking or patterns

7.7.2.3 Editing / compositing marks

7.7.3 Physical aspects of the scene:

7.7.3.1 Light quality, color, direction, contrast

7.7.3.2 Shadows

7.7.3.3 Relative scale

7.7.3.4 Composition

7.7.3.5 Physical, temporal, or geographic inconsistencies

7.7.4 Subject characteristics:

7.7.4.1 Human/animal features (hair, scars, blemishes, creases, vein patterns

7.7.4.2 Contact between objects (human/human, such as skin to skin, human / object, object / object)

7.7.4.3 Consistency in patterns and textures

8. Interpretation of results

8.1 ***Image content authentication results*** in the determination of the presence or absence of manipulation. Opinions may include the following:

8.1.1 **Support for no evidence of manipulation or alteration**

8.1.1.1 An opinion that the imagery appears to be consistent with its original structure and content is consistent with expectations. However, this is not definitive evidence that the image is unaltered.

8.1.2 **Inconclusive**

8.1.2.1 An opinion there is insufficient evidence to reach a determination of authenticity and/or the imagery is not fit for purpose

8.1.3 **Support for evidence of alteration but not manipulation**

8.1.3.1 An opinion the imagery is not in its original structure and/or content but does not appear to be altered in a manner that results in misrepresentation. However, this is not definitive evidence that the image was not manipulated.

8.1.4 **Support for evidence of manipulation**

8.1.4.1 An opinion the imagery has been altered from its original structure and/or content which results in misrepresentation.

8.2 ***Image source authentication*** results in the establishment of the provenance or origin of the image. Opinions may include the following:

8.2.1 **Support the imagery is authentic**

8.2.1.1 An opinion the imagery is a true representation of the image source.

8.2.2 **No support the imagery is inauthentic**

8.2.2.1 An opinion the imagery may be a true representation of the image source.

8.2.3 **Inconclusive**

8.2.3.1 An opinion there is insufficient evidence to reach a determination whether the imagery is a true or false representation of the image source.

8.2.4 **Support the imagery is inauthentic**

8.2.4.1 An opinion the source or provenance is established to be different than the purported source or provenance.

8.2.4.2 An opinion the imagery is a false representation of the image source.

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

8.4 The formation of an opinion should include the following steps:

8.4.1 Assess the significance of each observed characteristic.

8.4.2 Form an interpretation to address the requested analysis based on the observed features and any necessary research conducted. Interpretations must be properly qualified and address the limitations of the methodology and research.

8.4.3 Report the results, as well as a clear indication of the strength of the results (when appropriate).

8.4.3.1 Examiners should report the observed features, including those that do and do not support the specified results.

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

8.4.4 The results of the examination should undergo independent review by a comparably trained individual to verify the methodology and results. If disputes arise during review, a means for resolution of issues should be in place.

8.5 Forensic examiners should take care not to overstate results.

8.6 Bias is one potential source of uncertainty in any forensic analysis. It is the responsibility of the organization and the examiner to minimize the effects of bias when conducting examinations and performing reviews. Minimizing the effects of bias can be accomplished through awareness, training, and quality assurance measures, including the limitation of task irrelevant information and blind verification. Potential sources of bias and the steps taken to minimize the effects of bias should be documented.

9. Keywords

9.1 criminal justice system; image processing; digital image processing; forensic image authentication, content authentication, source authentication, image authenticity, image manipulation, image alteration.

NOTE: Appendices for general reference only during the review process (not to be included in the published standard guide)

ANNEX

X1. (Nonmandatory Information)

X1. WORK FLOW EXAMPLE 1 – CONTENT AUTHENTICATION

X1.1 A local police department receives a report of possible child exploitation and downloads imagery from the internet. After retrieval, imagery 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.

X1.2 Following the methodology described above, the laboratory proceeds:

X1.2.1 The request is reviewed, and it is:

X1.2.1.1 determined that the requested analysis is conducted by the laboratory;

X1.2.1.2 determined that all necessary items to support the requested analysis have been submitted;

X1.2.1.3 determined that the laboratory has the necessary equipment, materials, and resources needed to conduct the requested analysis; and

X1.2.1.4 assigned to an analyst.

X1.2.2 The analyst acquires the necessary imagery.

X1.2.2.1 The analyst determines if the images are of sufficient quality for the requested analysis. If the image quality is insufficient to proceed, then the analyst calls the investigating agency to determine if additional images can be submitted.

X1.2.2.2 The analyst reviews the images and selects relevant images for further analysis.

X1.2.3 The analyst makes copies of the selected imagery for use as working copies and safely stores the original imagery.

X1.2.4 The analyst examines the imagery file structures which includes 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.

X1.2.5 The analyst determines no image processing software tags exist within the metadata. This information is documented in the case notes.

X1.2.6 The analyst examines the content of the imagery. The following inconsistencies were observed and documented:

X1.2.6.1 Most of the images show no signs of lossy compression, but one portion of a single image shows 8x8 jpeg blocking.

X1.2.6.2 The portion of the suspect image appears to have a light source inconsistent with the remainder of the image.

X1.2.6.3 The scale of the subject depicted in the suspect portion is inconsistent with objects in the remainder of the image.

X1.2.6.4 The depth-of-field in the suspect portion is inconsistent with objects in the remainder of the image.

X1.2.7 The analyst concludes that one image of the submitted series appears to have been manipulated.

X1.2.8 A comparably trained individual in the laboratory independently reviews the results of the examination and arrives at the same conclusion.

X1.2.9 The analyst issues a report. Per the laboratory's Standard Operating Procedures (SOPs), the report includes a review of the materials received, the request, the methods used, the results obtained, the basis for the results, and the results.

APPENDIX

(Nonmandatory Information)

X1. X1. WORKFLOW EXAMPLE 2 – SOURCE AUTHENTICATION

X1.1 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 contacts their laboratory to determine if the imagery was captured by the recovered cell phones.

X1.2 Following the methodology described above, the laboratory proceeds:

X1.2.1 The request is reviewed and it is:

X1.2.1.1 determined that the requested analysis is conducted by the laboratory;

X1.2.1.2 determined that all necessary items to support the requested exam have been submitted;

X1.2.1.3 determined that the laboratory has the necessary equipment, materials, and resources needed to conduct the requested analysis; and

X1.2.1.4 assigned to an analyst.

X1.2.2 The analyst acquires the necessary materials.

X1.2.2.1 If laboratory policy requires, the analyst calls the investigating agency and verifies that all imagery and relevant phones have been received.

X1.2.2.2 The analyst reviews the images and selects relevant images for further analysis.

X1.2.3 The analyst makes copies of the selected imagery for use as working copies and safely stores the original imagery. Prior to capturing exemplar images with the submitted phones, the analyst requests permission from the investigating agency, because this action will change the data on the phones. The analyst is informed the phones in question have already been thoroughly documented, and receives appropriate permissions.

X1.2.4 The analyst examines the file structure of the questioned imagery which includes 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.

X1.2.5 The analyst determines no image processing software tags exist within the metadata. This information is documented in the case notes.

X1.2.6 The analyst examines the content of the imagery. The average luminance is determined to be above the threshold needed for Photo-Response Non-Uniformity (PRNU) examination.

X1.2.7 The PRNU pattern is calculated for each of the relevant images.

X1.2.8 Exemplar images are captured with the submitted phone cameras.

X1.2.9 The PRNU patterns are calculated for each set of exemplar images.

X1.2.10 The PRNU patterns are compared between the examined images and the exemplar images. A correlation value is calculated for each comparison.

X1.2.11 Based on the correlation values calculated, the analyst reaches the conclusion that the examined images were captured by one of the submitted phones.

X1.2.12 A comparably trained individual in the laboratory independently reviews the results of the examination.

X1.2.13 The analyst issues a report. Per the laboratory's SOPs, the report includes a review of the materials received, the request, the methods used, the results obtained, the basis for the results, and the results.